VERDONCK KLOOSTER & ASSOCIATES

ONDERZOEK INTERNETSTEMMEN VOOR KIEZERS IN HET BUITENLAND

Internetstemmen bij officiële verkiezingen van vertegenwoordigende overheidsorganen

VERDONCK KLOOSTER & ASSOCIATES

ONDERZOEK INTERNETSTEMMEN VOOR KIEZERS IN HET BUITENLAND

Internetstemmen bij officiële verkiezingen van vertegenwoordigende overheidsorganen

DATUM	28 januari 2014
STATUS	Definitief
VERSIE	1.0

INHOUDSOPGAVE

1 INLEIDING

1.1 Algemeen

In opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) is een onderzoek uitgevoerd naar de mogelijkheid van stemmen via internet voor kiezers in het buitenland bij formele verkiezingen van vertegenwoordigende organen of voor het houden van proeven/experimenten daarmee.

Het onderzoek bestond uit een viertal onderdelen:

1. Een inventarisatie en beschrijving van de systemen voor internetstemmen die andere landen hebben gebruikt voor het stemmen bij formele verkiezingen van vertegenwoordigende organen of voor het houden van proeven/experimenten daarmee.
2. Een analyse van de risico's die worden voorzien als gevolg van het stemmen per internet voor de kiezers in het buitenland in relatie tot de (internationale) waarborgen die gelden voor verkiezingen en of er maatregelen te treffen zijn om die risico's in afdoende mate af te dekken.
3. Een onderzoek naar de functionele, technische en beveiligingseisen die bepalend zijn voor een betrouwbare vorm van internetstemmen alsmede een onderzoek naar hoe invulling gegeven kan worden aan de rol van het stembureau bij verkiezingen via het internet.
4. Een schets van een methode om te waarborgen dat een internetstemsysteem aan de gestelde eisen voldoet, alsmede om te waarborgen dat de eisen voor het stemmen per internet worden onderhouden zodat het vertrouwen in het internetstemmen door de kiezers in het buitenland kan blijven bestaan?

Deze vier onderdelen zijn gevat in een viertal deelrapportages I t/m IV welke als bijlage zijn bijgevoegd. In de hoofdstukken 2 tot en met 5 zijn de belangrijkste bevindingen uit het onderzoek samengevat.

1.2 Definitie

In dit onderzoek is internetstemmen gedefinieerd als:

Internetstemmen is een wijze van stemmen waarbij de kiezer op elektronische wijze zijn stemvoorkeur kenbaar maakt, op een locatie waar geen toezicht wordt gehouden, en waarbij hij de stem overdraagt aan het stembureau via het openbare internet.

1.3 Bijlagen

I. Deel I – Internationale inventarisatie Internetstemmen
II. Deel II – Risicoanalyse internetstemmen
III. Deel III – Eisen aan een internetstemsysteem
IV. Deel IV – Toetsmethode internetstemsysteem

2 DEEL I: INTERNATIONALE INVENTARISATIE

2.1 Afbakening

In de inventarisatie zijn alle landen opgenomen waarvan bekend is dat zij in de periode 2000 – 2013 bij openbare verkiezingen voor vertegenwoordigende overheidsorganen kiezers de mogelijkheid hebben geboden om via internet te stemmen, waarbij deze stemmen meetelden in de officiële uitslag. Per land is een beschrijving gegeven met als doel om een internationaal overzicht te geven van de wijze waarop internetstemmen in andere landen is toegepast.

Die landen waar internetstemmen is ingezet bij verkiezingen, maar waarbij de via internet uitgebrachte stemmen niet in de officiële uitslag meetelden, zijn in deze inventarisatie buiten beschouwing gelaten. Eveneens zijn alle toepassingen van internetstemmen bij verkiezingen voor niet-overheidsorganisaties niet meegenomen in de inventarisatie, zoals universiteitsraadsverkiezingen, verkiezingen binnen politieke partijen, informele volksraadplegingen, ondernemingsraadsverkiezingen, aandeelhoudersverkiezingen, etc.

De twee gebruikte internetstemsystemen bij de Kiezen op Afstand experimenten in Nederland (bij de verkiezingen voor het Europees Parlement in juni 2004 en de Tweede Kamer in 2006) zijn niet opgenomen in de inventarisatie. Van deze internetstemsystemen zijn evaluatiebeschrijvingen beschikbaar via de handelingen van de Tweede Kamer en via de website van BZK.

2.2 Belangrijkste bevindingen

2.2.1 Internetstemmen wordt internationaal beperkt toegepast

Op het moment van deze inventarisatie, eind 2013, is internetstemmen beschikbaar als stemmethode in zeven landen. Alleen in Estland is internetstemmen op landelijke schaal ingevoerd, in de overige zes landen is internetstemmen voorbehouden aan een specifiek afgebakende groep kiezers. Veelal betreft het inwoners van specifieke gemeenten of staten, of kiezers die in het buitenland verblijven.

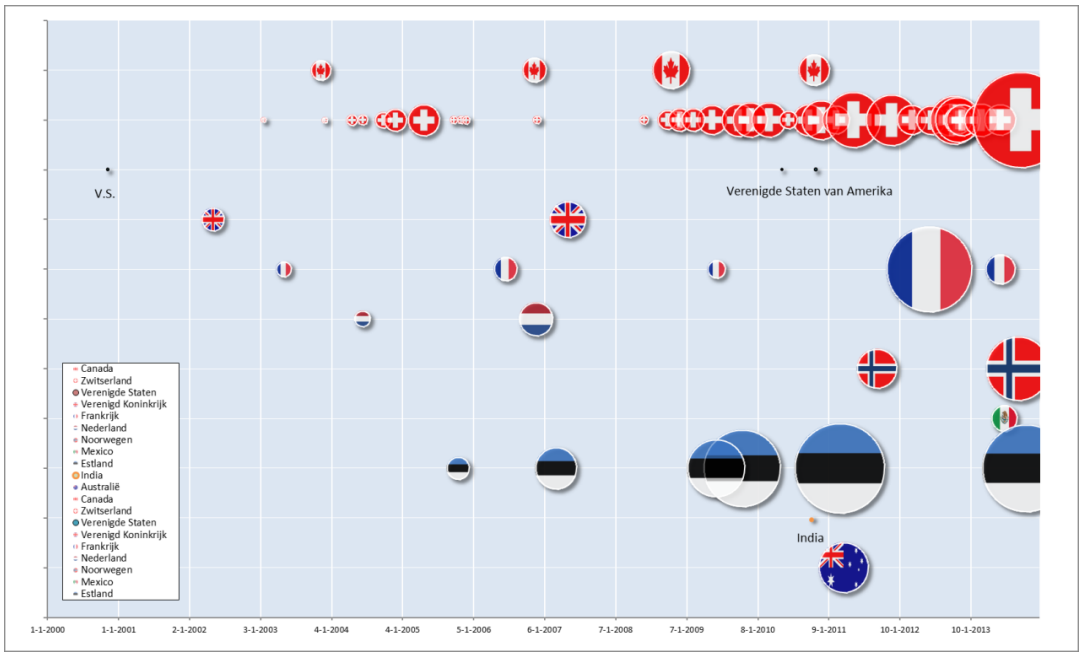
	Land	Regio / doelgroep	Formele status
1.	Australië	Kiezers in de staat New South Wales	Experiment
2.	Canada	Kiezers in 60 gemeenten in de staten Ontario en Nova Scotia	Ingevoerd voor gemeentelijke verkiezingen in twee staten, niet voor landelijke of statenverkiezingen
3.	Estland	Alle kiezers	Ingevoerd
4.	Frankrijk	Alle kiezers woonachtig buiten Frankrijk	Ingevoerd
5.	India	Kiezers in 6 gemeenten in de staat Gujarat	Experiment

	Land	Regio / doelgroep	Formele status
6.	Noorwegen	Kiezers in 12 gemeenten	Experiment
7.	Zwitserland	Kiezers in 13 kantons, met een limiet op het aantal kiesgerechtigden, inclusief kiezers woonachtig buiten Zwitserland	Experiment

Daarnaast zijn in de periode 2000 – 2013 in een viertal landen experimenten gehouden met internetstemmen, maar zijn deze experimenten beëindigd en is internetstemmen momenteel niet toegestaan:

8. Mexico
9. Nederland
10. Verenigd Koninkrijk
11. Verenigde Staten van Amerika

In onderstaande figuur zijn alle verkiezingen weergegeven in de periode 2000-2013 in de 11 landen waar internetstemmen is toegepast. De eerste internetverkiezing vond plaats op 7 november 2000 in de Verenigde Staten van Amerika.



Figuur 1 Overzicht internetstemmingen, omvang bol = aantal kiezers

In de figuur geeft de oppervlakte van de bol het aantal uitgebrachte stemmen via internet weer. Het aantal kiezers dat via internet stemt is internationaal gezien nog zeer beperkt in verhouding tot het totale electoraat. De grootste internetstemming, in termen van aantal kiezers dat via

internet stemde, was een referendum op 22 september 2013in Zwitserland. Toen stemden 158.500 kiezers via internet.

In totaal zijn er wereldwijd ruim 1,5 miljoen stemmen uitgebracht via internet bij formele verkiezingen.

2.2.2 Voorzichtige aanpak

In alle 11 landen waar internetstemmen is of wordt toegepast, en in alle landen die internetstemmen hebben onderzocht maar uiteindelijk besloten om geen experimenten te houden, speelt nadrukkelijk de zorg omtrent de veiligheid van internetstemmen.

Deze zorg leidde er toe dat in vrijwel alle landen de introductie van internetstemmen is voorafgegaan door een onderzoekstraject waarbij wetenschappers, (internationale) onderzoeksbureaus en leveranciers werden betrokken. Na de onderzoeksfase werd vervolgens op kleine schaal testen uitgevoerd met de ontwikkelde of aangekochte internetstemdienst. In vrijwel alle landen met uitzondering van Canada was het noodzakelijk om een aparte wettelijke basis te creëren om te kunnen experimenteren met internetstemmen. De voorzichtige aanpak betekende ook dat in de genoemde 11 landen internetstemmen niet de bestaande mogelijkheden om te stemmen verving, maar steeds is aangeboden als aanvullende stemmethode.

Als onderdeel van de voorzichtige aanpak hebben een aantal landen (Estland, Canada en Noorwegen) er voor gekozen om een internetstemsysteem in te voeren waarbij de kiezer zijn internetstem alleen voorafgaand aan de dag van stemming kan uitbrengen. Mocht er iets misgaan met het internetstemmen dan hebben de kiezers de mogelijkheid om op de dag van stemming alsnog hun stem op ‘traditionele wijze’ in een stemlokaal uit te brengen.

In Estland en Noorwegen is bovendien gekozen voor een kiessysteem waarbij de kiezer meer dan één stem mag uitbrengen via internet. Dit voor het geval de kiezer zich bedenkt, als hij vermoedt dat zijn stem niet goed is overgekomen door technische problemen, of in geval dat de kiezer niet in vrijheid heeft kunnen stemmen. In deze kiessystemen wordt steeds de laatst ontvangen internetstem meegeteld. Als de kiezer op de dag van stemming alsnog een stem uitbrengt in het stembureau dan telt alleen die stem.

2.2.3 Motieven voor invoering internetstemmen

De motieven om internetstemmen in te voeren verschillen per land en daarbinnen veelal ook per lokale overheid, maar grosso modo zijn in de landen die internetstemmen hebben beproefd of ingevoerd de volgende motieven bepalend geweest in de besluitvorming:

- Internetstemmen verbetert de toegankelijkheid.
- Internetstemmen is gemakkelijker.
- De wens om democratie te moderniseren met ICT.
- De wens om de opkomst te verhogen.

2.2.4 Opkomst niet significant gestegen, kosten wel

Er is door diverse overheden en internationale onderzoeksorganisaties onderzoek gedaan naar het effect van internetstemmen op de opkomst. In geen van deze onderzoeken is een positieve correlatie vastgesteld: internetstemmen leidde niet tot een significant hogere opkomst ten opzichte van de doelgroepen of gebieden waar geen internetstemmen werd aangeboden.

Wel zijn de kosten aanzienlijk gestegen, om een tweetal redenen. Allereerst is internetstemmen steeds ingezet als nieuw alternatief *naast* de bestaande stemmethoden. Ook indien de kosten per stem werden uitgerekend en vergeleken met de bestaande methode van stemmen bleek dat internetstemmen duurder was. In die berekeningen zijn de kosten voor de ontwikkeling en invoering meegenomen. Verondersteld mag worden dat deze kosten een eenmalige karakter hebben, maar in de praktijk blijkt dat dit niet zo te zijn doordat ook bij de tweede, derde en volgende internetstemming nog steeds een projectorganisatie actief is.

2.2.5 Beschouw internetstemmen als een langdurig proces van ontwikkeling, invoering en evaluatie

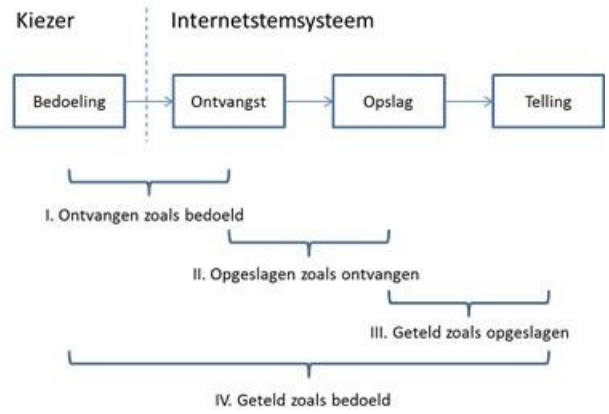
Uit de eerdere Kiezen op Afstand ervaringen én uit de ervaringen in het buitenland blijkt dat het ontwikkelen van een internetstemvoorziening niet als een eenmalige exercitie kan worden beschouwd. Zowel in Nederland, Noorwegen, Estland, Zwitserland (Geneve) als Frankrijk is de gebruikte internetstemvoorziening na toepassing in een verkiezing op onderdelen aangepast en in sommige gevallen zelfs volledig opnieuw ontwikkeld. Het is dan ook niet realistisch om te veronderstellen dat een kant-en-klaar systeem aangeschaft kan worden dat ingezet kan worden voor bijvoorbeeld de eerstvolgende vier of vijf verkiezingen zonder dat er aanpassingen nodig zijn.

Indien besloten wordt tot invoering, dan moet worden gerealiseerd dat een internetstemsysteem een grote complexiteit kent en eerder als een langdurig proces van ontwikkeling, invoering en evaluatie beschouwd moet worden dan een systeem wat eenmaal aangeschaft ongewijzigd gebruikt kan worden in vele jaren daarna.

2.2.6 Innovaties op het vlak van verificatie door kiezers

Internetstemmen moet, net als andere stemvormen, voldoen aan universele vereisten op het vlak van eerlijke vrije verkiezingen. Eén van de aandachtsgebieden betreft de *integriteit* en *controleerbaarheid*; een verkiezing moet verlopen conform de wettelijke regels, de uitkomst mag niet beïnvloedbaar zijn anders dan door het uitbrengen van rechtmatige stemmen en het verloop van de verkiezing moet controleerbaar zijn.

In de laatste jaren is er wetenschappelijk onderzoek gedaan op het gebied van verificatie mechanismen. Hierbij is gezocht naar methoden waarmee de kiezer zelf kan controleren of zijn stem correct is ontvangen, opgeslagen en geteld.



Een deel van dit onderzoek richt zich op de mogelijkheden voor kiezers om de 'Geteld zoals bedoeld' controle mogelijk te maken, omdat dit de kiezer zelf in staat stelt om er zeker van te zijn dat zijn stem niet is gemanipuleerd. De meest uitgebreide vorm van verificatie wordt *End-to-end universal verifiability* genoemd, waarbij niet alleen de kiezer zelf, maar ook anderen (zoals politieke partijen, toezichthouders, verkiezingswaarnemers en het orgaan dat de verkiezingen organiseert) kunnen verifiëren dat alle uitgebrachte stemmen correct zijn geteld zoals bedoeld.

Deze vergaande vormen van *voter verifiability* worden momenteel nog niet toegepast bij officiële verkiezingen. Zonder aanvullende, complexe cryptografische, maatregelen introduceert het namelijk een nieuwe, ongewenste, eigenschap: de kiezer kan mogelijk bewijzen wat hij gestemd heeft en daarmee is de kiezer in staat om zijn stem te verkopen. En in het geval van *end-to-end universal verifiability* moeten aanvullende maatregelen genomen worden om te voorkomen dat het stemgeheim wordt doorbroken. Ook ontstaan nieuwe juridische vraagstukken zoals hoe kan worden vastgesteld of een claim van een kiezer legitiem is en welke consequentie moet worden verbonden aan een legitieme claim. Mag in zo'n geval die kiezer opnieuw een stem uitbrengen of moet de hele stemming als ongeldig worden beschouwd?

Verificatie door de kiezers is voor het eerst beproefd in Nederland[1], bij de verkiezingen in 2006. Recenter is in Estland (2013) en Noorwegen (2011) een vorm van kiezersverificatie beproefd waarbij de kiezer kon verifiëren dat zijn stem was correct was ontvangen. Bij de meest recente verkiezingen in Noorwegen (2013) is daarnaast ook de verificatie vormen "Opgeslagen zoals ontvangen" en "Geteld zoals opgeslagen" beproefd.

Estland heeft er bewust voor gekozen om geen verdergaande vormen van verificatie te bieden, enerzijds om geen andere waarborgen en eigenschappen te introduceren in vergelijking tot hun

[1] In Nederland is in 2006 een vorm van kiezersverificatie geboden die uitging van universal verifiability; niet alleen de kiezer zelf kon controleren dat zijn uitgebrachte stem correct was geteld, maar ook anderen konden controleren dat alle ontvangen stemmen correct waren geteld.

briefstemsysteem, anderzijds omdat de complexiteit van de stemdienst sterk toeneemt (cryptografische protocol, additionele maatregelen om het cryptografische protocol en de bij behorende voorzieningen en procedures te beveiligen).

3 DEEL II: RISICOANALYSE INTERNETSTEMMEN

3.1 Inleiding

In het tweede deel van het onderzoek is onderzocht wat de risico's zijn die gepaard gaan met stemmen via internet.

Hiertoe is geanalyseerd welke realistische dreigingsscenario's zich kunnen voordoen. Per dreigingsscenario is onderzocht welke actor een belang zou kunnen hebben, op welke manieren het dreigingsscenario zich kan manifesteren, of het een bestaande of nieuwe dreiging is en op welke waarborgen en processtappen het dreigingsscenario betrekking heeft. Per scenario is een inschatting gemaakt van het risico. Dat wordt bepaald door zowel de kans dat de ongewenste gebeurtenis optreedt als het effect indien het zich voordoet. Hierbij is het effect zwaarder gewogen dan de kans, vanuit de overweging dat gegeven het absolute karakter van sommige waarborgen én het maatschappelijk belang van verkiezingen ook een dreigingsscenario met een kleine kans van optreden toch beschouwd moet worden als een middel of groot risico kans indien het effect respectievelijk middel of groot is.

3.2 Dreigingsscenario's met grootste risico

In onderstaande tabel zijn de dreigingsscenario's weergegeven waarvan het risico is ingeschat op Groot of Middel. Hierbij zijn de preventieve en correctieve maatregelen reeds meegewogen.

Risico	Dreigingsscenario's
G	Niet-kiesgerechtigde brengt stem uit
G	Manipuleren van de stem of uitslag
G	Relatie tussen kiezer en inhoud stem (doorbreken stemgeheim)
G	Incorrecte installatie
G	Incorrecte beheer/bediening
G	Functionele, technische of beveiligingsgebreken
M	Publiceren informatie over beveiliging internetstemsysteem
M	Verkopen stem
M	Dwang / beïnvloeding van kiezer
M	Kiezer brengt meer dan één stem uit
M	Chantage
M	Doelbewust verstoren van de verkiezing
M	Defacing / bekladding internetstemsysteem
M	Onvoldoende inzicht en begrip kiezers
M	Incorrecte de-installatie

Risico	Dreigingsscenario's
M	Onbeschikbaarheid

3.3 Internetstemmen kan niet voldoen aan alle waarborgen

In de risicoanalyse zijn meerdere dreigingsscenario's onderkend die de waarborg van integriteit raken, waaronder de twee dreigingsscenario's *Niet-kiesgerechtigde brengt stem uit* en *Manipuleren van de stem of uitslag*. De mate waarin aan de waarborg van integriteit kan worden voldaan hangt primair af van het ontwerp van het internetstemsysteem en de mate waarin dit ontwerp correct is geïmplementeerd. Het is echter onmogelijk om vanuit de overheid de computer van de kiezer te beschermen tegen manipulatie. Deze manipulatie (in een scenario waarbij een aanvaller heimelijk malware heeft weten te installeren op de computer van de kiezer en daarmee de uitgebrachte stem wijzigt) is daarnaast ook bijzonder lastig te detecteren.

Aan de waarborg van stemvrijheid kan niet worden voldaan. Internetstemmen vindt plaats vanuit een omgeving die niet door het stembureau (of door een andere overheidsorganisatie) kan worden gecontroleerd. Het risico dat dwang of beïnvloeding plaatsvindt op de kiezer is een van de restrisico's van stemmen door kiezers buiten Nederland, of dat nu internetstemmen, briefstemmen of volmachtstemmen betreft.

Doordat niet kan worden voldaan aan de waarborg van stemvrijheid geldt ook voor de waarborg van het stemgeheim dat dit niet door de overheid kan worden gegarandeerd *aan de kant van de kiezer*. Dit is overigens niet anders dan bij briefstemmen.

Een internetstemsysteem is kwetsbaar voor dreigingsscenario's die er opgericht zijn het verkiezingsproces te verstoren. In het bijzonder DDoS aanvallen op de servers van een internetstemsysteem hebben potentieel een groot effect doordat het internetstemsysteem onbeschikbaar raakt voor de kiezer. Met deze dreiging zal nadrukkelijk in het ontwerp van het internetstemsysteem rekening gehouden moeten worden om, voor zover mogelijk, de DDoS aanval te detecteren en tegenmaatregelen te nemen.

In de vergelijking met briefstemmen geldt dat voor veel van de dreigingen rondom internetstemmen de vereiste kennis (en in sommige gevallen ook inspanning) om een dreiging te ontwikkelen weliswaar hoog is, maar de dreiging daarna tegen marginale meerkosten is toe te passen. De schaal waarop de dreiging kan plaatsvinden kan dan ook zeer groot zijn en wordt niet meer bepaald door de vereiste menselijke inzet of middelen. In zekere zin kan gesteld worden dat de dreiging dan geautomatiseerd is. Recente ontwikkelingen laten overigens zien dat er steeds minder specialistische kennis nodig is om deze dreigingen te kunnen uitvoeren; cybercriminelen verhuren kant en klare malware, virussen en DDoS capaciteit tegen steeds lagere kosten.

3.4 De beperkte omvang van de doelgroep kiezers buiten Nederland verkleint het effect

Het is aannemelijk dat er een aantal actoren zijn die een belang kunnen hebben bij het manipuleren van de uitslag van een verkiezing in Nederland, om (geo)politieke, economische of militaire redenen. Het effect van één stem meer of minder op de zetelverdeling is in Nederlandse kiesstelsel echter beperkt door het systeem van evenredige vertegenwoordiging. Bij de verkiezingen voor de Tweede Kamer en het Europees parlement is in de afgelopen tien jaar het aantal vanuit het buitenland uitgebrachte stemmen nooit boven de kiesdrempel gekomen. Zelfs in het geval dat van alle internetkiezers de stem zou zijn gemanipuleerd dan nog leidt dat bij deze aantallen niet tot een directe zeteltoewijzing, hoogstens een voorkeursstem voor één of twee kandidaten of een wijziging van de restzetelverdeling. Als het aantal kiezers fors stijgt, bijvoorbeeld als gevolg van de invoering van de permanente registratie, dan neemt het reële effect op de uitslag uiteraard toe.

3.5 Afhankelijkheid van technologie

Het gebruik van computer- en communicatie technologie in het stemproces betekent dat het verloop van het stemproces voor mensen minder direct waarneembaar is en daarmee minder *transparant* en *controleerbaar*. Er zijn meerdere dreigingen denkbaar en realistisch op het stemgeheim, de kiesgerechtigdheid, de integriteit en de beschikbaarheid van de technische componenten van het internetstemsysteem, zonder dat de kiezer, het stembureau of waarnemers dit door hebben. Het vergt aanvullende maatregelen om deze dreigingen te ontdekken. Veel van deze maatregelen vergen overigens de inzet van programmatuur en computertechnologie, hetgeen in zichzelf een recursief effect heeft en de complexiteit van het internetstemsysteem vergroot.

Uit de risicoanalyse is gebleken dat voor het voorkomen van dreigingen maatregelen denkbaar zijn, die op zich zelf nieuwe dreigingen introduceren. Voor die afgeleide dreigingen dienen aanvullende maatregelen genomen te worden. Dit betekent dat het ontwerpproces van het internetstemsysteem in meerdere iteratieslagen moeten worden uitgevoerd, waarbij steeds opnieuw de risico's moeten worden beoordeeld na elke ontwerpslag. Dit geldt niet alleen voor alle maatregelen die genomen worden op het gebied van beveiliging van het internetstemsysteem, maar ook voor ontwerpkeuzes in het registratieproces of voor maatregelen die tot doel hebben om de beschikbaarheid te vergroten.

3.6 Een internetstemsysteem is een complex informatiesysteem

De complexiteit van een internetstemsysteem wordt niet primair bepaald door de functionaliteit van het internetstemsysteem, die is relatief eenvoudig. Wat het internetstemsysteem tot een complex informatiesysteem maakt zijn de stringente eisen die voortvloeien uit de waarborgen controleerbaarheid, integriteit, stemgeheim, uniciteit en beschikbaarheid. Deze waarborgen maken dat het systeem geen enkele gebreken mag bevatten, de exacte werking gegarandeerd en controleerbaar moet zijn, het systeem intensief beheerd en beveiligd moet worden en dat het systeem niet alleen sterk beschermd moet zijn tegen dreigingen van buitenaf, maar ook tegen misbruik en dreigingen van binnenuit (zoals beheerders). Naast een kwalitatief goed en doordacht

ontwerp is ook de wijze waarop het internetstemsysteem wordt ontwikkeld, geïnstalleerd, beheerd, bediend en ontmanteld bepalend of in de praktijk aan de waarborgen wordt voldaan.

3.7 Benut expertise van markt zonder afhankelijk te worden

De expertise om een internetstemsysteem te ontwikkelen is schaars binnen de overheid. Er zijn internationaal meerdere leveranciers actief die zich gespecialiseerd hebben in elektronische stemsystemen, waaronder internetstemmen. Het inschakelen van deze partijen (via een EU-aanbesteding) heeft als voordeel dat geprofiteerd kan worden van de specialistische expertise en de ervaringen die opgedaan zijn uit andere landen. Echter om een te grote afhankelijkheid van marktpartijen te voorkomen is het essentieel dat overheid zelf de expertise in huis haalt én houdt om als een goed opdrachtgever de regie te houden over het ontwerp en de (door)ontwikkeling van het internetstemsysteem. Dit is niet alleen in de projectfase van belang, maar ook wanneer internetstemmen definitief als stemmethode is ingevoerd. Door de democratische controle op de overheid kan het publieke belang van verkiezingen zo beter worden geborgd. En uiteindelijk ligt de verantwoordelijkheid voor het juiste verloop van de verkiezing niet bij een marktpartij, maar bij de overheid.

4 DEEL III: EISEN AAN EEN INTERNETSTEMSYSTEEM

4.1 Inleiding

In het derde deel van het onderzoek naar internetstemmen zijn de eisen beschreven die bepalend zijn voor een betrouwbare vorm van internetstemmen. Hierbij is onderscheid gemaakt naar proces-, functionele, technische en beveiligingseisen.

Tevens is onderzocht hoe de kiezers in het buitenland op een veilige en betrouwbare wijze kunnen worden voorzien van de stembescheiden die men nodig heeft om via internet te stemmen.

In het onderzoek is ook onderzocht welke eisen gesteld moeten worden om het stembureau een zinvolle taakinvulling te geven in het geval van internetstemmen.

4.2 Eisen

Een internetstemsysteem dient te voldoen aan de algemene beginselen die gesteld worden aan elk verkiezingssysteem. In internationaal verband wordt dit vaak aangeduid met de vijf principes universal, equal, free, secret en direct elections. De beginselen zijn in Nederland vervat in de waarborgen zoals die in 2007 beschreven zijn door de commissie Stemmen met vertrouwen.

Bij het opstellen van de eisen is als uitgangspunt gehanteerd dat het internetstemsysteem een beveiligingsniveau moet hebben dat minimaal gelijk is aan het systeem van briefstemmen.

De eisen zijn op onderdelen nog generiek van aard. In een later stadium zullen deze eisen, als onderdeel van het ontwerptraject, nader gedetailleerd moeten worden.

4.3 Ontwerpkeuzen

4.3.1 Kunnen herroepen van eerder uitgebrachte stem

In het programma van eisen is als uitgangspunt genomen dat een kiezer die via internet stemt meerdere pogingen mag doen om een stem uit te brengen, maar dat slechts één stem wordt meegeteld. Hiermee wordt een maatregel voorzien die het dreigingsscenario van “dwang / beïnvloeding van de kiezer” kan beperken. De kiezer kan een eerder onder dwang uitgebrachte stem herroepen door een nieuwe stem uit te brengen. Zoals in de risicoanalyse is beschreven biedt de maatregel geen absolute bescherming tegen vergaande vormen van dwang, zeker indien die geperkt gaan met fysieke bedreigingen of belemmeringen.

Dit betekent dat het internetstemsysteem moet beschikken over de functionaliteit om te bepalen welke ontvangen stemmen moeten worden meegeteld. Hiervoor is het nodig dat er wettelijk wordt vastgelegd welke van de ontvangen stem moet worden geteld. Het meest voor de hand liggend is om de laatst ontvangen stem te tellen.

4.3.2 Terugvaloptie briefstemmen

In het programma van eisen is er voor gekozen om de kiezer de mogelijkheid te geven om pas op het moment van stemmen te bepalen of hij per brief of via internet wil stemmen. Bij eerdere experimenten met Kiezen op Afstand in 2004 en 2006 diende de kiezer reeds bij de registratie aan te geven of hij via internet of per brief wilde stemmen.

Deze keuze maakt het mogelijk om kiezers bij een eventuele (langdurige) uitval van het internetstemsysteem een terugvaloptie aan te bieden: het alsnog per brief uitbrengen van de stem. Ook voorkomt deze werkwijze dat, in de situatie van de voorgenomen invoering van de permanente registratie, de kiezer per verkiezing alsnog moet aangeven op welke wijze hij wil stemmen.

De consequentie van deze keuze is dat kiezers niet alleen meerdere keren via internet kunnen stemmen (zie vorige paragraaf) maar naast hun internetstem ook een briefstem kunnen uitbrengen. Indien een kiezer zowel via internet als per brief stemt wordt alleen de per brief uitgebrachte stem meegeteld.

Om te voorkomen dat dit leidt tot het meetellen van meerdere stemmen per kiezer (waarborg uniciteit), zal bij de stemopneming van de internetstemmen rekening gehouden moet worden met eventuele per brief uitgebrachte stemmen. De briefstembureaus dienen daartoe door te geven aan het internetstembureau welke kiezers per brief hebben gestemd, opdat in het internetstembureau kan worden bepaald of diezelfde kiezer ook via internet heeft gestemd en deze stem vervolgens ter zijde te leggen bij het tellen van de stemmen.

De consequentie van deze terugvaloptie is ook dat er een nieuwe foutkans ontstaat die mogelijk afbreuk doet aan de waarborg van uniciteit. Indien er geen of een onjuiste relatie wordt gelegd tussen de kiezer per brief een stem uitbrengt en de stem of stemmen die deze kiezer via internet uitbrengt kan dit leiden tot een ten onrechte meetellen van meerdere stemmen van één en dezelfde kiezer of tot het ten onrechte niet meetellen van een internetstem van een kiezer.

4.4 De functie van een regulier stembureau is niet goed vorm te geven in geval van internetstemmen

Uit een vergelijking van de taken tussen een regulier stembureau en een internetstembureau blijkt dat bij internetstemmen een groot aantal taken van het reguliere stembureau komt te vervallen. Dit komt deels doordat voorheen handmatig uitgevoerd handelingen onderdeel zijn geworden van de functionaliteit van het internetstemsysteem, deels doordat taken die gerelateerd zijn aan de fysieke ruimte en inrichting van het stemlokaal niet van toepassing zijn en deels doordat er taken gerelateerd zijn aan stemmethoden (volmachtstemmen en stemmen in een willekeurig stemlokaal) die geen toepassing kennen bij internetstemmen.

Geconcludeerd moet worden dat het stembureau zoals bedacht is voor verkiezingen in een stemlokaal niet één op één vorm te geven is bij internetstemmen. Een internetstembureau kan niet op een vergelijkbare wijze de controlerende en sturende functie van het reguliere stembureau invullen.

5 DEEL IV: TOETSMETHODE INTERNETSTEMMEN

In het vierde deel van het onderzoek is een methode uitgewerkt om te controleren dat een internetstemsysteem voldoet aan de gestelde eisen. Deze methode heeft als doel om te beschrijven aan welke norm een (internetstem)systeem moet voldoen, hoe de toetsing tegen de norm verloopt en wie beslissingsbevoegd is over het vaststellen van de norm, hoe de norm wordt onderhouden en de wijze waarop de toetsing verloopt. Onder het begrip 'de norm' wordt hier verstaan het geheel aan eisen, standaarden en wet- en regelgeving waar, in dit geval het internetstemsysteem, aan moet voldoen. In de vierde deelrapportage is uitgewerkt hoe de norm en het protocol voor een internetstemsysteem er uit kan zien.

5.1 Nog geen internationale normering voorhanden

In internationaal verband is en wordt gewerkt aan certificatie van systemen voor internetstemmen. Deze werkzaamheden zijn tot nu toe voornamelijk uitgevoerd door de landen die geëxperimenteerd hebben met internetstemmen of die internetstemmen als stemmethode hebben ingevoerd. Veelal is daarbij een beroep gedaan op universiteiten, onderzoeksinstellingen en onafhankelijke auditors. Er is anno 2013 nog geen generiek certificatieschema voor internetstemsystemen vastgesteld door een internationale standaardisatie organisatie zoals ISO, IEC, ITU, IETF, IEEE of de CCRA. Wel is in Duitsland een Protection Profile opgesteld voor Online Voting Products conform de Common Criteria versie 3.1 Rev 2. Dit PP is opgesteld voor verkiezingen die plaatsvinden binnen verenigingen, besturen, universiteiten en alle andere niet-politieke officiële verkiezingen. Aanbevolen wordt om een dergelijk PP op te (laten) stellen voor officiële verkiezingen als onderdeel van de ontwerpfase van het internetstemsysteem. Mogelijk kan gebruik gemaakt kan worden van het eerdere werk dat in Duitsland is verricht.

5.2 Toetsen in acceptatieprocedure, geen certificatie

Voor de ontwikkeling en levering van (delen van) het internetstemsysteem wordt zeer waarschijnlijk een beroep gedaan op marktpartijen. Onderzocht is of hiervoor toetsmethoden als 'eigen verklaring' of 'certificatie' mogelijk zijn.

Een eigen verklaring geeft gelet op het belang en de risico's onvoldoende garantie dat aan de norm is voldaan. Certificatie in opdracht van een leverancier door een onafhankelijke certificatie instelling is in principe mogelijk, maar wordt meestal toegepast in situaties waar het afdoende is om een eenmalige type-certificering te verkrijgen (en niet alle exemplaren van het product getoetst hoeven te worden). Certificatie is in feite een eenmalige toets, waar meerdere afnemers gebruik van maken zodat ze niet zelf hoeven te toetsen. Certificatie wordt bemoeilijkt doordat een internationale norm waartegen een internetstemsysteem kan worden gecertificeerd nog ontbreekt. Het is ook niet waarschijnlijk dat in een dergelijke norm de precieze Nederlandse situatie en alle specifiek door de Nederlandse overheid gestelde eisen zijn vervat.

De methode waarbij de afnemer (de overheid) opdracht geeft aan een onafhankelijke instantie om het internetstemsysteem te toetsen tegen de norm als onderdeel van de acceptatieprocedure is het meest geschikt.

5.3 Instantie Normering Internetstemmen

Aanbevolen wordt om een instantie te creëren met als taak om de norm en het protocol op te stellen en te onderhouden. De leden van deze instantie worden benoemd door de minister van BZK. Eventueel kan de taak van deze instantie worden verankerd in wet- en regelgeving. Dit heeft als bijkomend voordeel dat de taak in openbaarheid wordt uitgevoerd.

VERDONCK KLOOSTER & ASSOCIATES

DEEL I - INTERNATIONALE INVENTARISATIE INTERNETSTEMMEN

Gebruik van Internetstemsystemen bij officiële verkiezingen van vertegenwoordigende overheidsorganen

INHOUDSOPGAVE

1 INLEIDING

1.1 Algemeen

In opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is een inventarisatie uitgevoerd van de systemen voor internetstemmen die andere landen hebben gebruikt voor het stemmen bij formele verkiezingen van vertegenwoordigende organen of voor het houden van proeven/experimenten daarmee.
Deze inventarisatie maakt onderdeel uit van een onderzoek naar de risico's van internetstemmen, en mogelijke maatregelen daartegen.

1.2 Afbakening

In deze rapportage zijn alle landen opgenomen waarvan bekend is dat zij in de periode 2000 – 2013 bij openbare verkiezingen voor vertegenwoordigende overheidsorganen kiezers de mogelijkheid hebben geboden om via internet te stemmen, waarbij deze stemmen meetelden in de officiële uitslag.
Per land is een beschrijving gegeven met als doel om een internationaal overzicht te geven van de wijze waarop internetstemmen in andere landen is toegepast. Deze rapportage heeft niet het doel om een uitputtende beschrijving te geven van de gebruikte stemdienst, het kiessysteem, toepasselijke wetgeving of een evaluatie van het 'succes' van een gehouden experiment.

Die landen waar internetstemmen is ingezet bij verkiezingen, maar waarbij de via internet uitgebrachte stemmen niet in de officiële uitslag meetelden zijn in deze inventarisatie buiten beschouwing gelaten.
Eveneens zijn alle toepassingen van internetstemmen bij verkiezingen voor niet-overheidsorganisaties niet meegenomen in de inventarisatie, zoals universiteitsraadsverkiezingen, verkiezingen binnen politieke partijen, informele volksraadplegingen, ondernemingsraadsverkiezingen, aandeelhoudersverkiezingen, etc.

De twee experimenten in Nederland (bij de verkiezingen voor het Europees Parlement in juni 2004 en de Tweede Kamer in 2006) zijn niet opgenomen in dit overzicht. Hiervan zijn evaluatiebeschrijvingen beschikbaar via de website van BZK.

EXPERIMENTEN

In heel veel landen is de inzet van internetstemmen steeds beschouwd als een experiment. Hiermee wordt gepoogd aan te duiden dat de mogelijkheid om via internet te stemmen een tijdelijk karakter heeft en dat nog niet is besloten om het definitief als stemmethode in te voeren. Met experiment wordt niet het houden van een test, pilot of proef bedoeld.

TERMINOLOGIE

Internationaal worden voor het begrip internetstemmen verschillende termen gebruikt. In angelsaksische landen wordt internetstemmen veelal aangeduid als 'e-voting', 'i-voting', 'online voting' of 'remote online voting'. In Frankrijk wordt de term 'vote electronique' gebruikt. Ook is er

in veel landen voor gekozen om internetstemmen een merknaam mee te geven, zoals “i-vote”, “Votachilango” of “Cybervote”.

In deze rapportage wordt internetstemmen gedefinieerd als:

Internetstemmen is een wijze van stemmen waarbij de kiezer op elektronische wijze zijn stemvoorkeur kenbaar maakt, op een locatie waar geen toezicht wordt gehouden, en waarbij hij de stem overdraagt aan het stembureau via het openbare internet.

	Toelichting:
‘op elektronische wijze’	Hierbij wordt bedoeld dat de kiezer zijn voorkeur elektronisch kenbaar maakt, meest waarschijnlijk met behulp van een computer (of smartphone, tablet, etc.). Dit in tegenstelling tot het kenbaar maken van de stem op papier. NB het downloaden van een stembiljet in bijvoorbeeld pdf formaat en vervolgens via reguliere post of mail versturen wordt niet gezien als internetstemmen.
‘locatie waar geen toezicht wordt gehouden’	De kiezer stemt op een locatie waar geen toezicht wordt gehouden[1]. Het toezicht (zoals door het stembureau in het stemlokaal) heeft onder meer ten doel om te waarborgen dat een kiezer in vrijheid (zelfstandig, zonder beïnvloeding of dwang) zijn stem kan uitbrengen.
‘overdraagt aan het stembureau’	Met overdracht aan ‘het stembureau’ wordt hier niet de letterlijke betekenis van het stembureau zoals bedoeld in de Nederlandse Kieswet, maar de overdracht van de stem aan een organisatie die de (veelal wettelijke) verantwoordelijkheid heeft voor de ontvangst van de stemmen en de stemopneming.
‘openbare internet’	De stem wordt verstuurd via het openbare internet. Experimenten waarbij private, afgeschermde, netwerken (zoals bijvoorbeeld een defensie netwerk) worden gebruikt worden niet beschouwd als internetstemmen

In deze rapportage wordt de term ‘elektronisch stemmen’ niet gebruikt, om verwarring met stemmachines in stemlokalen (soms ook aangeduid als stemcomputers) te voorkomen.

1.3 Methodologie

De inventarisatie is uitgevoerd op basis van publiekelijk beschikbare informatie, zoals officiële uitslagen, websites van overheden en verkiezingsautoriteiten, gepubliceerde evaluatierapporten

[1] In Finland is in 2008 een experiment gehouden in een drietal gemeenten waarbij kiezers in een stemlokaal hun stem uitbrachten op een computer, welke de resultaten doorstuurde via het internet naar een centraal opgestelde server.

en eerdere uitgevoerde inventarisaties. In het kader van deze inventarisatie is een bezoek gebracht aan de National Election Committee in Estland en het Ministry of Local Government and Regional Development in Noorwegen.

In Bijlage B is een overzicht gegeven van alle gebruikte bronnen.

In een aantal landen (Zwitserland, Canada, Verenigd Koninkrijk, Estland) is internetstemmen bij een groot aantal (veelal lokale) verkiezingen ingezet. In de beschrijving van de verkiezingen in die landen is niet elke verkiezing afzonderlijk beschreven.

1.4 Leeswijzer

In de hoofdstukken 3 tot en met 14 is per land een casus beschrijving gegeven van de aldaar gehouden verkiezingen waarbij internetstemmen was toegestaan. De landen zijn in alfabetische volgorde opgenomen. De belangrijkste constateringen en bevindingen die volgen uit de internationale inventarisatie zijn beschreven in hoofdstuk 2.

2 CONSTATERINGEN UIT INVENTARISATIE

2.1 Experimenten met internetstemmen in elf landen

Op het moment van deze inventarisatie, eind 2013, is internetstemmen beschikbaar als stemmethode in zeven landen. Alleen in Estland is internetstemmen op landelijke schaal ingevoerd, in de andere zes landen is internetstemmen voorbehouden aan een specifiek afgebakende groep kiezers. Veelal betreft het inwoners van specifieke gemeenten of staten, of kiezers die in het buitenland verblijven.

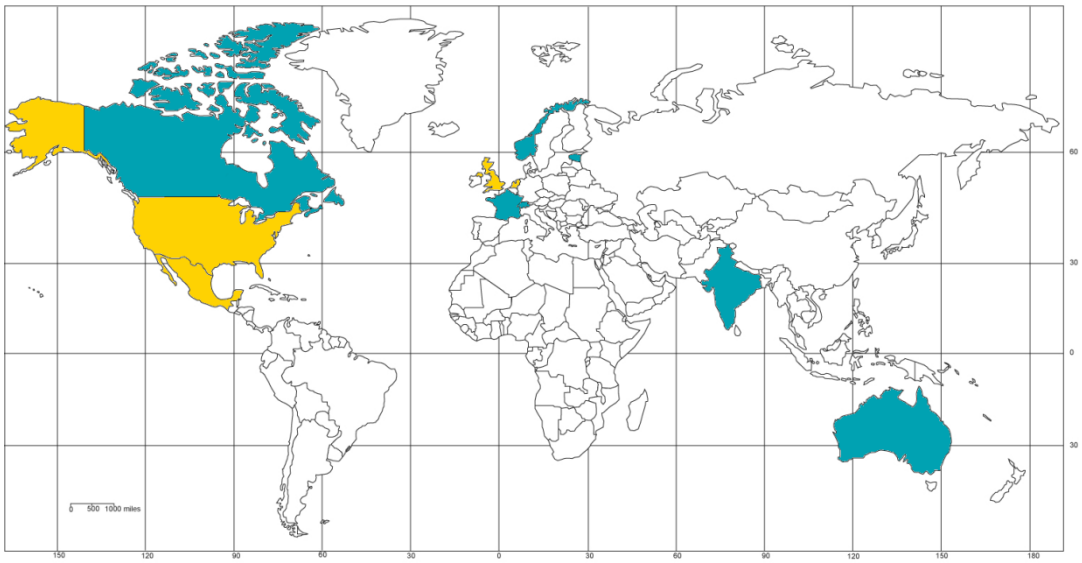
	Land	Regio / doelgroep	Formele status
1.	Australië	Kiezers in de staat New South Wales	Experiment
2.	Canada	Kiezers in 60 gemeenten in de staten Ontario en Nova Scotia	Ingevoerd voor gemeentelijke verkiezingen in twee staten, niet voor landelijke of statenverkiezingen
3.	Estland	Alle kiezers	Ingevoerd
4.	Frankrijk	Alle kiezers woonachtig buiten Frankrijk	Ingevoerd
5.	India	Kiezers in 6 gemeenten in de staat Gujarat	Experiment
6.	Noorwegen	Kiezers in 12 gemeenten	Experiment
7.	Zwitserland	Kiezers in 13 kantons, met een limiet op het aantal kiesgerechtigden	Experiment[2]

Daarnaast zijn in de periode 2000 – 2013 in de onderstaande vier landen experimenten gehouden met internetstemmen, maar zijn deze experimenten beëindigd en is deze stemmethode momenteel niet toegestaan:

8. Mexico
9. Nederland
10. Verenigd Koninkrijk
11. Verenigde Staten van Amerika

In onderstaande Figuur 1 zijn de zeven landen waar internet stemmen de status experiment of ingevoerd heeft weergegeven in blauwgroen. De overige vier landen zijn in geel weergegeven.

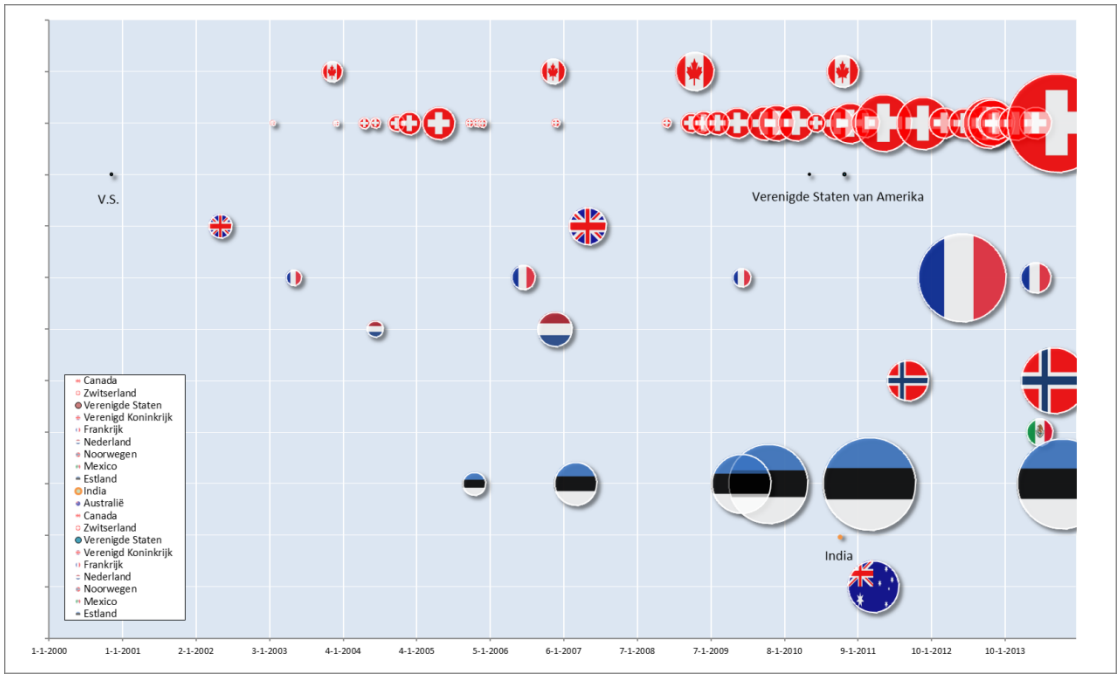
[2] Ondanks dat in sommige kantons reeds lang via internet gestemd kan worden is de formele status op dit moment nog experimenteel. Kantons hebben toestemming nodig van de federale overheid alvorens zij internetstemmen kunnen aanbieden. Zie voor meer informatie paragraaf 12.1.3.



Figuur 1 Overzicht landen – Landen waar experimenten met internetstemmen zijn gehouden

2.2 Historisch overzicht

In onderstaande figuur zijn alle verkiezingen weergegeven in de periode 2000-2013 in de 11 landen waar internetstemmen is toegepast. De eerste internetverkiezing vond plaats op 7 november 2000 in de Verenigde Staten van Amerika.

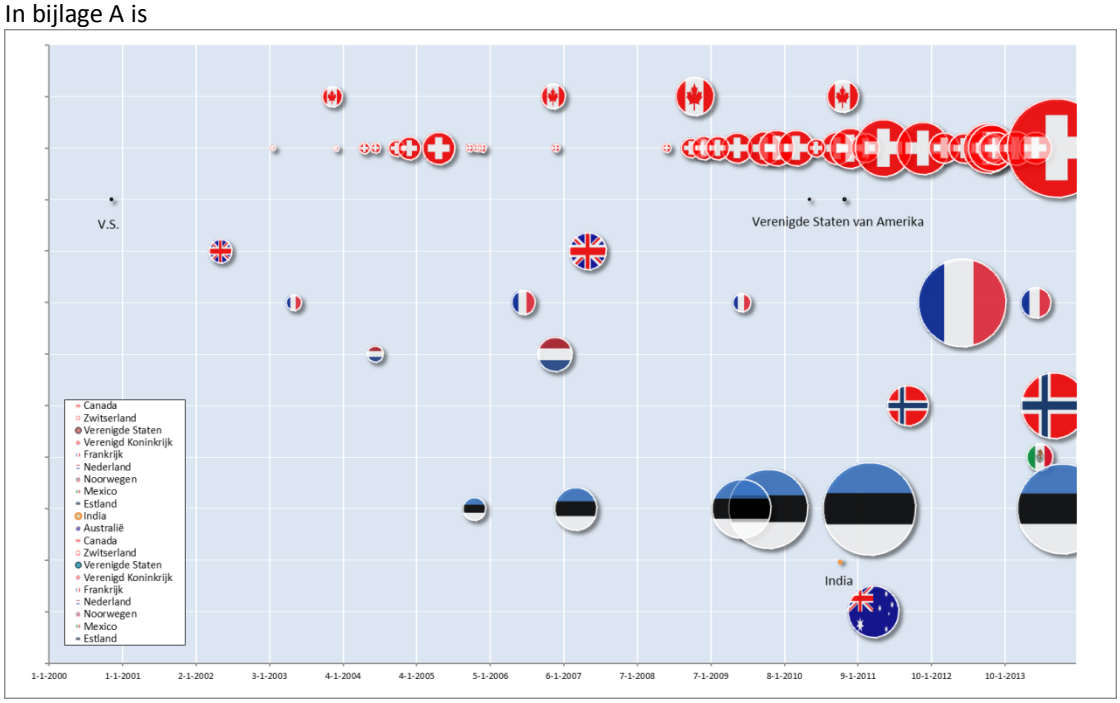


Figuur 2 Overzicht internetstemmingen, omvang bol = aantal kiezers

In de figuur geeft de oppervlakte van de bol het aantal uitgebrachte stemmen via internet weer.

Ter vergelijking is ook het aantal kiezers dat in Nederland in 2004 en 2006 via internet stemde in de figuur weergegeven.

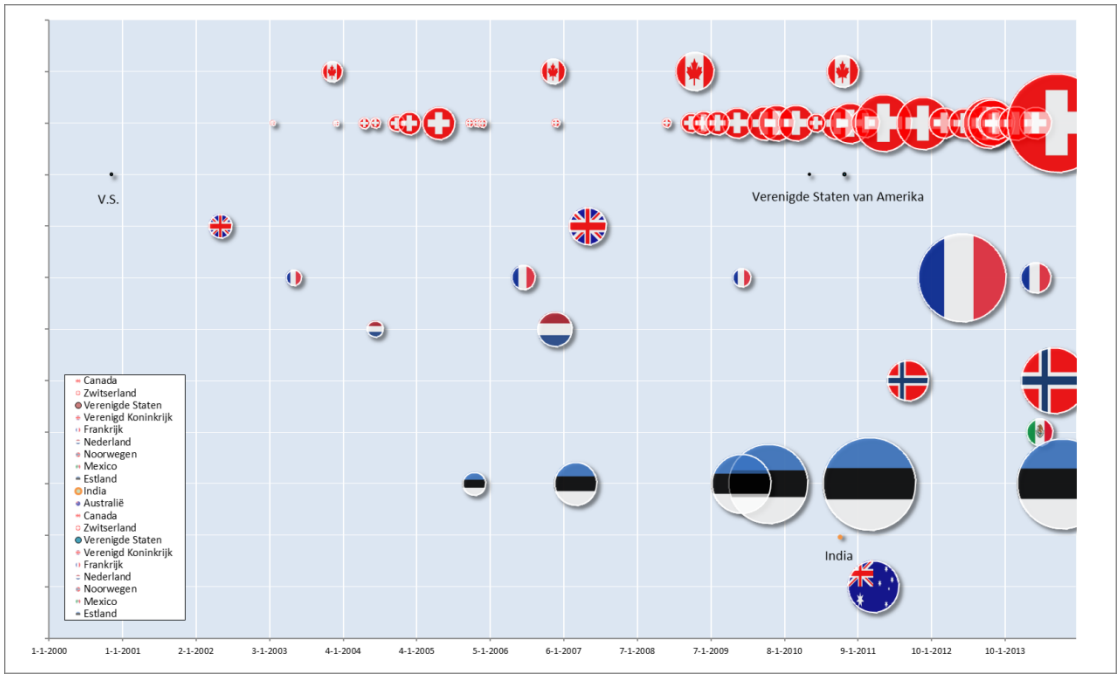
In bijlage A is



Figuur 2 in groot formaat opgenomen.

2.3 Aantal kiezers dat per internet stemt is nog beperkt

Uit



Figuur 2 is ook af te leiden dat het aantal kiezers dat via internet stemt internationaal gezien nog zeer beperkt is, in verhouding tot het totale electoraat. De grootste internetstemming in termen

van aantal kiezers dat via internet stemde is tijdens een referendum in Zwitserland geweest, op 22 september 2013. Toen stemden 158.500 kiezers via internet.
In totaal zijn er wereldwijd ruim 1,5 miljoen stemmen uitgebracht via internet bij formele verkiezingen.

In onderstaande tabel is van de zeven landen waar internetstemmen nu is ingevoerd het aantal kiezers dat via internet heeft gestemd afgezet tegen het totaal aantal kiezers dat deelnam aan die verkiezing. Voor de landen waarbij meerdere internetverkiezingen zijn gehouden is de verkiezing genomen met het hoogste aantal internetstemmers.

	Verkiezing	Aantal kiezers dat via internet stemde	% van kiezers dat via internet stemde
Australië	NSW - Parlementsverkiezing 2011	44.605	0,96 %
Canada	Halifax – Gemeenteraadsverkiezing 2008	25.206	24,96 %
Estland	Parlementsverkiezing 2011	140.764	24,3 %
Frankrijk	Parlementsverkiezing 2012	126.947	60,0 %
India	Gemeenteraadsverkiezing 2010	124	-
Mexico	Gouverneurverkiezing 2013	12.300	20,0%
Noorwegen	Parlementsverkiezing 2013	70.622	28,2%
Verenigd Koninkrijk	Gemeenteraadsverkiezing Swindon 2007	7.647	5,15%
Verenigde Staten	Generale verkiezing 2010	125	-
Zwitserland	Referendum 2013	158.500	6,58%

2.4 Motieven voor invoering internetstemmen

De motieven om internetstemmen in te voeren verschillen per land en daarbinnen veelal ook per lokale overheid, maar grosso modo zijn in de landen die internetstemmen hebben beproefd of ingevoerd de volgende motieven bepalend geweest in de besluitvorming: het verbetert de toegankelijkheid om te kunnen stemmen, het is gemakkelijker, wens om democratie te moderniseren met ICT en de wens om de opkomst te verhogen.

Motief	Toelichting(en)
'Toegankelijkheid en gemak voor de kiezer'	Een veel gebruikt argument is dat stemmen via internet meer gemak oplevert voor de kiezer, vooral wanneer afgezet tegen stemmen in een stemlokaal of afgezet tegen briefstemmen. Onder gemak wordt tijdwinst door afwezigheid van reistijd, geen hinder door weersomstandigheden, kunnen stemmen gedurende 24 uur in een meerdaagse periode en betere toegankelijkheid voor personen met

Motief	Toelichting(en)
	een lichamelijke beperking genoemd. Het gemak en de toegankelijkheid hangen ook samen met welke alternatieve stemmethoden geboden worden in een land. Zo kent maar een beperkt aantal van de onderzochte landen de mogelijkheid van onderhandse volmachten (zoals in Nederland) of worden sommige stemmethoden alleen aan specifieke doelgroepen geboden (zoals vervroegde stemperiode of briefstemmen).
'Modernisering van democratie'	In diverse landen is de wens om de democratie te moderniseren met behulp van ICT een belangrijke drijfveer geweest. Daarbij werd voorzien dat dankzij de inzet van ICT vaker (en tegen lagere kosten) volksraadplegingen worden gehouden, waardoor de democratische participatie van burgers toe zou nemen. Gesteld werd ook dat de bestaande methoden om te stemmen niet meer van deze tijd zijn. Kiezers zijn inmiddels volledig gewend om alles via internet af te handelen en om langs die weg ook hun meningen te delen en vinden dat stemmen in een stemlokaal of via brief ouderwets is.
'Verhoging van opkomst'	In veel Westerse landen is een meer-jaren trend waarneembaar van dalende opkomsten bij zowel nationale en lokale verkiezingen. Een veel gehoorde verklaring hiervoor is dat dit samenhangt met het moeten stemmen in persoon in een stemlokaal op een specifiek tijdstip. De stelling wordt geponeerd dat als de kiezer vanaf een willekeurige plek en op een zelfgekozen moment zou kunnen stemmen dit de opkomst doet vergroten, in het bijzonder onder de doelgroep jongeren.
'Efficiency en kostenbesparing'	Door via internet te stemmen kan bespaard worden op de kosten die samenhangen met de traditionele stemmethoden: inrichting van stemlokalen, reiskosten van de kiezers, vergoedingen voor stembureauleden, kosten van briefstemmen, tijd gemoeid met tellen, etc.
'e-overheid'	In Estland is de invoering van internetstemmen ook beschouwd als een logische vervolgstap in een meer-jaren overheidsbeleid om dienstverlening aan burgers via het internet aan te bieden.

2.5 Opkomst niet significant gestegen

Er is door diverse overheden en internationale onderzoeksorganisaties onderzoek gedaan naar de vraag of het bieden van de mogelijkheid tot internetstemmen een positief effect heeft op de opkomst. De beoogde stijging van de opkomst blijkt in de praktijk maar in zeer beperkte mate gerealiseerd te worden.

Onderzoek[3] naar de opkomst bij de verkiezingen van 2007 in Estland wees uit dat internetstemmen geen nieuwe kiezers trok. Wel was een verschuivingseffect waarneembaar, de groei in stemmen die via internet werden uitgebracht ging gepaard met een daling van de uitgebrachte stemmen in het stemlokaal. De opkomst in 2007 was 4% hoger dan in 2003, maar de onderzoekers wezen die groei toe aan een algehele stijging van de opkomst en de komst van een nieuwe politieke partij.
Uit het onderzoek bleek ook dat internetstemmen vooral veel gebruikt werd door hoog opgeleide kiezers die een sterke politieke affiniteit hadden.

In Zwitserland bleek uit diverse van de gehouden experimenten dat de opkomst met name steeg onder de doelgroep 'kiezers in het buitenland', waar in sommige gevallen tot 50% van de kiezers via internet stemde. De opkomst van kiezers die in Zwitserland woonden is geen stijging van de opkomst waargenomen. Ook hier trad een substitutie effect op, van stembureau naar internetstemmen.

In Noorwegen steeg de opkomst in de gemeenten die meededen aan het internetstem experiment bij de verkiezingen in 2011 met gemiddeld 3 procent. Echter, bij de gemeenten waar internetstemmen niet werd aangeboden steeg de opkomst gemiddeld ook met ongeveer 3%[4].

In die landen waar internetstemmen is gebruikt als stemmethode voor kiezers die in het buitenland wonen, maakt een groot percentage van die kiezers gebruik van internetstemmen.

2.6 Voorzichtige aanpak

In vrijwel alle[5] landen is de introductie van internetstemmen voorafgegaan door een onderzoekstraject waarbij veelal ook wetenschappers, (internationale) onderzoeksbureaus en leveranciers bij werden betrokken. Hierin is steeds uitgebreid aandacht besteed aan de eerdere experimenten in andere landen en werd in kaart gebracht welke risico's gepaard gaan met het stemmen via internet.
Veelal werd vervolgens eerst op kleine schaal testen uitgevoerd met de ontwikkelde of aangekochte internetstemdienst, alvorens internetstemmen bij de officiële verkiezing toe te staan.

Internetstemmen is in alle landen steeds beschouwd als een additioneel kanaal om te stemmen naast de bestaande mogelijkheden, om zodoende niet volledig afhankelijk te zijn van de juiste werking van de stemdienst.

---

[3] Daniel Bochsler, 2010. Centre for the Study of Imperfections in Democracies, http://www.eui.eu/Projects/EUDO-PublicOpinion/Documents/bochslere-voteeui2010.pdf

[4] Zie onder meer "Internet Voting in Norway 2011: Democratic and Organisational Experiences" van Harald Baldersheim, Universiteit van Oslo

[5] De (bestuurlijke) aanpak van de introductie van internetstemmingen in India is niet gepubliceerd.

Ook is in diverse landen eerst een aparte wettelijke basis gecreëerd, waarin het tijdelijk is toegestaan om een andere stemvorm te beproeven. Naast de tijdelijkheid worden ook de 'spelregels' van de internetstemming vastgelegd, bijvoorbeeld rondom de verantwoordelijkheden en bevoegdheden van toezichthouders of het gebruik van end-to-end verificatiemogelijkheden voor de kiezer.

Afgezien van een groot scala aan organisatorische en technische maatregelen zijn er in diverse landen ook beleidsmatige (veelal wettelijk verankerd) maatregelen genomen om de onderkende risico's te beperken:

a. Beschikbaarheid alleen voor specifieke doelgroep(en)
b. Beperking aantal kiezers
c. Experimenten bij lokale verkiezingen
d. Internetstem in vervroegde stemperiode
e. Herroepen internetstem

BESCHIKBAARHEID ALLEEN VOOR SPECIFIEKE DOELGROEP(EN)

In alle landen is er voor gekozen om internetstemmen in eerste instantie niet aan alle kiezers toe te staan. Vrijwel zonder uitzondering is gekozen voor een doelgroep benadering, waarbij de mogelijkheid van internetstemmen eerst aan specifieke groepen kiezers is aangeboden.
De meest voorkomende doelgroepen zijn kiezers die op de dag van stemming niet op de reguliere wijze(n) kunnen stemmen doordat ze elders verblijven, en kiezers die door een lichamelijke beperking problemen ondervinden om in een stemlokaal te stemmen.

	Verblijf elders	Lichamelijke beperking	Overige doelgroep, nl
Australië	Ja	ja	
Canada			
Estland	Ja	ja	
Frankrijk	Ja		
India			
Mexico	Ja		
Nederland	Ja		
Noorwegen	Nee	Ja	
Verenigd Koninkrijk	Nee		
Verenigde Staten	Ja, militairen		
Zwitserland	Ja	ja	

Estland biedt daarnaast een groot aantal andere stem-mogelijkheden aan, waaronder briefstemmen, thuisstemmen en stemmen in een periode voorafgaand aan de dag van stemming.

BEPERKING AANTAL KIEZERS

In Zwitserland heeft de federale regering ervoor gekozen om een wettelijke limiet in te stellen van het aantal kiezers dat gebruik mag maken van stemmen via internet. In eerste instantie is deze limiet gesteld op 10%; mocht er iets misgaan dan is de invloed op de uitslag beperkt. Naar mate er meer ervaring wordt opgedaan wordt besloten of de wettelijke limiet kan worden verhoogd.

EXPERIMENTEN BIJ LOKALE VERKIEZINGEN

In Noorwegen, Canada, Verenigd Koninkrijk en Zwitserland heeft de federale regering lokale overheden in staat gesteld om te experimenteren met internetstemmen, mede om de eerste ervaringen op te doen bij lokale verkiezingen. Directe toepassing bij landelijke verkiezingen (zoals parlements- of presidentsverkiezingen) werd hier te risicovol geacht.
Ondanks dat de vrijheid om te experimenteren aan lokale overheden werd gegeven, zijn er steeds vanuit nationaal / federaal niveau wel verschillende randvoorwaarden gesteld, is wetgeving aangepast en zijn middelen beschikbaar gesteld. Zo is bijvoorbeeld in Engeland in de periode 2002 tot 2007 een grote verscheidenheid aan experimenten uitgevoerd in meer dan twintig gemeenten.

INTERNETSTEMMEN IN VERVROEGDE STEMPERIODE

In Estland, Canada en Noorwegen is een systeem ingevoerd waarbij de kiezer zijn internetstem alleen voorafgaand aan de dag van stemming kan uitbrengen. Mocht er iets misgaan met het internetstemmen dan hebben de kiezers de mogelijkheid om op de dag van stemming alsnog hun stem op ‘traditionele wijze’ in een stemlokaal uit te brengen.

HERROEPEN INTERNETSTEM

In een aantal landen is gekozen voor een internetstemsysteem waarbij de kiezer meer dan één stem mag uitbrengen via internet. Dit voor het geval de kiezer zich bedenkt, als hij vermoedt dat zijn stem niet goed is overgekomen door technische problemen, of in geval dat de kiezer niet in vrijheid heeft kunnen stemmen. In Estland en Noorwegen wordt deze systematiek gehanteerd, waarbij steeds de laatst ontvangen internetstem telt. En als er op de dag van stemming alsnog een stem wordt uitgebracht in het stembureau, telt alleen die stem.
NB. in andere landen, zoals Australië en Canada, dient de kiezer vooraf een keuze te maken voor de stemmethode: als hij kiest om via internet te stemmen, dan is het niet meer toegestaan om in een stembureau te stemmen.

2.7 Verschillende authenticatiemethoden

Eén van de uitdagingen van stemmen via internet is de methode hoe een kiesgerechtigde persoon op afstand kan worden herkend. Met andere woorden: hoe weet de verkiezingsautoriteit zeker dat het de juiste, kiesgerechtigde, kiezer is die gebruik wil maken van de stemdienst? In de meeste landen is een kiezersregister de basis waartegen de verificatie plaatsvindt. In sommige landen, zoals Australië, Zwitserland, Estland en Noorwegen blijft de kiezer opgenomen in het kiezersregister, ook na een verhuizing naar het buitenland. In andere landen dient de kiezer er zelf voor te zorgen, via een registratieprocedure, dat hij in het kiezersregister wordt opgenomen.

In de eerste jaren gebruikten de meeste landen een systematiek van een gedeeld geheim: de kiezer maakt gebruik van een wachtwoord of stemcode die specifiek voor die verkiezing gegenereerd wordt door de verkiezingsautoriteit en toegestuurd wordt via de reguliere post (een 'out-of-band' kanaal) aan de kiezer. In Australië, Engeland en Frankrijk is dit omgedraaid, het is de kiezer die bij de registratie een wachtwoord/code bedenkt en toestuurt aan de verkiezingsautoriteit.
Later is in Frankrijk, net zoals in Neuchâtel - Zwitserland, gebruik gemaakt van een bestaand identiteitsmiddel dat voor meerdere overheidsdiensten gebruikt kan worden (inloggen op een generiek overheidsportaal).
Meer geavanceerd (en kostbaar) zijn de systemen waarin een smartcard wordt gebruikt voor de identificatie. De smartcard functioneert als een elektronische identiteitskaart en is in staat om cryptografische functies uit te voeren (zoals het plaatsen van een elektronische handtekening). De landen die dit gebruiken (Estland en Noorwegen) hebben deze E-ID niet specifiek ingevoerd voor hun internetverkiezingen, maar hadden deze infrastructuur al voor andere elektronische (overheids)diensten.
In India hebben, bij het eerste experiment in 2011, ambtenaren huisbezoeken gebracht om de identiteit van de kiezers vast te stellen. Het aantal geregistreerde kiezers was destijds overigens slechts 387.

In onderstaande tabel staat een overzicht van de registratie en authenticatie systematiek:

	Doelgroep	Separate registratie vereist voor internetstemmen?	Authenticatie middel
Australië	Kiezers binnenland	Ja	Kennis en bezit: Kiezer geeft zelf PINcode op bij registratie en ontvangt tweede code per post.
	Kiezers buitenland	Ja	Kennis en bezit: Kiezer geeft zelf PINcode op bij registratie en ontvangt tweede code per post.
Canada	Kiezers binnenland	Afhankelijk van gemeente	Kennis en bezit: Kiezer geeft zelf beveiligingsvraag en antwoord op bij registratie en ontvangt tweede code per post (systeem Markham).
Estland	Kiezers binnenland	Nee, afgeleid uit bevolkingsadministratie	E-ID kaart[6]
	Kiezers buitenland	Nee	E-ID kaart

[6] De E-ID kaart wordt van overheidswege verstrekt en kan gebruikt worden voor diverse e-overheidsdiensten. De E-ID kan ook als SIM kaart worden verkregen

	Doelgroep	Separate registratie vereist voor internetstemmen?	Authenticatie middel
Frankrijk	Kiezers buitenland	Ja	Kennis en bezit: Kiezer geeft zelf wachtwoord op bij registratie en ontvangt tweede code per post.
India	Kiezers binnenland	Ja	Kennis en persoonlijke identificatie: Ambtenaren brengen huisbezoek om de registratiegegevens en identiteit van de kiezer te controleren. Kiezer ontvangt gebruikersnaam per e-mail en wachtwoord via mobiele telefoon. Wachtwoord wordt door kiezer gewijzigd.
Mexico	Kiezers buitenland	Ja	Bezit: Kiezer ontvangt kaart met code.
Noorwegen	Kiezers binnenland	Nee, afgeleid uit bevolkingsadministratie	E-ID kaart[7]
Verenigd Koninkrijk	Kiezers binnenland	Ja	Kennis en Bezit: Kiezer geeft zelf wachtwoord op bij registratie en ontvangt tweede code per post.
Verenigde Staten	Kiezers buitenland	Ja	Kennis en bezit: kiezer geeft zelf PINcode op bij registratie en ontvangt tweede code per post.
Zwitserland	Kiezers binnenland	Nee	Bezit (persoonlijke PINcode op per post toegestuurde stemkaart).
	Kiezers buitenland	Ja	Bezit (persoonlijke PINcode op per post toegestuurde stemkaart).

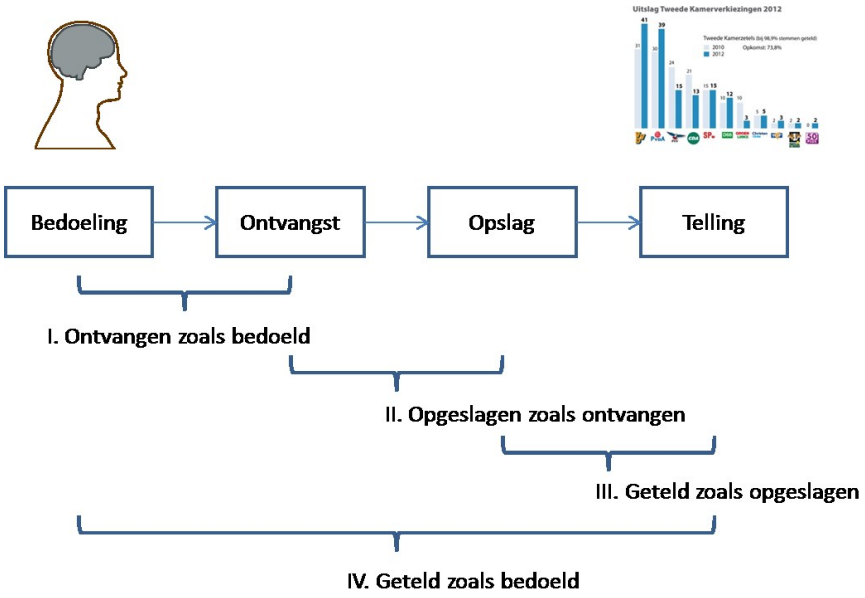
2.8 Verificatie door kiezers als controle mechanisme

In alle landen die experimenteren of experimenteerden met internetstemmen en in alle landen die internetstemmen hebben onderzocht maar besloten hebben geen experimenten te houden speelt nadrukkelijk de zorg omtrent de veiligheid van internetstemmen een rol. Internetstemmen moet, net als andere stemvormen, voldoen aan universele vereisten op het vlak van eerlijke vrije verkiezingen. Eén van de aandachtsgebieden betreft de *integriteit* en *controleerbaarheid*; een

[7] De E-ID kaart wordt van overheidswege verstrekt. Daarnaast kunnen Noren ook een bancaire E-ID kaart gebruiken

verkiezing moet verlopen conform de wettelijke regels, de uitkomst mag niet beïnvloedbaar zijn anders dan door het uitbrengen van rechtmatige stemmen en het verloop van de verkiezing moet objectief controleerbaar zijn.
Juist door het gebruik van computers en het internet bij internetstemmen zijn traditionele controlemethoden die gebaseerd zijn op menselijk waarnemen minder of niet geschikt. Daarnaast kent internetstemmen nieuwe dreigingen, die zich in de algemene internet praktijk reeds op vele manieren hebben gemanifesteerd (zoals cybercriminaliteit waaronder diefstal, identiteitsfraude en afpersing, cyberspionage en cyberoorlogsvoering).
In reactie op de zorgen omtrent het verlies aan controleerbaarheid en de nieuwe categorie dreigingen is de laatste jaren veel wetenschappelijk onderzoek gedaan op het gebied van *verificatie mechanismen*. Dit type van verificatie gaat verder dan gebruikelijke methoden als SSL en EV waarbij een derde partij[8] instaat voor de authenticiteit van een server / URL.
In het bijzonder is onderzoek gedaan naar *end-to-end individual verification;* verificatie door de kiezer zelf dat zijn stem precies zo is meegeteld zoals de kiezer het had bedoeld. Zonder aanvullende maatregelen introduceert end-to-end verifiability echter een nieuwe ongewenste eigenschap: de kiezer kan bewijzen wat hij gestemd heeft en daarmee is de kiezer in staat om zijn stem te verkopen.

In Figuur 3 en de onderstaande tabel is een overzicht gegeven van de primaire controle-eigenschappen van typen verificatie mechanismen.



Figuur 3 Typen verificatie mechanismen

[8] De derde partij (thrusted third party / TTP) heeft de identiteit van de server en de organisatie die de server en de URL in eigendom hebben geverifieerd.

	Verificatie mechanisme	Doel van verificatie	Verificatie door	Angelsaksische termen
I.	Ontvangen zoals bedoeld	Uitgebrachte stem is correct ontvangen door authentieke stemdienst	Kiezer	*cast as intended*
II.	Opgeslagen zoals ontvangen	Ontvangen stem is correct opgeslagen in de stembus	Kiezer / Verkiezingsorgaan	*stored as cast*
III.	Geteld zoals opgeslagen	Alle opgeslagen stemmen zijn correct geteld	Verkiezingsorgaan	*counted as stored*
IV.	Geteld zoals bedoeld	Stem geteld zoals uitgebracht	Kiezer	*counted as cast / End-to-end individual or universal verification*

End-to-end *universal* verifiability wordt in de internationale literatuur beschouwd als de meest uitgebreide en meest ultieme vorm van verificatie, omdat niet alleen de kiezer zelf, maar ook anderen (zoals politieke partijen, toezichthouders, verkiezingswaarnemers en het orgaan dat de verkiezingen organiseert) kunnen verifiëren dat alle uitgebrachte stemmen correct zijn geteld.

Verificatie door de kiezers is voor het eerst beproefd in Nederland[9], bij de verkiezingen in 2006. Recenter is in Estland (2013) en Noorwegen (2011) een vorm van “ontvangen zoals bedoeld” kiezersverificatie beproefd. Bij de meest recente verkiezingen in Noorwegen (2013) is daarnaast ook de verificatie vormen “Opgeslagen zoals ontvangen” en “Geteld zoals opgeslagen” beproefd.

Estland heeft er bewust voor gekozen om geen verdergaande vormen van verificatie te bieden, enerzijds om geen andere waarborgen en eigenschappen te introduceren in vergelijking tot hun briefstemsysteem, anderzijds omdat de complexiteit van de stemdienst sterk toeneemt (cryptografische protocol, additionele maatregelen om het cryptografische protocol en de bij behorende voorzieningen en procedures te beveiligen).

Ook in Zwitserland zijn plannen om een vorm van kiezers verificatie toe te gaan passen, als onderdeel van de volgende roll-out fase.

[9] In Nederland is in 2006 een vorm van kiezersverificatie geboden die uitging van universal verifiability; niet alleen de kiezer zelf kon controleren dat zijn uitgebrachte stem correct was geteld, maar ook anderen konden controleren dat alle ontvangen stemmen correct waren geteld.

2.9 Experimentele karakter leidt tot relatief hoge kosten

In onderstaand overzicht zijn, voor zover beschikbaar, per land de kosten weergegeven van internetstemmen. De opgave van kosten is steeds ontleend uit officiële evaluatierapporten. Er heeft door de auteurs van dit rapport geen validatie of normalisatie kunnen plaatsvinden van de kosten. Er is derhalve niet mogelijk om uit dit overzicht vergelijkende conclusies te trekken.

	Kosten (€)[10]	Aantal stemmen	Kosten per stem (€)
Australië	2.700.000	46.864	57
Canada	Onbekend	-	-
Estland	Onbekend	-	-
Frankrijk (2006)	2.000.000	10.201	196
India	Onbekend	-	-
Mexico	Onbekend	-	-
Noorwegen	Onbekend	-	-
Verenigd Koninkrijk (Swindon)	1.340.000	4.293	312
Verenigde Staten	Onbekend	-	-
Zwitserland (tot 2011)	8.000.000	100.000	80
Zwitserland (vanaf 2012)	2.100.000	120.000	18

Wel kan worden geconcludeerd dat de kosten over het algemeen hoog zijn, zeker wanneer toegerekend naar een individuele stem. Dat de kosten hoog zijn komt mede door de toerekening van kosten die inherent zijn aan de ontwikkeling en invoering van een nieuwe stemmethode. In veel landen is een separate projectorganisatie gedurende langere tijd belast met de voorbereiding en uitvoering van de verkiezing. Daarnaast zijn diverse kosten gemaakt voor de verwerving van een internetstem voorziening en is deze uitvoerig getest en onderzocht. Ook is er in de meeste landen vooraf uitvoerig onderzoek gedaan, alsmede (externe) evaluatie onderzoeken na afloop. Een deel van deze kosten zou in principe beschouwd mogen worden als eenmalige kosten, echter in veel landen is ook bij de tweede of derde internetstemming nog steeds een projectorganisatie actief en worden vervolgonderzoeken gehouden.
De variabele kosten zijn bij een internetstemming over het algemeen veel geringer dan de vaste kosten. Bij permanente invoering van internetstemmen en bij het gebruik voor grotere doelgroepen kunnen de kosten per stem aanzienlijk dalen. Of de kosten per stem in de praktijk ook daadwerkelijk dalen is echter niet met zekerheid te zeggen, dit is afhankelijk van de feitelijke invulling.

[10] Omgerekend van lokale valuta naar Euro tegen de huidige wisselkoers. Een conversie tegen de historische wisselkoers zou een meer correcte weergave geven in Euro's, echter deze historische wisselkoersen zijn niet voor elke valuta beschikbaar.

Aangezien internetstemmen steeds is ingezet als nieuw alternatief naast de bestaande stemmethoden, heeft dit in geen van de 11 landen geleid tot een verlaging van de totale uitgaven aan verkiezingen.

2.10 Stemdiensten in continue ontwikkeling

Opmerkelijk is dat in de landen waar meerdere internetverkiezingen zijn gehouden de internetstemdienst tussentijds geheel of gedeeltelijk verbouwd is. Zo zijn in Frankrijk drie compleet verschillende systemen gebruikt. In Noorwegen is men na het eerste experiment in 2011 compleet opnieuw begonnen voor de verkiezing van 2013. Ook in Zwitserland zijn de stemdiensten van Genève en Zürich al aan hun respectievelijke derde en tweede versie toe.

3 AUSTRALIË

3.1 Introductie

Sinds 2001 wordt er in diverse staten van Australië geëxperimenteerd met vormen van stemmen op afstand, waaronder stemmen via brief, fax, telefoon en vanuit kiosken. Deze experimenten waren steeds gericht op specifieke doelgroepen, zoals blinden en slechtzienden, militairen overzee en kiezers in het buitenland.
Op 26 maart 2011 vond de eerste echte toepassing van *internetstemmen* plaats bij de parlementsverkiezingen (de 'Legislative Assembly' en 'Legislative Council') van de staat New South Wales. Het systeem, 'iVote' genaamd, is specifiek beschikbaar gesteld voor de doelgroep van blinden en slechtzienden en kiezers die op meer dan 20 km afstand wonen van een stemlokaal. Naast internetstemmen biedt het systeem ook de mogelijkheid om stemmen per telefoon uit te brengen. Sinds de verkiezing van 2011 is internetstemmen ook toegepast bij meerdere tussentijdse verkiezingen[11] in de staat NSW, de meest recente op 19 oktober 2013. Er zijn geen andere staten in Australië waar internetstemmen wordt toegepast.

3.1.1 Staatsinrichting en bestuur

Australië is een constitutionele monarchie waar de machten op federaal niveau verdeeld zijn. De Britse koningin Elizabeth II is mede de koningin van Australië. Zij laat zich vertegenwoordigen door de gouverneur-generaal op federaal niveau. Op staatsniveau wordt zij vertegenwoordigd door gouverneurs. Volgens gemaakte afspraken behoren de gouverneurs actie te ondernemen op basis van advies uitgebracht door de ministers[12].

Het parlement van Australië wordt gekozen door het volk. Binnen het parlement bevinden zich twee Kamers, het Huis van Afgevaardigden en de Senaat. De ministers, welke uit de twee Kamers worden verkozen, hebben de uitvoerende macht in handen[13].

Het staatsbestuur van Australië bestaat verder uit drie verschillende niveaus. Allereerst heeft Australië een federaal bestuur. Daaronder bevinden zich de zes staten, welke verdeeld zijn over twee territoria. Ondanks dat de staten hun eigen bestuur hebben vormen zij wel één natie. Op het onderste niveau bevinden zich ongeveer 700 lokale overheidsinstanties.

Daarnaast is Australië, net zoals 52 andere onafhankelijke soevereine staten, lid van 'het Gemenebest van Naties', voorheen het Brits Gemenebest. De in totaal 53 staten zijn gezamenlijk

[11] Deze 'by-elections' worden gehouden indien een van de leden van het parlement terugtreed of overlijd. De tussentijdse verkiezing wordt gehouden in het kiesdistrict welke door het parlementslid werd vertegenwoordigd.

[12] http://en.wikipedia.org/wiki/Australia

[13] http://www.belgium.embassy.gov.au/bslsflemish/AusReg.html

vrijwillig een verbintenis aangegaan, waarvan de Britse koningin Elizabeth II het symbolische staatshoofd is[14].

3.1.2 Historie internetstemmen

Vanaf 2006 wordt er geëxperimenteerd met stemmen op afstand in Australië. Dit waren echter geen experimenten met internetstemmen, maar met stemmen via fax, telefoon of kiosken.
In 2007 is een experiment gehouden met een stemsysteem dat nog het meest lijkt op internetstemmen, al liep al het verkeer over het eigen defensienetwerk en niet over het publieke internet. Aan dit experiment deden in totaal 1.511 militairen mee.

De New South Wales (NSW) Electoral Commission (NSWEC) heeft op verzoek van de premier van NSW in 2010 een haalbaarheidsstudie[15] uitgevoerd naar de mogelijkheid van internetstemmen voor blinden en slechtzienden. Het primaire doel was het onderzoeken van een alternatief voor het ruim 60 pagina's tellende braille stembiljet voor blinde- en slechtziende kiezers bij de eerstvolgende verkiezingen in 2011. Op 23 juli 2010 werd het rapport van de haalbaarheidsstudie opgeleverd, waarin werd bepleit om internetstemmen ook toe te staan voor andere doelgroepen, zoals gehandicapten en kiezers in verafgelegen gebieden. Gelet op de zeer korte tijd tot aan de verkiezingen in 2011, begon de NSWEC alvast met de aanbesteding in de zomer van 2010, vooruitlopend op goedkeuring van het parlement. Op basis van het positieve haalbaarheidsonderzoek besloot het parlement daadwerkelijk tot invoering en stemde op 24 november 2010 in met de hiervoor benodigde aanpassingen van de kieswet. Op 7 december 2010 werd de wet geamendeerd om de doelgroep te verruimen met alle kiezers die niet in het stemlokaal kunnen stemmen op de dag van stemming.
De kiezers binnen de doelgroep konden hun stem uitbrengen in een periode van 12 dagen voorafgaand aan de dag van stemming (zondag 26 maart 2011).

3.1.3 Organisatie internetstemmen

De Australian Electoral Commission is de federale overheidsinstelling die de federale verkiezingen en referendums organiseert, uitvoert en daar ook toezicht over houdt. Zij legt verantwoording af aan de Joint Standing Committee on Electoral Matters van het Australische parlement. Verder heeft iedere afzonderlijke staat en territorium zijn eigen Electoral Commission die verantwoordelijk is voor de organisatie van de staats en lokale verkiezingen[16].
De NSWEC heeft het internetstemmen project zelf ter hand genomen. Gegeven de zeer korte tijdslijnen tot aan de verkiezing is hierbij intensieve ondersteuning verkregen van de leveranciers.

[14] http://nl.wikipedia.org/wiki/Gemenebest_van_Naties

[15] http://www.elections.nsw.gov.au/__data/assets/pdf_file/0006/84498/20100723_NSWEC_iVote_Feasibility_Report_.pdf

[16] http://en.wikipedia.org/wiki/Australian_Electoral_Commission

3.2 Kiesgerechtigdheid

In Australië zijn alle personen met de Australische nationaliteit vanaf 18 jaar kiesgerechtigd, met uitzondering van personen met een gevangenisstraf van 5 jaar of langer, of wanneer veroordeeld voor verraad[17]. Daarnaast zijn Britse burgers die voor 26 januari 1984 op de kiezerslijst stonden bevoegd om hun stem uit te brengen tijdens nationale- en staatsverkiezingen in Australië.

Kiezers zijn verplicht zich te laten registreren op de kiezerslijst van hun staat. Deze kiezerslijst wordt mede gebruikt door de AEC om de kiezerslijst voor heel Australië op te stellen. Kiezers kunnen verzoeken om op de kiezerslijst opgenomen te worden als 'general postal voter', zij krijgen dan automatisch een stembescheiden toegestuurd om per post te stemmen.

Kiezers zijn in Australië verplicht te stemmen, tenzij er een valide reden is opgegeven waarom niet gestemd kan worden[18].

Kiezers die naar het buitenland vertrekken voor een periode van minder dan 6 jaar kunnen zich bij de NSWEC en de AEC laten registreren als 'overseas elector'; zij ontvangen daarna stembescheiden om per post te stemmen.

3.3 Aantal kiesgerechtigden en opkomst

In totaal hebben er 4.635.810 kiezers hun stem uitgebracht in de staatsverkiezing van NSW op 26 maart 2011. Van dit aantal hadden zich vooraf 51.103 kiezers laten registreren om te stemmen via iVote. Uiteindelijk hebben 44.605 kiezers via internet hun stem uitgebracht.

In onderstaande tabel is het aantal internetstemmers per doelgroep aangegeven:

	Via Internet	Via Telefoon	Totaal
Blinden, slechtzienden	450	218	668
Gehandicapten	1.136	160	1.296
Kiezers woonachtig > 20 km van stemlokaal	1.542	101	1.643
Kiezers buiten NSW op de dag van stemming	41.477	1.780	43.257
Totaal	**44.605**	**2.259**	**46.864**

bron: NSW Electoral Commission

3.4 Andere beschikbare stemmethoden

Kiezers in New South Wales hebben diverse mogelijkheden om deel te nemen aan de verkiezingen:

- stemmen in een stemlokaal op de dag van stemming,
- stemmen op het gemeentehuis in een periode van enkele weken voorafgaand aan de dag van stemming (toegestaan onder bepaalde condities na indienen van een verzoekschrift)

[17] http://wiki.answers.com/Q/Who_is_eligible_to_vote_in_Australia?#slide3

[18] http://www.aec.gov.au/voting/

- stemmen per brief (toegestaan onder bepaalde condities na indienen van een verzoekschrift)
- stemmen in speciale aangewezen locaties zoals ziekenhuizen en verzorgingstehuizen

Stemmen via volmacht is niet toegestaan.

3.5 Internet stemsysteem

Het internetstemsysteem is ontwikkeld door de Amerikaanse firma Everyone Counts[19]. De intellectuele eigendomsrechten van het stemsysteem zijn in handen van de leverancier. Er zijn een aantal randsystemen, zoals het registratiesysteem en bijbehorende documentatie waar de NSWEC de eigendomsrechten van in handen heeft. De source code is niet openbaar gemaakt vanwege veiligheidsredenen en omdat kennis van het specifieke stemsysteem dus intellectueel eigendom is[20].

3.6 Procesbeschrijving[21]

3.6.1 Registratie van kiezers

Gebruik van het iVote systeem is voorbehouden aan kiezers die op de kiezerslijst staan én die zich vooraf laten registeren voor het gebruik van iVote. De registratie kan zowel online als telefonisch. Gedurende het aanmeldingsproces wordt de kiezer gevraagd een 6-cijferige pincode op te geven. Ter bevestiging van het registratieverzoek krijgt de kiezer een brief gestuurd naar het adres waarmee hij op de kiezerslijst staat.
De registratieperiode liep van 17 februari 2011 tot en met 23 maart 2011, 2 dagen voor de dag van stemming.

3.6.2 Stembescheiden

De kiezer ontvangt een 8-cijferig iVote nummer via de reguliere post en (op verzoek ook per SMS of email). Aan gehandicapten, blinden en slechtzienden wordt de iVote code via de telefoon doorgegeven. Aan kiezers die aangeven dat zij geen iVote nummer hebben gekregen wordt een nieuwe iVote code toegestuurd (en de oude ongeldig verklaard).

3.6.3 Stemming

Het uitbrengen van de stem verloopt in een aantal stappen.

1. De kiezer voert zijn 8-cijferig iVote nummer en zijn 7-cijferig zelfgekozen PIN in.

[19] http://www.everyonecounts.com

[20] http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf

[21] http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BN/2012-2013/EVoting#_Toc338074394

2. De kiezer geeft op het scherm zijn voorkeursvolgorde aan van de kandidaten door op één of meerdere kandidaten te dubbelklikken (in de volgorde van zijn voorkeur). Hij stelt zo zijn stembiljet samen.
3. Voordat de stem definitief wordt uitgebracht krijgt de kiezer nogmaals zijn ingevoerde kandidaten te zien.
4. De kiezer krijgt een ontvangstbewijs op het scherm.

Kiezers kunnen één keer hun stem uitbrengen.

Een demonstratieversie van het stemsysteem is beschikbaar op de website https://by-practise.ivote.nsw.gov.au/app/2/2

3.6.4 Verificatie door kiezer

Met het ontvangstbewijs kan de kiezer na de telling controleren of zijn stem is ontvangen. Deze controle verloopt als volgt: de kiezer voert zijn iVote nummer in op de website van de stemdienst (of door te bellen naar een interactive voice response systeem). Vervolgens wordt een ontvangstbewijs getoond / voorgelezen, welke overeen moet komen met het eerder ontvangen bewijs.

3.6.5 Rol overige instanties en evaluatie

De uitvoering van de verkiezing was in handen van de NSWEC en de leverancier. Geen andere organisaties waren betrokken bij de uitvoering.

In de aangepaste kieswetgeving zijn bepalingen opgenomen om het internetstemsysteem te laten auditen. PricewaterhouseCoopers (PwC) heeft zowel voor als na de verkiezing een audit uitgevoerd op het gebruikte stemsysteem iVote. De firma Birlasoft heeft beveiligingstesten uitgevoerd. Daarnaast heeft The Allen Consulting Group een evaluatie gedaan van de ondersteunende technologie van het stemsysteem. De rapporten kunnen via de volgende link gevonden worden: http://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports.

De PWC audit na afloop van de verkiezing richtte zich op de volgende onderwerpen:

- De accuraatheid en compleetheid van de (online) uitgebrachte stemmen
- De veiligheid van het stemsysteem, onderverdeeld in:
    - iVote penetratie test (web en IVR).
    - iVote source code review.
    - Cryptografie audit.
    - iVote infrastructuur van het beveiligingsontwerp, inclusief processen, mensen en technologie.

De volgende incidenten zijn gerapporteerd:

- Kiezers hadden een 7-cijferig íVote nummer ontvangen in plaats van een 8-cijferig nummer. 182 kiezers hebben gestemd met dit 7-cijferige nummer. Zij waren gevraagd om met een nieuwe pincode nogmaals hun stem uit te brengen.
- 842 kiezers ontvingen een herinnering om een stem uit te brengen terwijl zij al hun stem hadden uitgebracht. Deze kiezers hebben vervolgens een bericht ontvangen dat hun stem wel was meegeteld.
- De 'inter-site link' tussen de afzonderlijke datacenters werd verbroken (met een duur van 12 uur).
- Het stemsysteem heeft in totaal 8 minuten niet gewerkt. Dit had geen gevolgen voor de uitgebrachte stemmen.
- Het systeem accepteerde 43 stembiljetten met de letter 'N' in plaats van een numerieke code. Ieder stembiljet is apart in behandeling genomen.

Het evaluatierapport van the Allen Consulting Group (2011) concludeerde dat het systeem aan de verwachtingen voldeed en dat de beoogde doelen behaald waren; "Due to the pioneering nature of the iVote system, an assessment of the system's effectiveness in meeting its aims is essential. This study has shown that the iVote system has been effective at meeting these aims. iVote was effective in facilitating a secret and independently verifiable vote for voters who are blind or vision impaired. iVote was also identified by users as making voting easier and more convenient. Additionally, it has been successfully demonstrated to work and be appropriate in a real election environment."

Ook the Allen Consulting Group heeft aanbevelingen gedaan, gebaseerd op meningen van kiezers, om het stemmen via internet in de toekomst efficiënter en effectiever te laten verlopen, namelijk;

- De meest voorkomende suggestie van de ondervraagde kiezers was dat het systeem onder een breder publiek uitgezet diende te worden.
- Velen gaven aan dat deze nieuwe manier van stemmen te weinig gepromoot was. Voor eventueel toekomstig gebruik diende hier meer aandacht aan besteed te worden.
- Wanneer NSW van plan was om iVote in de toekomst vaker in te zetten, werd aanbevolen zich te verdiepen in eventuele kosten synergiën (denk aan het inkopen van hardware welke hergebruikt kan worden door andere gemeenten).
- Door het publiekelijk beschikbaar maken van computers zou bij toekomstige verkiezingen het gebruik van deze nieuwe technologie vergroot kunnen worden.
- De website van iVote was voor een groep kiezers te ingewikkeld in het gebruik.
- Er werd aanbevolen om het registratieproces te vergemakkelijken.
- Er was behoefte aan duidelijkere instructies voor iVote (handleidingen, enz.).
- Kleine technische foutjes dienden opgelost te worden (6% heeft last gehad van deze technische foutjes).
- Traditionele post werd niet als een prettig communicatiemiddel ervaren door de kiezers[22].

[22] http://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports

3.6.6 Beveiligingsmaatregelen

De NSW Electoral Commission (NSWEC) had voorafgaand aan de selectie van de leverancier een aantal veiligheidseisen opgesteld waaraan het systeem zou moeten voldoen:

- Het systeem heeft een 'highly tampered-evident' ontwerp. Hiermee wordt bedoeld dat het snel duidelijk moet zijn wanneer een persoon ongeautoriseerd toegang probeert te krijgen of heeft gekregen tot het systeem.
- In geval dat de kiezer thuis online stemt dient direct de veiligheid van het gebruikte apparaat automatisch gemeten of beoordeeld te worden.
- Er zijn meerdere opslaglocaties in het ontwerp ingebouwd (back-up) en verder heeft het systeem geen gedeelde infrastructuur.
- Het systeem maakt gebruik van moderne beveiligingstechnieken om op die manier zeker te stellen dat het systeem betrouwbaar en accuraat opereert en daarnaast is een 'security-in-depth design' een pre.

3.6.7 Eigendomsrechten

De eigendomsrechten van het onlinestemsysteem zijn in handen van de leverancier, Everyone Counts. Een aantal randsystemen zoals het registratiesysteem en bijbehorende documentatie zijn in handen van NSWEC[23].

3.6.8 Kosten

NSWEC heeft ongeveer 3,5 mln. $ AUD uitgegeven voor het iVote project bij de 2011 verkiezing, omgerekend tegen de toenmalige wisselkoers is dat € 2,7 mln. Per uitgebrachte stem waren de kosten 74 $ AUD.

Zie voor een gedetailleerde specificatie van de kosten tabel 6.1 uit het evaluatierapport[24]. In dit rapport is ook een vergelijking gemaakt met de kosten van de bestaande methoden van stemmen, eerdere experimenten en stemmen met braille stembiljetten.

[23] http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf

[24] http://www.elections.nsw.gov.au/__data/assets/pdf_file/0004/93766/July_2011_Final_ACG_iVote_Report_ELE01-C_Final.pdf

4 CANADA

4.1 Introductie

Al sinds het begin van de jaren '90 is Canada de mogelijkheden van internetstemmen aan het verkennen. De verkenningen hebben geleid tot een rapport "*Technology and the Voting Process*" [25] waarin positief wordt geconcludeerd over de toekomst van internetstemmen. Volgens het rapport is Canada één van de meest technologisch gevorderde landen ter wereld en kent het land één van de meest efficiënte en gerespecteerde kiessystemen ter wereld.
Sinds het verschijnen van die studie is er op federaal niveau weinig voortgang geweest op het gebied van internetstemmen. Wel zijn er op lokaal niveau experimenten gehouden in meerdere gemeenten.

4.1.1 Staatsinrichting en bestuur

Canada is een federatie en is onderverdeeld in 10 provincies (*provinces*) en 3 territoria (*territories*) met als staatsvorm een parlementaire democratie. Canada is een constitutionele monarchie binnen het Gemenebest en omvat een Kroon, een Senaat en een Lagerhuis. Het Britse staatshoofd wordt vertegenwoordigd door een benoemde Gouverneur-Generaal, die wordt bijgestaan door een kabinet, de 'privy council'.

De grootste politieke partij levert de premier en de ministers, die uit de leden van het Federale Parlement worden gekozen. De Senaat kent een regionale verdeling en de 105 leden worden door de premier benoemd. Het Lagerhuis kent eveneens een regionale indeling. De 301 leden worden voor vijf jaar middels algemeen kiesrecht gekozen. Vanaf 18 jaar is er actief kiesrecht.

[25] http://www.elections.ca/content.aspx?section=res&dir=rec/tech/tec&document=index&lang=e

Elke provincie heeft een eigen constitutie, een luitenant-gouverneur, die wordt voorgedragen door de Gouverneur-Generaal en één wetgevende kamer. De territoria worden door een regeringsambtenaar (*commissioner*) bestuurd en heeft één wetgevende kamer, de 'Territorial Council'.[26] Iedere provincie heeft de vrijheid om een eigen wijze van stemmen hanteren.

4.1.2 Historie internetstemmen

De eerste ervaring in Canada met internetstemmen was in de provincie Ontario in 2003. Twaalf gemeenten maakten toen gebruik van internetstemmen bij de gemeenteraadsverkiezing. Vanaf 2003 is dit aantal gegroeid naar meer dan 60 gemeenten in 2012, in met name Ontario en Nova Scotia. Tegelijkertijd zijn meerdere gemeenten bezig om de mogelijkheden verder te verkennen[27] .

Naast Ontario en Nova Scotia zijn ook een aantal andere provincies stappen aan het zetten om de mogelijkheden van internetstemmen te verkennen. Zo heeft de provincie British Colombia een onderzoek laten uitvoeren door Elections BC (onafhankelijk orgaan belast met verkiezingen). Dit onderzoek is te vinden op http://www.elections.bc.ca/docs/Internet-Voting-Discussion-Paper.pdf

Internetstemmen is nog niet toegepast bij federale verkiezingen.

In deze inventarisatie worden twee gemeenten specifiek toegelicht in Canada waar internetstemmen is doorgevoerd: Markham (Ontario) (2003, 2006, 2010) en Halifax (Nova Scotia) (2008). Markham was de eerste gemeente die experimenteerde met internetstemmen. In Halifax werd naast stemmen via internet ook de mogelijkheid geboden om te stemmen via telefoon.

4.2 Kiesgerechtigdheid

Om te mogen stemmen (federale verkiezingen) moet je:

- Canadees burger zijn;
- minimaal 18 jaar zijn op de verkiezingsdag;
- geregistreerd staan in het Nationaal Register als kiezer.[28]

Canadese burgers, wonend buiten Canada hebben recht om te stemmen, indien zij:

- ooit in Canada hebben gewoond;
- van plan zijn terug te gaan naar Canada;
- minder dan vijf jaar achter elkaar woonachtig zijn buiten Canada (tenzij werkzaam voor federaal of provinciaal orgaan, werkzaam voor internationale organisaties of werkzaam zijn voor de Canadese krijgsmacht).[29]

---

[26] http://www.landenweb.net

[27] Zie http://civix.ca/blog/category/online-voting/ en "THE EXPERIENCES OF CANADIAN MUNICIPALITIES WITH INTERNET VOTING", N. Goodman Carleton University dec 2010, voor een overzicht van de status en aantallen kiezers per gemeente.

[28] http://www.elections.ca

4.3 Aantal kiesgerechtigden en opkomst

Halifax (2008)

Totaal aantal kiesgerechtigden: ca. 280.000
Opkomst: ca. 101.000 (36%)
Van afstand: 28.709 (37%)
87.8% via internet
12.2% via telefoon[30]

Markham (2003, 2006, 2010)

De totale opkomst steeg 300% in 2003 en nog eens een extra 48% in 2006.[31]

Totaal aantal kiesgerechtigden: ca. 66.000

Online geregistreerd:	Online gestemd:
2003: 11.708 (7.5% van kiesgerechtigden)	7.210 (61.6% van geregistreerde kiezers)
2006: 16.251 (9.7% van kiesgerechtigden)	10.639 (65% van geregistreerde kiezers)
2010: 17.231 (9.3% van kiesgerechtigden)	10.597 (61.5% van geregistreerde kiezers) [32] [33]

4.4 Andere beschikbare stemmethoden

De beschikbare stemmethoden verschilt per gemeente. Veel voorkomend zijn stemmen via stembureau, post en telefoon.

4.5 Internet stemsysteem

Halifax

Bij de verkiezingen in Halifax is gebruik gemaakt van het systeem Intelivote. ISI Intelivote Systems, Inc. is gevestigd in Canada (Nova Scotia) en heeft eerder voor andere Canadese en Engelse gemeenten de verkiezingen verzorgd.

Markham

Bij de verkiezingen in Markham is in 2003 en 2006 gebruikt gemaakt van een systeem geleverd door een Amerikaans bedrijf, Election Systems and Software. In 2010 is gebruik gemaakt van het systeem Intelivote.

---

[29] http://www.elections.ca/content.aspx?section=vot&dir=reg/etr&document=index&lang=e

[30] HRM's Experience with Electronic Voting, Carleton University, januari 2010

[31] Goodman, Internet Voting in Canadian Municipalities: What Can We Learn?, 2010, (http://www.cpsa-acsp.ca/papers-2010/Goodman.pdf)

[32] Markham's Online Voting Experience, 2010 Workshop on Internet Voting

[33] Markham Votes 2014 -Internet Voting Program, Presentatie Special General Committee Meeting , november 2012

4.6 Procesbeschrijving

4.6.1 Registratie van kiezers

Halifax

Het was niet nodig om je als kiezer vooraf te registreren wanneer de kiezer zijn stem via internet wilde uitbrengen. De kiezers kregen de optie om met een toegestuurde pincode te stemmen, nadat zij eerst een captcha hadden uitgevoerd en ook de geboortedatum hadden ingevuld.[34]

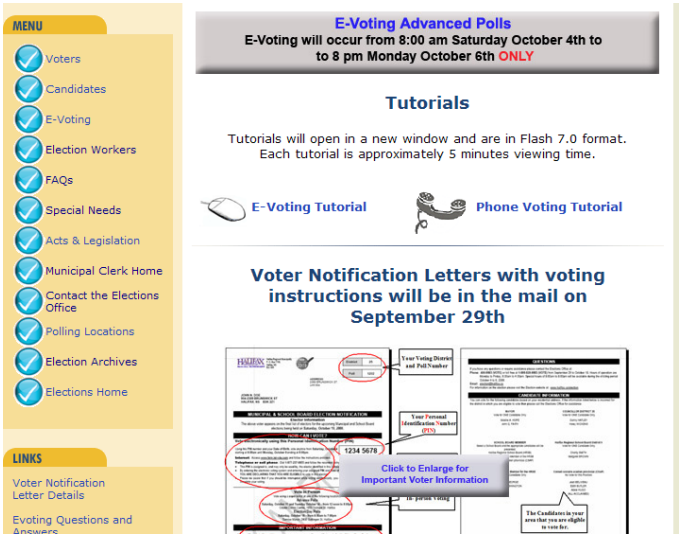
Markham

Het was een verplichting om je vooraf te registreren wanneer de kiezer via internet zijn stem wilde uitbrengen. Om dit mogelijk te maken ontving iedere kiezer een registratie pakket. Tijdens de registratie moest de kiezer een 'beveiligingsvraag' kiezen, welke terug kwam tijdens de daadwerkelijke stemming (denk aan: wat is de naam van je eerste huisdier?). Wanneer men geregistreerd was betekende dat automatisch dat de kiezer van een lijst werd verwijderd waardoor fysiek stemmen in een stembureau niet meer mogelijk was. De geregistreerde kiezers kregen vervolgens via de post een pincode toegestuurd, welke dus in combinatie met het beantwoorden van de unieke beveiligingsvraag als authenticatiemiddel is gebruikt.

4.6.2 Stembescheiden

Halifax

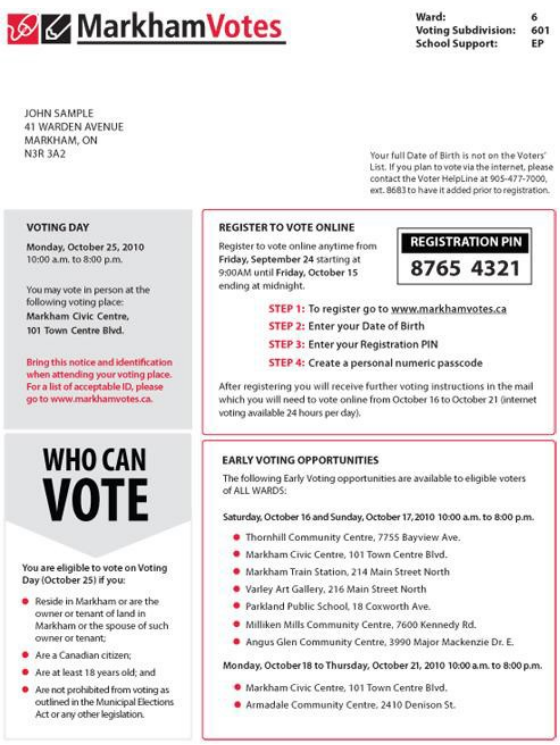
De kiezer ontving allereerst een brief met daarin zijn/haar 'e-voting ID', een 8-cijferig nummer en bijbehorende instructies. In de brief stond eveneens de URL via welke gestemd kon worden.



[34] A Comparative Assessment of Electronic Voting, Canada-Europe Transatlantic Dialogue, februari 2010

Markham

Alle in aanmerking komende kiezers ontvingen een kiezer informatiepakket. Dit pakket bevatte de registratie pincode en het website-adres voor het stemsysteem.



MarkhamVotes

Ward: 6
Voting Subdivision: 601
School Support: EP

JOHN SAMPLE
41 WARDEN AVENUE
MARKHAM, ON
N3R 3A2

Your full Date of Birth is not on the Voters' List. If you plan to vote via the internet, please contact the Voter HelpLine at 905-477-7000, ext. 8683 to have it added prior to registration.

VOTING DAY

Monday, October 25, 2010
10:00 a.m. to 8:00 p.m.

You may vote in person at the following voting place:
Markham Civic Centre,
101 Town Centre Blvd.

Bring this notice and identification when attending your voting place. For a list of acceptable ID, please go to www.markhamvotes.ca.

REGISTER TO VOTE ONLINE

Register to vote online anytime from Friday, September 24 starting at 9:00AM until Friday, October 15 ending at midnight.

REGISTRATION PIN
8765 4321

STEP 1: To register go to www.markhamvotes.ca
STEP 2: Enter your Date of Birth
STEP 3: Enter your Registration PIN
STEP 4: Create a personal numeric passcode

After registering you will receive further voting instructions in the mail which you will need to vote online from October 16 to October 21 (internet voting available 24 hours per day).

WHO CAN VOTE

You are eligible to vote on Voting Day (October 25) if you:

- Reside in Markham or are the owner or tenant of land in Markham or the spouse of such owner or tenant;
- Are a Canadian citizen;
- Are at least 18 years old; and
- Are not prohibited from voting as outlined in the Municipal Elections Act or any other legislation.

EARLY VOTING OPPORTUNITIES

The following Early Voting opportunities are available to eligible voters of ALL WARDS:

Saturday, October 16 and Sunday, October 17, 2010 10:00 a.m. to 8:00 p.m.

- Thornhill Community Centre, 7755 Bayview Ave.
- Markham Civic Centre, 101 Town Centre Blvd.
- Markham Train Station, 214 Main Street North
- Varley Art Gallery, 216 Main Street North
- Parkland Public School, 18 Coxworth Ave.
- Milliken Mills Community Centre, 7600 Kennedy Rd.
- Angus Glen Community Centre, 3990 Major Mackenzie Dr. E.

Monday, October 18 to Thursday, October 21, 2010 10:00 a.m. to 8:00 p.m.

- Markham Civic Centre, 101 Town Centre Blvd.
- Armadale Community Centre, 2410 Denison St.

4.6.3 Stemming

Halifax

Om een stem uit te brengen diende de kiezer:

1) Online registeren ('e-voting' ID, 8-cijferig PIN en geboortedatum invoeren);
2) Stem uitbrengen in het digitale stembiljet. [35]

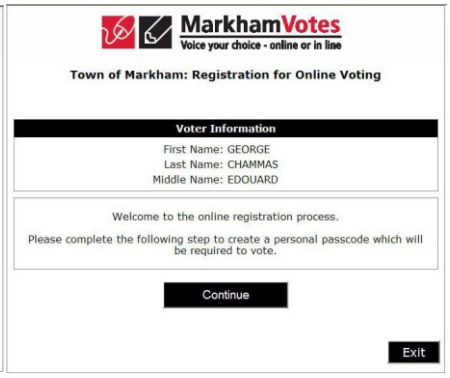
Markham

Om een stem uit te brengen diende de kiezer:

1) Online te registeren (persoonlijke toegangscode aanmaken);
2) Ontvangen van een toegangscode om te stemmen;
3) Naar de juiste URL gaan;
4) Een "stem" knop aanklikken;
5) Akkoord gaan met een verklaring;
6) Een CAPTCHA uitvoeren (een invoer om computers en mensen uit elkaar te houden);
7) De persoonlijke toegangscode invoeren;
8) De toegangscode om te stemmen invoeren;
9) Keuze aangeven in het online stembiljet;

[35] A Comparative Assessment of Electronic Voting, Canada-Europe Transatlantic Dialogue, februari 2010

10) De "Stem nu" knop aanklikken.[36]



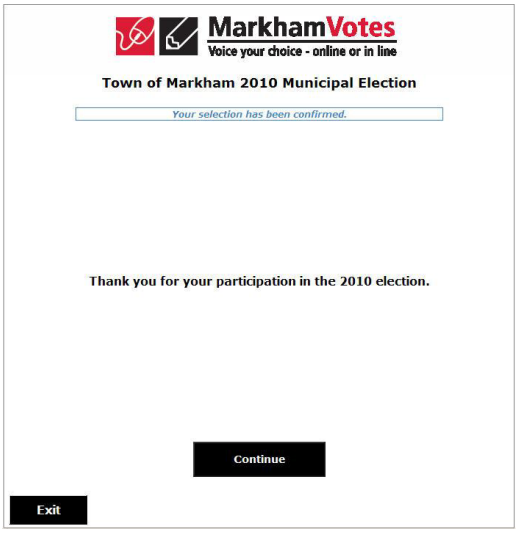
4.6.4 Verificatie door kiezer

Halifax

Na het uitbrengen van de stem krijgt de kiezer op zijn scherm een code te zien waarmee later opgezocht kan worden of de stem meegenomen is in de telling.

Markham

Geen verificatie.



4.6.5 Rol overige instanties

De opdrachtgever waren de gemeenten zelf, Halifax en Markham. De systemen zijn respectievelijk ontwikkeld of geleverd door Election Systems and Software en ISI Intelivote Systems, Inc.

[36] Office of the Returning Officer, Town of Markham, Internet Voting Procedures (Markham, ON: July 22, 2010), page 7.

4.6.6 Beveiligingsmaatregelen

Halifax

Halifax schatte in dat stemmen via post het meest risicovol is. Om de noodzaak van registratie van kiezers voor internet / telefoon stemmen weg te nemen, en daarmee het risico van uit de post gestolen registratiekaarten weg te nemen, gebruikte Halifax een pincode en geboortedatum voor de online authenticatie. Daarnaast scherpte Halifax de wetgeving aan om verkiezingsfraude strenger te sanctioneren in verband met internetstemmen.[37]

Markham

In een 'Request for Proposal' van Markham voor een internetstemsysteem voor 2010 zijn enkele eisen aangegeven die de veiligheid van het systeem betreffen. Een aantal opvallende eisen zijn:

- Het systeem hanteert minimaal een twee-stappen proces, om te registeren en om te stemmen.
- Het systeem biedt de mogelijkheid voor het zetten van een digitale handtekening.
- De online interface van het systeem moet via een webbrowser lopen in standaard HTML en JavaScript. Aanvullende installaties of plug-ins zijn niet acceptabel.

In een studie van de stad Markham uit 2010 zijn aanbevelingen gedaan betreffende de veiligheid en controleerbaarheid. Deze aanbevelingen waren onder andere:

- De leverancier moet beschikken over de laatste technieken om internetaanvallen te voorkomen.
- Het moet duidelijk worden gemaakt dat fraude strafbaar is volgens de wet.
- De gemeente moet real-time afwijkende stempatronen of aanroepen van de servers via bijvoorbeeld niet lokale adressen kunnen identificeren en analyseren.
- Er moeten procedures komen om een audit trail te kunnen tonen van de internetstemmen[38].

4.6.7 Eigendom

Halifax

Geen informatie gevonden over het eigendom van het systeem.

Markham

Het stemsysteem is eigendom van ISI Intelivote Systems, Inc.[39]

---

[37] A Survey of Internet Voting, U.S. Election Assistance Commission, september 2011

[38] A Study of Internet Voting Security Risks and Accessibility Opportunities for the Town of Markham, Town of Markham, 2010
http://www.markham.ca/markham/ccbs/indexfile/Agendas/2010/General/gc100503/Approval%20of%20Alternative%20Voting%20Methods%20-%202010%20Municipal%20Election.htm

[39] International Experience with E-voting, Norwegian E-vote Project, juni 2012

4.6.8 Kosten

Halifax

Halifax had een budget van 1,3 miljoen dollar voor de verkiezing in 2008. Hiervan is 487.151 dollar betaald aan de internet provider voor het elektronisch stemmen.[40]

Markham

Markham heeft aan de leverancier (ES&S) 25.000 dollar betaald in 2003 en 52.000 dollar in 2006 voor de ontwikkeling en de bouw van de website.[41]

In 2010 waren de kosten per kiezer 0.81 dollar voor internetstemmen en 5.63 dollar voor fysiek stemmen.[42]

[40] Goodman, Internet Voting in Canadian Municipalities: What Can We Learn?, 2010, (http://www.cpsa-acsp.ca/papers-2010/Goodman.pdf)

[41] Internet Voting: The Canadian Municipal Experience (http://www.revparl.ca/english/issue.asp?param=199&art=1393)

[42] Markham Votes 2014 -Internet Voting Program, Presentatie Special General Committee Meeting

, november 2012

5 ESTLAND

5.1 Introductie

Estland is het eerste land dat internetstemmen heeft toegestaan voor alle kiesgerechtigde inwoners van het land, tijdens de parlementsverkiezingen in 2007. In 2005, 2009 en 2013 is internetstemmen ingezet bij lokale verkiezingen, in 2007 en 2011 tijdens parlementaire verkiezingen en in 2009 bij de verkiezing van het Europese Parlement.

5.1.1 Staatsinrichting en bestuur

50 jaar lang is Estland onderdeel geweest van de Sovjet-Unie. Destijds was er al wel een Estse regering aanwezig, alleen voerde zij het beleid uit zoals bepaald door de Sovjet-Unie. In 1991 verkreeg Estland weer zijn onafhankelijkheid, sindsdien is de regering van Estland op de volgende manier vormgegeven: een president welke is gekozen door het parlement, een staatshoofd en een wetgevende kamer, de Riigikogu genoemd. De minister-president en zijn ministers hebben de uitvoerende macht in handen, wie door het staatshoofd benoemd worden. Het parlement bestaat uit 101 leden welke om de 4 jaar opnieuw gekozen worden. Daarnaast is Estland verdeeld in 15 verschillende regio's (Maakond) en zes stadsdistricten; Tallinn, Tartu, Narva, Kohtla-Jäve, Pärnu en Sillamaë[43].

5.1.2 Historie internetstemmen

De eerst zittende regering na het verkrijgen van de onafhankelijkheid in 1991 ontwikkelde al snel een strategie voor een elektronische overheid, waarin het gebruik van nieuwe technologieën en ICT een grote rol speel speelde. Zo heeft de Estse overheid in 2002 een e-ID stelsel geïntroduceerd, voor elektronische authenticatie van personen. De elektronische identiteitskaart is fysiek gecombineerd op de nationale identiteitskaart. In 2011 waren meer dan een miljoen Esten in het bezit van een e-ID kaart. Het bezit van de e-ID is niet verplicht, maar wel vereist om gebruik te kunnen maken van de (vele) online overheidsdiensten op het terrein van belastingen, gezondheidszorg, politie en scholen.

In 2001 kondigde het ministerie van justitie voor het eerst haar intentie aan om internetstemmen te gaan verkennen. Allereerst zijn een tweetal technische analyses uitgevoerd vanuit de wetenschappelijke wereld. Uit de eerste analyse bleek dat het onrealistisch was om internetstemmen op korte termijn op landelijk niveau in te voeren door het gebrek aan een geschikte technologie. Het rapport gaf aan dat er eerst een onderzoeksprogramma naar internetstemmen benodigd was voor een eventuele implementatie van internetstemmen. Wel achtte beide ministeries het onvermijdelijk dat internetstemmen in de toekomst ingevoerd zou gaan worden.
In 2002 werd de “Riigikogu election act” aangenomen welke het stemmen via internet met de e-ID wettelijk mogelijk maakte, maar niet voor 2005. In 2003 startte de Vabariigi Valimiskomisjon

[43] http://www.landenweb.net/estland/samenleving/

("National Electoral Committee") een projectgroep, welke in 2004 een 'general concept' document opleverde. Dit concept werd de basis voor een aanbesteding, die gewonnen werd door de firma Cybernetica AS.

In januari 2005 is gestart met een experiment in de hoofdstad Talinn. Op 16 oktober 2005 vonden de eerste echte (lokale) verkiezingen plaats waarbij het internetstemsysteem is gebruikt.

Nadien zijn er meerdere verkiezingen gehouden waarbij het internetstemsysteem is ingezet:

- Parlementsverkiezingen 4 maart 2007
- Europese parlementsverkiezingen 7 juni 2009
- Lokale verkiezingen 18 oktober 2009
- Parlementsverkiezingen 6 maart 2011
- Lokale verkiezingen 20 oktober 2013

5.1.3 Organisatie internetstemmen

In Estland heeft Estonian National Electoral Committee (ENEC) de verantwoordelijkheid voor de organisatie en uitvoering van de verkiezingen[44]. De ENEC is een bij wet ingestelde organisatie die onafhankelijk is van de regering.

Sinds 2012 is als onderdeel van de NEC een aparte organisatie opgericht specifiek voor internetstemmen, de Electronic Voting Committee. De EVC is verantwoordelijk voor de uitvoering van de internetverkiezingen, terwijl de ENEC een toezichthoudende rol toebedeeld heeft gekregen[45].

Andere betrokken partijen zijn het ministerie van Binnenlandse Zaken (levert de kiezerslijst aan en verzorgt de uitgifte van de e-ID kaarten), het Estonian Informatics Centre (onderdeel van het ministerie van Datacommunicatie en is verantwoordelijk voor de fysieke hosting van de servers, de internetverbindingen en de operationele informatie beveiliging tegen cyberaanvallen), de leverancier en een onafhankelijke auditor (KPMG Baltics SA).

5.2 Kiesgerechtigdheid

Personen met de Estse nationaliteit mogen vanaf 18 jaar hun stem uitbrengen tijdens gemeenteraadsverkiezingen, het nationale parlement, referenda en Europese verkiezingen. Voor gemeenteraadsverkiezingen zijn alle inwoners ongeacht nationaliteit kiesgerechtigd.

Gevangenen die daadwerkelijk veroordeelt zijn voor een overtreding mogen niet hun stem uitbrengen. Ook kan het gerechtshof de bevoegdheid om te stemmen afnemen. In de verkiezing van 2011 werden 1.989 personen van de kiezerslijst afgehaald doordat hun bevoegdheid om te

[44] http://www.epicos.com/EPCompanyProfileWeb/GeneralInformation.aspx?id=29977

[45] http://vvk.ee/voting-methods-in-estonia/engindex/

stemmen was ontnomen en 1.416 veroordeelde gevangenen werden van de kiezerslijst afgehaald[46].

5.3 Aantal kiesgerechtigden en opkomst

In onderstaande tabel[47] is het aantal geldige getelde internetstemmen weergegeven per verkiezing. Het betreft hier het aantal getelde stemmen, de via internet uitgebrachte stemmen die later geannuleerd zijn (doordat alsnog een stem in een stemlokaal is uitgebracht) zijn van het aantal uitgebrachte stemmen reeds afgetrokken.

Verkiezing	Aantal kiesgerechtigden	Stemmen via internet	Stemmen via internet (in %)
2005 – Lokaal	1.059.292	9.287	1,9%
2007 – Parlement	897.243	30.243	5,5%
2009 - Europees parlement	909.628	58.614	14,7%
2009 - Lokaal	1.094.317	104.313	15,8%
2011 – Parlement	913.346	140.764	24,3%
2013 - Lokaal	1.086.935	133.662	21,2%

Zie de website van het internet stembureau https://www.valimised.ee/eng/ voor meer statistieken.

5.4 Andere beschikbare stemmethoden

Estland kent een grote verscheidenheid aan andere stemmethoden. Naast het stemmen in het stemlokaal op de dag van de verkiezing is het kiezers ook toegestaan om gedurende een aantal dagen in de 10 dagen voorafgaand aan de stemming te stemmen. Kiezers kunnen hun stem uitbrengen in een stemlokaal in de eigen gemeente, maar ook in andere gemeenten in het land. Thuisstemmen is voorbehouden aan kiezers die niet in staat zijn om naar het stemlokaal te komen of om anderszins te stemmen. Op de dag van stemming komen twee stembureauleden naar het huisadres van de kiezer om zodoende te kunnen stemmen.

Kiezers in het buitenland kunnen tussen de 15e en de 10e dag voor de dag van stemming hun stem uitbrengen op de locatie van de diplomatieke posten in het buitenland. Daarnaast kan gestemd worden per reguliere post en via internet. Zeevarende kiezers kunnen hun stem uitbrengen op het schip zelf. Stemmen per post vergt een voorafgaande registratie en wordt weinig gebruikt.

Kiezers in Estland	Kiezers buiten Estland
• In stemlokaal in eigen gemeente op dag van stemming	• Per post • Op diplomatieke posten

[46] http://www.osce.org/odihr/77557

[47] Zie de website van de NEC voor meer statistieken http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics

• Advance voting: in stemlokaal in eigen gemeente op de 6e t/m 3e dag voor de van stemming of in stemlokaal buiten de eigen gemeente op de 10e t/m 7e dag voor de dag van stemming • Thuis • Internet op de 10e t/m 4e dag voor de dag van stemming	• Op schepen • Via internet op de 10e t/m 4e dag voor de dag van stemming

5.5 Internetstemsysteem

Het internetstemsysteem is ontworpen naar dezelfde principes en opzet van briefstemmen, mede opdat internetstemmen zo vertrouwd mogelijk zou zijn voor de kiezers. Ook het dubbele envelop principe van briefstemmen is meegenomen in het ontwerp, door de stem te versleutelen en daarna te voorzien van een elektronische handtekening.

Eén van de eigenschappen van het internetstemsysteem uit Estland is dat een kiezer meerdere keren zijn stem mag uitbrengen. In dat geval wordt steeds de laatst uitgebrachte stem geteld. De kiezer kan zijn elektronische stem(men) wijzigen of annuleren door *tijdens* de advance voting periode een stem uit te brengen in een stemlokaal. Op de dag van stemming zelf is annuleren of wijzigen van de stem niet meer mogelijk.
Het NEC stuurt aan het einde van de internetstemperiode de kiezerslijst met alle internetstemmers naar de stembureaus. De stembureaus geven op deze lijst aan welke kiezers alsnog in een stembureau hun stem hebben uitgebracht en retourneren dit aan de NEC, welke zo kan bepalen welke internetstemmen geannuleerd dienen te worden. In de afgelopen verkiezingen maakt ongeveer 0,1% van de internetstemmers gebruik van de mogelijkheid om alsnog in een stembureau te stemmen, zie ook de tabel hieronder.

Verkiezing	Aantal meervoudige stemmen	In %	Aantal geannuleerde stemmen	In %
2005 – Lokaal	364	3,91%	30	0,32%
2007 – Parlement	789	2,61%	32	0,11%
2009 – EP	910	1,55%	55	0,09%
2009 - Lokaal	2373	2,27%	100	0,10%
2011 – Parlement	4384	3,11%	82	0,06%
2013 - Lokaal	3045	2,28%	146	0,11%

Tabel 1 Aantal meervoudige en geannuleerde internetstemmen. % is ten opzichte van aantal uitgebrachte stemmen

Door de jaren heen zijn diverse veranderingen doorgevoerd in het systeem. Aan de serverzijde waren de meeste aanpassingen gericht op technische verbeteringen in de architectuur van de

software, het elimineren van mogelijke menselijke fouten en het inrichten van een aparte server voor logbestanden. De client die de kiezer gebruikt is volledig herschreven en is nu een separaat programma dat gedownload moet worden van de NEC website, voorheen draaide het programma in de browser van de gebruiker. Daarnaast is het sinds 2011 mogelijk voor kiezers om mobile-ID te gebruiken voor de authenticatie en het zetten van de digitale handtekening. Zie ook paragraaf 5.6.2.
De broncode van de servers van het internetstemsysteem is in 2013 gepubliceerd[48], de broncode van de client applicatie is niet vrijgegeven.

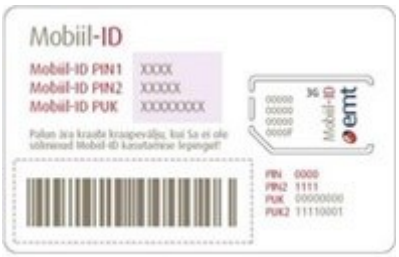
5.6 Procesbeschrijving[49]

5.6.1 Registratie van kiezers

De kiezer hoeft zich vooraf niet te registreren om via internet te kunnen stemmen. De kiesgerechtigdheid wordt afgeleid van de bevolkingsadministratie.

5.6.2 Stemming

Voor de authenticatie van de kiezer wordt het in Estland wijdverspreide stelsel van elektronische identiteiten gebruikt. Elke inwoner van Estland ouder dan 15 jaar kan een e-ID kaart aanvragen. Bij de e-ID kaart worden ook een tweetal persoonlijke codes verstrekt, alsmede een digitaal certificaat (opgeslagen op de chip van de e-ID). Om de e-ID kaart te kunnen gebruiken is een smartcard reader nodig.



Sinds 2007 kent Estland ook een mobiele versie van de e-ID kaart, mobile-ID genaamd. Hierbij wordt een speciale SIM kaart gebruikt die verkregen kan worden bij de mobiele operators. Het grote voordeel van mobile-ID is dat geen smartcard reader noodzakelijk is om een digitale handtekening te kunnen zetten. Mobile-ID kon vanaf de parlementsverkiezingen van 2011 gebruikt worden voor internetstemmen.

De procesgang voor de kiezer (verkorte weergave):

1. Om te stemmen logt de kiezer in bij de website van de stemdienst https://www.valimised.ee. De kiezer download vervolgens een I-voting applicatie en installeert deze op zijn computer. De applicatie is verkrijgbaar in versies voor Windows, OS-X en Linux operating systemen.

[48] Zie https://github.com/vvk-ehk/evalimine

[49] http://vvk.ee/voting-methods-in-estonia/engindex/#verification

2. De kiezer logt in met zijn e-ID of mobile-ID. De server bepaalt de kiesgerechtigdheid door de digitale id te vergelijken met de kiezerslijst.
3. Wanneer de kiezer toegang heeft verkregen wordt een lijst met kandidaten getoond.
4. De kiezer maakt vervolgens een keuze en de stem wordt versleuteld.
5. De kiezer bevestigt de keuze door middel van het zetten van een digitale handtekening (het invoeren van de tweede pincode PIN2).
6. Na het valideren van de digitale handtekening wordt de digitale handtekening gescheiden van de versleutelde stem.
7. De stem wordt op een separate server opgeslagen.

5.6.3 Verificatie door kiezer

Bij de lokale verkiezingen van oktober 2013 is een vorm van kiezersverificatie getest. Toepassing van verificatie bij bindende verkiezingen is wettelijk niet toegestaan voor 2015.
De verificatie is een ("Ontvangen als bedoeld" / "cast as intented") verificatie.

Het Estlandse systeem van verificatie wijkt af van de verificatiesystemen die in andere landen worden gebruikt, zoals in Noorwegen. In Noorwegen wordt een verificatiecode naar de kiezer gestuurd via een SMS. In Estland wordt de verificatiecode naar de computer gestuurd, maar wordt de mobiele telefoon gebruikt als tweede computer om cryptografische functies uit te voeren. Het systeem werkt als volgt[50]:

> De computer van de kiezer versleutelt de combinatie van gekozen kandidaat en een willekeurig nummer met de publieke sleutel van de stemdienst. De versleutelde stem wordt voorzien van de digitale handtekening van de kiezer. Op zijn computer ontvangt de kiezer een sessie-code en deze wordt samen met het willekeurige nummer als QR-code op het scherm getoond.

[50] Zie http://vvk.ee/public/Verification_of_I-Votes.pdf

De kiezer gebruikt een app op zijn smartphone / tablet om de QR-code te lezen en stuurt de sessie-code terug naar de stemdienst. De stemdienst weet zo dat er een verificatie plaatsvindt. De stemdienst stuurt vervolgens de versleutelde en gesigneerde stem terug naar de smartphone. De stemdienst stuurt ook de gegevens van alle kandidaten naar de smartphone. De smartphone genereert vervolgens voor alle kandidaten een versleutelde waarde met gebruikmaking van het willekeurige nummer. Vervolgens vergelijkt de smartphone de versleutelde waardes van de kandidaten met de versleutelde waarde van de stem van de kiezer. Indien deze overeenkomt dan kan de stem worden bevestigd.

5.6.4 Rol overige instanties

Behalve dat de National Electoral Committe (NEC) betrokken is bij de organisatie, het toezicht houden op en het testen van het systeem, is zoals besproken de Electronic Voting Committee ook betrokken bij de uitvoering van internetstemmen. De IT afdeling van de Riigikogu speelt ook een rol bij de testen, aangezien de NEC niet alle expertise in huis heeft. Cybernetica AS is daarnaast de primaire leverancier van het onlinestemsysteem. Cyber Defence League is een andere partij welke het systeem uitvoerig getest heeft. Het systeem is verder niet gecertificeerd door onafhankelijke partijen, al hoewel de NEC wel externen inhuurt, zoals bijvoorbeeld KPMG in 2011, om onafhankelijke audits uit te voeren. Ook OSCE/ODIHR heeft regelmatig evaluaties uitgevoerd van de Estse verkiezingen en daarmee ook het gebruik van internetstemmen. De meest recente versie[51] is in 2011 geschreven. In dit rapport worden aanbevelingen (mede op basis van voorgevallen incidenten) gedaan door de OSCE/ODIHR om de verkiezingen in de toekomst efficiënter, effectiever en veiliger in te richten.

5.6.5 Beveiligingsmaatregelen

Er zijn diverse beveiligingsmaatregelen getroffen om ten eerste de betrouwbaarheid en veiligheid van de stemmen die via internet zijn uitgebracht te waarborgen (door middel van bepaalde versleutelingstechnieken), de communicatie via het internet te beveiligen tegen aanvallen die schadelijk kunnen zijn en te zorgen dat het systeem minimale kans heeft op uitval[52].

Eén van de maatregelen die zijn getroffen om de betrouwbaarheid te waarborgen is dat iedereen de mogelijkheid heeft (zolang de verkiezing nog open is) zo vaak te kunnen stemmen als zij zelf willen. Zo probeert de NEC te voorkomen dat stemmen onder druk worden uitgebracht. Ook is het zo dat wanneer iemand op een stembureau zijn stem uitbrengt dit er automatisch voor zorgt dat de elektronische stem niet meer wordt meegeteld, om zo dubbelstemmen te voorkomen[53].

Nadat er in 2007 tijdens de de Riigikogu verkiezing een DDos-aanval is uitgevoerd op de Estse webservers, heeft de overheid maatregelen getroffen om dergelijke aanvallen te voorkomen in de

[51] http://www.osce.org/odihr/77557

[52] http://www.osce.org/odihr/77557

[53] http://triinu.net/e-voting/master%20thesis%20e-voting%20security.pdf

toekomst. Eén van die maatregelen heeft te maken met het betrekken van de Computer Emergency Response Team of Estonia (CERT-EE) en de CDL. Het systeem wordt nu door hun getest en gemonitord. Door hen te betrekken is het mogelijk om op grote schaal mensen in te zetten mocht er iets dergelijks nog een keer gebeuren. Hierdoor wordt ook het vertrouwen van het publiek in het systeem vergroot[54].

Om te zorgen dat er een minimale kans bestaat dat het systeem uitvalt tijdens een verkiezing wordt gebruik gemaakt van een back-up server. Er is wordt dus gebruik gemaakt van twee servers, één voor het transporteren van de stem en de ander voor het opslaan van de stem. Deze opereren parallel aan elkaar, zodat als de één uitvalt de ander blijft draaien.

5.6.6 Eigendom

Het internetstemsysteem is ontwikkeld door een private organisatie Cybernetica, in opdracht van de Estse overheid. Het (intellectueel) eigendom van de internetstemdienst ligt bij de NEC.

5.6.7 Kosten

In de periode 2003-2005 waren de uitgaven aan het e-voting project € 320.000. Dit betrof de voorbereidingen en het eerste experiment. Er is geen informatie gevonden over de kosten van de latere experimenten

[54] http://www.osce.org/odihr/77557

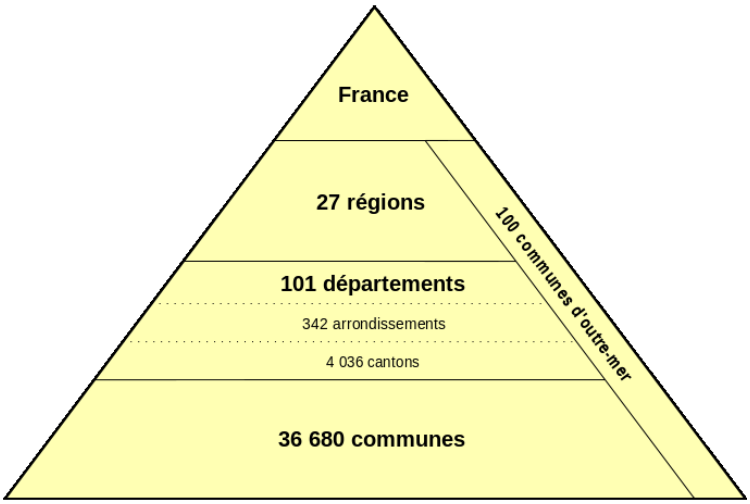
6 FRANKRIJK

6.1 Introductie

Nadat Frankrijk meerdere experimenten heeft gehouden gebruikt de L'Asemblée des Francais de l'Etranger (AFE), een politiek orgaan die Fransen in het buitenland vertegenwoordigt, sinds 2003 internetstemmen om de vertegenwoordigers binnen dit orgaan te verkiezen (2003, 2006 en 2009). Ook heeft Frankrijk stemmen via internet als alternatief aangeboden aan Fransen die in het buitenland verbleven om hun stem uit te brengen tijdens de parlementsverkiezing in 2012.

6.1.1 Staatsinrichting en bestuur

Het bestuur van Frankrijk is opgedeeld in verschillende lagen. Op de bovenste laag vinden we het nationale niveau, namelijk de Franse staat. Het niveau hieronder bestaat uit 27 verschillende regio's, waarvan er 5 regio's buiten Europa liggen. Nog een niveau lager vinden we 101 departementen, waarvan er 5 overzee liggen. Deze zijn onderverdeeld 342 arrondissementen. Deze arrondissementen zijn ook weer onderverdeeld, namelijk in kantons, waarvan er in totaal 4.036 zijn. Het laagste niveau bestaat uit 36.680 gemeenten[55].



Bron: http://commons.wikimedia.org/wiki/File:Administration_territoriale_fran%C3%A7aise.svg

Frankrijk hanteert een democratisch besturingssysteem. Binnen dit systeem heeft de president, veel macht; de uitvoerende macht heeft namelijk meer te zeggen dan de wetgevende macht binnen Frankrijk. De president kan mede regeringen benoemen en ontslaan, door zelf vroegtijdig op te stappen. De president wordt voor een periode van 5 jaar direct gekozen door het volk tijdens landelijke verkiezingen. Daarnaast vertegenwoordigen de president en de bisschop van het Catalaanse Urgell gezamenlijk het opperbestuur van Andorra. Ook zijn er nog twee andere

[55] http://nl.wikipedia.org/wiki/Departement_(Frankrijk)

politieke organen, het Assemblée Nationale en de Senaat, welke samen de volksvertegenwoordiging vormen binnen Frankrijk[56].

6.1.2 Historie internetstemmen

De historie van stemmen via internet in Frankrijk gaat terug naar 2001, met een experiment in het plaatsje Voisins-le-Bretonneux. Aldaar is een proef gedaan met internetstemmen, al was het de kiezers niet toegestaan om vanuit huis te stemmen. De kiezers konden in het gemeentehuis van het plaatsje stemmen op een tweetal computers, welke voorzien waren van internetstemsoftware van election.com.

In 2002 zijn er eveneens 2 experimenten gehouden; in juni in het plaatsje Vandoeuvre-les-Nancy tijdens de presidentiële verkiezing en in Issy-les-Moulineaux tijdens een lokale verkiezing.
In 2007 heeft een politieke partij, de UMP, internetstemmen ingezet tijdens de verkiezing om een voorzitter te selecteren[57].

Internetstemmen is voor het eerst in 2003 in een bindende verkiezing ingezet door het Franse Ministerie van Buitenlandse en Europese zaken. Dit was tijdens een verkiezing van de Assemblée des Français de l'étranger (AFE), een politiek orgaan dat Fransen woonachtig in het buitenland vertegenwoordigt in de senaat. In totaal heeft de AFE 155 leden, waarvan er 12 plaatsnemen in de Senaat[58]. Ook is internetstemmen wederom gebruikt bij de verkiezingen in 2006 en 2009.

Bij deze verkiezingen van 2003, 2006 en 2009 voor de AFE zijn drie verschillende internetstemsystemen gebruikt. Daarna is een contract voor onbepaalde tijd getekend bij de firma Scytl (http://www.scytl.com/index.html). Door dit contract is het mogelijk om internetstemmen in iedere gewenste verkiezing in te zetten[59].

In 2012 is bij de parlementsverkiezingen van 10 in 17 juni (verkiezing in twee ronden) internetstemmen toegestaan voor alle Fransen die ten tijde van de verkiezing in het buitenland verbleven[60]. In dat jaar waren in april ook presidentsverkiezingen, maar internetstemmen is toen niet ingezet. Door een besluit van de constitutionele raad op 15 januari 2013 is een deel van de parlementsverkiezing ongeldig verklaard, waardoor op 10 juni 2013 in een tweetal districten tussentijdse parlementsverkiezingen zijn gehouden.

---

[56] http://nl.wikipedia.org/wiki/Frankrijk

[57] http://en.wikipedia.org/wiki/Electronic_voting_examples

[58] http://www.assemblee-afe.fr/

[59] http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf

[60] http://phys.org/news/2012-02-expat-french-internet-vote.html

6.1.3 Organisatie internetstemmen

Het ministerie van binnenlandse zaken heeft de uitvoering en de coördinatie van de verkiezingen in Frankrijk in handen. Voor de regio's die overzee liggen zijn er lokale verkiezingscomités in het leven geroepen[61].

Met de aanpassing van Franse kieswet per 2011 is een “Bureau de Vote Électronique” ingesteld, welke eindverantwoordelijk is voor het goed en eerlijk functioneren van de internetverkiezing. Dit bureau bestaat uit zeven vertegenwoordigers, zijnde een lid van de Raad van State, de Directeur van de afdeling ‘Franse burgers in het buitenland’ van het ministerie van Buitenlandse Zaken, een vertegenwoordiger van het ministerie van Binnenlandse Zaken, de directeur van de ANSSI en drie gekozen leden van de AFE. Voor elk van hen wordt een plaatsvervanger benoemd onder dezelfde omstandigheden. Het bureau had bij de laatste verkiezing in 2012 ook de taak om de cryptografische sleutels te bewaren. Eens in de drie jaar wordt de rol en samenstelling van dit bureau heroverwogen en worden de stemprocedures van internetstemmen herzien.

Het ministerie van buitenlandse en Europese zaken, afdeling ‘Franse burgers in het buitenland’ was opdrachtgever voor de ontwikkeling en verwerving van het internetstemsystemen. Een stuurgroep was ingesteld bestaande uit een grote groep vertegenwoordigers van alle betrokken organisaties, inclusief betrokken leveranciers en een onafhankelijke auditor.
Bij de ontwikkeling werden (onder meer) de richtlijnen opgevolgd van de Commission Nationale Informatique et Liberté (vergelijkbaar met het College Bescherming Persoonsgegevens uit Nederland) voor het inzetten van internetstemmen.

6.2 Kiesgerechtigdheid

Alle staatsburgers van Frankrijk die 18 jaar of ouder zijn hebben stemrecht[62].

Internetstemmen is *alleen* voorbehouden aan Franse staatsburgers die woonachtig zijn in het buitenland.

6.3 Aantal kiesgerechtigden en opkomst[63]

Jaar	Aantal kiesgerechtigden	Aantal geregistreerde internetkiezers	Via internet uitgebrachte stemmen	% Internet-stemmen t.o.v. totaal aantal uitgebrachte stemmen
2003	50.000 geregistreerde Franse	Nvt	4.384	60%

[61] https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDoQFjAB&url=http%3A%2F%2Fwww.essex.ac.uk%2Fgovernment%2Felectoralmalpractice%2F2_ManagementBodiesConduct.doc&ei=oDVqUp2TBKWB4gTluIDwCQ&usg=AFQjCNEGkd1E3813u9NdcyrfIsbD4XMKgw&sig2=fkuGxwFHQ_Uz5LEZraaxXw

[62] http://www.diplomatie.gouv.fr/

[63] http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf

Jaar	Aantal kiesgerechtigden	Aantal geregistreerde internetkiezers	Via internet uitgebrachte stemmen	% Internet-stemmen t.o.v. totaal aantal uitgebrachte stemmen
	burgers woonachtig in Noord-Amerika			
2006	525.000 Franse 'expats' woonachtig in Azië, Europa en het Midden-Oosten.	Onbekend	10.201	14%
2009	340.000 geregistreerde Franse burgers woonachtig in Afrika en Noord-en Zuid-Amerika	Onbekend	6.026	9%
2012	Onbekend	210.000	126.947 (1e ronde) 117.676 (2e ronde)	60% 56%
2013	onbekend	151.762 111.387	15.429 5.186	10% 5%

6.4 Andere beschikbare stemmethoden

Kiezers woonachtig buiten Frankrijk kunnen tijdens de verkiezingen hun stem ook uitbrengen via de post, op een stembureau in Frankrijk of door een volmacht af te geven[64]. Stemmen bij volmacht is niet toegestaan voor AFE verkiezingen.

6.5 Internet stemsysteem – AFE (2003, 2006 en 2009)

In 2003, 2006 en 2009 is voor elke verkiezing een ander systeem gebruikt. Over het systeem dat in 2003 gebruikt is, is weinig informatie bekend. Wel is bekend dat Election Europe, voormalig bekend als Election.com, de leverancier was en dat het systeem intellectuele eigendom was van deze leverancier. Alle gebruikte systemen zijn closed source software.

In 2006 is het systeem van EADS gebruikt, genaamd 'Cybervote'. Er waren een aantal problemen met dit systeem; zo konden kiezers niet vanuit alle landen online hun stem uitbrengen door beperkingen van de versleutelingstechniek en ondervonden de kiezers die geen Windows hadden problemen tijdens het stemmen[65].

In 2009 werd het 'Pnyx' systeem gebruikt, ontwikkeld door Scytl. Dit systeem is, in aangepaste vorm, later ook in Noorwegen ingezet. Frankrijk heeft ook na de verkiezing van 2009 een contract

[64] http://aceproject.org/ero-en/regions/europe/FR/france-final-report-parliamentary-elections-of-10/at_download/file

[65] Bijlage II - Internetstemmen buitenland, 2007 ICTU

getekend bij Scytl. Dit contract staat toe dat Frankrijk ongelimiteerd het systeem in kan zetten tijdens verkiezingen[66].

6.6 Procesbeschrijving

6.6.1 Registratie van kiezers

In 2003 was registratie niet vereist en kregen alle kiezers een brief toegestuurd per reguliere post met een code en een wachtwoord voor toegang tot de stemwebsite.
Vanaf 2006 was registratie verplicht, welke toen bestond uit het sturen van een verzoek naar het consulaat in het land waar men verbleef. Nadien werd een toegangscode opgestuurd voor toegang tot de stemdienst.
In 2009 dienden kiezers zich te registeren via de e-portaal GAEL (Guichet d'Administration Electronique) van de Franse overheid. De registratie vereiste het invoeren van de persoonlijke NUMIC (consulair ID-nummer), naam, geboortedatum en paspoortnummer en het aanmaken van een persoonlijk wachtwoord[67].

6.6.2 Stembescheiden en stemming

Over het gebruikte systeem in *2003* is geen verdere informatie gevonden.

In *2006* kon men door middel van een identifier en een toegangscode zichzelf identificeren. Om te kunnen stemmen via internet was het nodig een JAVA-applicatie te downloaden. Deze applicatie functioneerde als de user-interface. Men verkoos een JAVA-applicatie boven een website, omdat JAVA het mogelijk maakte om cryptografische functies uit te voeren (versleuteling van de stem en het signeren met een digitale handtekening)[68].

In *2009* is het systeem ontwikkeld door Scytl in samenwerking met AtosOrigin. Ook bij deze stemdienst werd een JAVA-applicatie gedownload om een beveiligde verbinding te leggen met het portaal van het onlinestemsysteem. De kiezer had vervolgens de mogelijkheid om zich in te loggen met het wachtwoord en het consulaire identificatienummer. Na ingelogd te zijn verscheen er een lijst met mogelijke kandidaten waaruit gekozen kon worden, gelinkt aan het bijbehorende kiesdistrict van de kiezer[69].

6.6.3 Verificatie door kiezer

Het is onbekend of in 2003 verificatie van de stem mogelijk was.

---

[66] http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf

[67] http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf

[68] http://www.cs.princeton.edu/~appel/papers/urne.pdf

[69] http://www.osce.org/odihr/elections/93621

In 2006 en 2009 ontvingen de kiezers een bewijs wanneer hun stem was aangekomen bij en opgeslagen was op de server[70].

6.7 Internetstemsysteem – parlementsverkiezing 2012 / 2013

In 2012 is bij de parlementsverkiezing hetzelfde systeem 'Pnyx' gebruikt als dat gebruikt is in 2009 bij de AFE verkiezing.

De stemdienst is toegankelijk via https://scrutin.diplomatie.gouv.fr/

6.8 Procesbeschrijving

6.8.1 Registratie van kiezers

In 2012 / 2013 dienden kiezers eveneens een registratieproces te doorlopen om via internet hun stem uit te brengen. Zij dienden hun mailadres en telefoonnummer te registreren bij het consulaat, zodat zij instructies toegezonden konden krijgen voor het gebruiken van het onlinestemsysteem.

6.8.2 Verificatie door kiezer

In 2012 ontving de kiezer een bevestiging in de vorm van een code. Met deze code konden kiezers vaststellen of de stem was ontvangen. Met deze code was het niet mogelijk om na te kijken of de stem ook correct was gedeponeerd in de stembus, of dat deze juist was meegeteld[71].

6.8.3 Rol overige instanties

Tijdens de verkiezing in 2003 werd de Franse overheid ondersteund door het 'Forum des droits sur l'Internet'. Dit is een private instantie die aanbevelingen heeft gedaan over het gebruik van internetstemmen in de toekomst binnen Frankrijk.

Bij de verkiezingen van 2009 en 2012 hield het Bureau de Vote Électronique toezicht op de correcte uitvoering van de verkiezing.

In opdracht van het ministerie van Buitenlandse Zaken is in 2009 een audit gedaan op het systeem van Scytl door de firma Opida. Hierbij werd als baseline de richtlijnen van de CNIL en ANSSI gebruikt.[72]

6.8.4 Beveiligingsmaatregelen

In 2006 was het internetstemmen op een aantal locaties stopgezet. Dit hing samen met het lage aantal uitgebrachte stemmen, waardoor het erg gemakkelijk traceerbaar was wie welke stem had uitgebracht en hierdoor de privacy in het geding kwam[73].

---

[70] http://www.osce.org/odihr/elections/89000

[71] http://www.osce.org/odihr/elections/93621

[72] http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf

Daarnaast is niet alles perfect verlopen tijdens de verkiezing in 2006. Zo kon men niet in alle landen via internet een stem uitbrengen door encryptiebeperkingen. Ook waren er wat problemen met kiezers die geen Windows gebruikten. Ook bleek dat het versturen van de codes via de post niet erg efficiënt te zijn[74].

Tijdens de verkiezing in 2009 waren er nieuwe risico beperkende maatregelen genomen;

- Er is een review van de source code uitgevoerd: Opida en andere externe waarnemers hebben een review van deze source code mogen uitvoeren;
- Het onlinestemsysteem is gecertificeerd: Opida, vertegenwoordigers van het ministerie en externe waarnemers hebben het systeem gecertificeerd;
- Er is een continue audit uitgevoerd: Opida en andere partijen hebben voor, tijdens en na de verkiezingen diverse audits uitgevoerd;
- Er is end-to-end versleuteling toegepast: De stem werd direct na de stemming versleuteld en gesigneerd met een digitale handtekening. Dit gebeurde voordat de stem bij de servers aankwam;
- Er is een gemixt protocol toegepast: Er kon geen enkele relatie gelegd worden tussen de stemming en de stem zelf door het gebruik van dit gemixte protocol (m.b.t. versleutelings- en decoderingsproces);
- Verifieerbaar door de kiezer: Het was mogelijk voor de kiezer om te controleren of hun uitgebrachte stem ook daadwerkelijk was opgeslagen op de server[75].

Tijdens de parlementsverkiezing van 2012 zijn een aantal problemen opgetreden. De eerste had er mee te maken dat rond de 1e verkiezingsronde de JAVA virtual machine (programma om de JAVA-code uit te kunnen voeren op PC's) ge-update werd. Uiteindelijk werd een workaround ontworpen waarmee kiezers de oude versie van de JAVA virtual machine konden terug installeren. Door dit probleem konden een aantal kiezers niet stemmen.
Een ander probleem ontstond bij de officiële telling doordat de digitale handtekening van één uitgebrachte stem niet goed was geplaatst, waardoor de stem niet meegeteld werd.

Door de Pirate Party, een politieke partij, werden vragen opgeworpen gerelateerd aan de transparantie en veiligheid van het systeem. Zo vond deze partij dat de elektronische sleutels van de stembus gegenereerd waren door onrechtmatige tools. The Pirate Party heeft gevraagd of zij de source code mochten inzien, wat hun geweigerd werd. Zij hebben een klacht bij de Constitutional Court ingediend en een verzoek ingediend om de internetstemmen te laten vervallen. Hier is geen gehoor aan gegeven.

---

[73] http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf

[74] Bijlage II - Internetstemmen buitenland, 2007 ICTU

[75] http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf

6.8.5 Eigendomsrechten

In alle gevallen behoren de intellectuele eigendomsrechten tot de leveranciers[76].

6.8.6 Kosten

In 2003 heeft het systeem 70.000 euro gekost. In 2006 waren de kosten 2 miljoen euro[77]. De kosten van het gebruikte systeem in 2009 en 2012 zijn onbekend.

[76] http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf

[77] Bijlage II - Internetstemmen buitenland, 2007 ICTU

7 INDIA

7.1 Introductie

In 1947 verkreeg India onafhankelijkheid van het Britse Rijk. India is sindsdien wel lid gebleven binnen het Gemenebest. Het land kreeg een grondwet in 1950, gevolgd door de eerste landelijke verkiezingen in 1952. Al sinds de jaren '80 wordt er in India elektronisch gestemd middels stemcomputers. De eerste experimenten met stemmen via internet dateren uit 2010.

7.1.1 Staatsinrichting en bestuur

India is een parlementaire democratie met een federale bestuursvorm. Het hoogste regeringsorgaan is de gekozen volksvertegenwoordiging waarvan ook alle ministers lid zijn en daaraan verantwoording schuldig zijn. Het parlement omvat twee Kamers: het rechtstreeks gekozen Lagerhuis, *Lok Sabha*, en het indirect gekozen Hogerhuis, *Rajya Sabha*. Op deelstaatniveau bestaat vaak hetzelfde tweekamersysteem. Het Lagerhuis telt 545 leden en wordt elke vijf jaar rechtstreeks gekozen volgens een districtenstelsel. Het Hogerhuis heeft 245 leden die door de parlementen van de deelstaten gekozen worden. Elke twee jaar vinden er verkiezingen plaats voor een derde van de zetels van het Hogerhuis.

De federatie is onderverdeeld in 29 deelstaten en 6 unieterritoria. Daaronder is er een onderverdeling in districten, talugs of tehsils (enkele honderden dorpen), steden en dorpen.

7.1.2 Historie internetstemmen

Het initiatief tot internetstemmen kwam van Minister Narendra Modi in januari 2010, toen hij de verkiezingscommissaris van Gujarat, K.C. Kapoor, opdracht gaf om manieren te vinden om burgers meer aan te moedigen om te stemmen. Naar aanleiding van deze opdracht heeft de State Election

Commission (SEC) van de deelstaat Gujarat onderzoek gedaan naar de mogelijkheid van stemmen via internet.[78]
Dit heeft in september 2010 geleid tot de eerste online stemming voor een bindende verkiezing in zes gemeenten (Ahmedabad, Surat, Rajkot, Vadodara, Bhavnagar Jamnagar) in India[79]. In maart 2011 zijn ook de Gandhinagar municipal corporation verkiezingen via internet uitgevoerd.

In 2011 heeft het internetstemmenproject de prijs 'eWorld Forum Award' gewonnen, ingesteld door de Indiase minister van ICT[80] en in 2013 heeft het de prijs '2013 eGovernance award' gewonnen, gesponsord door de Indiase overheid.

7.1.3 Organisatie internetstemmen

De verantwoordelijkheid voor internetstemmen ligt bij de 'State Election Commission (SEC)' van Gujarat (zie ook http://sec.gujarat.gov.in/). Zij introduceerde internetstemmen om zo het verkiezingsproces verder te automatiseren en moderniseren, waarmee zij hoopte de opkomst te vergroten.

7.2 Kiesgerechtigdheid

Iedere staatsburger die minimaal 18 jaar is op de eerste dag (1 januari) van het jaar waarin de kiezerslijst wordt voorbereid is kiesgerechtigd. Deze persoon dient geregistreerd te zijn in het kiesdistrict waar hij/zij ook verblijft.[81]

7.3 Aantal kiesgerechtigden en opkomst

Er zijn in de zes gemeenten in totaal 8,61 miljoen kiesgerechtigden.

387 kiezers hadden zich geregistreerd, 182 hiervan waren goedgekeurd na controle van de identiteit. Van deze 182 waren er 124 stemmen uitgebracht via internet.[82] [83]

7.4 Andere beschikbare stemmethoden

Stemmen in een stembureau (afhankelijk van het stembureau met stemcomputer of met stembiljet).

7.5 Internet stemsysteem

Het stemsysteem heet Online Voting System (OVS) en is ontwikkeld door Scytl in samenwerking met Tata Consulting Services. Hiervoor is door de deelstaat Gujarat een vijfjarig contact

[78] http://www.indianexpress.com/news/gujarat-ready-to-click-take-first-step-in-evoting/635417/

[79] http://www.ndtv.com/article/cities/gujarat-civic-elections-witness-first-ever-online-voting-58739

[80] http://www.scytl.com/scytls-internet-voting-project-in-india-receives-the-2011-eworld-forum-award/index.html

[81] A guide for the Voters, Election Commission of Inda, 2006 (http://eci.nic.in/eci_main/ECI_voters_guideline_2006.pdf)

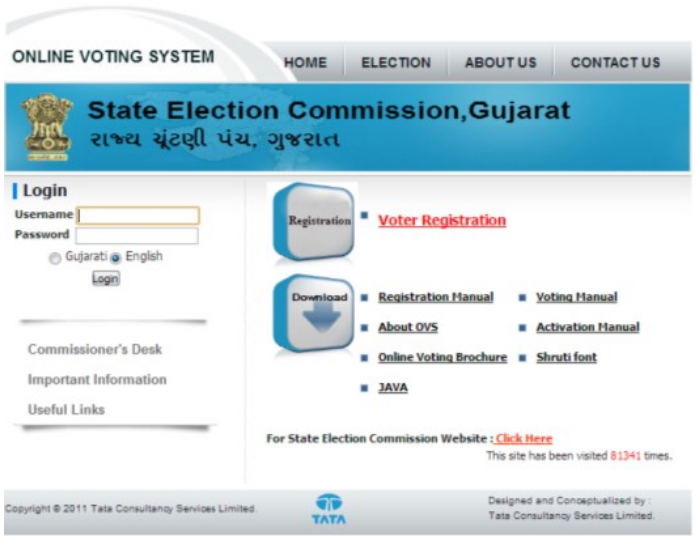
[82] http://www.ndtv.com/article/cities/gujarat-civic-elections-witness-first-ever-online-voting-58739

[83] http://www.business-standard.com/article/beyond-business/e-voting-for-it-land-111072300044_1.html

afgesloten.[84] Het systeem ondersteunt zowel de Engelse taal als de talen gesproken binnen de gemeentes.

7.6 Procesbeschrijving

7.6.1 Registratie van kiezers



De registratie verloopt in meerdere stappen.

Stap 1: Online registeren via http://www.onlinevotinggujarat.gov.in. Hierbij dient de kiezer zijn naam, adres, leeftijd, telefoonnummer en emailadres in te vullen en aan te geven of hij/zij via internet of op een stembureau wil stemmen.
Stap 2: Door ambtenaren van de SEC wordt een huisbezoek afgelegd om de gegevens van de kiezer te controleren[85].
Stap 3: Ontvangst van gebruikersnaam per e-mail en wachtwoord via mobiele telefoon.
Stap 4: Activering van kiezersaccount door gebruikersnaam en wachtwoord via de site in te vullen, waarna de kiezer direct zijn wachtwoord dient te wijzigen.[86]

7.6.2 Stembescheiden

Er worden geen verdere stembescheiden toegezonden. Om te stemmen logt de kiezer in met zijn gebruikersnaam en gewijzigde wachtwoord.

7.6.3 Stemming

Om te kunnen stemmen volgt de kiezer de volgende stappen[87]:

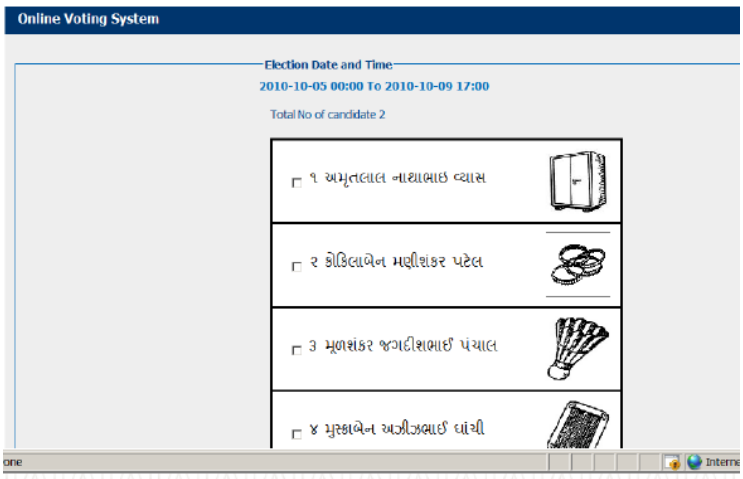
---

[84] http://www.scytl.com/customer/state-of-gujarat/index.html

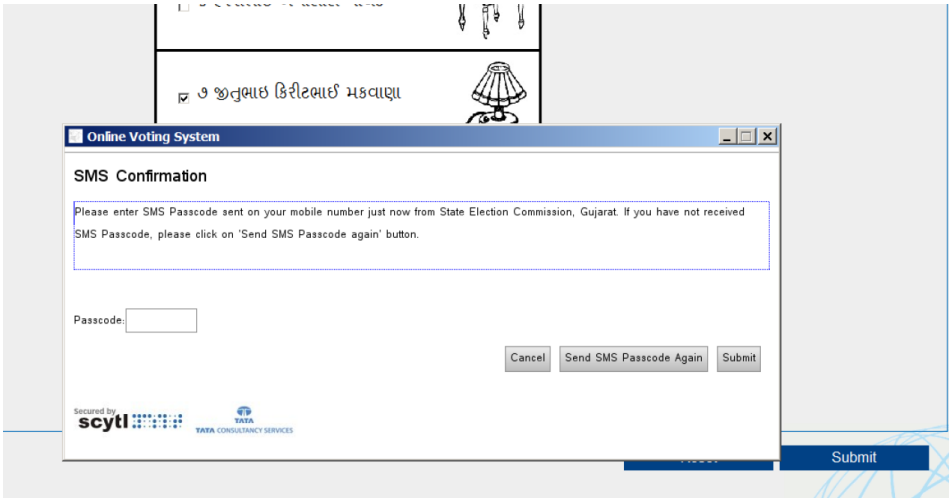
[85] http://awards.eletsonline.com/2011/11/15/online-voting-system/

[86] http://www.business-standard.com/article/beyond-business/e-voting-for-it-land-111072300044_1.html

Stap 1: Inloggen op de onlinevotinggujarat.gov.in website met gebruikersnaam en wachtwoord
Stap 2: Kandidaat selecteren (kiezer kan maximaal 3 kandidaten selecteren)

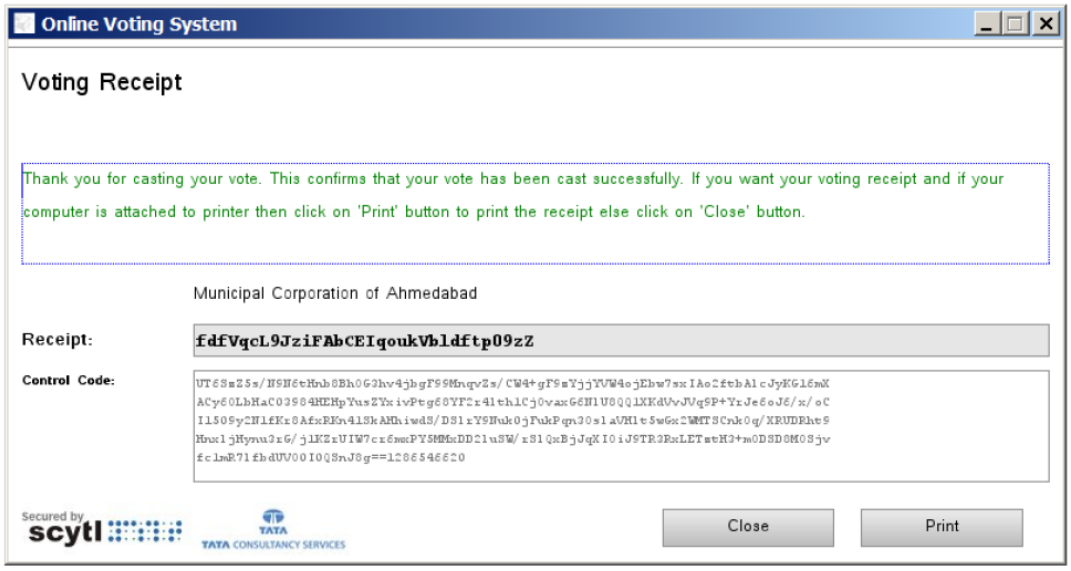


Stap 3: Selectie bevestigen en versturen stem
Stap 4: De kiezer ontvangt direct daarna op zijn mobiele telefoon een wachtwoord
Stap 5: Invullen van het wachtwoord.



Stap 6: De stemdienst toont een ontvangstbevestiging aan de kiezer, deze kan worden geprint of gekopieerd.

[87] Zie ook de handleiding voor de kiezer op https://onlinevotinggujarat.gov.in/ovs-portal/eVoterManual.pdf



7.6.4 Verificatie door kiezer

De voting receipt die de kiezer in de laatste stap ontvangt kan gebruikt worden door de kiezer om de ontvangst van zijn/haar stem te controleren. Hoe dit verificatieproces in India precies verloopt wordt niet duidelijk uit de openbare bronnen.

7.6.5 Rol overige instanties

De State Election Commission (SEC) van de deelstaat Gujarat heeft onderzoek gedaan naar de mogelijkheden van stemmen via internet en is ook opdrachtgever van de ontwikkeling.
Het systeem is ontwikkeld door Scytl samen met Tata Consultancy Services. Het Indiase bureau Indusface.com heeft de veiligheid van het systeem bewaakt tijdens de ontwikkeling.

7.6.6 Beveiligingsmaatregelen

Er zijn vier eisen aan het system gesteld: authenticatie, beschikbaarheid, vertrouwelijkheid en integriteit. Het SEC heeft een extern auditbureau aangehaakt, Indusface. Dit bureau was verantwoordelijk voor het bewaken van de veiligheid van het stemsysteem.
Het datacenter wat gebruikt werd voor het stemsysteem bestond uit 32 servers, een back-up server en een data recovery team wat direct in actie kon komen als er iets zou gebeuren.[88] Het datacenter is verdeeld in verschillende modules, heeft een hoge bandbreedte en verschillende firewalls. De kiezer kon bovendien de website controleren aan de hand van het certificaat van de website.[89] Elke module controleerde de geldigheid van input of stemmen. Daarnaast worden de activiteiten (stemmen) continu gemonitord en wordt er actie ondernomen zodra er iets verdachts is gedetecteerd. De website die gebruikt wordt is bovendien enkel op de verkiezingsdag online

[88] http://www.business-standard.com/article/beyond-business/e-voting-for-it-land-111072300044_1.html

[89] http://awards.eletsonline.com/2011/11/15/online-voting-system/

zodat het datacenter, welke gekoppeld is aan de website, slechts beperkt te bereiken is en daardoor moeilijker te hacken is.[90]

7.6.7 Eigendom

Scytl heeft het systeem samen met Tata Consultancy Services ontwikkeld. Onbekend is hoe het eigendom van het systeem is belegd.

7.6.8 Kosten

De kosten die zijn uitgegeven voor het ontwikkelen van het online stemsysteem door de State Election Commisson bedragen 340 miljoen roepi (ca. 4 miljoen euro), 150 miljoen roepi (ca. 1,8 miljoen euro) hiervan is uitgegeven aan software en het datacenter. [91]

[90] http://www.cio.in/case-study/click-vote

[91] http://www.ndtv.com/article/cities/gujarat-civic-elections-witness-first-ever-online-voting-58739

8 MEXICO

8.1 Introductie

De eerste keer dat er in Mexico internetstemmen is gebruikt bij een bindende verkiezing was in 2012 bij de verkiezing voor de nieuwe gouverneur van Mexico-City. De mogelijkheid van internetstemmen was alleen beschikbaar voor kiesgerechtigden die tijdens de verkiezing in het buitenland verbleven[92].

8.1.1 Staatsinrichting en bestuur

Mexico is ingericht als een federale republiek. In de Mexicaanse staatsinrichting wordt onderscheid gemaakt naar de wetgevende, uitvoerende en rechterlijke macht. De wetgevende macht van Mexico, Congreso de la Unión genaamd, bestaat uit twee afzonderlijke Kamers. Dit zijn de Kamer van Senatoren, Cámara de Senadores, en de Kamer van Afgevaardigden, Cámara de Diputados. Om de 3 jaar worden de verkiezingen voor de Cámara de Diputados gehouden en voor de Cámara de Senadores worden deze om de 6 jaar gehouden.
De president heeft de uitvoerende macht in handen. De president is naast staatshoofd van Mexico ook de regeringsleider. Een president kan maar voor één termijn (periode van 6 jaar) gekozen worden, een herverkiezing is niet mogelijk.
Het Hooggerechtshof van de Natie, de Suprema Corte de Justicia de la Nación, oefent de rechterlijke macht uit samen met een groot aantal lagere en gespecialiseerde rechtbanken. Dit specifieke gerechtshof heeft in totaal 11 leden, welke door het Congres om de 15 jaar worden gekozen.

Mexico is opgedeeld in 31 staten en één Federaal District (Mexico-Stad). Iedere staat heeft een gouverneur (het hoofd van de staat), een staatscongres en een eigen grondwet. De gouverneurs worden om de 6 jaar gekozen in directe verkiezingen en het staatscongres wordt om de 3 jaar gekozen. Ook de gouverneur kan niet herkozen worden.

De staten zijn verder onderverdeeld in 2.438 gemeenten met allen een burgemeester aan het hoofd welke wordt bijgestaan door 'regidores'. De burgermeesters worden voor een periode van 3 jaar vastgesteld.

Mexico-Stad is een uitzondering en is niet onderverdeeld in gemeentes, Mexico-Stad bestaat uit 16 districten[93]. Sinds 1997 heeft Mexico-Stad, het Federale District, een regeringsleider en daarnaast een wetgevende assemblee.

[92] http://www.businesswire.com/news/home/20120809005061/en/Mexico-Sets-Precedent-Scytl%E2%80%99s-Internet-Voting-Technology

[93] http://nl.wikipedia.org/wiki/Mexico_(land)

8.1.2 Historie internetstemmen

Mexico is sinds 2000 aan het kijken naar de mogelijkheden van elektronisch stemmen in stemlokalen. Er zijn in 3 staten meerdere niet-bindende experimenten gehouden (Mexico-City, Coahuila en San Luis Potosí). Op nationaal niveau zijn geen experimenten gehouden.

Het e-voting experiment in Mexico-City startte in 2001. De eerste keer dat er in Mexico internetstemmen is gebruikt bij een bindende verkiezing was in 2012 bij de verkiezing voor de nieuwe gouverneur van Mexico-City. De mogelijkheid van internetstemmen was alleen beschikbaar voor kiesgerechtigden die tijdens de verkiezing in het buitenland verbleven[94].

8.1.3 Organisatie internetstemmen

De federale verkiezingen in Mexico worden georganiseerd door het 'Instituto Federal Electoral'. De staten verkiezingen worden georganiseerd door statelijke kiesinstanties. Voor Mexico-stad is het 'Instituto Electoral del Distrito (http://www.iefd.org.mx) Federal' verantwoordelijk voor de verkiezingen.

8.2 Kiesgerechtigdheid

Personen vanaf 18 jaar hebben kiesrecht in Mexico. Zij zijn vanaf deze leeftijd verplicht hun stem uit te brengen, al staat er geen straf op wanneer dit niet gedaan wordt[95].

8.3 Aantal kiesgerechtigden en opkomst

61.687 kiezers hadden zich geregistreerd om te stemmen via internet vanuit 113 verschillende landen[96]. De stemming was open tussen 28 juni 2012 8:00 uur en 1 juli 2012 18:00 uur. In totaal zijn er 2.639 stemmen via internet uitgebracht (en 5.272 per post) [97].

8.4 Andere beschikbare stemmethoden

De kiesgerechtigden die tijdens de verkiezing in 2012 in het buitenland verbleven hadden ook de mogelijkheid om via de post hun stem uit te brengen[98].

8.5 Internet stemsysteem

Het gebruikte internetstemsysteem is ontwikkeld door Scytl, genaamd 'Pnyx'.

---

[94] http://www.businesswire.com/news/home/20120809005061/en/Mexico-Sets-Precedent-Scytl%E2%80%99s-Internet-Voting-Technology

[95] http://nl.wikipedia.org/wiki/Mexico_(land)

[96] http://www.sandiegored.com/noticias/22717/Mexican-migrants-to-vote-online-for-first-time/

[97] http://www.iedf.org.mx/index.php/boletines-y-comunicados/87-2012boletines/2139-exitosa-la-votacion-por-internet

[98] http://www.businesswire.com/news/home/20120809005061/en/Mexico-Sets-Precedent-Scytl%E2%80%99s-Internet-Voting-Technology

8.6 Procesbeschrijving

8.6.1 Registratie van kiezers

Kiezers die wilden stemmen via internet konden zich tussen 1 oktober 2011 en 15 maart 2012 registreren.

8.6.2 Stembescheiden en stemming

Na de registratie ontving de kiezer een link naar het Sistema de Contraseñas ('wachtwoorden systeem'). In de periode 15 mei tot 1 juli 2012 kon de kiezer via die link een wachtwoord bestaande uit 16 karakters te verkrijgen na invoer van een user-id, email adres en persoonsgegevens. De kiezer werd geacht dit wachtwoord af te drukken of te onthouden.

Vanaf 27 juni 8:00 uur tot en met 1 juli 2012 18:00 kon de kiezer inloggen in het Sistema de Vota ('Stemsysteem') met zijn user-id en het wachtwoord.

Voor meer informatie zie ook het voorlichtingsfilmpje op
http://www.youtube.com/watch?v=fU61D8IxMKw

8.6.3 Verificatie door kiezer

Het stemsysteem toonde aan de kiezer een bewijs van ontvangst van de stem (numerieke code). Na afloop van de stemming werd op de website van de IEDF alle verificatiecodes gepubliceerd.

8.6.4 Rol overige instanties

Op het onlinestemsysteem is een audit uitgevoerd door Telefónica Security Engineering. De audit bevestigde dat het systeem voldeed aan de veiligheidstandaarden en eisen van IEDF.

Het stemproces werd daarnaast gemonitord door andere partijen (verkiezingswaarnemers, leiders van Mexicaanse gemeenschappen, vertegenwoordigers van politieke partijen en 'State Election Management Bodies').

8.6.5 Beveiligingsmaatregelen

Zoals hierboven is vermeld is er een audit uitgevoerd op het onlinestemsysteem. Deze bevestigde dat het systeem voldeed aan de veiligheidsstandaarden en eisen opgesteld door IEDF. Daarnaast had ook 'The Electoral Tribunal of the Federal Judiciary' het systeem geëvalueerd en ook zij hebben het systeem goedgekeurd. Tijdens het stemproces hebben zoals ook al eerder genoemd diverse partijen het systeem en het proces in de gaten gehouden (verkiezingswaarnemers, leiders van Mexicaanse gemeenschappen, vertegenwoordigers van politieke partijen en 'State Election Management Bodies'). Zij hebben het stemmen via internet als succesvol ervaren.

8.6.6 Eigendom

Onbekend.

9 NOORWEGEN

9.1 Introductie

Bij de parlementsverkiezing op 9 september 2013 was het inwoners van 12 gemeenten toegestaan om via internet hun stem uit te brengen in een 'early voting' periode van 12 augustus 2013 tot aan 6 september 2013. Op de dag van stemmig zelf kon niet via internet worden gestemd. In het Noorse internetstemsysteem kunnen kiezers zo vaak een stem uitbrengen als ze willen, de laatst uitgebrachte stem wordt meegeteld. Indien een kiezer op de dag van stemming (9 september) ook in een stemlokaal zijn stem uitbrengt, wordt deze stem en niet de internetstem meegeteld.

9.1.1 Staatsinrichting en bestuur

Noorwegen is een constitutionele monarchie. De wetgevende macht berust bij het Storting (parlement). De leden worden voor vier jaar gekozen volgens een districtenstelsel. Het land is ingedeeld in negentien provincies, met aan het hoofd een gouverneur. Elke provincie vormt een kiesdistrict en op basis van het aantal inwoners en de oppervlakte per provincie is het aantal zetels in het parlement bepaald. Verder kent Noorwegen op lokaal niveau ruim 450 gemeenten.
Het parlement kent een mengvorm van een één- en tweekamersysteem: weliswaar is er slechts één kamer, maar die deelt zichzelf in een Lagting (3 van de leden) en een Odelsting (H). Nieuwe wetgeving wordt eerst behandeld in het Odelsting en vervolgens in het Lagting.
De uitvoerende macht berust formeel bij de koning, maar de staatsraad bepaalt de inhoud van de Koninklijke besluiten, die door de minister-president mede moeten worden ondertekend. De koning benoemt de leden van de regering, die verantwoording schuldig is aan het parlement.

9.1.2 Historie internetstemmen

De Noorse regering heeft in 2004 opdracht gegeven aan een werkgroep om te onderzoeken wat het potentieel en de mogelijkheden zijn om elektronisch stemmen in te voeren in Noorwegen. In 2006 verscheen het eindrapport[99] van de werkgroep met daarin een zeer uitvoerige analyse van mogelijkheden om het stemproces te moderniseren vanuit een democratische, juridische, technische en administratieve invalshoek. De werkgroep concludeerde dat elektronisch stemmen het gemakkelijker en goedkoper zou maken voor de kiezer om zijn democratische rechten uit te oefenen. De werkgroep stelde voor om te starten met proeven en een systematische evaluatie, met als doel om zowel technische oplossingen te testen als het vertrouwen in elektronisch stemmen onder de kiezers te laten groeien. Hierna zou een geleidelijke en stapsgewijze invoering van elektronisch stemmen kunnen plaatsvinden.
Op basis van onder meer dit rapport besloot de regering om een serie van experimenten te gaan uitvoeren met internetstemmen. De beoogde effecten waren een betere toegankelijkheid tot het stemproces voor alle groepen kiezers, een efficiëntere organisatie van de verkiezing, lagere uitvoeringskosten en een versnelling in het opstellen van de uitslag door elektronisch te tellen.

[99] http://www.regjeringen.no/upload/kilde/krd/red/2006/0087/ddd/pdfv/298587-evalg_rapport_engelsk201106.pdf

Hiervoor werd het E-vote 2011 project ingericht wat tot doel had om een systeem voor internetstemmen te verwerven voor parlementaire, gemeentelijke en provinciale verkiezingen en deze te beproeven in een tiental gemeenten bij de verkiezingen in september 2011.

In de opzet van het experiment met internetstemmen werd gekozen om internetstemmen te positioneren als aanvullende mogelijkheid om te stemmen, naast de bestaande mogelijkheden om in een stemlokaal en per brief[100] te stemmen. De regering koos daarnaast voor een opzet waarin kiezers meerdere stemmen konden uitbrengen via internet in een periode *voorafgaand* aan de dag van stemming, én daarnaast altijd nog hun stem konden uitbrengen in het stemlokaal. Voor deze opzet werd gekozen vanwege twee redenen: i) voorkomen dat er niet gestemd kan worden als het internetstemsysteem tijdelijk niet beschikbaar zou zijn en ii) als maatregel om kiezers die problemen zouden ondervinden met internetstemmen toch de gelegenheid te bieden om hun stem uit te brengen. Door deze opzet konden ook kiezers die door derden onder druk werden gezet om op een bepaalde kandidaat te stemmen toch hun eigen stem uitbrengen in de gecontroleerde omgeving van het stembureau.

Bij de verkiezing konden kiezers via internet stemmen in de periode van 10 augustus tot 9 september 2011 (31 dagen). Bijna de helft van de uitgebrachte stemmen werd uitgebracht in de laatste week. Van de 167.506 kiesgerechtigden brachten 28.001 kiezers hun stem uit via internet.

In december 2012 besloot[101] de regering, op grond van de overwegend positieve evaluatie van de experimenten uit 2011 om nieuwe experimenten te houden bij de parlementsverkiezingen van 2013.

De Noorse kieswetgeving staat het houden van experimenten met andere vormen van stemmen toe zolang deze experimenten niet afwijken van de basisprincipes zoals vastgelegd in de kieswet. Door deze opzet kon de Noorse regering experimenten houden met internetstemmen zonder hiervoor de kieswet te hoeven wijzigen.

9.1.3 Organisatie internetstemmen

Het ‘eValg’ (vertaald ‘eVote’ of ‘eStem’) project is ondergebracht bij het ministerie van Local Government and Regional Development.
Het project heeft een stuurgroep die zich met name richt op verstrekken van resources, prioriteitstelling en bestuurlijk draagvlaak. Ook draagt zij zorg voor de externe audits en kwaliteitszorg. De externe quality assurance werd uitgevoerd door de firma DNV.

[100] De periode om per brief te stemmen liep van 1 juli tot 9 augustus voor kiezers woonachtig in Noorwegen, en van 1 juli tot 2 september voor kiezers buiten Noorwegen.

[101] Zie ook wetsvoorstel http://www.regjeringen.no/en/dep/krd/documents/white/prop/2012-2013/prop-52-l-20122013.html?id=709907

De projectgroep is verantwoordelijk voor de uitvoering van de experimenten en de verwerving van de stemdienst. De projectgroep ondersteunt de deelnemende gemeenten bij de uitvoering van de eVote experimenten. Zij legt verantwoording af aan de stuurgroep over de voortgang.

In de governance van het project zijn vier 'reference groups' opgenomen, die het project vanuit de invalshoek van politieke partijen, inhoudelijke experts, gemeenten en gebruikers begeleid en voorziet van adviezen.

9.2 Kiesgerechtigdheid

Het kiesrecht komt toe aan alle inwoners van Noorwegen die ouder zijn dan 18 jaar en die opgenomen zijn in het kiezersregister.

9.3 Aantal kiesgerechtigden en opkomst

Noorwegen kent ongeveer 3,5 miljoen kiesgerechtigde personen.

Bij de verkiezing in 2011 namen 10 gemeenten deel aan het experiment met internetstemmen. Van de 167.506 kiesgerechtigden brachten 28.001 kiezers hun stem uit via internet.

Bij de verkiezing in 2013 namen dezelfde 10 plus 2 nieuwe gemeenten deel aan het experiment met ongeveer 250.000 kiesgerechtigden. Bij die verkiezing heeft 36% van de kiezers in de twaalf deelnemende gemeenten gestemd via internet, 11% per brief en 53% in het stemlokaal. In totaal zijn 72.969 internetstemmen uitgebracht door 70.622 kiezers. Noot: het aantal stemmen is groter dan het aantal kiezers aangezien kiezers meerdere stemmen mochten uitbrengen.

Het percentage internetstemmen steeg van 16% naar 28% van de kiesgerechtigde inwoners van de deelnemende gemeenten.

9.4 Andere beschikbare stemmethoden

Kiezers in Noorwegen brengen normaliter hun stem uit bij een stembureau. De kiezer mag zijn stem uitbrengen bij elk stembureau in het land; de verkiezingsautoriteit draagt zorg voor de distributie van de uitgebrachte stem naar de gemeente waar de kiezer staat geregistreerd. Kiezers kunnen hun stem al enkele weken voorafgaand aan de dag van stemming uitbrengen tijdens een 'early voting' en een 'advance voting' periode. De stem kan dan worden uitgebracht bij een willekeurig gemeentehuis in het land. Op de dag van stemming zelf kan de kiezer alleen zijn stem uitbrengen in de gemeente waar hij is ingeschreven.

Kiezers buiten Noorwegen kunnen hun stem in persoon uitbrengen bij een ambassade of bij een aantal daartoe aangewezen stembureaus in het buitenland. De kiezer moet zich hierbij legitimeren. De door de kiezer ingeleverde stem wordt in een dubbele envelop per post naar de verkiezingsautoriteit in Noorwegen gestuurd. Kiezers die niet naar een ambassade kunnen komen mogen per brief stemmen.

9.5 Internet stemsysteem

De Noorse overheid is in 2010 een tender procedure gestart voor de verwerving van een internetstemsysteem. De tender is gewonnen door de firma Scytl Secure Electronic Voting SA. Bij de ontwikkeling van de stemdienst is intensief samengewerkt door de Noorse overheid, academische onderzoeksgroepen en Scytl.
Alle documentatie die in het kader van deze tender is ontvangen van leveranciers is vanuit het oogpunt van transparantie via internet[102] openbaar gemaakt, alsook alle latere technische documentatie.

Naast het internetstemsysteem wordt in Noorwegen één landelijk ICT administratief systeem ("EVA") gebruikt voor het kiezersregister, kandidatenlijsten, stemresultaten, etc.

9.6 Procesbeschrijving

9.6.1 Registratie van kiezers

In Noorwegen wordt de kiesgerechtigdheid afgeleid van de bevolkingsregistratie. Op grond hiervan wordt het kiezersregister gevuld.

Kiezers buiten Noorwegen zijn in de eerste tien jaar na hun vertrek uit Noorwegen nog ingeschreven in het kiezersregister van de gemeente waar zij laatstelijk stonden ingeschreven. Na tien jaar vervalt de inschrijving. Wil de kiezer daarna alsnog meedoen met de verkiezing, dan dient hij zich bij deze gemeenten opnieuw te laten registreren. Deze registratiehandeling kan ook worden uitgevoerd tijdens het stemmen zelf, door ondertekening van de retourenvelop van de briefstem. Hierbij is geen bewijs van de Noorse nationaliteit vereist, een verklaring is afdoende.

9.6.2 Stembescheiden

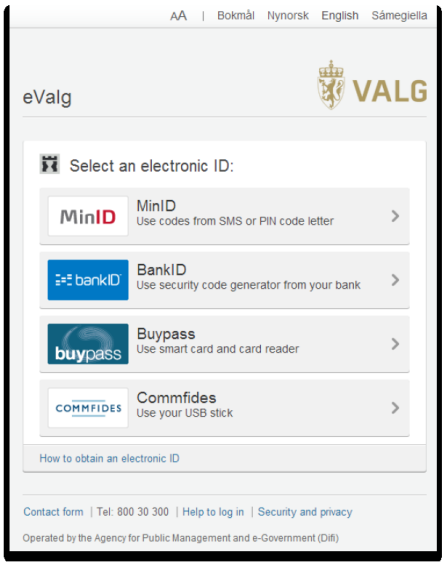
Als onderdeel van de stembescheiden ontvangt de kiezer, ruim voorafgaand aan de verkiezing, een stemkaart. Op deze stemkaart staan geen wachtwoorden, PIN codes of anderszins identificerende gegevens die de kiezer moet gebruiken om te kunnen stemmen. De identificatie geschiedt doordat de kiezer op de stemdienst inlogt met zijn elektronische ID die hij ook voor andere e-overheidsdiensten gebruikt. Daarnaast kunnen ook private e-IDs worden gebruikt.

9.6.3 Stemming

Voor de kiezer verloopt het uitbrengen van de stem als volgt:

1. Invoeren van de correcte URL ("evalg.stat.no") in zijn browser. De stemdienst verifieert of de computer en browser van kiezer aan de minimumeisen voldoet

[102] Zie https://brukerveiledning.valg.no/Dokumentasjon/Internettstemmegivning.aspx



2. Vervolgens selecteert de kiezer het elektronische ID middel waarmee hij zich wenst te authentiseren. In het Noorse internetstemsysteem kan gebruik gemaakt worden van MinID (een door de overheid uitgegeven elektronisch identificatiemiddel vergelijkbaar met Nederlandse DigiD), BankID (een elektronisch identificatiemiddel uitgegeven door banken in Noorwegen), Buypass en Commfides (een tweetal private e-ID oplossingen).
3. Het stemsysteem verifieert aan de hand van de identiteit van de kiezer of deze woont in éénn van de aan het experiment deelnemende gemeenten, en aan welke verkiezingen de kiezer kan deelnemen (in geval meerdere verkiezingen gecombineerd worden).
4. De kiezer stemt in twee stappen; eerst door een partij te selecteren, daarna door de rangorde van de kandidaten te bepalen. De partijen worden in willekeurige volgorde getoond op het scherm, deze volgorde wisselt per keer dat de kiezer inlogt. Naast het aanpassen van de rangorde van de kandidaten kan de kiezer ook kandidaten verwijderen van de lijst.
5. Na bevestiging van de keuze wordt de stem versleuteld en ondertekend met een elektronische handtekening.
6. De kiezer ontvangt een return code op zijn mobiele telefoon via SMS. Deze return code moet overeenkomen met de code (één voor elke partij) zoals gedrukt op de oproepingskaart. De codes verschillen per kiezer.
7. Indien gewenst kan de kiezer verifiëren dat zijn stem daadwerkelijk is opgenomen in de stembus.

9.6.4 Verificatie door kiezer

Het Noorse internetstemsysteem kent een tweetal verificatiemethodes voor de kiezer. De eerste methode maakt het mogelijk om te verifiëren dat de inhoud van de stem correct is ontvangen. Daarnaast kan de kiezer aldus vaststellen dat hij met ‘de echte’ stemdienst contact heeft. Na het uitbrengen van de stem ontving de kiezer een SMS bericht op zijn mobiele telefoon met een ‘return code’ en informatie over het aantal keren dat door hem is gestemd. De return code moet

overeenkomen met de informatie op de stemkaart. Los van dat deze methode door kiezers werd ervaren als maatregel om vertrouwen te krijgen in de juiste werking, werd deze verificatiemethode door de Noorse overheid juist ook gebruikt als indirecte methode om te kunnen detecteren of er op grote schaal computers van kiezers gemanipuleerd werden. In dit 'piep-systeem' is het wel noodzakelijk dat kiezers de return codes verifiëren. Echter, ook bij een klein percentage kiezers dat daadwerkelijk de verificatie doet kan met grote zekerheid worden bepaald of er manipulatie plaatsvindt.[103] In het 2011 experiment gaf 90% van de geënquêteerde kiezers aan de return codes geverifieerd te hebben.

De tweede methode maakt het mogelijk om te verifiëren dat alle ontvangen stemmen ook daadwerkelijk in de stembus zijn opgeslagen én dat alle stemmen in de stembus ook daadwerkelijk worden geteld. Deze verificatie kan zowel door kiezers, door de overheid als door onafhankelijke buitenstaanders worden uitgevoerd.
Hiertoe wordt, gedurende de verkiezingsperiode, elk uur de volledige inhoud van de stembus gepubliceerd[104] op het internet. De kiezer kan de hashwaarde van zijn versleutelde stem vergelijken met de lijst van alle ontvangen stemmen en zo verifiëren dat zijn stem is opgeslagen.

Daarnaast maakt het Noorse systeem het mogelijk om wiskundig te bewijzen dat de ontvangen stemmen correct zijn geteld.

9.6.5 Rol overige instanties

Het ministerie van 'Local Government and Regional Development' is verantwoordelijk voor de kieswetgeving in Noorwegen. De meer operationele kant van de uitvoering van een verkiezing ligt in handen van gemeenten. Voor het E-vote project heeft het ministerie een actievere rol op zich genomen bij het ontwerpen en verwerven van de stemdienst en bij het uitvoeren van de verkiezing.
De organisatie van de verkiezing is in handen van 'electoral bodies' (vgl met stembureaus) op drie niveaus: nationaal (alleen bij parlementsverkiezingen), provinciaal (18 electoral bodies) en gemeentelijk (428 electorial bodies en 3000 stembureaus). De electoral bodies vervullen verschillende taken op de drie niveaus: het tellen van de stemmen gebeurd op lokaal niveau, hierop wordt toegezien door de electoral body op provinciaal niveau etc.

Specifiek voor het internetstemmen is een Internet Election Committee in het leven geroepen. Dit bestaat uit 9 deskundigen die namens de gemeenten toezicht houden op de stemming en op het tellen van de stemming. Bij vermoeden van misstanden zijn zij gerechtigd de stemming te staken.

---

[103] Zie ook de ervaringen van de Noorse overheid met verifiable voting technologiën: http://www.e-voting.cc/wp-content/uploads/downloads/2012/07/21-33_Stenerud-Bull_Norway.pdf

[104] De versleutelde en ondertekende lijst van stemmen is gepubliceerd op https://github.com/KRD-KOMM-VL/evalg#!

De Noorse regering besloot bij aanvang van het E-vote 2011 project dat, gegeven de beperkte internationale ervaring met internetstemmen, de experimenten grondig geëvalueerd moesten worden door onafhankelijke externe partijen. Hiertoe werden met een tweetal onderzoeksgroepen een contract getekend: het Instituut voor Sociaal Onderzoek (ISF), in samenwerking met onder andere het Noorse Instituut voor Stedelijke en Regionale Onderzoek, Uni Rokkan Centrum , Universiteit van Oslo en het Noorse Computing Center. Zij hebben beoordeeld of het experiment effect had op de toegankelijkheid en opkomst, of de kiezers vertrouwen hadden in het experiment, wat de standpunten van politiek geïnteresseerde jongeren waren, de houding van de media en de houding van de kiezers. Het tweede onderzoek[105] werd uitgevoerd door de Internationale Stichting voor Electoral Systems (IFES) uit de Verenigde Staten.

9.6.6 Eigendom

De stemdienst is eigendom van de Noorse overheid. Leverancier Scytl is eigenaar van enkele patenten op delen van programmatuur die gebruikt is in de stemdienst, waarvoor zij een niet-exclusief levenslang gebruiksrecht hebben verstrekt aan de Noorse overheid.

9.6.7 Kosten

Onbekend.

9.6.8 Leerpunten uit evaluatie

Het gebruikte internetstemsysteem is door verschillende partijen en vanuit verschillende invalshoeken geëvalueerd in en na 2011 en 2013. Zo zijn er zijn diverse academische onderzoeken uitgevoerd, een broncode review op de implementatie van de gebruikte cryptografie[106] en onderzoeken naar het effect op de opkomst. Ook de OVSE heeft een waarnemersmissie gestuurd om de verkiezingen in Noorwegen te observeren. Daarnaast zijn er verificaties uitgevoerd van de correcte werking van de stemdienst, conform de ontwerpeigenschappen van de stemdienst. Onderstaand zijn enkele van de vele bevindingen opgenomen.
NB. van de in 2013 gebruikte stemdienst is nog geen evaluatierapport in het Engels verschenen.

9.6.9 Complexe productie van stemkaarten

In de evaluatie van het e-vote experiment in 2011 bleek dat de productie van de gepersonaliseerde stemkaarten met return-codes complex, foutgevoelig en kwetsbaar was. Om de kaarten te kunnen produceren zijn zowel de gegevens van de kiezers nodig, als ook de voor elke kiezer verschillende return-codes. Er zijn specifieke maatregelen getroffen om te voorkomen dat de overheid zelf, of de drukker, de beschikking heeft over de relatie tussen deze gegevens (dit zou immers het stemgeheim kunnen doorbreken). Hiervoor is zowel cryptografie ingezet als het in meerdere gescheiden stappen opdelen van het printproces. De massale productie van de 168.000

[105] http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/Speed-Efficiency-and-Compliance-an-Evaluation-of-E-Voting-in-Norway.aspx

[106] Zie Mnemonic Rapport Kildekodegjennomgang

stemkaarten verliep niet zonder problemen. Enkele kiezers ontvingen andere return-codes via SMS dan degenen die waren afgedrukt op de stemkaart. Volgende de Noorse overheid was er geen sprake van manipulatie, aangezien de return-code die de kiezers ontvingen niet overeenkwamen met een van de andere return codes op de kaart van de kiezer.
Bij de generatie van de bestanden die noodzakelijk waren voor het drukken van de stemkaarten ondervond de Noorse overheid verschillende problemen. Zo bleek dat enkele partijen niet waren meegenomen in de bestanden, waardoor deze opnieuw moesten worden gegenereerd. Echter door de bomaanslag op 22 juli 2011 waren de gebouwen van het ministerie waar de computers stonden om de bestanden te genereren tijdelijk ontoegankelijk. Uiteindelijk konden de bestanden pas enkele dagen voor de opening van de stemperiode worden gegenereerd. Het productieproces van de stemkaarten nam meer tijd in beslag dan verwacht, waardoor de opening van de stemming in een tweetal gemeenten enkele uren moest worden verschoven.

9.6.10 Cryptografisch sleutelmanagement

In het Noorse stemsysteem wordt uitvoerig gebruik gemaakt van cryptografie. Zowel ten behoeve van de versleuteling van de stem, als voor onderlinge identificatie van alle componenten van de internetstemdienst (signing certificaten). In de praktijk bleek het management van alle sleutelparen (15) zeer complex, zowel door de vereiste veilige opslag van de cryptografische sleutels en de bijbehorende wachtwoorden als de vereiste organisatorische taakscheiding om te waarborgen dat niemand zelfstandig toegang kon krijgen tot de sleutels.

9.6.11 Veiligheidsmaatregelen verkleinen de mogelijkheid om juiste werking vast te stellen

De vereiste beveiligingsmaatregelen maakte dat de flexibiliteit van de organisatie beperkt was, maar ook dat de mogelijkheden om te testen beperkt waren. Het was juist door het gebruik van alle cryptografische sleutels en andere veiligheidsmaatregelen (het systeem was zo ontwikkeld dat het onmogelijk was om een stem uit te brengen voorafgaand aan de stemperiode) niet mogelijk om met volledige zekerheid voorafgaand aan de stemming te bepalen of de stemdienst correct zou werken in de productiesituatie.

10 VERENIGD KONINKRIJK

10.1 Introductie

Het Verenigd Koninkrijk heeft tussen 2002 en 2007 meerdere e-voting experimenten gehouden. Dit waren niet alleen experimenten voor het gebruik van internetstemmen, maar ook andere vormen van moderne technologie zoals stemmen via de sms of via digitale tv.

10.1.1 Staatsinrichting en bestuur

Het Verenigd Koninkrijk is als een parlementaire monarchie ingericht. Uitzonderlijk aan het Verenigd Koninkrijk is dat het geen geschreven grondwet heeft, maar dat deze bestaat uit statuten, gewoonterecht en conventies. De koning/koningin heeft formeel veel macht, zo heeft hij/zij het recht het parlement bij elkaar te roepen en te ontbinden, het benoemen van de premier, de oorlog te verklaren aan andere landen en daarnaast ook verdragen te ondertekenen. Dit zijn formele rechten, al zal het niet snel gebeuren dat er tegen de wil van de gekozen regering in wordt gegaan.

Het parlement van het Verenigd Koninkrijk is opgedeeld in een Hoger- en Lagerhuis. De primaire taak van dit Hogerhuis is het herzien en corrigeren van wetten. Het Lagerhuis is de partij met de wetgevende macht in handen[107].

De landen binnen het Verenigd Koninkrijk hanteren ieder een eigen besturingsbestel. Zo heeft Engeland in totaal 9 bestuurlijke regio's, welke opgedeeld zijn in totaal 82 counties (graafschappen). Noord-Ierland is in districten opgedeeld, 26 in totaal. Schotland bestaat uit 32 raadsgebieden en Wales is daarnaast opgedeeld in 22 bestuurlijke gebieden[108]. Londen is een uitzondering op het besturingsbestel van Engeland. Londen bestaat momenteel uit 32 autonome ‘boroughs’ en uit 'de City of London'[109].

10.1.2 Historie internetstemmen

In het jaar 2000 begon het Verenigd Koninkrijk met een meerjaren traject waarin het uitvoerig experimenteerde met verschillende vormen van stemmen; stemmen via de telefoon/sms, stemmen via elektronische stemmachines, het gebruik van scanners maar ook internetstemmen. Dit werd mogelijk gemaakt door het aannemen van de 'The Representation of the People Act 2000'. Deze experimenten liepen door tot en met 2007, met uitzondering van het jaar 2001 en 2005 (destijds waren er geen lokale verkiezingen).

---

[107] http://www.stepstone.nl/content/NL/NL/career/CarriereadviesBuitenlandLandenprofielenVerenigdKoninkrijk.htm#Sociale situatie

[108] http://nl.wikipedia.org/wiki/Verenigd_Koninkrijk#Staatsstructuur

[109] http://www.landenweb.net/engeland/samenleving/

In 2007 heeft de Electoral Commission, na het uitvoeren van een aantal evaluaties de overheid aangeraden om te stoppen met het uitvoeren van e-voting experimenten. De belangrijkste argumentatie van de Electoral Commission was dat het geen zin heeft verder te gaan met de experimenten zolang er geen duidelijke strategie en toekomstvisie is voor het moderniseren van het verkiezingsproces. Zij bevestigde dat er veel geleerd was tijdens deze experimenten, maar dat zolang het niet duidelijk is welke weg de overheid wil inslaan het geen zin heeft nog meer experimenten te houden. Deze experimenten zijn op basis daarvan na 2007 stopgezet[110].

10.1.3 Organisatie internetstemmen

De Election Commission is een formele instantie opgezet door het parlement met als doel de verkiezingen en referendums goed te organiseren en deze soepel te laten verlopen. Dit doen zij door middel van het bieden van ondersteuning en advies. Ook zorgen zij ervoor dat kiezers alle benodigde informatie tot hun beschikking hebben om hun stem (op wat voor manier dan ook) te kunnen uitbrengen[111]. Deze partij is eveneens wettelijk verplicht om een evaluatie te doen van ieder e-voting experiment[112]. Daarnaast hebben de lokale overheden ook functionarissen die verantwoordelijkheid dragen voor de experimenten. Op basis van gepubliceerde evaluaties kan de conclusie getrokken worden dat de lokale functionarissen vaak het management samen met de leverancier in handen hebben.

10.2 Kiesgerechtigdheid

Wanneer een persoon 16 jaar of ouder is en de Britse of Ierse nationaliteit heeft, of wanneer een persoon een officiële burger van de 'Commonwealth' of Europa is en woonachtig is in het Verenigd Koninkrijk, dan mag men zich registreren om te stemmen. Pas vanaf 18 jaar kan men daadwerkelijke een stem uitbrengen[113].

10.3 Aantal kiesgerechtigden en opkomst

De volgende gemeenten hebben tijdens de experimenten in 2002 internetstemmen ingezet:

Locatie	Leverancier	Opkomst (% via internet)
Liverpool City Council	elections.com	1093 (16.4%)
Sheffield City Council	elections.com	2904 (22.1%)
St. Albans City & District	Oracle	825 (26.5%)
Crewe & Nantwich Borough Council	Oracle	364 (16.5%)

[110] http://www.edri.org/edrigram/number5.16/uk-electoral-report

[111] http://www.electoralcommission.org.uk/our-work/roles-and-responsibilities

[112] http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0015/13218/KeyfindingsandrecommendationssummarypaperE_N_S_W_.pdf

[113] http://www.aboutmyvote.co.uk/who_can_register_to_vote.aspx

Locatie	Leverancier	Opkomst (% via internet)
Swindon Borough Council	Votehere.net	4293 (10.8%)

De volgende gemeenten hebben tijdens de experimenten in 2003 internetstemmen ingezet:

Locatie	Leverancier
Stroud	Athena
Swindon	Athena
Kerrier	Opt2Vote/Athena
Vale Royale	Opt2Vote/Athena
Shrewsbury & Atcham	Opt2Vote/DRS/Athena
Stratford on Avon	Strand/Powervote/Athena
Ipswich	Unisys
Norwich	Unisys
Sheffield	Unisys
South Somerset	Unisys
St Albans	Unisys
Chorley	Unisys
Rushmoor	Unisys
South Tyneside	Unisys

Gemiddeld over alle deelnemende gemeenten heeft 12.6% van de kiezers zijn stem via het internet uitgebracht.

De volgende gemeenten hebben tijdens de experimenten in 2007 internetstemmen ingezet:

Locatie	Leverancier	Opkomst* (% via internet)
Rushmoor Borough Council	ES&S	3.827 (6.3%)
Sheffield City Council	Opt2Vote	7.647 (5.25%)
Shrewsbury & Atcham Borough Council	Opt2Vote	1.737 (4.3%
South Bucks District Council	ES&S	2.276 (16.3)
Swindon Borough Council	Tata Consultancy Services	7.647 (5.15%)

*Kiezers die gebruik hebben gemaakt van e-voting. In sommige gevallen hield dit ook telefonisch stemmen in.

Vanwege de verscheidenheid aan experimenten is er voor gekozen om in de rest van dit rapport alléén de experimenten uit het jaar 2007 te beschrijven. Op het internet zijn evaluaties van de eerdere experimenten te vinden.

10.3.1 Registratie van kiezers

Kiezers die wilden stemmen via internet dienden zich vooraf te registreren. De procedures hiervoor waren in iedere gemeente hetzelfde.

Om zich te registreren diende de kiezer een handtekening, geboortedatum en een zelf te kiezen wachtwoord op een formulier in te vullen. Dit wachtwoord moest bestaan uit zes-cijfers. Doordat steeds de term 'password' werd gebruikt vulde veel kiezers een woord in, waardoor de automatische verwerking in veel gevallen spaak liep. Het registratieformulier werd door de kiezers teruggezonden naar de lokale overheid en de informatie werd vervolgens in het registratiesysteem overgenomen. In sommige gemeenten gebeurde dit geautomatiseerd[114].

10.3.2 Stembescheiden

Ook de stembescheiden werden in de verschillende gemeenten op een vergelijkbare manier verstrekt. Wanneer het registratieproces was doorlopen kreeg de geregistreerde kiezer een stemkaart toegestuurd. Op deze stemkaart stond een uniek 'voter identification number' (VIN). Dit nummer was nodig om in te kunnen loggen in het onlinestemsysteem. Dit werd tezamen met de persoonlijke gegevens van de kiezers (opgeslagen in het registratiesysteem) als authenticatiemiddel gebruikt.

10.4 Internetstemsysteem - Rushmoor Borough Council en South Bucks District Council

10.4.1 Andere beschikbare stemmethoden

In Rushmoor Borough Council en South Bucks District was het ook mogelijk om via de post, op een stembureau, via de telefoon of via een volmacht te stemmen.

10.4.2 Internet stemsysteem

Tijdens de experimenten in Rushmoor Borough Council en South Bucks District Council is hetzelfde onlinestemsysteem gebruikt, ontwikkeld door Election Systems & Software. Het systeem werkte naar behoren. Van de 6.686 kiezers die zich registreerden, hebben 4.157 daadwerkelijk geprobeerd te stemmen, en 3.827 kiezers hebben succesvol een stem uitgebracht.

[114] http://www.umic.pt/images/stories/publicacoes1/Electronicvotingsummarypaper_27194-20114__E__N__S__W__.pdf

10.5 Procesbeschrijving

10.5.1 Stemming

1. De kiezer ging naar een bepaalde website. Deze staat weergegeven op de officiële stemkaart die de kiezers hadden ontvangen, maar ook op de officiële website van de verkiezingen.
2. De kiezer diende een willekeurige code (CAPTCHA) in te voeren, om geautomatiseerde inlogpogingen te voorkomen.
3. Vervolgens voerde de kiezer de VIN en zijn persoonlijke gegevens (gebruikersnaam en geboortedatum) in te voeren.
4. Wanneer de gegevens correct waren kreeg de kiezer vervolgens het stembiljet te zien en kan met de muis de juiste kandidaat aanvinken. Het systeem liet de gekozen nogmaals zien te bevestiging door de kiezer.
5. De stem werd verstuurd.

10.5.2 Verificatie door kiezer

Het systeem ontwikkeld door ES&S bood een optie om te controleren of de stem was aangekomen bij de server. Nadat de stem was verstuurd werd er een unieke ontvangstcode getoond aan de kiezer. Deze ontvangstcodes werden ook opgeslagen in de stembus. Na afloop van de verkiezing werden alle ontvangstcodes gepubliceerd, zodat de kiezer kon controleren dat zijn stem meegeteld was. De ontvangstcode was verder betekenisloos en bevatte geen informatie over de kiezer of over de kandidaat.

Voor meer informatie zie: “Technical Evaluation of Rushmoor Borough Council e-voting Pilot 2007” op de website http://www.electoralcommission.org.uk/

10.6 Internetstemsysteem - Sheffield City Council en Shrewsbury & Atcham Borough Council

10.6.1 Andere beschikbare stemmethoden

Het was ook mogelijk om een stem via de post, op een stembureau, via de telefoon/sms en via een volmacht uit te brengen in Sheffield City Council. In Shrewsbury & Atcham Borough Council boden zij dezelfde opties, behalve het stemmen via de sms.

10.6.2 Internet stemsysteem

Tijdens de experimenten in Sheffield City Council en Shrewsbury & Atcham Borough Council is hetzelfde internetstemsysteem gebruikt van Opt2Vote. Beide experimenten werden als succesvol geëvalueerd.

10.7 Procesbeschrijving

10.7.1 Stemming

1. De kiezer ging naar de volgende website: www.voteSheffield.com.
2. De kiezer logde in door het wachtwoord, de geboortedatum en de VIN in te voeren.

3. De kiezer kon aangeven voor welke verkiezing hij eerst een stem wil uitbrengen (indien van toepassing).
4. Iedere kandidaat had een 4-cijferig nummer toegewezen gekregen, welke ook op de stemkaart was geprint.
5. Nadat de kiezer het 4-cijferige nummer van zijn kandidaat had ingevoerd en de kiezer zijn stem heeft bevestigd, kwam er een pop-up met de naam van de geselecteerde kandidaat en de vraag of de kiezer de juiste kandidaat geselecteerd had. Wanneer de kiezer hier een bevestigend antwoord op gaf, werd de stem uitgebracht.

10.7.2 Verificatie door kiezer

Opt2Vote bood geen verificatieoptie om te controleren of de stem daadwerkelijk was aangekomen en meegeteld[115].

10.8 Internetstemsysteem - Swindon Borough Council

10.8.1 Andere beschikbare stemmethoden

Swindon Borough Council bood ook de mogelijkheid om via de post, telefonisch of op een stembureau een stem uit te brengen.

10.8.2 Internet stemsysteem

Tijdens de experimenten in Swindon Borough Council is het systeem van Tata Consulting Services gebruikt. Het systeem werkte naar behoren en er zijn geen grote problemen geconstateerd. 13.234 kiezers hadden zich laten registreren om via internet te stemmen. Slechts 7.647 kiezers brachten daadwerkelijk hun stem uit.

10.9 Procesbeschrijving

10.9.1 Stemming

1. De kiezer voerde op de website van het stembureau zijn Voter Identification Number in (die hij in een PIN mailer envelop thuis had ontvangen) en de overige persoonlijke gegevens (wachtwoord en geboortedatum).
2. De kiezers kon een gewenste taal selecteren (beperkte keuze).
3. De kiezer kon aangeven voor welke verkiezing hij eerst een stem wilde uitbrengen (indien van toepassing).
4. De kiezer kreeg vervolgens het stembiljet te zien en kon met de muis de juiste kandidaat aanvinken.
5. De kiezer werd om een bevestiging van de keuze gevraagd.
6. De stem werd definitief uitgebracht.

---

[115] http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0020/16193/Actica_Sheffield_27247-20138__E__N__S__W__.pdf

10.9.2 Verificatie door kiezer

Het systeem van Tata Consultancy Services bood de mogelijkheid om de bevestiging van de uitgebrachte stem uit te printen.

10.9.3 Rol overige instanties

Naast de Electoral Commission en de lokale overheden waren er ook andere partijen betrokken bij de experimenten. De 'Open Rights Group', onderdeel van European Digital Rights (EDRi), is een instantie die zich bezig houdt met het waarborgen van de vrijheid van meningsuiting, privacy, innovatie, creativiteit en de rechten van consumenten (op het internet). Zij hebben in 2007 tijdens de experimenten een groep van technische experts ingezet om evaluaties uit te voeren op de gebruikte systemen. Zij deelde de mening van de Electoral Commission, om de experimenten stop te zetten[116].

Ipsos MORI, een sociaal onderzoeksbureau, heeft op verzoek van de Electoral Commission een onderzoek uitgevoerd naar de houding van kiezers tegenover het stemmen via internet. Uit het rapport bleek dat de kiezer positief tegenover deze nieuwe stemmethodiek stond en een derde gaf aan dat men hierdoor getriggerd werd om een stem uit te brengen[117].

10.9.4 Beveiligingsmaatregelen

Uit het rapport van de Electoral Commission blijkt dat er weinig beveiligingsmaatregelen genomen zijn. De Electoral Commission geeft aan dat dit komt doordat kleine lokale overheden de middelen daarvoor niet hebben. Zij raden daarom de overheid aan te zorgen dat de onlinestemsystemen geaccrediteerd en gecertificeerd kunnen worden. Dit is benodigd om de systemen veiliger en betrouwbaarder te maken[118].

10.9.5 Eigendomsrechten

De verschillende systemen waren grotendeels intellectueel eigendom van de leveranciers[119].

10.9.6 Kosten:

Locatie	Kosten
Rushmoor Borough Council	£ 524.375.00
Sheffield City Council	£ 698.95.00

[116] https://www.openrightsgroup.org/blog/2007/org-welcomes-electoral-commission-recommendation-to-halt-experimenten

[117] http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0017/16109/MORIPublicopinionandthe2003electoralexperimentenchemes_10314-8349__E__N__S__W__.pdf

[118] http://www.umic.pt/images/stories/publicacoes1/Electronicvotingsummarypaper_27194-20114__E__N__S__W__.pdf

[119] http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic6_Assessment.pdf

Locatie	Kosten
Shrewsbury & Atcham Borough Council	£ 512.950
South Bucks District Council	£ 595.220
Swindon Borough Council	£ 1.126.636

*In deze kosten zitten ook de kosten voor het beschikbaar stellen van het stemmen via telefoon

10.9.7 Evaluatie:

Zoals aangegeven onder het kopje 'organisatie internetstemmen' is de Electoral Commission verplicht iedere afzonderlijk experiment te evalueren. Nadat alle experimenten in 2007 waren afgelopen heeft de Electoral Commission een aantal aanbevelingen gedaan aan de hand van de resultaten van deze evaluaties. De aanbevelingen zijn als volgt:

- Er zijn velen lessen geleerd tijdens de experimenten, maar de commissie ziet geen toegevoegde waarde in het houden van nog meer experimenten, en raden daarom aan te stoppen met de experimenten.
- Zij raden af enige experimenten te starten zonder dat er een duidelijk strategie voor de inzet van moderne technologieën in verkiezingen is gevormd.
- De commissie raadt aan minimaal een jaar te wachten met het starten van nieuwe experimenten. In deze tijd kan er een duidelijke strategie gevormd worden en is er genoeg tijd om hierover te debatteren. Ook wordt het personeel (betrokken bij deze experimenten) wat rust gegund.
- In de nieuwe strategie zou de overheid een duidelijk standpunt moeten innemen over de inzet van moderne technologieën in verkiezingen. Dus aangeven of dat zij willen dat stemmen via internet verplicht wordt, dat het optioneel is, of dat het helemaal niet meer ingezet zal gaan worden.
- De commissie raadt aan dat om het signeren, om een stembiljet in ontvangst te mogen nemen, te elimineren uit het proces, aangezien hier geen toegevoegde waarde ligt (zolang er geen gebruik wordt gemaakt van individuele registraties).
- De commissie raadt aan de leveranciers in kaart te brengen, op basis van de kwaliteit die zij leveren. Eveneens moeten de in kaart gebrachte issues opgelost worden (het ontbreken van een duidelijk toekomstplan met betrekking tot e-voting en het ontbreken van individuele registraties)[120].

120 http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0015/13218/Keyfindingsandrecommendationssummarypaper_27191-20111__E__N__S__W__.pdf

11 VERENIGDE STATEN VAN AMERIKA

11.1 Introductie

Het kiesrecht van Amerikaanse burgers en geüniformeerd personeel, zoals de krijgsmacht, is vastgelegd in een wet uit 1986, de '*Uniformed and Overseas citizens Absentee Voting Act (UOCAVA)*'. In potentie betreft dit ca. zes miljoen kiezers[121]. Deze wet legt de verantwoordelijk voor het mogelijk maken van stemmen voor deze groepen bij het ministerie van Defensie. Het ministerie heeft vervolgens een programma in het leven geroepen die uitvoering moet geven aan de wet, het '*Federal Voting Assistance Program (FVAP)*'.
De wetgeving beschrijft het gebruik van binnenlandse en buitenlandse postsystemen om te kunnen stemmen. Midden jaren '90 werd echter duidelijk dat stemmen via de post niet voldeed vanwege onbetrouwbaarheid en omdat veel stemmen niet tijdig werden ontvangen. In 1997 begon het FVAP de mogelijkheden van elektronisch stemmen te onderzoeken, wat heeft geleid tot een eerste experiment project in 2000, het project Voting Over the Internet (VOI).[122] [123] [124]

11.1.1 Staatsinrichting en bestuur

De Verenigde Staten is sinds 1776 een soevereine staat met als staatshoofd een president. Het is federatie van 50 staten en kent een sterke democratische traditie. De wetgevende macht ligt bij het Congres dat bestaat uit twee kamers, de Senaat (Senate) en het Huis van Afgevaardigden (*House of Representatives*). De Senaat telt twee leden van iedere staat en iedere twee jaar zijn er verkiezingen voor een derde van de Senaatszetels. Senatoren worden direct door de bevolking gekozen. Het Huis van Afgevaardigden bestaat uit 435 leden en wordt voor twee jaar gekozen.
De uitvoerende macht ligt bij de President. Deze wordt voor vier jaar gekozen in algemene verkiezingen via het systeem van kiesmannen (per staat naar rato van het aantal zetels in het Congres).[125]
In opmaat naar de presidentsverkiezingen worden door de grotere politieke partijen ook zogeheten *primaries* gehouden, verkiezingen die er toe dienen om een kandidaat te selecteren die namens de partij als kandidaat deelneemt aan de presidentsverkiezingen. Deze primary verkiezingen worden deels door de partij zelf georganiseerd (zgn. caucuses) maar ook door overheden.

11.1.2 Historie internetstemmen

Het 'Federal Voting Assistance Program (FVAP)' heeft bij de presidentsverkiezingen in 2000 een experiment gehouden met internetstemmen, het project 'Voting Over the Internet (VOI)'. Dit was het allereerste experiment met internetstemmen waarbij de uitslag meetelde voor de officiële

[121] http://en.wikipedia.org/wiki/Federal_Voting_Assistance_Program

[122] A Survey of Internet Voting, U.S. Election Assistance Commission, september 2011

[123] http://www.fvap.gov/global/index.html

[124] http://blog.usa.gov/post/35067724772/can-you-vote-online

[125] http://www.theusa.nl/bestuursamenleving/staatsinrichting.htm

uitslag. Een zeer kleine groep in het buitenland verblijvende militairen kon daarbij via internet stemmen.
Naar aanleiding van dit experiment, waarbij uiteindelijk 84 militairen een stem hebben uitgebracht via internet, heeft het Congres opdracht gegeven om het experiment te herhalen voor de presidentsverkiezingen van 2004 in een aantal counties in de staten Arkansas, Florida, Hawaii, Minnesota, Ohio, North, Carolina, South Carolina, Utah en Washington die zich op de verkiezingsdag in het buitenland bevonden. Voor dit experiment is een systeem ontwikkeld, het *'Secure Registration and Voting Experiment (SERVE)'*. Het experiment is uiteindelijk enkele maanden voor de verkiezing in 2004 stopgezet door de opdrachtgever, het ministerie van Defensie. In een verklaring werd destijds gesteld dat SERVE niet de legitimiteit van uitgebrachte stemmen kan garanderen en daarmee de integriteit van de verkiezingsuitslag in gevaar zou brengen. De kosten van het programma (SERVE) uit 2004 bedroegen $ 22 miljoen.[126]

Het eerstvolgende experiment met internetstemmen vond plaats tijdens de verkiezingen in 2010 in de staat West-Virginia. Ook hier betrof het de doelgroep kiezers in het buitenland. Het aantal kiezers dat meedeed was beperkt tot 125.
Een experiment in de staat Washington DC bij dezelfde verkiezing is vlak voor tijd afgelast nadat bleek dat deze was gehackt[127].

De discussie over de inzet van internet in het stemproces loopt nog altijd.[128]

11.2 Kiesgerechtigdheid

Om te mogen stemmen moet je een Amerikaans staatsburger zijn, minimaal 18 jaar en geregistreerd staan als kiezer. Er kunnen per staat afwijkende regelingen zijn, zoals een kiesgerechtigde leeftijd van 17 jaar.[129]

11.3 Aantal kiesgerechtigden en opkomst

Het totaal aantal kiesgerechtigden die onder de '*Uniformed and Overseas citizens Absentee Voting Act (UOCAVA)*' vallen betreft een groep met ca. zes miljoen potentiële kiezers.[130] De doelgroep van het SERVE project waren de kiezers die binnen de 55 deelnemende counties vielen, ca. 100.000.[131] Vanwege het annuleren van het project begin 2004 zijn er geen stemmen uitgebracht via het systeem.

---

[126] Kiezen op Afstand in het buitenland, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, april 2004

[127] Zie https://www.documentcloud.org/documents/322266-attacking-the-washington-d-c-internet-voting.html

[128] Zie bijvoorbeeld: http://usatoday30.usatoday.com/news/opinion/editorials/story/2012-09-19/electronic-voting-fraud-security/57809062/1 en https://freedom-to-tinker.com/blog/jeremyepstein/review-fvap-uocava-workshop/

[129] http://www.usa.gov/Citizen/Topics/Voting/Register.shtml

[130] http://en.wikipedia.org/wiki/Federal_Voting_Assistance_Program

[131] Analyzing Internet Voting Security, An extensive assessment of a proposed Internet-based voting system. Communications of the ACM, oktober 2004/Vol. 47, No. 10

Bij de verkiezing in West-Virginia in 2010 zijn 125 stemmen uitgebracht.

In de volgende paragrafen is het gebruikte stemsysteem van West-Virginia beschreven, aangezien dit het enige internetstemsysteem is dat daadwerkelijk gebruikt is in de Verenigde Staten van Amerika bij een officiële verkiezing.

11.4 Andere beschikbare stemmethoden

De kiezer had ook de optie om via de post zijn stem uit te brengen. Daarnaast participeerde West-Virginia ook in een ander project, waarbij er een stembiljet van het internet gedownload kon worden en deze of via de post, fax of mail opgestuurd kon worden.

11.5 Internet stemsysteem

Na een uitgebreid screeningsproces, uitgevoerd door de staat zelf, waren twee leveranciers geselecteerd welke bevoegd waren om de verschillende counties te voorzien van een internetstemsysteem. Dit waren Scytl en Everyone Counts. Zie hieronder een overzicht van de verschillende counties en de gebruikte internetsystemen:

Date	County	Technology Providers
5/11/2010	Kanawha	Everyone Counts
5/11/2010	Jackson	Scytl
5/11/2010	Marshall	Scytl
5/11/2010	Monongalia	Everyone Counts
5/11/2010	Wood	Everyone Counts
11/2/2010	Mason	Scytl
11/2/2010	Monroe	Everyone Counts
11/2/2010	Putnam	Everyone Counts

11.6 Procesbeschrijving

11.6.1 Registratie van kiezers

De kiezer diende zich vooraf te registreren om via internet te kunnen stemmen, door middel van een 'Federal Post Card Application (FPCA)' of een 'Electronic Voting Absentee Ballot Application'.

11.6.2 Stembescheiden

De kiezer ontving na de registratie een mail van de 'county clerk' of van de leverancier. In deze mail stond de link via welke de stem uitgebracht kon worden en een gebruikersnaam.

11.6.3 Stemming

De kiezer logde in op de website met de gegevens uit de mail. Vervolgens diende de kiezer de juiste stembiljetten te selecteren en zijn/haar keuze te maken. Voor de daadwerkelijke stemming diende de 'Cast Ballot' knop aangeklikt te worden.

11.6.4 Verificatie door kiezer

Na de stemming ontving de kiezer een 'receipt code'. Hiermee werd bevestigd dat de stem goed was aangekomen en juist was verwerkt. Met deze code kon het stembiljet niet meer ingezien worden. Wanneer de stem door het systeem werd geweigerd ontving men hier een bericht van.

11.6.5 Rol overige instanties

De staat West-Virginia zelf was verantwoordelijk voor de voorselectie van de leveranciers. Scytl en Everyone Counts waren beide leverancier van de gebruikte systemen. Zij hebben de software kosteloos aangeboden aan de staat, omdat zij op deze manier konden tonen welke mogelijkheden internetstemmen te bieden heeft.

11.6.6 Beveiligingsmaatregelen

Beide leveranciers waren vereist meerdere servers te installeren tijdens de verkiezing, zowel op locatie als op afstand. Op deze manier werd getracht het risico van het offline gaan van het onlinestemsysteem te minimaliseren. Ieder systeem gebruikte een 2048-bit encryptieprotocol en zij waren zo ontwikkeld dat zij voldeden aan de specifieke eisen die de staat had gesteld (met beide andere 'programming languages' en 'system design architectures').
Het systeem gebruikte separate versleutelings-en decoderingsalgoritmes, om zo sleutels te creëren die de link legden tussen de stem en de kiezer. Ook was afgesproken met de leverancier dat de data ontvangen of verstrekt door hun door zo min mogelijk mensen zou kunnen worden ingezien, én dat de mensen die de informatie wel mochten inzien waren verplicht een 'Confidentiality Statement' te ondertekenen. Eveneens werd er een kopie gemaakt van alle relevante informatie waarover de leveranciers beschikten. Deze werd overhandigd aan de Secretary of State voordat de informatie werd verwijderd.

11.6.7 Eigendom

De intellectuele eigendomsrechten behoorden in beide gevallen toe aan de leveranciers.

11.6.8 Kosten

De kosten waren voor de rekening van de leveranciers. Zij boden de software kosteloos aan om te tonen wat de mogelijkheden van internetstemmen zijn.

11.6.9 Evaluatie

De deelnemende counties hebben aangegeven geen problemen te hebben gehad met de internetstemsystemen. Toch heeft de 'Secretary of the State' aangegeven meer onderzoek te willen voordat het internetstemmen weer wordt toegestaan voor UOCAVA burgers. Er dient meer aandacht besteed te worden aan de risico's die aan internetstemmen verbonden zitten, aan de kosten en aan additionele beveiligingsmaatregelen. Ook heeft de 'Secretary of the State' geconstateerd dat de twee gebruikte systemen niet voldoen aan de 'Cryptographic Algorithm Validation Program (CAVP)', vastgesteld door het 'National Institute of Standards and Technology's (NIST)'. Ondanks dat dit geen verplichting is, is het voldoen aan deze standaard wel een voorkeur van de staat voor eventuele toekomstige experimenten.

12 ZWITSERLAND

12.1 Introductie

Sinds 1998 wordt in Zwitserland gewerkt aan de mogelijkheid om via internet te stemmen, als uitvloeisel van de nationale strategie voor een informatiesamenleving[132]. De mogelijkheid van 'Vote electronique' wordt geboden naast de mogelijkheden om in het stemlokaal en per post te stemmen. Stemmen per post is, in tegenstelling tot de situatie in Nederland, ook toegestaan voor kiezers binnen Zwitserland. De mogelijkheid om per post te stemmen is in 1984 gecreëerd en sindsdien stemt de meerderheid (90%) van de kiezers per post. In de stemlokalen wordt niet met stemcomputers gestemd. Na de introductie van internetstemmen is met name het aantal poststemmers iets afgenomen[133].

12.1.1 Staatsinrichting en bestuur

Zwitserland is een federale bondsstaat en republiek. Op federaal bondsniveau is er een wetgevende macht ("Bundesversamlung") bestaande uit een tweetal kamers: Nationalrat en Ständerat. Het bestuur is sterk decentraal ingericht met grote autonomie voor de kantons (26) en daarbinnen de gemeenten (2500). De kantons hebben een eigen regering en parlement ("Kantonsrat"), een eigen grondwet en eigen rechtspraak. Alles wat niet op grond van de grondwet is toebedeeld aan het federale bestuur valt onder de bevoegdheid van de kantons. Op het gebied van kieswetgeving zijn op federaal niveau minimale voorwaarden bepaald, waarbij de invulling in kiesprocedures verschilt per kanton.

Zwitserland kent een zogenaamde semi-directe democratie, waarin aan burgers de mogelijkheid toekomt om voor elke wet op elk niveau (gemeente, kanton, federaal) een referendum aan te vragen. Grondwetswijzigingen worden altijd middels een referendum voorgelegd aan de kiezer. Door dit systeem vinden vier tot zes keer per jaar verkiezingen / volksraadplegingen plaats.

12.1.2 Historie internetstemmen

In 2000 heeft het Zwitserse federale parlement een haalbaarheidsstudie laten uitvoeren naar de mogelijkheid van electronisch stemmen. Hiertoe is een samenwerking opgezet tussen de federale overheid en enkele kantons. De kantons verschillen onderling aanzienlijk in hun bestuurlijke en politieke inrichting en kennen afwijkende kieswetten en procedures / systemen voor verkiezingen. Om deze diversiteitsreden heeft Zwitserland er voor gekozen om, onder coördinatie van een landelijke projectorganisatie, meerdere internetstemsystemen te laten ontwikkelen in een drietal

---

[132] Zie "Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz 1998", http://www.bakom.admin.ch/themen/infosociety/00695/ Deze strategie is herijkt in 2006 en 2012.

[133] Zie o.a. "Analysis of the 26th September 2004 ballot as held in four Geneva municipalities" door het e-democracy center van de Universiteit van Genéve. Bij deze verkiezing werd 73 % van de stemmen uitgebracht per post, 21 % via internet en 6 % in een stemlokaal. In veel gemeenten zijn stembureaus slechts enkele uren open op de dag van stemming. Zie ook http://www.ge.ch/evoting/english/doc/rapports/rapport_26sept_english_final.pdf en

kantons: Genéve, Neuchâtel en Zürich. Het systeem uit Genève maakt gebruik van een centraal kiezersregister, aangezien de gemeenten binnen het kanton al onderling de bevolkingsregisters aan elkaar hadden gekoppeld. In Zürich voeren de gemeenten nog een separate bevolkings- en kiezersregistratie, waardoor daar ook een ander internetstemsysteem is ontwikkeld. In Neuchâtel is een ander systeem ontwikkeld, waarbij stemmen onderdeel is van een elektronische portaal ("Guichet Unique Neuchâtelois[134]") voor allerlei e-government diensten aan burgers.

12.1.3 Geleidelijke invoering

Sindsdien zijn vele experimenten uitgevoerd bij verkiezingen en referenda in zowel gemeenten, kantons als op federaal niveau. Vanuit de federale overheid zijn, gegeven het experimentele karakter, limieten gesteld aan het aantal kiezers dat per internet kan stemmen. Deze limiet lag in de eerste jaren op 10% van het totaal aantal Zwitsere kiesgerechtigden. Binnen sommige kantons is een 30% limiet van toepassing. Als gevolg van deze plafonds kunnen in totaal ongeveer 500.000 kiezers meedoen. Deze limiet wordt in de praktijk toegepast door specifieke gemeenten binnen specifieke kantons toestemming te geven om via internet te stemmen.
Per 1 januari 2008 is middels een referendum besloten om internetstemmen voor kiezers in het buitenland een wettelijke basis te geven en de experimentele fase te verlengen. Sindsdien wordt gewerkt aan een stapsgewijze invoering en doorontwikkeling, zowel op federaal als kantonaal niveau. Op 19 juni 2013 is een routekaart gepubliceerd waarbij ook de limieten stap voor stap worden opgevoerd, van 10 naar 30%, van 30% naar 50% en uiteindelijk naar 100%. In deze routekaart worden ook prioritaire doelgroepen benoemd, zoals kiezers buiten Zwitserland en gehandicapten. Voor deze doelgroepen is per 2012 de limiet in het aantal kiezers dat per internet mag stemmen opgeheven[135].

De limieten zijn bedoeld om een gecontroleerde uitbreiding van deze nieuwe manier van stemmen te introduceren in het land en om de valkuilen te vermijden van te snel en te weinig voorbereid uitrollen van nieuwe technologieën.

Eind 2013 is internetstemmen ingevoerd in 13 van de 26 kantons. Bij de meest recente verkiezingen (Referendum op 22 september 2013) waren er 158.500 stemgerechtigden (inclusief kiesgerechtigde Zwitsers in het buitenland). Van de kiezers die stemden, stemde meer dan 50% van de kiezers via internet.[136]

---

[134] Zie https://www.guichetunique.ch/public/

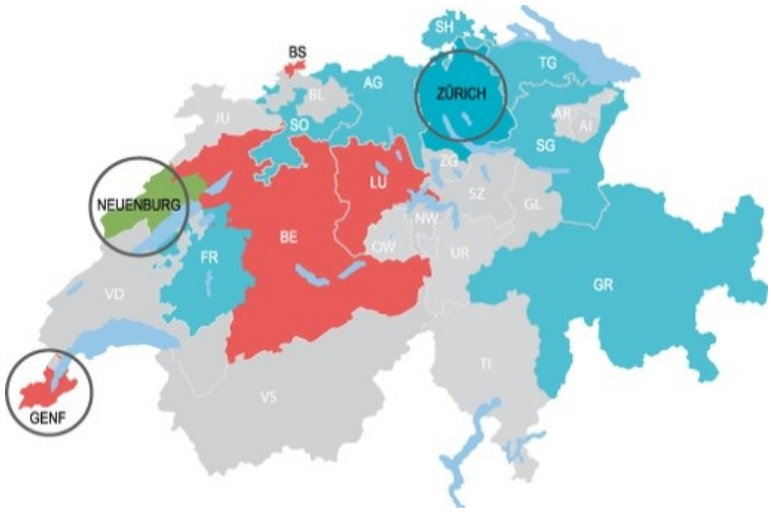
[135] Wel is het internetstemmen voorbehouden aan Zwitsers woonachtig in landen die het Wassenaar Arrangement hebben ondertekend. Deze landen staan het gebruik van specifieke cryptografische technologie toe die gebruikt wordt in de internetstemsystemen. zie ook http://www.wassenaar.org/

[136] Zie http://www.bk.admin.ch/themen/pore/evoting/00773/

12.1.4 Drie internetstemsystemen

Op dit moment zijn er drie internetstemsystemen beschikbaar die in drie kantons zijn ontwikkeld: Genève, Neuchâtel en Zürich. Andere kantons hebben de mogelijkheid om gebruik te maken van één van deze internetstemdiensten, of om (op eigen kosten) een eigen internetstemdienst te ontwikkelen. De kantons van Basel, Bern en Luzern hebben de uitvoering van internetstemmen in handen gegeven van het kanton Genéve.

In onderstaand figuur (status 2011) is aangegeven welke kantons gebruik maken van welk internetstemsysteem: Rood: Genéve, Blauw: Zürich, Groen: Neuchâtel. In de volgende paragrafen wordt gefocust op de systemen uit Genève en Zürich. Door de kleinschaligheid waarop het systeem uit Neuchâtel wordt toegepast, wordt deze buiten beschouwing gelaten.



12.1.5 Organisatie internetstemmen

Op federaal niveau is er een projectorganisatie ingericht binnen de Sektion Politische Rechte[137] van de Bundeskanzlei. Daarnaast zijn projectorganisaties actief binnen de kantons.

De federale projectorganisatie kent een landelijke stuurgroep “Steuerungsauschuss Vote électronique” die bestaat uit vertegenwoordigers van de federale en kantonale overheden, onder voorzitterschap van de bondskanselier. De projectorganisatie kent daarnaast een begeleidingsgroep die is samengesteld uit vertegenwoordigers de Confederatie en de kantons. Zij adviseert de projectgroep elektronisch stemmen in operationele en technische kwesties. Daarnaast is er een werkgroep waarin informatie en "best practices" tussen kantons wordt uitgewisseld.

[137] Zie http://www.bk.admin.ch/themen/pore/evoting/index.html?lang=de

12.2 Zwitserland – KANTON GENÈVE

In 2001 is het Geneva internet voting project gestart. In de periode 2002 tot en met 2005 zijn testen uitgevoerd en in 2003, 2004 en 2005 is de mogelijkheid van internetstemmen ('eEnabled' genaamd) geboden aan kiezers in meerdere gemeentelijke referenda. De uitslag van de uitgebrachte internetstemmen telden bindend mee voor de uitslag.
Vanaf 2009 werd het ook mogelijk voor kiezers die in het buitenland wonen om deel te nemen aan de verkiezing via een eEnabled verkiezing. In de jaren daarna zijn ook Bern, Luzern, Obwalden en Uri samen gaan werken met het Geneefse kanton om voor verkiezingen in hun kanton gebruik te kunnen maken van dezelfde internetstemtechnologie.

In 2011 is de mogelijkheid van internetstemmen voor het eerst geboden bij een nationale verkiezing, in 2012 was de eerste verkiezing voor een heel kanton.

12.3 Kiesgerechtigdheid

Alle personen met de Zwitserse nationaliteit die ouder zijn dan 18 jaar en die wonen in Genève zijn kiesgerechtigd voor verkiezingen binnen het kanton. Voor gemeentelijke stemmingen dient de kiezer minimaal drie maanden in de gemeente te wonen.
Sommige[138] personen met de Zwitserse nationaliteit die ouder zijn dan 18 jaar en die in het buitenland wonen zijn kiesgerechtigd voor federale (nationale) verkiezingen. Daarnaast kunnen kantons aanvullende rechten geven voor verkiezingen binnen het kanton. Zo maakt het kanton Genève het mogelijk voor kiezers buiten Zwitserland om deel te nemen aan de verkiezingen binnen het kanton, na registratie bij het Zwitserse consulaat in het land waar zij woonachtig zijn.

Buitenlanders die minimaal 8 jaar woonachtig zijn in Zwitserland zijn kiesgerechtigd voor gemeentelijke verkiezingen en referenda van de gemeente waarin zijn wonen.

12.4 Aantal kiesgerechtigden en opkomst

Doordat het Geneva Internet voting systeem meerdere verschillende soorten verkiezingen en referenda is gebruikt binnen diverse gemeenten en het kanton varieert het aantal kiesgerechtigden per verkiezing. De eerste toepassing in 2003 was voor een paar duizend kiezers, de grootste verkiezing was op 15 mei 2011 met 241.780 kiezers die via internet konden stemmen.

Van het totaal aantal uitgebrachte stemmen wordt ongeveer 15 - 20% uitgebracht via internet. Van de kiezers die vanuit het buitenland stemmen, stemt ongeveer 45% via het internet.

Op deze locatie: http://www.ge.ch/evoting/doc/list_of_GVA_ballots.pdf is een volledig overzicht beschikbaar van elk gehouden experiment, referendum en verkiezing sinds 2003 met het aantal kiesgerechtigden, het aantal kiezers dat via internet heeft gestemd als percentage van het totaal

[138] Alleen Zwitsers die wonen in de Europese Unie of in landen die het Wassenaar verdrag hebben geratificeerd

aantal stemmen en het deel van de stemmen van kiezers buiten Zwitserland dat via internet heeft gestemd.

12.5 Andere beschikbare stemmethoden

Kiezers in Genève hebben de beschikking over drie methoden om te stemmen: in een stembureau, per post of via internet. Stemmen bij onderhandse volmacht is verboden en strafbaar.

12.6 Internetstemsysteem

Het internetstemsysteem wordt “Geneva Internet Voting system” genoemd. Het is in eigen beheer ontwikkeld door het kanton Genéve. Naar eigen zeggen is 85% van de software open source software, de rest is eigendom van het kanton.

12.7 Procesbeschrijving

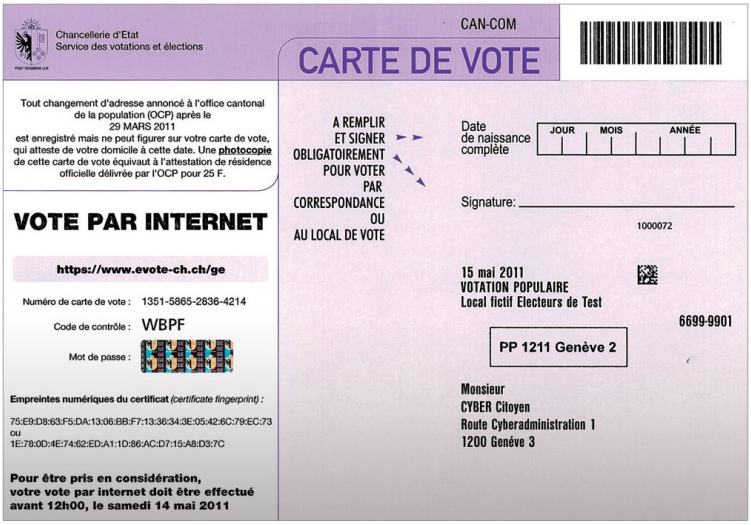
12.7.1 Registratie van kiezers

In het kanton Genève wonende kiezers hoeven zich niet vooraf te registreren om te kunnen stemmen. Alle kiesgerechtigde personen zijn opgenomen in de bevolkingsadministratie van de gemeenten binnen het kanton. Acht weken voorafgaand aan de stemming worden op basis van de bevolkingsadministratie de stembescheiden geproduceerd.

Kiezers buiten Zwitserland kunnen zich *in persoon* registreren bij de Zwitserse diplomatieke vertegenwoordiging (ambassade of consulaat) in het land waar zij verblijven. Zij moeten een inschrijfformulier invullen, waarbij ze naast de eigen persoonsgegevens ook de persoonsgegevens van hun vader en moeder opgeven. De Zwitserse ambassade stuurt het inschrijfformulier door aan de dienst “Stemmen en verkiezingen” van het kanton Genève. Na ontvangst van de aanvraag voor registratie registreert het kanton de persoon in haar kiezersregister, mits de persoon niet nog is ingeschreven in het register van een andere gemeente. De registratie is geldig voor 4 jaar, na die tijd wordt de registratie verwijderd (tenzij deze tussentijds is geactualiseerd).

12.7.2 Stembescheiden

De kiezer ontvang een stemkaart per reguliere post. Een voorbeeld is hieronder afgebeeld. Deze stemkaart kan ook gebruikt worden voor het stemmen in een stembureau en stemmen per post. Op de stemkaart staat een uniek, specifiek voor die verkiezing gegenereerd, stemkaart nummer ter identificatie van de kiezer. Om te stemmen voert de kiezer deze code in, alsook een drietal gedeelde ‘geheimen’: een wachtwoord, de geboortedatum en de ‘gemeente van afkomst’. De ‘gemeente van afkomst’ staat ook op het ID bewijs en paspoort.



12.7.3 Stemming

De kiezer brengt de stem uit via de website https://www.evote-ch.ch/

Het stemmen verloopt in een aantal stappen:
1. Invoeren van 16 cijferige stemkaart-nummer: “Numéro de carte de vote”.
2. Accepteren van juridische bepalingen (waaronder het verbod op volmachtstemmen).
3. Stemmen op stembiljet.
Bij een referendum bestaat de keuze uit Oui of Non. In een stemming kunnen meerdere referenda van verschillende niveaus (kanton, federaal, etc.) worden gecombineerd. Bij een verkiezing kiest de kiezer een lijst van kandidaten, maar kan ook zijn eigen lijst van kandidaten samenstellen.
4. Controleer de controle code. Op het scherm wordt een controle code getoond die overeen dient te komen met de ‘Code de controle’ op de stemkaart (‘WBPF’ in bovenstaand voorbeeld). Dit ter bevestiging dat de kiezer daadwerkelijk stemt op de website van Genève .
5. Invoeren wachtwoord (“Mot de passe”, afgedrukt op stemkaart onder hologram/kraslaag) , geboortedatum en ‘gemeente van afkomst’.
6. Uitbrengen van de stem.

Een demonstratie versie van het stemsysteem is beschikbaar via:
http://www.ge.ch/evoting/demo/en/demo_evoting_Genève_en.asp

12.7.4 Verificatie door kiezer

De huidige versie (najaar 2013) van het internetstemsysteem kent geen verificatiemogelijkheid voor de kiezer om te verifiëren of zijn stem (correct) is meegeteld.
In de routekaart voor de verdere ontwikkeling van het internetstemsysteem is deze mogelijkheid opgenomen voor 2014.

12.7.5 Rol overige instanties

Zwitserland heeft bij wet een Service de Votations et Elections' / CEC (Central Electoral Commission) ingesteld. Zij vervullen zowel een operationele taak (in de versleuteling en ontsleuteling van de stembus) als een onafhankelijke toezichtstaak.
In het beveiligingsconcept van het internetstemsysteem is een nadrukkelijke scheiding van taken en rollen tussen verschillende organisaties en personen opgenomen.
Dit begint bij de initialisatie van het internetstemsysteem en het verzegelen van de elektronische stembus voorafgaand aan de stemming. Voor deze stappen zijn zeven partijen benodigd: een vertegenwoordiger van de kanselarij, vier vertegenwoordigers van de 'Service de Votations et Elections' / CEC (Central Electoral Commission), een vertegenwoordiger van de Voting and Elections Department, een notaris, een IT security officer van de politie, de netwerkbeheerder van het internetstemsysteem en de systeembeheerder van het internetstemsysteem.
Deze partijen zijn ook gezamenlijk nodig om de stembus te ontcijferen.

12.7.6 Beveiligingsmaatregelen

Op deze pagina is meer informatie te vinden over de opzet van het internetstemsysteem:
http://www.ge.ch/evoting/english/doc/Uncovering_the_veil.pdf

Een paar van de opvallende beveiligingsmaatregelen:

- Authenticatie van de kiezer op basis van gedeeld geheim. De kiezer ontvangt per post een stemkaart met daarop een tweetal unieke gegevens, daarnaast voert de kiezer een tweetal gegevens in die bij de overheid reeds bekend zijn (geboortedatum en gemeenteplaats van afkomst).
- In alle stappen van het stemproces zijn meerdere personen van meerdere organisaties vereist (zie boven), voor zowel toegang tot het stemsysteem, voor de generatie van cryptografische sleutels, voor het initialiseren van de stemdienst, het verzegelen van de stembus en het tellen van de stemmen.
- De CEC is gerechtigd om teststemmen uit te brengen. Deze teststemmen worden zowel uitgebracht voorafgaand aan de stemming, alsook tijdens de stemming. Tijdens de stemming brengt de CEC stemmen uit binnen een eigen kiesdistrict, welke zij ook vastlegt op papier. Na stemopneming worden de stemmen op het eigen kiesdistrict vergeleken met de papieren stemmen.
- De stemdienst zet een secure channel op tussen webclient en stemdienst, door gebruik te maken van TLS. Hiermee wordt een wederzijdse authenticatie bewerkstelligd. Het hiervoor benodigde certificaat aan de webclient zijde wordt door de evoting java applet gegenereerd op basis van het voting card nummer.
- Aanvullend op SSL / TLS encryptie wordt ook de inhoud van de uitgewisselde berichten versleuteld ('overencryptie').
- De stemdienst controleert de syntax van ontvangen stembiljetten, om de integriteit van de stembus te bewaken door te voorkomen dat onjuiste berichten / code wordt verwerkt.
- De stemdienst genereert een vier-letterige controle code, welke ook afgedrukt staat op de stemkaart. De kiezer kan hiermee controleren dat hij met de echte stemdienst contact heeft.

- Voorafgaand aan het tellen van de stemmen worden de stemmen elektronisch 'door elkaar geschud' om te voorkomen dat er een relatie gelegd kan worden tussen de stem en een kiezer op basis van de volgorde van binnenkomst.
- Met cryptografische algoritmes wordt bewerkstelligd dat de versleutelde waarde van een stem van een specifieke kiezer bij elke versleuteling anders is. Dit te voorkoming van een Rainbow Table aanval.
- Het stemkaartnummer is een versleutelde waarde van de werkelijke identificatie van een kiezer.

12.7.7 Eigendom

De overheid is houder van alle intellectuele eigendomsrechten van het Geneva Internet Voting systeem en is verantwoordelijk voor de productie, het beheer en de doorontwikkeling. Het is een expliciete keuze om alles in eigendom te houden (en niet als product of dienst in te kopen / huren) omdat dit 'de legitimiteit van de verkiezing' vergroot.

12.7.8 Kosten

Het kanton Genève heeft 1,7 mln CHF (€ 1,36 mln) uitgegeven aan ontwikkelingskosten van de stemdienst. Een groot deel daarvan (1,4 mln CHF) is gefinancierd met een bijdrage van de federale overheid.
In haar evaluatie rapport[139] stelt het kanton dat de kosten van het houden van een verkiezing 880.000 CHF bedragen (voor briefstemmen en stembureaus). De meerkosten voor het bieden van internetstemmen bedraagt 69.000 CHF per verkiezing.

12.8 Zwitserland – KANTON Zürich

12.9 Kiesgerechtigdheid

Gelijk aan de beschrijving onder het kanton Genève .

12.10 Aantal kiesgerechtigden en opkomst

Bij de eerste experimenten in de periode 2004-2006 waren ongeveer 17.000 inwoners van drie gemeenten gerechtigd om via internet te stemmen, zij vertegenwoordigen ongeveer 2% van het totaal aantal kiesgerechtigden binnen het kanton.
In de tweede testfase in de periode 2008-2011 waren 88.000 kiezers in dertien gemeenten gerechtigd om te stemmen. Gedurende de acht verkiezingen in die periode schommelde het percentage kiezers dat op internet stemde tussen de 20% en 27% van het totaal aantal uitgebrachte stemmen. Gemiddeld werd in die periode 65% van de stemmen per brief uitgebracht, en de rest in een stemlokaal.

[139] State Council Report RD 639 Zie pagina 27 e.v. www.ge.ch/evoting/english/doc/rapports/EN_RD_639_and_Annex.pdf

Bij de verkiezing op 26 september 2010 konden voor het eerst ook kiezers die in het buitenland verbleven via internet stemmen. Het betrof hier kiezers uit de stad Zürich. De opkomst van de 7.090 kiesgerechtigden bedroeg 2.048 (29%), hiervan stemde 52% via internet, en 48% per brief.

12.11 Andere beschikbare stemmethoden

In Zürich kon zowel op een stembureau een stem worden uitgebracht, als via de post en de telefoon.

12.12 Internetstemsysteem

Het systeem is in opdracht van het kanton ontwikkeld door de firma Unisys. Hierbij zijn gedurende de twee fasen aanpassingen en verbeteringen doorgevoerd. In de eerste fase bood het systeem de mogelijkheid om ook per SMS te stemmen. In de doorontwikkeling van het systeem in de tweede fase is die mogelijkheid vervallen.

12.13 Procesbeschrijving

12.13.1 Registratie van kiezers

De kiezer die woonden in de dertien gemeenten binnen het kanton Zürich hoefden zich niet vooraf te registreren om te kunnen stemmen. Rond zeven weken voorafgaand aan de dag van stemming wordt de kiesgerechtigdheid vastgesteld op basis van de bevolkingsadministraties van de deelnemende gemeenten binnen het kanton. Een aantal weken voorafgaand aan de stemming wordt aan de kiezers een stemkaart “stimmrechtsausweis” toegestuurd.

Kiezers buiten Zwitserland kunnen zich *in persoon* registreren bij de Zwitserse diplomatieke vertegenwoordiging (ambassade of consulaat) in het land waar zij verblijven. Zij moeten een inschrijfformulier invullen, waarbij ze naast de eigen persoonsgegevens ook de persoonsgegevens van hun vader en moeder opgeven. De Zwitserse ambassade stuurt het inschrijfformulier door aan de gemeenten binnen het kanton Zürich. Na ontvangst van de aanvraag voor registratie registreert het kanton de persoon haar kiezersregister, mits de persoon niet nog is ingeschreven in het register van een andere gemeente. De registratie is geldig voor 4 jaar, na die tijd wordt de registratie verwijderd (tenzij deze tussentijds is geactualiseerd).
Kiezers in het buitenland kunnen alleen internetstemmen als hun gemeente op het e-voting systeem is aangesloten. Van de 171 gemeenten in het kanton waren 13 aangesloten (in de fase 2008-2011). Van de ongeveer 16.000 kiezers in het buitenland zijn 10.000 afkomstig uit de 13 deelnemende gemeenten.

12.13.2 Stembescheiden

De kiezer ontvangt per reguliere post een stimmrechtsausweis die gebruikt kan worden voor zowel stemmen via internet als stemmen in een stemlokaal. Onderstaand een voorbeeld van de stemkaart die de gemeente Uster heeft gebruikt:

Op de kaart staat een aantal gegevens die de kiezer in dient te voeren in de website van de stemdienst: een User ID (‘A4DF5Q3B’ in bovenstaand voorbeeld en een PIN code (‘A3RTW7B2’ in bovenstaand voorbeeld). De PIN code is afgeschermd met een kraslaag onder een afscheurbare papieren klepje. Op de kaart is ook een controlesymbool gedrukt (hond in bovenstaand voorbeeld), waarmee de kiezer kan verifiëren of hij verbinding heeft met de echte stemdienst. Indien een kiezer in een stemlokaal aankomt met een stimmrechtsausweis waarvan de kraslaag is opengekrast, dan wordt aangenomen dat de kiezer al via internet heeft gestemd of dat heeft geprobeerd.

12.13.3 Stemming

De kiezer kan in een periode van ongeveer 4 weken tot aan de zaterdag 12:00 uur voorafgaand aan de dag van stemming (zondag) zijn stem uitbrengen via de website (https://www.evoting.zh.ch/)
De keuze om de periode van internetstemmen te laten plaatsvinden voorafgaand aan de dag van stemming is ingegeven om bij eventuele uitval van het internetstemsysteem de kiezers de mogelijkheid te geven om alsnog de stem uit te brengen in het stemlokaal.
NB dit betreft het systeem dat gebruikt is bij de tweede fase van experimenten.

Een demoversie is beschikbaar via http://eVotingdemo.zh.ch

Het stemmen verloopt in een aantal stappen:
1. Invoeren van User ID.
2. Maken van keuze door aanvinken op stembiljet op het scherm.
3. Verifiëren van het controle symbool op het scherm met het controle symbool op de stemkaart.
4. Invoeren van geboortedatum.
5. Invoeren PIN code.
6. Uitbrengen van de stem.

Op de stimmrechtsausweis zijn twee controlegegevens afgedrukt die de kiezer kan gebruiken om te controleren of hij met de echte stemdienst verbinding heeft: de 'vingerafdruk' van het SSL certificaat van de stemdienst en het grafische symbool (afbeeldingen van dieren) dat niet voor elke kiezer gelijk is (en overeen moet komen met hetgeen op het scherm wordt getoond).

12.13.4 Verificatie door kiezer

De huidige versie van het internetstemsysteem kent geen verificatiemogelijkheid voor de kiezer om te verifiëren of zijn stem (correct) is meegeteld.
In de eerste fase kende het internetstemsysteem ook de mogelijkheid van stemmen per SMS. In die variant werd wel gebruik gemaakt van retourcodes. In de praktijk bleek het invoeren van de codes voor veel kiezers ingewikkeld en daardoor foutgevoelig te zijn, waardoor deze mogelijkheid is komen te vervallen.

12.13.5 Rol overige instanties

Zwitserland heeft bij wet een Service de Votations et Elections' / CEC (Central Electoral Commission) ingesteld. Zij vervullen zowel een operationele taak (in de versleuteling en ontsleuteling van de stembus) als een onafhankelijke toezichtstaak.

12.13.6 Eigendom

Het eigendom van het internetstemsysteem is in handen van het kanton Zürich. Zij heeft een niet-exclusief en niet-overdraagbaar recht van gebruik op de software verstrekt aan zeven andere kantons (kostenloos). Alle overige kosten gemoeid met de infrastructuur, personeel alsook onderhoud van de software zijn voor rekening van de andere kantons. In tegenstelling tot het kanton Genève levert het kanton Zürich geen diensten aan de andere kantons, de kantons zijn zelf verantwoordelijk voor het functioneren van het systeem. Deze kantons hebben een onderhoudsovereenkomst gesloten met dezelfde leverancier (Unisys).

12.13.7 Kosten

Naar opgave van het kanton[140] bedroegen de uitgaven voor de experimenten in de periode 2004-2006 7,9 mln. CHF (€ 6,3 mln.) voor het kanton en 0.5 mln. CHF voor de drie gemeenten. In het 'tussenjaar' 2007 (waarin geen verkiezingen plaatsvonden) waren de uitgaven 0,7 mln. CHF voor exploitatie en onderhoud. In de tweede fase 2008-2011 bedroegen de uitgaven 2,5 mln. CHF, exclusief personele kosten aan de kant van de gemeenten en kanton.
Inclusief personele kosten heeft het kanton ongeveer 10 mln. CHF uitgegeven in de hele periode 2004 tot 2011. De 10 mln. CHF is inclusief een bijdrage van 2,3 mln. CHF van de federale overheid in ruil voor het beschikbaar stellen van het internetstemsysteem aan andere geïnteresseerde

[140] Evaluation der E-Voting Testphase im kanton Zürich 2008-2011
http://data.rrb.zh.ch/appl/rrbzhch.nsf/0/C12574C2002FAA1FC1257942004EB439/$file/Evaluation_E-Voting_Z%C3%BCrich.pdf

kantons. Hiertoe is in 2009 een consortium gevormd van zeven andere kantons die met een kopie van het Zürich internetstemsysteem aan de slag zijn gegaan. Deze zeven kantons gebruiken het systeem alleen voor kiezers in het buitenland, waarbij de eerste stemming in september 2010 plaatsvond.
In het evaluatierapport uit 2011 is een begroting opgenomen voor de noodzakelijke aanpassingen en voor de exploitatie en onderhoud van het stemsysteem voor de jaren 2012 – 2014. De voorziene extra kosten zijn 2.1 mln. CHF voor toepassing in alle gemeenten in het kanton. De prijs per stem bedraagt dan 18 CHF op basis van 120.000 kiezers. Indien internetstemmen ook aan alle in het buitenland woonachtige Zwitsers uit het kanton wordt aangeboden zijn de voorziene extra kosten 4.1 mln. CHF (24 CHF per stem op basis van 174.000 kiezers).

12.13.8 Evaluatie

In November 2011 is een evaluatierapportage [141]verschenen van de tweede fase van experimenten. Daarin wordt geconstateerd dat de stemdienst naar behoren heeft gefunctioneerd en er geen grote beveiligingsincidenten hebben plaatsgevonden. Wel zijn er meerdere storingen geweest:

- Onbeschikbaarheid van de stemdienst gedurende enkele uren door onjuiste firewall instelling.
- Drukfouten in een batch van 4000 stemkaarten, waardoor de pin code onleesbaar was. Deze kiezers konden niet via internet stemmen.
- Drukfouten in een batch van 140 stemkaarten waarbij de kraslaag niet over de pin code maar over het retouradres werd aangebracht. Individuele gevallen waar de pin code niet meer leesbaar is, of waar de afscheurklep vastgeplakt zit aan de kraslaag.
- De stemdienst kon met sommige browserversies niet worden bereikt.
- Een gemeente maakte het resultaat van de stemming bekend, zonder daarbij de via internet uitgebrachte stemmen mee te tellen. Men was vergeten om de resultaten van de internetstemming handmatig in te voeren in het systeem van de uitslagen.
- Bij een burgemeestersverkiezing in 2010 kon via het internetstemsysteem alleen op de zittende kandidaat worden gestemd.
- Veel van de kiezersregister blijken fouten te bevatten, waaronder onjuiste geboortedata van kiezers in het buitenland. Hierdoor kunnen meerdere kiezers niet stemmen.

12.13.9 Aanbevelingen

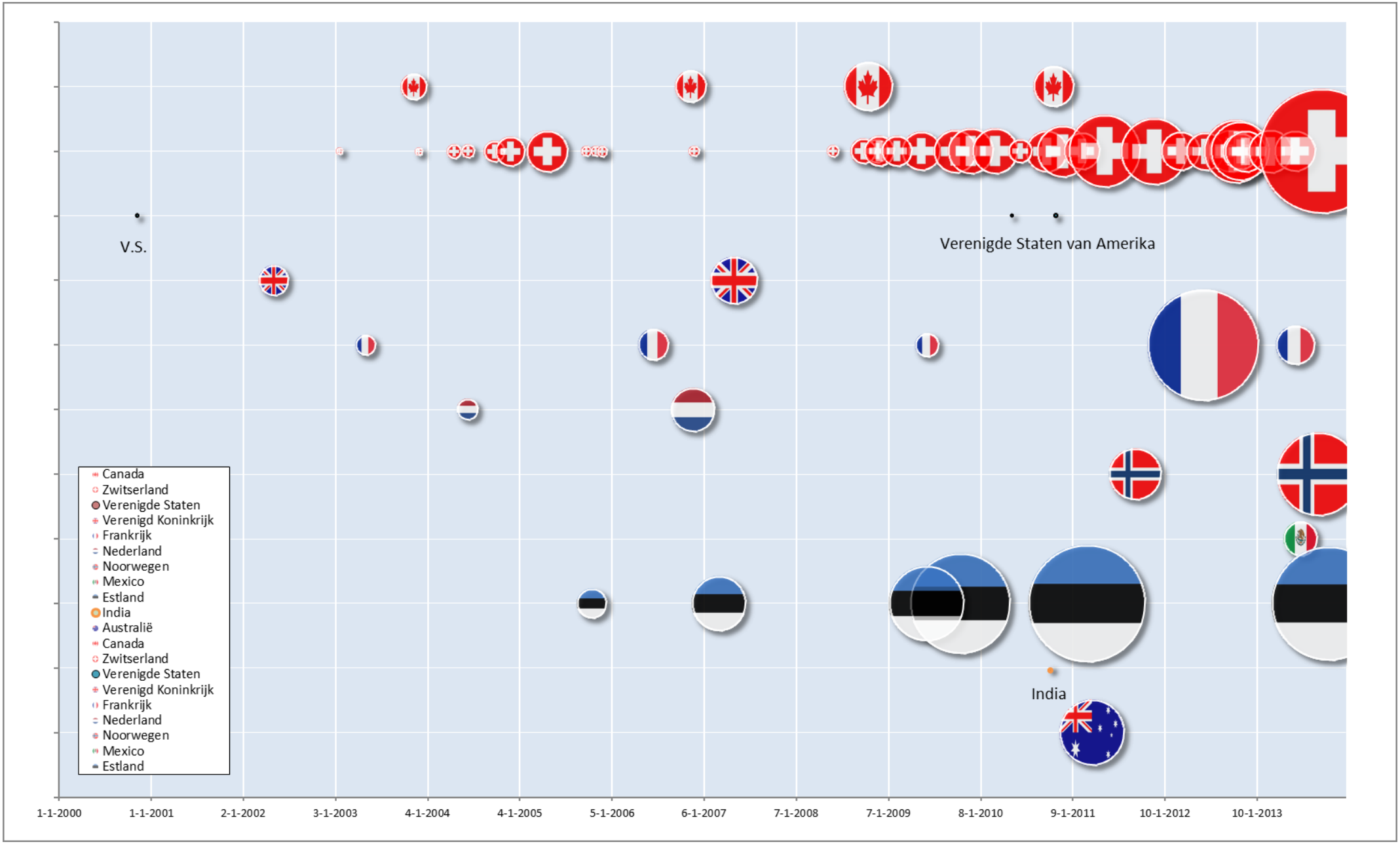
In de evaluatie is geconstateerd dat de volgende verbeteringen noodzakelijk zijn voor toekomstige internetstemsysteem:

1. Van decentraal stemregister naar centraal stemregister. De huidige decentrale opzet van de stemregisters bij de gemeenten vergt een aanzienlijke inspanning doordat naar elk stemregister een interfaces gebouwd en onderhouden moet worden.

[141] Zie http://data.rrb.zh.ch/appl/rrbzhch.nsf/0/C12574C2002FAA1FC1257942004EB439/%24file/Evaluation_E-Voting_Z%C3%BCrich.pdf?OpenElement In bijlage 7 (p 73 en 74) zijn incidenten beschreven.

2. Gebruik van het elektronische portaal ‘ZH-Services’ voor communicatie tussen overheid en burger, als oplossing voor de praktische problemen bij het drukken, personaliseren en per post versturen van de stembescheiden.
3. Doorvoeren van nieuwe technologische innovaties op het gebied van informatiebeveiliging om beter bestand te zijn tegen aanvallen.
4. Het juist functioneren van het systeem moet verifieerbaar zijn.
5. Functionele verbeteringen om alle soorten stemmingen / referenda aan te kunnen.

A Bijlage: Historisch overzicht internetstemmen


V.S.
Verenigde Staten van Amerika
India
Canada
Zwitserland
Verenigde Staten
Verenigd Koninkrijk
Frankrijk
Nederland
Noorwegen
Mexico
Estland
India
Australië
Canada
Zwitserland
Verenigde Staten
Verenigd Koninkrijk
Frankrijk
Nederland
Noorwegen
Mexico
Estland
1-1-2000
1-1-2001
2-1-2002
3-1-2003
4-1-2004
4-1-2005
5-1-2006
6-1-2007
7-1-2008
7-1-2009
8-1-2010
9-1-2011
10-1-2012
10-1-2013

B Bijlage: Bronnen

B1. Australië

Jaar	Titel	Organisatie / Auteur	Toelichting
2006	International Experiences of Electronic Voting and Their Implications for New South Wales	Associate Professor Rodney Smith Department of Government and International Relations University of Sydney	Rapport in opdracht van NSWEC over internationale ervaringen
23-7-2010	Report on the Feasibility of providing "iVote" Remote Electronic Voting System	NSW Electoral Commission	Haalbaarheidsonderzoek naar elektronische stemmen op afstand voor blinden- en slechtzienden en andere personen met een handicap
7-3-2011	Technology Assisted Voting Audit, Pre Implementation Report	PWC	Audit rapportage iVote systeem voorafgaand aan State Election van 26 maart 2011
21-6-2011	Technology Assisted Voting Audit, Post Implementation Report	PWC	Audit rapportage iVote systeem na afloop van State Election van 26 maart 2011
11-7-2011	Evaluation of technology assisted voting provided at the New South Wales State General Election March 2011	Allen Consulting Group	Evaluatierapport met uitgebreide statistische analyse en gedrag van kiezers bij State Election van 26 maart 2011
25-8-2011	iVote Technology Assisted Voting	Ian Brightwell, NSWEC	Presentatie over toepassing i-vote bij State Election van 26 maart 2011
15-10-2012	e-voting: the promise and the practice	Brenton Holmes, Politics and Public Administration Section Parliament of Australia	Overzichtsrapport over toepassing van elektronisch stemmen (waaronder internetstemmen)
8-2013	iVote Strategy for the NSW State General Election 2015	Ian Brightwell, NSWEC	Rapport met plannen voor de toepassing van i-vote bij de State Election in 2015
10-9-2013	Internet voting in Australian election systems	Australian Electoral Commission in opdracht van Electoral Council of Australia and New Zealand (ECANZ)	Onderzoek naar mogelijkheden om internetstemmen breder in te zetten in Australië

B2. Canada

Jaar	Titel	Organisatie / Auteur	Toelichting
2-2010	A comparative Assessment of Electronic Voting	Carleton University, Nicole Goodman, et al	Rapport opgesteld in opdracht van de Canada-Europe Transatlantic Dialogue voor Elections Canada en behandelt internationale ervaringen met internetstemmen ervaringen met internetstemmen binnen Canada
2010	Internet Voting: The Canadian Municipal Experience	Nicole Goodman, et al	Artikel gebaseerd op rapport " A comparative Assessment of Electronic Voting"
26-1-2010	Markham's Online Voting Experience	Kimberley Kitteringham, Town Clerk Markham & Andrew Brouwer, Deputy Town Clerk	Presentatie tijdens Workshop over Internet Voting met ervaringen uit Markham uit 2006
1-2010	HRM's Experience with Electronic Voting	Cathy Mellett, Halifax Regional Municipality	Presentatie tijdens Workshop over Internet Voting met ervaringen uit Halifax
8-2011	Discussion Paper: Internet Voting	Elections BC	Rapport over internetstemmen uitgebracht door de organisatie die verantwoordelijk is voor de verkiezingen in de staat British Columbia
11-2012	Issues Guide:Internet Voting	Nicole Goodman	Rapport met kwesties internetstemmen in opdracht van The Centre for Public Involvement, University of Alberta
13-11-2012	Markham Votes 2014 -Internet Voting Program	Stephen Huycke, Acting Deputy Clerk Teodor Tecsa,	Presentatie voor de gemeenteraad om instemming te krijgen voor toepassing internetstemmen bij verkiezingen in 2014
23-10-2013	Preliminary Report	Independent Panel on Internet Voting, ingesteld door Chief Electoral Officer op verzoek van minister van Justitie	Rapport waarin risico's van internet stemmen worden beschouwd, met als conclusie dat experimenten voor specifieke doelgroepen aanvaardbaar zijn, maar geen brede implementatie in de hele provincie. Rapport wordt gebruikt als basis voor een publieke consultatie (af te ronden in december 2013). Zie http://www.internetvotingpanel.ca/

B3. Estland

Jaar	Titel	Organisatie / Auteur	Toelichting
2005	Overview E-voting system	National Election Committee	Rapport met technische en organisatorisch overzicht van internetstemsysteem,

Jaar	Titel	Organisatie / Auteur	Toelichting
			te gebruiken bij de verkiezingen in 2005
1-2005	E-voting pilot in Tallinn	National Election Committee	Presentatie met resultaten eerste pilot internetstemmen
2006	Internet Voting at the Elections of Local Government Councils on October 2005	Ülle Madise, Priit Vinkel, Epp Maaten	Overzicht van internetstemsysteem, projectmatige voorbereidingen en analyse resultaten bij gemeenteraadsverkiezing in 2005
6-3-2006	E-Voting in the 2005 local elections in Estonia	Fabian Breuer and Alexander H. Trechsel, European University Institute	Rapport met resultaten van onderzoek onder kiezers bij verkiezingen in 2005
2007	Practical Security Analysis of E-voting Systems	Ahto Buldas, Triinu Mägi	Onderzoek naar beveiliging van internetstemsysteem Estland in vergelijking met SERVE systeem (USA)
28-6-2007	OSCE/ODIHR Election Assessment Mission Report	OSCE / OVSE	Rapport van waarnemersmissie OVSE bij parlementsverkiezingen in 2007
31-7-2007	Internet voting in the March 2007 Parliamentary Elections in Estonia	Alexander H. Trechsel, Director of the European Union Democracy Observatory (EUDO), Robert Schuman Centre for Advanced Studies, European University Institute, Florence	Rapport in opdracht van Raad van Europa met resultaten van een onderzoek onder kiezers in Estland die deelnamen aan de Parlementsverkiezing in maart 2007
1-2010	Internet Voting in Estonia, A Comparative Analysis of Four Elections since 2005	Alexander H. Trechsel, Director of the European Union Democracy Observatory (EUDO), Robert Schuman Centre for Advanced Studies, European University Institute, Florence	Vergelijkend onderzoek naar gedrag en voorkeur onder kiezers in Estland
27-12-2010	E-voting concept security: analysis and measures. EH-02-02	National Electoral Committee	Risico-analyse en set van maatregelen opgesteld in opdracht van de National Election Committee . Is geactualiseerde versie van document uit 2003
2011	The Application of I-voting for Estonian Parliamentary Elections of 2011	Sven Heiberg, Peeter Laud en Jan Willemson	Overzicht van internetstemsysteem en analyse van gebeurtenissen tijdens Riigikogu Elections in 2011.
16-5-2011	OSCE/ODIHR Election Assessment Mission Report	OSCE / OVSE	Rapport van waarnemersmissie OVSE bij parlementsverkiezingen in 2011
10-2011	Internet Voting in Estonia, A Comparative Analysis of Five Elections since 2005	Alexander H. Trechsel, Director of the European Union Democracy Observatory (EUDO), Robert Schuman Centre for Advanced Studies, European University Institute, Florence	Vergelijkend onderzoek naar de toepassing van internetstemmen bij vijf verkiezingen in Estland
7-2013	What is Verification of I-votes	Vabariigi Valimiskomisjon (National Election Committee)	Presentatie met uitleg verificatiesysteem voor kiezers

B4. Frankrijk

Jaar	Titel	Organisatie / Auteur	Toelichting
10-9-2012	OSCE/ODIHR Election Assessment Mission Final Report	OSCE / OVSE	Rapport van waarnemersmissie OVSE bij parlementsverkiezingen in 2012
14-6-2006	Ceci n'est pas une urne, On the Internet vote for the Assembl´ee des Franc¸ais de l''etranger	Andrew Appel	Artikel waarin auteur zijn ervaringen als waarnemer bij de verkiezingen in 2006 beschrijft
17-7-2011	Décret no 2011-843 du 15 juillet 2011 relatif à l'élection de députés par les Français établis hors de France	JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE	Wet waarin internetstemmen voor kiezers buiten Frankrijk wordt geregeld
1-6-2011	Dossier de Presse	Parti Pirate	Dossier opgesteld door Franse politieke groepering 'Le Parti Pirate', een tegenstander van internetstemmen.

B5. India

Jaar	Titel	Organisatie / Auteur	Toelichting
	Online Voting Brochure	State Election Commission Gujarat	Handleiding voor kiezers voor registratie en gebruik Online Voting System
	Account Activation Manual	Tata Consulting Services	Handleiding voor kiezers voor registratie en activering account
	Online Voting System State	Tata Consulting Services	Presentatie met overzicht stappen internetstemsysteem
6-11-2013	Information on Internet Voting Projects	Scytl	Toelichting referentieproject India door leverancier Scytl
18-6-2010	Gujarat ready to click take first step in evoting	Indian Express	Nieuwsartikel over toepassing internetstemmen. http://www.indianexpress.com/news/gujarat-ready-to-click-take-first-step-in-evoting/635417/
10-10-2010	Gujarat civic elections witness first ever online voting	New Delhi Television	Nieuwsartikel over toepassing internetstemmen. http://www.ndtv.com/article/cities/gujarat-civic-elections-witness-first-ever-

Jaar	Titel	Organisatie / Auteur	Toelichting
			online-voting-58739
23-7-2011	E-voting for IT land	Business Standard	Nieuwsartikel over toepassing internetstemmen. http://www.business-standard.com/article/beyond-business/e-voting-for-it-land-111072300044_1.html

B6. Mexico

Jaar	Titel	Organisatie / Auteur	Toelichting
6-11-2013	Information on Internet Voting Projects	Scytl	Toelichting referentieproject India door leverancier Scytl

B7. Noorwegen

Jaar	Titel	Organisatie / Auteur	Toelichting
2-2006	Electronic voting – challenges and opportunities		Eindrapport onderzoekscommissie die haalbaarheidsstudie heeft verricht naar mogelijkheden voor internetstemmen
8-9-2013	Safety first! Verifiability in the Norwegian e-voting system	C. Bull, Ministry of Local Government and Regional Development	Presentatie over transparantie en verificatie door kiezer in Noorse internetstemsysteem
2012	When Reality Comes Knocking Norwegian Experiences with Verifiable Electronic Voting	I. Stenerud, C. Bull	Artikel met praktijkervaringen toepassing van internetstemmen in Noorse verkiezing in 2011.
1-2013	Internet Voting in Norway 2011: Democratic and Organisational Experiences	Harald Baldersheim, University of Oslo. Jo Saglie, Signe Bock Segaard, Institute for Social Research, Oslo	Engelstalig samenvatting van evaluatie rapport zoals gepresenteerd tijdens de 4th International Conference on Democracy as Idea and Practice
7-2012	Cast as intended in Norway	Scytl	Presentatie met voorstel voor verificatie methodiek voor kiezers
28-6-2012	Noorse Kieswet, Act No 57 van 28 juni 2012		Engelse vertaling van Noorse Kieswet

Jaar	Titel	Organisatie / Auteur	Toelichting
26-8-2013	Election Manual, overview of election rules	Ministry of Local Government and Regional Development	Uitgebreide handleiding met instructies en verwijzingen naar wetsartikelen voor leden van stembureaus
7-8-2013	Technical report Source code audit of Norwegian electronic voting system	Tor E. Bjørstad, Mnemonic	Broncode review in opdracht van Ministry of Local Government and Regional Development
2012	E-val I demokratisk perpektiv, Sluttrapport. 2012:5	Signe Bock Segaard, Harald Baldersheim og Jo Saglie, Institute for samfunnsforskning	Noors evaluatierapport
6-2012	Evote International Experience	Jordi Barrat i Esteve, Ben Goldsmith and John Turner, International Foundation for Electoral Systems (IFES)	Onderzoek naar internationale ervaringen met internetstemmen i.o.v. Ministry of Local Government and Regional Development
6-2012	Compliance with International Standards	Jordi Barrat i Esteve, Ben Goldsmith and John Turner, International Foundation for Electoral Systems (IFES)	Onderzoek naar mate waarin Noorse internetstemsysteem voldoet aan internationale standaarden
6-2012	Speed and Efficiency of the vote counting process	Jordi Barrat i Esteve, Ben Goldsmith and John Turner, International Foundation for Electoral Systems (IFES)	Onderzoek naar verschil in snelheid, efficientie en kwaliteit van tellen van stemmen in gemeenten waar internetstemmen was toegepast bij verkiezing in 2011
26-5-2004	Use of electronic media for voting in elections to the storting, county councils and municipal councils	Ministry of Local Government and Regional Development	Mandaat van werkgroep die onderzoek deed naar invoering internetstemmen
2-12-2011	Information Report on the test on E-voting in the framework of local elections in Norway on 12 September 2011	The Congress of Local and Regional Authorities, Raad van Europa	Verslag bezoek aan Noorwegen
2005	Observing electronic voting	Kåre Vollan, Norwegian Centre for Human Rights/NORDEM	Rapport met beschrijving van kwesties rondom waarnemingsmissies bij elektronische verkiezingen
2-3-2012	INTERNET VOTING PILOT PROJECT LOCAL GOVERNMENT ELECTIONS OSCE/ODIHR Election Expert Team Report	OSCE / OVSE	Rapport van waarnemersmissie OVSE bij parlementsverkiezingen in 2011
1-2-2011	Project mandate for e-vote 2011-project	Ministry of Local Government and Regional Development	Projectplan
14-12-2012	Prop. 52 L. Endringer i valgloven og kommuneloven (statlig	Ministry of Local Government and Regional Development	Wetsvoorstel aanpassingen Noorse kieswet ivm internetstemmen

Jaar	Titel	Organisatie / Auteur	Toelichting
	ansvar for manntall, nye prosedyrer ved forhåndsstemmegivning mv.		
25-9-2009	e-Vote 2011 Security Objectives	Ministry of Local Government and Regional Development	Eisen beveiliging internetstemsysteem
15-4-2013	eValg2011 platform. Update for 2013 Parliamentary elections. Electronic Voting Software Security Target EAL 4+	Scytl	Rapport met beschrijving beveiligingsdomein Internetstemsysteem
9-3-2010	Analysis of an internet voting protocol	Kristian Gjsteen	Technische beschrijving Noorse aanpassing op protocol

B8. Verenigd Koninkrijk

Jaar	Titel	Organisatie / Auteur	Toelichting
8-2007	Electronic voting May 2007 electoral pilot schemes	The Electoral Commission	Samenvatting van bevindingen van pilots internetstemmen en telefonisch stemmen bij verkiezingen in 2007
31-7-2007	Technical Evaluation of Rushmoor Borough Council e-voting Pilot 2007	Attica Consulting	Evaluatierapport Rushmoor Borough Council
30-7-2007	Technical Evaluation of Shrewsbury and Atcham Borough Council e-voting Pilot 2007	Attica Consulting	Evaluatierapport Shrewsbury and Atcham Borough Council
30-7-2007	Technical Evaluation of Sheffield City Council e-voting Pilot 2007	Attica Consulting	Evaluatierapport Sheffield City Council
31-7-2007	Technical Evaluation of Swindon Borough Council e-voting Pilot 2007	Attica Consulting	Evaluatierapport Swindon Borough Council
2007	Local elections pilot schemes 2007 main research report	Martin Boon (ICM Research), Professor John Curtice (University of Strathclyde), Sebastian Martin (Black Box Research) in opdracht van The Electoral Commission	Evaluatie rapport met bevindingen van pilots internetstemmen en telefonisch stemmen bij verkiezingen in 2007

B9. Verenigde Staten van Amerika

Jaar	Titel	Organisatie / Auteur	Toelichting
14-7-2011	Update on U.S. Demo Internet Voting Project	David Beirne, Federal Voting Assistance Program (FVAP), Department of Defense	
21-1-2004	A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)	David Jefferson, Dr. Aviel D. Rubin, Dr. Barbara Simons, David Wagner	Rapport van de Security Peer Review Group naar de beveiliging van het internstemsysteem SERVE, bedoeld voor gebruik bij de 2004 verkiezingen
10-2004	ANALYZING INTERNET VOTING SECURITY, An extensive assessment of a proposed Internet-based voting system.	David Jefferson, Dr. Aviel D. Rubin, Dr. Barbara Simons, David Wagner	Artikel over beveiliging SERVE systeem, verschenen in COMMUNICATIONS OF THE ACM October 2004/Vol. 47, No. 10
16-9-2010	Evote 2010	Election Assistance Commission	Presentatie gegeven tijdens OVSE Seminar over ontwikkelingen op gebied van verkiezingen in V.S.
19-1-2011	Legislative Report, West Virginia Uniformed Services and Overseas Citizen Online Voting Pilot Project	Natalie E. Tennant, West Virginia Secretary of State	Korte evaluatie van toepassing internetstemmen in West-Virginia
	Secure Electronic Registration and Voting Experiment	Federal Voting Assistance Program (FVAP), Department of Defense	Beschrijving project methodologie van SERVE systeem. http://www.fvap.gov/resources/media/serve.pdf
14-9-2011	A Survey of Internet voting	US Election Assistance Commission	Internationaal overzicht internetstemsystemen
6-2001	Voting Over the Internet Pilot Project Assessment Report	Federal Voting Assistance Program (FVAP), Department of Defense	Beschrijving project toepassing internetstemmen voor militairen bij verkiezingen in november 2000

B10. Zwitserland

Jaar	Titel	Organisatie / Auteur	Toelichting
2-4-2013	Rapport du Conseil d'Etat au Grand Conseil sur l'audit triennal du système genevois de vote électronique	Secrétariat du Grand Conseil	Audit rapportage internetstemsysteem Geneve, inclusief broncode review en technische analyse
8-2011	Ein Gemeinschaftsprojekt vom Bund und den Kantonen	Schweizerische Eidgenossenschaft, Bundeskanzlei BK	Informatiebrochure internetstemmen
3-2012	Strategie des Bundesrates für eine Informationsgesellschaft	Schweizerische Eidgenossenschaft, departement für Umwelt,	Geactualiseerde E-government strategie Zwitserse federale overheid

Jaar	Titel	Organisatie / Auteur	Toelichting
	in der Schweiz	Verkehr, Energie und Kommunikation UVEK	
3-2009	Three Case Studies from Switzerland:E-Voting. Berkman Center Research Publication No. 2009-03.1 at Harvard	Jan Gerlach and Urs Gasser, Berkman Center	Case study beschrijving
18-2-1998	Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz	Schweizerischen Bundesrates	E-government strategie Zwitserse federale overheid uit 1998
30-1-2012	SWISS CONFEDERATION FEDERAL ASSEMBLY ELECTIONS 23 October 2011 OSCE/ODIHR Election Assessment Mission Report	OSCE / OVSE	Rapport van waarnemersmissie OVSE bij Federale Assemblee verkiezingen in 2011
3-2013	Strategische Planung Vote électronique – "Roadmap plus" (2013-2018)	Schweizerische Eidgenossenschaft, Bundeskanzlei BK	Meerjarenstrategie internetstemmen
7-2007	State Council's Report to the Grand Council on the Geneva electronic voting project	State Chancellery , REPUBLIC AND CANTON OF GENEVA	Engelse vertaling van officiele rapport van Geneefse regering aan Geneefse parlement over internetstemmen bij verkiezing in 2006
3-2013	The geneva internet voting project	State Chancellery , REPUBLIC AND CANTON OF GENEVA	Folder over internetstemsysteem en -project
2006	Success Factors of Geneva's e-Voting System	Chevallier M, Warynski M and Sandoz A. Verschenen in The Electronic Journal of e-Government Volume 4 Issue 2, pp 55 - 62, available online at www.ejeg.com	Rapport over internetstemsysteem, succesfactoren en profiel van de kiezers
2013	List of all eEnabled official ballots conducted in Geneva since the start of the internet voting project	State Chancellery , REPUBLIC AND CANTON OF GENEVA	Overzicht van alle verkiezingen waarin internetstemmen is toegepast
7-2005	Analysis of the 26th September 2004 ballot as held in four Geneva municipalities (Anières, Carouge, Cologny and Meyrin)	Thomas Christin (Universities of St. Gall, Zurich and Toronto) and Prof. Dr Alexander H. Trechsel (Geneva University and European University Institute, Florence (Italy)	Onderzoek onder kiezers naar beweegredenen van kiezers en effect van internetstemmen
	Uncovering the veil on Geneva's internet voting solution	State Chancellery of Geneva Information Technology Centre of the State of Geneva	Technische beschrijving van stemprotocol
19-6-2013	Canton de Neuchâtel - Statistique du mode de vote	Canton de Neuchâtel	Statistieken over stemgedrag bij verkiezing in canton Neuchâtel in 2013

Jaar	Titel	Organisatie / Auteur	Toelichting
11-2011	Evaluation der E-voting Testphase im Kanton Zürich 2008-2011	Kanton Zürich, Direktion der Justiz und des Innern	Duitstalig evaluatie rapport over experimenten met internetstemmen in Zürich

VERDONCK KLOOSTER & ASSOCIATES

DEEL II - RISICOANALYSE INTERNETSTEMMEN

VERDONCK KLOOSTER & ASSOCIATES

DEEL II - RISICOANALYSE INTERNETSTEMMEN

DATUM	28 januari 2014
STATUS	Definitief
VERSIE	1.0

MANAGEMENTSAMENVATTING

In opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties is een analyse uitgevoerd van de te voorziene risico's als gevolg van het stemmen per internet voor de kiezers in het buitenland in relatie tot de (internationale) waarborgen die gelden voor verkiezingen en de maatregelen die te treffen zijn om de risico's in afdoende mate af te dekken.

Onderzocht is welke realistische dreigingsscenario's zich kunnen voordoen. Per dreigingsscenario is onderzocht welke actor een belang zou kunnen hebben, op welke manieren het dreigingsscenario zich kan manifesteren, of het een bestaande of nieuwe dreiging is en op welke waarborgen en processtappen het dreigingsscenario betrekking heeft. Per scenario is een inschatting gemaakt van het risico. Dat wordt bepaald door zowel de kans dat de ongewenste gebeurtenis optreedt als het effect indien het zich voordoet. Hierbij wordt het effect zwaarder gewogen dan de kans, vanuit de overweging dat gegeven het absolute karakter van sommige waarborgen én het maatschappelijk belang van verkiezingen ook een dreigingsscenario met een kleine kans van optreden toch beschouwd moet worden als een middel of groot risico kans indien het effect respectievelijk middel of groot is.

In onderstaande tabel zijn de dreigingsscenario's weergegeven waarvan het risico is ingeschat op Groot of Middel. Hierbij zijn de preventieve en correctieve maatregelen reeds meegewogen.

Risico	Dreigingsscenario's
G	Niet-kiesgerechtigde brengt stem uit
G	Manipuleren van de stem of uitslag
G	Relatie tussen kiezer en inhoud stem (doorbreken stemgeheim)
G	Incorrecte installatie
G	Incorrecte beheer/bediening
G	Functionele, technische of beveiligingsgebreken
M	Publiceren informatie over beveiliging internetstemsysteem
M	Verkopen stem
M	Dwang / beïnvloeding van kiezer
M	Kiezer brengt meer dan één stem uit
M	Chantage
M	Doelbewust verstoren van de verkiezing
M	Defacing / bekladding internetstemsysteem
M	Onvoldoende inzicht en begrip kiezers
M	Incorrecte de-installatie
M	Onbeschikbaarheid

In de risicoanalyse zijn meerdere dreigingsscenario's onderkend die de waarborg van integriteit raken, waaronder de twee dreigingsscenario's *Niet-kiesgerechtigde brengt stem uit* en *Manipuleren van de stem of uitslag* waarvan het risico als groot is ingeschat. De mate waarin aan de waarborg van integriteit kan worden voldaan hangt primair af van het ontwerp van het internetstemsysteem en de mate waarin dit ontwerp correct is geïmplementeerd. Het is echter onmogelijk om vanuit de overheid de computer van de kiezer te beschermen tegen manipulatie. Deze manipulatie (in een scenario waarbij een aanvaller heimelijk malware heeft weten te installeren op de computer van de kiezer en daarmee de uitgebrachte stem wijzigt) is daarnaast ook bijzonder lastig te detecteren.

Aan de waarborg van stemvrijheid kan niet worden voldaan. Internetstemmen vindt plaats vanuit een omgeving die niet door het stembureau (of door een andere overheidsorganisatie) kan worden gecontroleerd. Het risico dat dwang of beïnvloeding plaatsvindt op de kiezer is een van de restrisico's van stemmen door kiezers buiten Nederland, of dat nu internetstemmen, briefstemmen of volmachtstemmen betreft.

Doordat niet kan worden voldaan aan de waarborg van stemvrijheid geldt ook voor de waarborg van het stemgeheim dat dit niet door de overheid kan worden gegarandeerd *aan de kant van de kiezer*. Dit is overigens niet anders dan bij briefstemmen.

Een internetstemsysteem is kwetsbaar voor dreigingsscenario's die er opgericht zijn het verkiezingsproces te verstoren. In het bijzonder DDoS aanvallen op de servers van een internetstemsysteem hebben potentieel een groot effect doordat het internetstemsysteem onbeschikbaar raakt voor de kiezer. Met deze dreiging zal nadrukkelijk in het ontwerp van het internetstemsysteem rekening gehouden moeten worden.

In de vergelijking met briefstemmen geldt dat voor veel van de dreigingen rondom internetstemmen de vereiste kennis (en in sommige gevallen ook inspanning) om een dreiging te ontwikkelen weliswaar hoog is, maar de dreiging daarna tegen marginale meerkosten is toe te passen. De schaal waarop de dreiging kan plaatsvinden kan dan ook zeer groot zijn en wordt niet meer bepaald door de vereiste menselijke inzet of middelen. In zekere zin kan gesteld worden dat de dreiging dan geautomatiseerd is. Dit fenomeen is bijvoorbeeld zichtbaar bij computervirussen; alleen bij de ontwikkeling is menselijke inspanning en middelen nodig, de verdere verspreiding wordt door computers uitgevoerd. Recente ontwikkelingen laten overigens zien dat er steeds minder specialistische kennis nodig is om deze dreigingen te kunnen uitvoeren; cybercriminelen verhuren kant en klare malware, virussen en DDoS capaciteit tegen steeds lagere kosten.

Het is aannemelijk dat er een aantal actoren zijn die een belang kunnen hebben bij het manipuleren van de uitslag van een verkiezing in Nederland, om (geo)politieke, economische of militaire redenen. Het effect van één stem meer of minder op de zetelverdeling is in Nederlandse kiesstelsel echter beperkt door het systeem van evenredige vertegenwoordiging. Bij de

verkiezingen voor de Tweede Kamer en het Europees parlement is in de afgelopen tien jaar het aantal vanuit het buitenland uitgebrachte stemmen nooit boven de kiesdrempel gekomen. Zelfs in het geval dat van alle internetkiezers de stem zou zijn gemanipuleerd dan nog leidt dat bij deze aantallen niet tot een directe zeteltoewijzing, hoogstens een voorkeursstem voor één of twee kandidaten of een wijziging van de restzetelverdeling. Als het aantal kiezers fors stijgt, bijvoorbeeld als gevolg van de invoering van de permanente registratie, dan neemt het reële effect op de uitslag uiteraard toe.

Het gebruik van computer- en communicatie technologie in het stemproces betekent dat het verloop van het stemproces voor mensen minder direct waarneembaar is en daarmee minder *transparant* en *controleerbaar*. Er zijn meerdere dreigingen denkbaar en realistisch op het stemgeheim, de kiesgerechtigdheid, de integriteit en de beschikbaarheid van de technische componenten van het internetstemsysteem, zonder dat de kiezer, het stembureau of waarnemers dit door hebben. Het vergt aanvullende maatregelen om deze dreigingen te ontdekken. Veel van deze maatregelen vergen overigens de inzet van programmatuur en computertechnologie, hetgeen in zichzelf een recursief effect heeft en de complexiteit van het internetstemsysteem vergroot.

Uit de risicoanalyse is gebleken dat voor het voorkomen van dreigingen maatregelen denkbaar zijn, die op zich zelf nieuwe dreigingen introduceren. Voor die afgeleide dreigingen dienen aanvullende maatregelen genomen te worden. Dit betekent dat het ontwerpproces van het internetstemsysteem in meerdere iteratieslagen moeten worden uitgevoerd, waarbij steeds opnieuw de risico's moeten worden beoordeeld na elke ontwerpslag. Dit geldt niet alleen voor alle maatregelen die genomen worden op het gebied van beveiliging van het internetstemsysteem, maar ook voor ontwerpkeuzes in het registratieproces of voor maatregelen die tot doel hebben om de beschikbaarheid te vergroten.

Een internetstemsysteem is een complex informatiesysteem. De complexiteit wordt niet bepaald door de functionaliteit van het internetstemsysteem, die is relatief eenvoudig. Wat het complex maakt zijn de stringente eisen die voortvloeien uit de waarborgen controleerbaarheid, integriteit, stemgeheim, uniciteit en beschikbaarheid die maken dat het systeem geen enkele gebreken mag bevatten, de exacte werking gegarandeerd en controleerbaar moet zijn, het systeem intensief beheerd en beveiligd moet worden en dat het systeem niet alleen sterk beschermd moet zijn tegen dreigingen van buitenaf, maar ook tegen misbruik en dreigingen van binnenuit (zoals beheerders). Naast een kwalitatief goed en doordacht ontwerp is ook de wijze waarop het internetstemsysteem wordt ontwikkeld, geïnstalleerd, beheerd, bediend en ontmanteld bepalend of in de praktijk aan de waarborgen wordt voldaan.

INHOUDSOPGAVE

1 INLEIDING

1.1 Risicoanalyse

In opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties is een analyse uitgevoerd van de te voorziene risico's als gevolg van het stemmen per internet voor de kiezers in het buitenland in relatie tot de (internationale) waarborgen die gelden voor verkiezingen en of er maatregelen te treffen zijn om die risico's in afdoende mate af te dekken.

De risicoanalyse dient ook inzicht te geven in maatregelen die getroffen kunnen worden om die risico's in afdoende mate af te dekken, of – als er geen maatregelen te treffen zijn – welk kans dat het risico zich daadwerkelijk voor zal doen (en de impact van het risico).

De nu gevraagde analyse is anders dan de in 2004 en 2006 opgestelde risicoanalyses voor stemmen per internet uit het Kiezen op Afstand project, aangezien destijds een risicoanalyse op een specifiek internetstemsysteem (met bijbehorende procesinrichting en administratieve organisatie) is uitgevoerd en er nu nog geen internetstemsysteem is ontworpen.

De uitgevoerde risicoanalyse is een gebaseerd op het *proces van internetstemmen*, de *doelgroep* kiezers in het buitenland en stemmethode(n) die daar nu voor zijn toegestaan en de *waarborgen* waar elk verkiezingsproces aan moet voldoen.

Voor het proces van internetstemmen is een generiek procesmodel op hoofdlijnen gehanteerd, welke is afgeleid van de procesinrichtingen uit de eerdere Nederlandse experimenten en de wijze waarop in het buitenland internetstemmen wordt toegepast.

Het voert verder dan de opdracht van deze risicoanalyse om een ontwerp te maken van een internetstemsysteem of proces. Sommige dreigingen en waarborgen kunnen respectievelijk worden afgewend of gerealiseerd door maatregelen te nemen, welke weer nieuwe dreigingen introduceren waardoor andere maatregelen vereist zijn. Een dergelijk iteratief ontwerpproces met een stapsgewijze verkenning van maatregelen was geen onderdeel van de opdracht en is om die reden niet uitgevoerd. Volstaan is met per dreiging aan te geven welke preventieve en welke correctieve maatregelen genomen kunnen worden.

Een risicoanalyse heeft een beperkte houdbaarheid. Zeker in het internetdomein ontstaan er continue nieuwe (technologische) dreigingen en worden nieuwe maatregelen uitgedacht. Mocht besloten worden tot nieuwe experimenten met internetstemmen in Nederland dan dient deze analyse geactualiseerd te worden bij de start van het ontwerptraject voor een internetstemsysteem. Gedurende het ontwerptraject is een verdieping van de risicoanalyse noodzakelijk naar de specifieke risico's van het ontworpen / verworven / ontwikkelde internetstemsysteem. Aan de hand van de specifieke risico's kunnen dan maatregelen worden ontworpen om de dreigingen te voorkomen, te detecteren en te corrigeren .

Ook in de periode na het ontwerptraject en de ontwikkeling van een internetstemsysteem verdient het aanbeveling om de risicoanalyse steeds te actualiseren.

Elke risicoanalyse is in zekere mate een subjectieve inschatting. Dit geldt voor zowel de onderkende dreigingen, de inschatting van kans en effect en welke basisniveau van vertrouwen als vertrekpunt wordt genomen. Als wantrouwen in de instituten (overheid, (centraal) stembureau en gemeenten) die nu de verkiezingen organiseren of samenspanning door meerdere personen het vertrekpunt is, dan kennen veel dreigingsscenario's een groot risico. Dit geldt dan ook voor de huidige vormen van stemmen.

1.2 Afbakening

De risicoanalyse richt zich, conform de opdracht, op de toepassing van internetstemmen voor de doelgroep kiezers *buiten* Nederland. Een risicoanalyse voor de toepassing van internetstemmen voor kiezers *binnen* Nederland lag niet in de opdracht en is niet onderzocht.
De doelgroep kiezers buiten Nederland kan nu op drie manieren stemmen: door te stemmen per brief, het geven van een volmacht aan een andere kiezer of door af te reizen naar Nederland om aldaar te stemmen in een stemlokaal. In hoofdstuk 4 wordt de meeste gebruikte methode (briefstemmen) behandeld.

Deze risicoanalyse richt zich, conform opdracht, specifiek op het uitbrengen van de stem via internet. Er is geen risicoanalyse uitgevoerd op aanpalende processen zoals het proces van kandidaatstelling, het registratieproces voor kiezers buiten Nederland en het proces waarin de uitslag wordt bepaald. In de risicoanalyse is aangegeven waar en wanneer de risico's van internetstemmen worden beïnvloed door een van deze gerelateerde kiesprocessen.

1.3 Aanpak

De risicoanalyse is uitgevoerd op basis van i) de waarborgen die generieke eisen stellen aan elk verkiezingsproces en stemmethoden, ii) de procesinrichting zoals die nu geldt voor de doelgroep kiezers in het buitenland en iii) de stemmethoden (in het bijzonder briefstemmen) waar deze doelgroep gebruik van kan maken.

Per fase van het stemproces en per waarborg zijn de dreigingsscenario's onderzocht. Omdat er veel manieren en middelen zijn waarmee een dreiging kan worden uitgevoerd, wordt een dreigingsscenario als uitgangspunt genomen. Voor de bepaling van de dreigingsscenario's is gebruik gemaakt van de ervaringen uit eerdere experimenten uit Nederland, uit andere landen en inzichten van experts.

Bij elk van deze dreigingsscenario's wordt aangegeven wat de *kans* is dat het dreigingsscenario zich voordoet, en wat het *effect* is als het zich voordoet. Hierbij is in de overweging van de kans dat een dreigingsscenario optreed in de afweging meegenomen of er actor is die een belang heeft bij de dreiging en de middelen heeft om de dreiging uit te voeren.

Bij elk van de dreigingsscenario's is aangegeven welke *maatregelen* getroffen kunnen worden, zowel preventief als correctief. Dit lijst met maatregelen is niet uitputtend. Een uitputtende lijst kan pas worden gemaakt zodra er een specifiek ontwerp ligt van een internetstemsysteem. De risico's zijn in eerste instantie ingeschat zonder het effect van de mogelijke maatregelen en vervolgens inclusief het effect van de maatregelen.

Tenslotte is een inschatting gemaakt van de risico's van de dreigingsscenario's: het risico dat overblijft nadat alle maatregelen in ogenschouw zijn genomen.

1.4 Leeswijzer

In dit rapport is in de hoofdstukken 2, 3 en 4 een nadere introductie gegeven van respectievelijk de waarborgen, de generieke procesinrichting en het bestaande proces van briefstemmen. In hoofdstuk 5 zijn de dreigingsscenario's beschreven, inclusief de mogelijke organisaties / personen (actoren) die de dreiging kunnen uitvoeren en de maatregelen tegen deze dreigingen. In hoofdstuk 7 is een overzicht gegeven van de risico's en maatregelen zoals die in andere landen wordt gehanteerd. Tenslotte is in het laatste hoofdstuk een samenvatting opgenomen van de belangrijkste risico's.

1.5 Geraadpleegde bronnen

In het kader van deze analyse zijn gesprekken gevoerd met de volgende personen.

Persoon	Functie, Organisatie
Henrik Nore, Christian Bull, Ida Sofie Gebhardt Stenerud	Kommunal- og Regionaldepartementet (Ministry of Local Government and Regional Development Noorwegen)
Tarvi Martens	i-voting project manager, National Electoral Committee, Estland
Bart Jacobs,	Hoogleraar Software Security and Correctness, Radboud University Nijmegen
Jaap-Henk Hoepman	Universitair hoofddocent computer security, privacy and identity management, Radboud University Nijmegen
Berry Schoenmakers	Universitair hoofddocent en onderzoeker Discrete Mathematics, Cryptografie, Universiteit Eindhoven, Faculteit Wiskunde en Informatica
Anne-Marie Oostveen	Research Fellow Social Informatics, Oxford Internet Institute (Verenigd Koninkrijk)

De auteurs zijn deze personen zeer erkentelijk voor het delen van hun inzichten en zienswijzen.

In internationaal verband is onderzoek gedaan en gepubliceerd over de risico's van stemmen via internet. Bij het inventariseren van mogelijke dreigingen is gebruik gemaakt van internationale risicoanalyses en wetenschappelijke publicaties. In de Bijlage D is een lijst opgenomen met geraadpleegde bronnen.

1.6 Aannames

Bij het uitvoeren van de risico-analyse zijn de volgende aannames gedaan:

a. Het in Nederland gebruikte kiesstelsel van evenredige vertegenwoordiging blijft onveranderd;
b. Kiezers in het buitenland kunnen gedurende een meerdaagse periode hun stem uitbrengen, ook bij gebruik van internetstemmen als stemmethode;
c. Er wordt gestemd door de kiezer met een computer of een ander geschikt apparaat (zoals tablet, smartphone etc.). In deze risicoanalyse is geen onderscheid gemaakt in de risico's die samenhangen met het type apparaat.
d. Internetstemmen vervangt niet bestaande vormen van stemmen, maar wordt aangeboden als aanvullend alternatief.

1.7 Begrippen

INTERNETSTEMMEN

Internetstemmen is een wijze van stemmen waarbij de kiezer op elektronische wijze zijn stemvoorkeur kenbaar maakt, op een locatie waar geen toezicht wordt gehouden door een verkiezingsautoriteit, en waarbij hij de stem overdraagt aan het stembureau via het openbare internet.

KIEZER

In dit document wordt met de term kiezer een kiesgerechtigd persoon aangeduid. Met kiezer wordt niet specifiek gedoeld op de persoon die de handeling uitvoert om zijn stem uit te brengen (het feitelijke kiezen). De term kiezer doelt op zowel mannen als vrouwen, maar wordt in dit document in het mannelijk woordgeslacht gehanteerd.

RISICO

Een *risico* wordt in dit rapport gedefinieerd als de *kans* op het optreden van een ongewenste gebeurtenis (door een oorzaak) met een (veelal negatief) *effect*. De grootte van het risico wordt bepaald door zowel de kans als het effect.

DREIGING

De ongewenste gebeurtenis wordt in dit rapport aangeduid als een *dreiging*. Daarbij wordt aansluiting gezocht bij de definitie[1] van een (be)dreiging:

"Een bedreiging is een proces of gebeurtenis die in potentie een verstorende invloed heeft op de betrouwbaarheid van een object. In het kader van informatiebeveiliging betreft het dan de

[1] Informatiebeveiliging onder controle, Paul Overbeek e.a.

objecten van de informatievoorziening: apparatuur, programmatuur, gegevens, procedures en mensen"

We onderkennen vier categorieën van dreigingen:

- Bewust menselijk handelen
- Onbewust onbekwaam menselijk handelen
- Systeem en Technisch falen
- Calamiteiten / “Force majeur”

DREIGINGSSCENARIO

In dit rapport wordt gebruik gemaakt van het begrip dreigingsscenario. Dit is een beschrijving van de ongewenste gebeurtenis (dreiging) in een context waarbij de dreiging zich in het verloop van tijd kan ontwikkelen vanuit een hoofdoorzaak tot een bepaald gevolg (effect).

INTERNETSTEMSYSTEEM

Het internetstemsysteem is het geheel van mensen, processen, middelen (waaronder de programmatuur, computerapparatuur en netwerkapparatuur) wat nodig is om een kiezer een stem uit te laten brengen via het internet. Een internetstemsysteem kent een typische client-server opbouw met i) client-programmatuur waarmee de kiezers een stem kunnen uitbrengen en ii) server-programmatuur die zorgt voor de authenticatie van de kiezers, opslaan van ontvangen stemmen en tellen van de opgeslagen stemmen.

2 WAARBORGEN VERKIEZINGSPROCES

2.1 Waarborgen verkiezingsproces

In het rapport "*Stemmen met vertrouwen"* heeft de adviescommissie inrichting verkiezingsproces gesteld dat het verkiezingsproces in Nederland ten minste moet voldoen aan acht waarborgen. Elke stemmethode die gebruikt wordt mag geen afbreuk doen aan deze waarborgen, ongeacht of de stemmen op papier, bij volmacht of elektronisch worden uitgebracht. Deze waarborgen gelden dus ook voor internetstemmen.

Deze waarborgen zijn deels verankerd in onze Grondwet, en deels vastgelegd in internationale en Europese verdragen waartoe Nederland is toegetreden. Daarnaast heeft de Raad van Europa in 2004 op 30 september 2004 een aanbeveling Rec(2004)11 opgesteld waarin expliciet de juridische, operationele en technische vereisten staan waar een verkiezing aan moet voldoen, in het bijzonder wanneer een vorm van elektronische stemmen wordt toegepast.

Waarborg	Omschrijving[2]
1. Transparantie	Het verkiezingsproces moet zo zijn ingericht, dat het helder van structuur en opzet is, zodat in beginsel iedereen inzicht in de structuur ervan kan hebben. Er zijn in het verkiezingsproces geen geheimen. Vragen moeten beantwoord kunnen worden; de antwoorden moeten controleerbaar en verifieerbaar zijn.
2. Controleerbaarheid	Het verkiezingsproces moet objectief controleerbaar zijn. De controle instrumenten kunnen, afhankelijk van de vorm van stemmen waartoe wordt besloten, verschillen.
3. Integriteit	Het verkiezingsproces moet correct verlopen en de uitkomst mag niet beïnvloedbaar zijn anders dan door het uitbrengen van rechtmatige stemmen.
4. Kiesgerechtigdheid	Alleen kiesgerechtigde personen mogen aan de verkiezing deelnemen.
5. Stemvrijheid	Iedere kiesgerechtigde moet bij het uitbrengen van zijn of haar stem zijn of haar keuze in alle vrijheid, vrij van beïnvloeding, kunnen bepalen.
6. Stemgeheim	Het moet onmogelijk zijn om een verband te leggen tussen de identiteit van de persoon die de stem uitbrengt en de inhoud van de uitgebrachte stem. Het proces moet zodanig zijn ingericht, dat het onmogelijk is de kiezer te laten aantonen hoe hij of zij gestemd heeft.
7. Uniciteit	Iedere kiesgerechtigde mag, gegeven het Nederlandse kiesstelsel, één stem per verkiezing uitbrengen, die bij de stemopneming precies één keer meegeteld mag en moet worden.

[2] Zie rapport "Stemmen met vertrouwen" van de adviescommissie inrichting verkiezingsproces, 27 september 2007 onder voorzitterschap van dhr. F. Korthals Altes.

Waarborg	Omschrijving[2]
8. Toegankelijkheid	Kiesgerechtigden moeten zoveel mogelijk in de gelegenheid gesteld worden om direct deel te nemen aan het verkiezingsproces. Indien dat onmogelijk is, moet de mogelijkheid openstaan om indirect – door het verlenen van een volmacht – aan de verkiezing deel te nemen.

In deze risicoanalyse zijn naast de bovenstaande waarborgen een tweetal aanvullende waarborgen gehanteerd die samenhangen met het gebruik van technologie in een internetstemsysteem.

Waarborg	Omschrijving
9. Beschikbaarheid	Indien in het verkiezingsproces gebruik gemaakt wordt van (technische) voorzieningen dan moeten deze dusdanig beschikbaar zijn dat een tijdelijke verstoring van de voorziening niet betekent dat een kiezer niet meer zijn stem kan uitbrengen. Bij complete uitval dient de kiezer via een andere stemmethode te kunnen stemmen.
10. Tijdigheid	De kiezer wordt tijdig voorzien van middelen om te kunnen stemmen zodat deze zijn stem tijdig kan uitbrengen en de stemmen tijdig kunnen worden geteld. Voldoen aan wettelijke termijnen.

Ter verduidelijking, bovenstaande waarborgen moeten niet verward worden met de (complete) set van eisen waarmee een internetstemsysteem kan worden gespecificeerd. De waarborgen vormen een normenkader voor het gehele verkiezingsproces, en stellen daarmee kwalitatieve eisen aan de procesinrichting, de procedures en de ingezette middelen.

2.2 Afweging tussen waarborgen

De adviescommissie inrichting verkiezingsproces gaf in haar rapport reeds aan dat er een balans moet worden gevonden tussen de waarborgen, omdat het in de praktijk niet mogelijk is om aan alle waarborgen in absolute zin te voldoen. Sommige waarborgen (of de implementatie daarvan) kunnen namelijk afbreuk doen aan andere waarborgen. Bij eerdere introducties van vernieuwingen in het stemproces werd dit ook al onderkend. Zo draagt stemmen per brief bij aan een grotere toegankelijkheid van de verkiezingen voor kiezers in het buitenland, maar levert de kiezer in dat geval wel in op de waarborg van stemvrijheid. Het stemmen buiten het stembureau betekent dat de stemvrijheid en het stemgeheim niet gewaarborgd kan worden en er derhalve vormen van dwang zich kunnen voordoen waardoor de kiezer niet volledig vrij is om te stemmen conform zijn intentie.
Een ander voorbeeld is het systeem van volmacht stemmen. Ook dat is ingevoerd om de toegankelijkheid van het stemproces te vergroten; kiezers die zelf niet in staat zijn om te stemmen kunnen een andere kiezer vragen voor hem of haar een stem uit te brengen. Stemmen bij volmacht maakt het echter mogelijk dat een kiezer zijn stem verkoopt, hetgeen in strijd is met de waarborg van het stemgeheim. Om het effect hiervan te beperken is in de Kieswet bepaald dat het

aantal volmachtstemmen dat een gemachtigde mag uitbrengen beperkt is tot twee en dat de gemachtigde deze stemmen tegelijkertijd moet uitbrengen met zijn eigen stem.

De waarborgen zijn niet in alle gevallen even absoluut. De waarborg van het stemgeheim is dat wel, de stem is of geheim of niet, er is geen tussenvariant van 'een beetje geheim'. Andere waarborgen zoals transparantie en toegankelijkheid kennen een mate van subjectiviteit. Er is immers geen universele definitie van wat een 'heldere structuur en opzet' van een verkiezingsproces is.

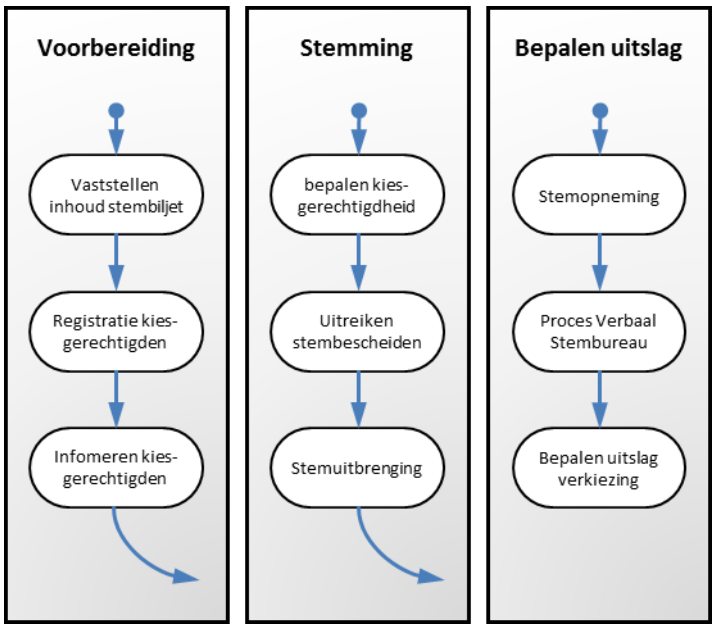
De adviescommissie heeft, gelet op het in de praktijk niet absolute karakter van de waarborgen en het spanningsveld dat tussen sommige waarborgen (kan) ontstaan, een "pas toe of leg uit" regime aanbevolen: aan de waarborgen moeten worden voldaan, of leg uit waarom een andere balans is gekozen tussen de waarborgen.

3 PROCESBESCHRIJVING

3.1 Algemeen procesmodel voor verkiezingen

De risico's van stemmen via internet zijn niet alleen afhankelijk van de wijze waarop een stem wordt uitgebracht (via internet of niet), maar ook van de wijze waarop het totale proces is ingericht. Dit wordt in dit hoofdstuk nader uiteengezet. Daarbij is relevant dat er een - op onderdelen - andere procesinrichting geldt voor de doelgroep kiezers buiten Nederland dan voor kiezers die in Nederland wonen.

Als inleiding van die afwijkende procesinrichting wordt eerst een algemeen procesmodel van een verkiezing geïntroduceerd. Een verkiezing kan gezien worden als een proces met op het hoogste abstractieniveau een drietal fasen: de voorbereiding van de verkiezing, de stemming en tenslotte de bepaling van de uitslag.



De voorbereidingsfase kent drie hoofdstappen: de kandidaatstelling, het bepalen van de kiesgerechtigdheid en het oproepen / informeren van de kiezer. De registratie van de kiezers vindt plaats aan de hand van de bevolkingsadministratie. In deze voorbereidingsfase zijn met name de gemeente(n) (registratie kiesgerechtigdheid), de Kiesraad (kandidaatstelling) en de rijksoverheid (voorlichtingscampagnes) actief. De voorbereidingsfase begint normaliter 9 maanden tot een jaar voorafgaand aan de dag van stemming en loopt door tot aan de dag van stemming.

In de fase van de feitelijke stemming zijn het primair stembureaus (inclusief hoofdstembureau en centraal stembureau) die de werkzaamheden verrichten. In het stembureau wordt eerst de kiesgerechtigdheid geverifieerd van de personen die zich bij het stembureau melden als kiezer. Aan de kiesgerechtigde personen worden de stembescheiden (stembiljet, overzicht van

kandidaten etc.) uitgereikt. Nadat alle kiezers hun stem hebben uitgebracht wordt de stemming gesloten. Na de stemming wordt gestart met de stemopneming: het tellen van alle geldige (en ongeldige) uitgebrachte stemmen, het bepalen van de uitslag / zetelverdeling en het vastleggen in een proces-verbaal.

3.2 Afwijkende processtappen voor kiezers buiten Nederland

Voor kiezers buiten Nederland[3] zijn er vier processtappen die anders verlopen: de voorafgaande registratie, de wijze waarop de kiezer de stembescheiden krijgt, het uitbrengen van de stem en tenslotte de stemopneming. De afwijkende opzet en invulling van de processtappen hangt samen met zowel het stemmen op afstand als de wijze waarop wordt gestemd.

3.2.1 Registratie kiesgerechtigden

Een kiezer kan een verzoek indienen om zich te laten registreren als kiezer buiten Nederland. Dit kan de kiezer doen in een periode van 6 maanden voorafgaand aan de dag van stemming tot op de 28e dag voor de dag van stemming. Dit verzoek geldt voor een specifieke verkiezing[4]. Op een registratieformulier geeft de kiezer ook aan hoe hij wil stemmen (per brief, per kiezerspas, of bij volmacht).
De gemeente Den Haag[5] verwerkt deze registratieverzoeken en toetst of de persoon kiesgerechtigd is. Indien niet aan de vereisten wordt voldaan wordt het registratieverzoek afgewezen. De kiezer kan bezwaar maken tegen deze afwijzing. Er is dus sprake van een voorafgaande toets op de kiesgerechtigdheid.

3.2.2 Uitreiken stembescheiden

Na definitieve vaststelling van de kandidatenlijst worden de stembiljetten gedrukt en stuurt de gemeente Den Haag de stembescheiden (stembiljet, retourenvelop, briefstembewijs en overzicht van kandidatenlijsten) toe aan de kiezers in het buitenland. Het ministerie van BZK houdt bij de verkiezingen van de leden van het Europese Parlement van 22 mei 2014 een experiment waarbij het stembiljet per e-mail wordt toegezonden aan de kiezer die daartoe hebben verzocht. Het

[3] In artikel M1 van de Kieswet is bepaald welke kiezers hiertoe gerechtigd zijn: kiezers die op de dag van kandidaatstelling hun werkelijke woonplaats buiten Nederland hebben en aan kiezers die op de dag van stemming wegens beroep of werkzaamheden of wegens het beroep of werkzaamheden van zijn echtgenoot, levensgezel of ouder buiten Nederland verblijven.

[4] In de huidige Kieswet is bepaald dat de kiezer zich per verkiezing moet registreren. De minister van BZK heeft aangekondigd de invoering van een permanente registratie te overwegen, in welk geval een eenmalige registratie afdoende is.

[5] Voor inwoners van Aruba, Curaçao en Sint Maarten geldt met ingang van 2013 dat niet de gemeente Den Haag maar de Nederlandse vertegenwoordiging in die landen zorg draagt voor de registratie.

formaat van het stembiljet[6] is aangepast naar 'A4' zodat een kiezer dit biljet zelf kan afdrukken en invullen.

3.2.3 Stemuitbrenging

De kiezer buiten Nederland kan op verschillende manieren stemmen: door per brief te stemmen, door een volmacht te verlenen aan een andere kiezer of door af te reizen naar Nederland. In de navolgende beschrijving beperken we ons tot het stemmen per brief. De kiezer brengt zijn stem uit door een kandidaat aan te kruisen op het stembiljet en het ingevulde stembiljet in de daarvoor bestemde enveloppe te doen. Daarna stopt de kiezer de enveloppe met het stembiljet en het ondertekende briefstembewijs in de (oranje) retourenveloppe. De kiezer stuurt de retourenveloppe per reguliere post terug. De retourenveloppes zijn reeds voorzien van een adres van een briefstembureau. De briefstem moet uiterlijk 15:00 uur lokale tijd op de dag van stemming per post ontvangen zijn (in Den Haag, of bij de briefstembureaus in het buitenland of bij de Nederlandse vertegenwoordigingen op Aruba, Curaçao of Sint Maarten).

3.2.4 Stemopneming

De stemopneming is geregeld in artikel M10 van de Kieswet. Om alle ontvangen briefstemmen te verwerken worden briefstembureaus ingericht. De voorzitter van het (brief)stembureau opent de retourenveloppe en neemt het briefstembewijs en de enveloppe met het stembiljet eruit. Hij controleert of de verklaring (het briefstembewijs) dat de kiezer het stembiljet persoonlijk heeft ingevuld, is ondertekend en of de daaronder geplaatste handtekening overeenstemt met de handtekening onder het registratieformulier. Vervolgens wordt het stembiljet ongeopend doorgegeven aan een ander lid van het stembureau die de enveloppe met het stembiljet in de stembus steekt. De telling van de stemmen verloopt daarna gelijk aan het proces van tellen zoals in stembureaus in Nederland.

3.3 Afwijkende processtappen voor internetstemmen

Ten tijde van het uitvoeren van deze risicoanalyse was er nog geen vastgesteld procesontwerp beschikbaar voor het stemmen via internet. Voor het doel van de analyse is de aanname gedaan dat het proces op hoofdlijnen een gelijke inrichting kent als voor briefstemmen, maar dat de authenticatie van de kiezer en het toesturen van de stembescheiden anders zal verlopen.

<u>Uitreiken authenticatiemiddel en Authenticatie</u>

Het registratieproces gaat nu uit van een fysieke ondertekening[7] van het registratieverzoek. Die handtekening heeft later in het proces van stemopneming de functie van authenticatiemiddel,

---

[6] Zie voor meer informatie https://www.verkiezingen2014.nl/stemmenvanuitbuitenland/het-nieuwe-stembiljet

[7] Het vereiste van de fysieke handtekening maakte dat tot voor kort de kiezer zijn registratieverzoek per post in moest sturen. Met ingang van 2013 is het ook toegestaan dat een kiezer het registratieverzoek inscant en per e-mail toestuurt.

doordat het briefstembureau de handtekening op het briefstembewijs vergelijkt met de handtekening op het registratieverzoek.
Ook bij stemmen via internet is er een vorm van authenticatie nodig om na te gaan of de stem afkomstig is van een kiesgerechtigde kiezer. De methode van authenticatie[8], en de wijze waarop de kiezer zijn authenticatiemiddelen verkrijgt moeten in een later ontwerpstadium worden afgewogen en bepaald.
In deze risicoanalyse hanteren we als aanname dat de kiezer een authenticatiemiddel uitgereikt krijgt als onderdeel van de fysieke stembescheiden die per reguliere post naar de kiezer worden toegestuurd. Dit is ook de werkwijze zoals deze in de Kiezen op Afstand projecten in 2004 en 2006 is gevolgd en de werkwijze die in diverse andere landen wordt gehanteerd.

Geen 'uitreiking' stembiljet
Een andere aanname bij het opstellen van deze risicoanalyse is dat de kiezer geen stembiljet meer uitgereikt krijgt, maar dat de kiezer op de website, of in het programma waarmee hij stemt, een overzicht van kandidaten gepresenteerd krijgt waaruit hij zij keuze kan maken.

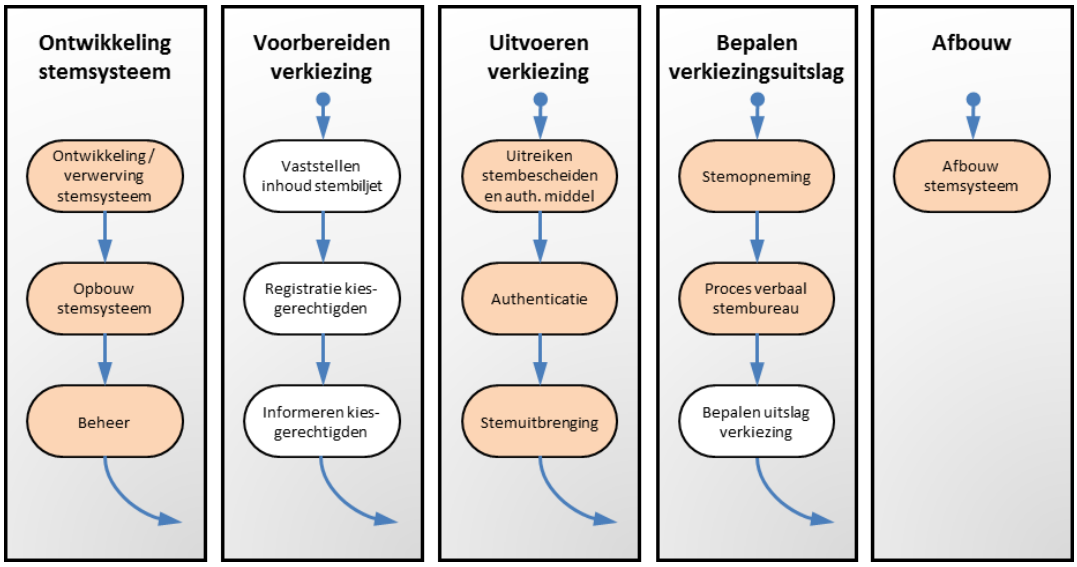
3.3.1 Nieuwe processtappen gerelateerd aan gebruik van internetstemsysteem

Bij het gebruik van een internetstemsysteem zijn er ook twee nieuwe fasen in het verkiezingsproces die niet direct verband houden met de stemming maar wel noodzakelijk zijn voor de stemming.

De eerste nieuwe fase betreft de ontwikkeling of verwerving van het internetstemsysteem, het opbouwen en het operationeel beheren van het internetstemsysteem. De ontwikkeling / verwerving heeft een typisch projectmatig karakter: het betreft een tijdelijke inspanning om een systeem te specificeren en om dit te (laten) ontwikkelen en te testen. De opbouw van het internetstemsysteem vindt plaats een aantal maanden voorafgaand aan de verkiezing waarna deze in beheer wordt genomen. De beheerfase loopt door tot na het vaststellen van de definitieve uitslag en het opstellen van het proces-verbaal.

De tweede nieuwe fase is de afbouw van het internetstemsysteem en vindt na afloop van de verkiezing plaats. In deze fase wordt het internetstemsysteem ontkoppeld van het internet, alle gegevensdragers gewist of vernietigd opdat er geen digitale sporen achterblijven.

[8] Er zijn verschillende authenticatiesystemen denkbaar: een eenmalig wachtwoord, een combinatie van een eenmalige wachtwoord en een door de kiezer zelf opgegeven geheim, het gebruik van tokens, een elektronische identiteitskaart etc.



In bovenstaande figuur zijn deze twee nieuwe fasen weergegeven. Tevens is met een kleur aangegeven welke processtappen afwijken bij de toepassing van internetstemmen voor kiezers in het buitenland.

4 DOELGROEP EN METHODE VAN BRIEFSTEMMEN

4.1 Doelgroep kiezers buiten Nederland

Met kiezers buiten Nederland worden de kiezers bedoeld die op de dag van de kandidaatstelling zijn werkelijke woonplaats buiten Nederland hebben, dan wel op de dag der stemming buiten Nederland zullen verblijven.

Deze groep kiezers kunnen nu op drie manieren stemmen: stemmen per brief[9], het geven van een volmacht aan een andere kiezer en het afreizen naar Nederland om aldaar te stemmen in een stemlokaal. De regels omtrent stemmen per brief zijn in de Kieswet vastgelegd in hoofdstuk M.

De doelgroep kiezers buiten Nederland is bijzonder doordat het deze doelgroep is toegestaan om te stemmen in een ongecontroleerde omgeving, buiten het toezicht van een stembureau. Bij de toepassing van internetstemmen speelt een soortgelijke situatie. In dit hoofdstuk wordt teruggekeken naar de eerdere overwegingen van regering en parlement over dreigingen en risico's van briefstemmen.

4.2 Historie stemmen per brief

Reeds in 1958 is in het parlement gesproken over de mogelijkheid van briefstemmen naar analogie van de wijze waarop dit in Duitsland mogelijk was. De nota over het Duitse systeem is destijds door het parlement voor kennisgeving aangenomen. Op meerdere momenten daarna is in het parlement aan de orde gekomen of briefstemmen moest worden ingevoerd, onder meer om in het buitenland gelegerde dienstplichtige militairen te kunnen laten stemmen. Uiteindelijk is in 1983 een wetsvoorstel[10] aanvaard waarin de Kieswet is aangepast om stemmen per brief mogelijk te maken.

De mogelijkheid van briefstemmen is destijds met name geïntroduceerd om de toegankelijkheid tot het stemproces te verbeteren. Voorheen had de doelgroep 'kiezers in het buitenland' slechts twee mogelijkheden om deel te nemen aan de verkiezingen, of door een volmacht te geven aan een kiezer die wel in Nederland verbleef of door af te reizen naar Nederland.
Met de wijziging van de Kieswet in 1993 werden de mogelijkheid gecreëerd om briefstembureaus te openen op diplomatieke en consulaire vertegenwoordigingen in het buitenland. Met de instelling hiervan werd niet beoogd om een grotere opkomst te bevorderen, maar een snellere verzending per post mogelijk te maken.

---

[9] Bij de invoering in 1983 was de mogelijkheid van stemmen per brief voorbehouden aan Nederlanders, woonachtig in het buitenland, die in openbare dienst werkzaam waren, en Nederlandse kiesgerechtigden voor de Europese verkiezingen die ingezetene waren in een van de andere lid-Staten.

[10] Zie kst 17819 Nr 2 Wijziging van de Kieswet met betrekking tot het stemmen per brief en de Memorie van Toelichting kst 17819 Nr 3.

4.3 Inherente risico's van stemmen per brief

In het verleden is door de regering in het parlementaire debat op meerdere momenten gewezen op de risico's van briefstemmen. In hoofdzaak is steeds gewezen op drie risico's:

1. Er kan niet worden voldaan aan de beginselen van een vrije en geheime stemming zoals vastgelegd in art. 53 tweede lid van de Grondwet;
2. Misbruik van de mogelijkheid tot briefstemmen;
3. Stemmen worden niet tijdig ontvangen.

Bij de invoering in 1983 vond er slechts in beperkte mate een discussie plaats over deze risico's. Het risico van misbruik en beïnvloeding van de kiezer werd in de MvT op het wetsvoorstel uit 1983 vooral aanwezig geacht bij personen die in inrichtingen en tehuizen verbleven:

"Het gevaar voor onregelmatigheden bij de verkiezingen (invulling van stembiljetten door een ander dan de daartoe gerechtigde, beïnvloeding van de kiezer) blijkt echter juist in inrichtingen het grootst te zijn. (…) Het zou bijzonder moeilijk zijn maatregelen te treffen, die voldoende waarborgen scheppen om te voorkomen, dat in tehuizen en inrichtingen onregelmatigheden kunnen plaatsvinden. Bovendien hebben de Belgische ervaringen geleerd, dat het stemmen per brief een extra belasting van de administratie betekent, waarop men ingespeeld moet raken. Een en ander is voor de Regering reden om het stemmen per brief vooralsnog tot de kiesgerechtigden woonachtig in het buitenland te beperken. Pas wanneer enige tijd ervaring is opgedaan met het stemmen per brief door Nederlanders woonachtig in het buitenland, kan overzien worden of uitbreiding van de categorie briefstemmers mogelijk is."

Om die reden koos de regering er toen voor om de doelgroep te beperken.

In 2003 verwoordde de toenmalige minister van BZK Remkes van 25 maart 2003[11] de discussie uit 1983 als volgt:

"Slechts in beperkte mate is over het waarborgen van de geheime en vrije stemming discussie gevoerd bij de invoering van het briefstemmen in 1983. Het hierboven genoemde briefstembewijs is de enige bepaling die bij dit wetsvoorstel in dit verband als extra waarborg is opgenomen. In zijn advies[12] bij het oorspronkelijke voorstel van wet merkte de Raad van State op dat te weinig aandacht werd besteed aan het beginsel van geheime stemming. Op de opmerkingen van de Raad over de geheime stemming werd kort ingegaan door de regering in het nader rapport en dit heeft geresulteerd in een wijziging van het wetsvoorstel met betrekking tot de procedure in het stembureau. Een algemeen inhoudelijke discussie over het onderwerp is echter niet gevoerd.

De kans op onregelmatigheden werd door de regering namelijk klein geacht bij de categorie kiezers waar het briefstemmen voor zou gaan gelden. Bij de mondelinge behandeling van het

[11] Zie kst-28600-VII, nr 47 alsmede de bijlage 1 bij deze brief.

[12] Zie Kamerstukken II 1982/83, 17 819, nr. A-C, blz. 3.

wetsvoorstel erkende de toenmalige Minister van Binnenlandse Zaken, Rietkerk, wel dat het stemmen per brief zekere risico's met zich brengt en verwees daarbij naar de het feit dat de kiezer buiten een stemlokaal stemt en er daarom niet op kan worden toegezien dat in het geheim en in volledige vrijheid gestemd wordt. Naar de mening van de regering bleven deze gesignaleerde gevaren echter beperkt tot aanvaardbare proporties aangezien het stemmen per brief alleen mogelijk werd gemaakt voor in het buitenland woonachtige of verblijvende kiezers. Bij het stemmen per brief zijn de risico's voor het geheime en vrije karakter van de stemming derhalve aanvaardbaar geacht, omdat het een beperkte groep kiezers betreft en deze groep, zonder de mogelijkheid van briefstemmen, nauwelijks in staat zou kunnen zijn om te stemmen."

In dezelfde brief geeft de toenmalige minister van BZK Remkes in antwoord op een motie[13] van de Kamer aan dat hij stemmen per brief niet overweegt in te voeren voor kiezers binnen Nederland:

"Over de invoering van briefstemmen is enkele jaren geleden met de Kamer van gedachten gewisseld. De uitkomst van dat debat is geweest dat briefstemmen, gelet op de bezwaren die daaraan verbonden zijn, uitsluitend aan de kiezers in het buitenland zou worden toegestaan. De bezwaren die toentertijd (risico van «Family voting», verkiezingsfraude door onder meer het ronselen van stemmen; vergroting van de werklast voor gemeenten, etc) werden genoemd, gelden naar mijn mening nog steeds. Daarnaast zie ik, ten opzichte van pc- en telefoonstemmen, het bijkomende nadeel dat de kiezer bij briefstemmen geen bevestiging krijgt dat zijn stem is uitgebracht en is opgenomen in de stembus. Dit alles overziend ben ik niet bereid om experimenten uit te voeren met briefstemmen."

Dit standpunt werd ook eerder al in 1997 al ingenomen door de toenmalige minister van Binnenlandse Zaken Hans Dijkstal en minister van Buitenlandse Zaken Hans van Mierlo. Zij schreven[14] aan de Kamer : "*Het onderhavige wetsvoorstel is gericht op een technische verbetering van de briefstemprocedure voor de kiezers die thans van deze procedure gebruik mogen maken. Een eventuele uitbreiding van de kiezersgroep die van de briefstemprocedure gebruik mag maken, is wat de ondergetekenden betreft niet aan de orde.*"

4.3.1 Maatregelen om de risico's van briefstemmen te beperken

Om de hierboven genoemde risico's van briefstemmen te beperken / voorkomen zijn verschillende maatregelen getroffen, welke zijn weergegeven in onderstaande tabel. De maatregelen zijn dekkend noch sluitend; niet alle risico's bij briefstemmen zijn te voorkomen of te corrigeren. In het bijzonder het risico van dat de kiezer niet in vrijheid kan stemmen is niet te voorkomen.

[13] Te Veldhuis/Rehwinkel (over andere manieren van stemmen, 28 600-VII, nr. 11, 5 november 2002)

[14] Zie kst 25306, Nr 5 Wijziging van de Kieswet inzake de uitoefening van het kiesrecht door Nederlanders buiten Nederland. Nota naar aanleiding van verslag

Risico's van briefstemmen:	Maatregelen
Geen geheime stemming	- Bij uitbrengen van de stem: geen maatregel. Het is aan de kiezer om zijn stem uit te brengen op een plek en moment waar geen anderen bij zijn. - Bij stemopneming: door principe van de 'dubbele envelop'. In het briefstembureau worden in twee separate stappen de ingekomen briefstemmen verwerkt: eerst wordt aan de hand van het briefstembewijs gekeken of de stem afkomstig is van een geregistreerde kiezer waarna de gesloten envelop met het stembiljet in een stembus wordt gedeponeerd. In de twee stap worden alle stemmen uit de stembus geteld. Op deze wijze wordt gewaarborgd dat de stem niet kan worden gerelateerd aan een kiezer. Daarnaast is de zitting van het briefstembureau openbaar, eenieder is het toegestaan om te kijken of de procedure van stemopneming correct verloopt. - Bij transport van de briefstem: geen maatregel. Er zijn geen maatregelen ingevoerd om te voorkomen dat een briefstem wordt onderschept en wordt ingezien. Dit proces is onttrokken aan enige vorm van controle, afgezien van de aanwezige controles die (internationale) postbedrijven zelf hebben ingevoerd. Wel zijn er wettelijke bepalingen die het inzien van de briefstem verbieden en strafbaar stellen (grondrecht van briefgeheim en strafbepalingen art 201 Sr Boek 2, titel 8 en hoofdstuk Z van de Kieswet).
Geen vrije stemming	- Inherent aan het feit dat de kiezer zijn stembiljet invult op een door hem te bepalen moment en plaats kan er geen toezicht plaatsvinden vanuit een onafhankelijk stembureau. Daardoor is er geen mogelijkheid om de principes van een vrije stemming te waarborgen. - De belangrijkste maatregel die in dit kader is genomen is *ter beperking van het effect* : beperken van de groep kiezers die gebruik mag maken van de mogelijkheid van briefstemmen.
Misbruik	- Registratieprocedure. De kiezer dient voorafgaand aan elke verkiezing een verzoek in om gebruik te mogen maken van de mogelijkheid tot briefstemmen. Dit verzoek wordt ingediend door een formulier in te sturen, voorzien van handtekening en een kopie van een bewijs van Nederlanderschap. - Briefstembewijs. De kiezer ontvangt een briefstembewijs (vgl. bewijs aan toonder) voorzien van echtheidskenmerken. De kiezer dient dit briefstembewijs voorzien van een handtekening mee te sturen met het stembiljet. Door het briefstembureau wordt de op de briefstembewijs geplaatste handtekening vergeleken met de handtekening op het registratieverzoek. Dit is geen sluitende controle, omdat de personen die de controle uitvoeren geen specialisten zijn in het beoordelen van de authenticiteit van de handtekening.

Risico's van briefstemmen:	Maatregelen
Stemmen worden niet tijdig ontvangen[15]	- Ten eerste wordt in de Kieswet het risico van een te late ontvangst van de briefstembescheiden en het risico van een te late aankomst van de stem bij de kiezer gelegd. Dit omdat anders een 'aanzienlijke vertraging' van het vaststellen van de uitslag zou kunnen worden verwacht. In de MvT van de Kieswet uit 1983 wordt gesteld : "de mogelijkheid per brief te stemmen is een tegemoetkoming aan de kiezer; deze moet de voordelen daarvan afwegen tegen het risico dat zijn stem verloren gaat. De kiezer kan immers ook gebruik maken van de mogelijkheid bij volmacht te stemmen." - Recent (3 juli 2013) is er een wijziging van de Kieswet doorgevoerd om het risico van de late ontvangst te verkleinen. Kiezers op Aruba, Curacao en Sint Maarten kunnen zich laten registreren bij de Nederlandse vertegenwoordiging aldaar en ontvangen ook vandaaruit hun briefstembescheiden. - Bij de verkiezingen voor de leden van het Europese Parlement in 2014 wordt een proef uitgevoerd om het stembiljet per e-mail toe te zenden.

4.4 Risico's van briefstemmen in de praktijk

Er is geen goed beeld voorhanden van de mate waarin de bovengenoemde risico's "geen geheime stemming" en "geen vrije stemming" zich in de praktijk voordoen. Bij het ministerie van BZK noch bij de gemeente Den Haag zijn meldingen bekend van kiezers die niet in vrijheid hun stem hebben kunnen uitbrengen. Ook in de andere landen die onderzocht zijn in het kader van de inventarisatie internetstemmen zijn geen publicaties of meldingen gevonden die er op kunnen wijzen dat het probleem van beïnvloeding of dwang zich bij briefstemmen of internetstemmen in de praktijk heeft voorgedaan. Hieruit mag echter niet worden afgeleid dat het risico zich niet heeft voorgedaan.

Er is wel een beter beeld over de problemen die zich bij briefstemmen voordoen met de registratie en postverzending. De Wereldomroep heeft op basis van door haar ontvangen klachten van kiezers in het buitenland een "zwartboek Verkiezingen 2010" uitgebracht. De problemen en bezwaren die daarin worden genoemd hebben veelal te maken met het registratieproces (administratieve last van steeds opnieuw moeten registreren, fouten bij overnemen persoons- en adresgegevens, onterechte afwijzingen) en de lange doorlooptijd en onbetrouwbaarheid van de

[15] De kiezer die per brief stemt krijgt geen bericht van het briefstembureau of zijn stem tijdig is ontvangen of niet.

internationale post. Ook in andere landen komen veelvuldig klachten naar voren van kiezers uit het buitenland die niet tijdig hebben kunnen stemmen[16].

4.5 Verschillen stemmen per brief en stemmen via internet

In de manier waarop de kiezer zijn stem uitbrengt wijkt internetstemmen uiteraard af van het stemmen per brief. Maar wat zijn nu de principiële verschillen tussen de twee stemvormen, mede indien beschouwd vanuit een risico-perspectief?

In deze vergelijking is de aanname gehanteerd dat er geen verschillen zijn in de procesinrichting: de kiezer dient zich eerst te registreren, ontvangt stembescheiden, maakt zijn keuze op een stembiljet en verstuurd het stembiljet naar het stembureau. Uiteraard zijn er wel verschillen in hoe deze processtappen worden uitgevoerd en in welke vorm informatie en bescheiden worden toegestuurd.

1. Verminderde mogelijkheid tot menselijk waarnemen

Het gebruik van computer en communicatie technologie in het stemproces betekent dat het verloop van het stemproces voor mensen verminderd direct waarneembaar is en daarmee minder *transparant* en *controleerbaar*. Er kunnen zich allerlei dreigingen voordoen ten aanzien van de waarborgen stemgeheim, de kiesgerechtigdheid, de integriteit en de beschikbaarheid van een internetstemsysteem, zonder dat de kiezer, het stembureau of waarnemers dit door hebben. Om deze dreigingen te ontdekken zijn specifieke maatregelen nodig. Veel van deze maatregelen zijn overigens ICT maatregelen, hetgeen tot een recursief effect leidt: ook de correcte werking van deze detectiemaatregelen is niet direct waarneembaar (en vergt specifieke test- en controlemaatregelen). Om het stemproces voor mensen goed waarneembaar, transparant en controleerbaar te maken zijn zo aanvullende maatregelen nodig die de complexiteit van het internetstemsysteem vergroten.

2. Automatisering van fraude

In de paragrafen hiervoor werd al duidelijk dat mogelijkheden tot misbruik niet exclusief zijn voorbehouden aan internetstemmen. Ook in het briefstemproces is het mogelijk om te frauderen. Zo is het mogelijk om de briefstembescheiden van een individuele kiezer te onderscheppen in de post en namens de kiezer een stem uit te brengen. De (enige) controle hiertegen is de vergelijking tussen de handtekening op het briefstembewijs en de handtekening van de oorspronkelijke registratie. Aangezien in het reguliere (handels) verkeer frequent de handtekening wordt gebruikt,

[16] Zie onder meer België waar bij de federale verkiezingen in juni 2010 slechts 2/3e van de stemmen uit het buitenland tijdig aankwamen (http://www.gva.be/nieuws/binnenland/aid987124/slechts-twee-derde-briefstemmen-op-tijd.aspx)

zijn er mogelijkheden[17] om aan de handtekening van een persoon te komen. Indien een kopie van de handtekening eenmaal in bezit is, is vervalsing niet heel moeilijk, juist ook omdat de controle op de handtekening bij het briefstembureau niet door experts gebeurd. Om een dergelijke aanval echt effect te laten hebben op de uitslag, is fraude op grote schaal nodig. Fraude op grote schaal betekent ook een recht evenredig grote inspanning, wat maakt dat er maar weinig partijen zijn die dit zelfstandig kunnen en daar de middelen voor (over) hebben.

In de vergelijking met briefstemmen geldt dat voor veel van de dreigingen rondom internetstemmen de vereiste kennis (en in sommige gevallen ook inspanning) om een dreiging te ontwikkelen weliswaar hoog is, maar de dreiging daarna tegen marginale meerkosten is toe te passen. De schaal waarop de dreiging kan plaatsvinden kan dan ook zeer groot zijn en wordt niet meer bepaald door de vereiste menselijke inzet of middelen. In zekere zin kan gesteld worden dat de dreiging dan geautomatiseerd is. Dit fenomeen is bijvoorbeeld zichtbaar bij computervirussen; alleen bij de ontwikkeling is menselijke inspanning en middelen nodig, de verdere verspreiding wordt door computers uitgevoerd. Recente ontwikkelingen laten overigens zien dat er steeds minder specialistische kennis nodig is om deze dreigingen te kunnen uitvoeren; cybercriminelen verhuren kant en klare malware, virussen en DDoS capaciteit tegen steeds lagere kosten[18].
Is de dreiging eenmaal ontwikkeld of verkregen dan is het met een beperkte inspanning mogelijk om grote aantallen kiezers te weerhouden van het uitbrengen van een stem of om van grote aantallen via het internet uitgebrachte stemmen kennis te nemen of deze te veranderen zonder medeweten van de kiezer en ongeacht de fysieke locatie van de kiezer.

3. Hyper-aandacht

Naast deze principiële verschillen is er ook een ander effect dat we hier aanduiden als het "*Hyper-aandacht" effect*. Elke introductie van nieuwe internet of ICT gebaseerde dienstverlening door de overheid ontvangt al veel aandacht van de media, beveiligingsonderzoekers, hackers, etc. Echter in het geval van internetstemmen zal deze aandacht nog intensiever zijn. Elke fout of onvolkomenheid die optreedt of zou kunnen optreden bij internetstemmen zal breed worden uitgemeten. Hierbij wordt domineert het effect de kans; ook al is de kans zeer klein, als het *kan* misgaan dan wordt daar het maximale *effect* naar toegerekend. Ter illustratie het voorbeeld dat briefstembescheiden bezorgd worden bij de buren van een kiezer in het buitenland. Dit kan er toe leiden dat een niet-kiesgerechtigde kan gaan stemmen. Dit risico zal naar verwachting als acceptabel worden gezien, omdat het slechts één kiezer betreft. Indien echter bij internetstemmen blijkt dat de inloggegevens bij een andere niet-kiesgerechtigde terechtkomen

[17] Daarnaast is het kiezers sinds kort toegestaan om per (niet beveiligde) e-mail hun registratieverzoek (inclusief scan van legitimatiebewijs) toe te sturen. Het is voor aanvallers niet moeilijk om deze e-mails te onderscheppen.

[18] In het Cyber Security Perspectives 2013 rapport van Nationaal Cyber Security Centrum wordt deze trend "Mainstream cyber attacks increasingly become available to the masses" ook benoemd en wordt het voorbeeld gegeven van een DDoS aanval die voor 10 dollar per uur te huur is.

heeft dit een veel groter effect, omdat in zo'n geval aangenomen wordt dat dit zich dan ook op massale schaal zich kan voordoen.

5 DREIGINGSSCENARIO'S

5.1 Focus op risico's gerelateerd aan internetstemmen voor kiezers buiten Nederland

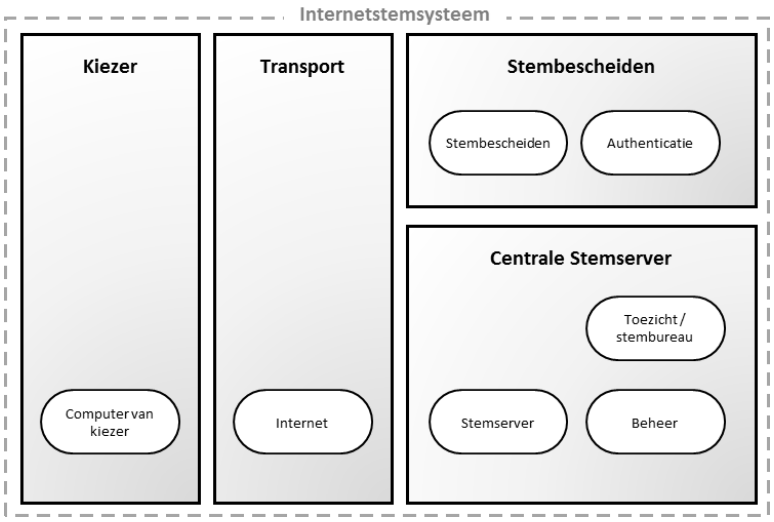
De nu uitgevoerde analyse is een analyse gebaseerd op het proces van internetstemmen, de doelgroep kiezers in het buitenland en stemmethode(n) die daar nu voor zijn toegestaan en de waarborgen waar elk verkiezingsproces aan moet voldoen.

Gegeven de focus van de risico analyse zijn een aantal categorieën risico's buiten beschouwing gelaten omdat deze niet specifiek betrekking hebben op stemmen via internet. Dat betekent uiteraard niet dat met deze risico's geen rekening gehouden hoeft te worden gehouden.

Categorie risico's buiten beschouwing	Voorbeelden van risico's
Project	• Projectbegroting wordt overschreden • Uitlopen op planning • Niet tijdige levering door toeleveranciers
Juridisch	• Juridische procedures n.a.v. eventuele (EU-) aanbesteding • Wetsvoorstel wordt niet of niet tijdig aangenomen • Stemsysteem maakt inbreuk op intellectuele eigendomsrechten (patenten) van derden
Politiek-bestuurlijk	• Draagvlak experiment verdwijnt door andere bewindspersoon of politieke prioriteiten
Organisatie	• Onvoldoende deskundigheid bij toeleverancier(s) • Beschikbaarheid van eigen personeel • et cetera

5.2 Onderzoeksdomeinen

Ten behoeve van de risicoanalyse is het internetstemsysteem onderverdeeld in een aantal logisch van elkaar te scheiden domeinen. In de risicoanalyse wordt gerefereerd aan deze domeinen.



Domein	Toelichting
Stembescheiden	Het geheel van mensen, processen, systemen en middelen dat gebruikt voor de productie en verzending van de stembescheiden en de productie, uitgifte aan en verificatie van authenticatiemiddelen van kiezers.
Kiezer	De kiezer, en zijn systemen (computer, programmatuur, internetaansluiting) en middelen benodigd om te kunnen stemmen.
Transport	De gebruikte publieke of private middelen of diensten voor het elektronisch of per post overbrengen van gegevens of documenten.
Centrale stemserver	Het geheel van mensen, processen, systemen en middelen dat voorziet in de centrale functionaliteit van het internetstemsysteem. Voorbeelden van centrale functies zijn: distributie van stemprogrammatuur aan de kiezer, opslaan van ontvangen stemmen, tellen van stemmen, etc. Het stemserver domein kan meerdere separate objecten bevatten.
Toezicht (stembureau)	Het geheel van mensen, processen, systemen en middelen dat toezicht houdt op het correcte verloop van de verkiezing en dat benodigd is voor de bediening van de Server.

Het registratiesysteem wordt beschouwd als een separaat systeem welke geen onderdeel uitmaakt van het *internetstemsysteem*.

5.3 Inschatting van kans en effect

In deze risicoanalyse is per dreigingsscenario een inschatting gemaakt van het risico, welke bepaald wordt door de *kans* op het optreden van een ongewenste gebeurtenis (door een oorzaak) met een (veelal negatief) *effect*. De grootte van het risico wordt bepaald door zowel de kans als het effect.

Hierbij wordt het effect zwaarder gewogen dan de kans, vanuit de overweging dat gegeven het absolute karakter van sommige waarborgen én het maatschappelijk belang van verkiezingen ook een dreigingsscenario met een kleine kans van optreden toch beschouwd moet worden als een middel of groot risico kans indien het effect respectievelijk middel of groot is.

Weging Risico		Effect		
		Klein	Middel	Groot
Kans	Klein	*Klein*	*Middel*	*Groot*
	Middel	*Klein*	*Middel*	*Groot*
	Groot	*Middel*	*Groot*	*Groot*

Bij de inschatting van de kans is gekeken naar een aantal dimensies:

- de kwetsbaarheid van het proces c.q. internetstemsysteem;
- heeft de dreiging zich eerder in Nederland of in het buitenland in de praktijk voorgedaan;
- de waarschijnlijkheid dat een dreigingsscenario zich zal voordoen;
- is er een actor met een reëel belang die beschikt ook over de benodigde middelen?

De inschatting van de kans is een kwalitatieve inschatting, er is geen stochastische of mathematische modellering toegepast.

De kans dat een dreigingsscenario daadwerkelijk optreedt wordt mede beïnvloed door de maatregelen die genomen worden om de dreiging te voorkomen.

Voor de inschatting van het effect is gekeken naar de volgende dimensies:

- worden één of meer waarborgen getroffen?
- de schaal van de dreiging; hoeveel kiezers worden getroffen ?
- heeft de dreiging een effect op de uitslag van de verkiezing?

Net als voor de kans geldt dat het effect van een dreigingsscenario mede bepaald wordt door de maatregelen die genomen worden om het effect te mitigeren. Deze maatregelen worden per dreigingsscenario beschreven.

5.4 Actoren

Relevant voor de inschatting van de waarschijnlijkheid dat een dreiging optreedt is de aanwezigheid van een organisatie of persoon die een reëel belang heeft bij het effect van de dreiging én die beschikt over de middelen om de dreiging uit te voeren. Deze organisatie of persoon wordt een actor genoemd. In onderstaande tabel is een overzicht gegeven van de actoren met hun mogelijke belangen. Dit overzicht is overgenomen vanuit het Cybersecuritybeeld

Nederland[19] dat jaarlijks door het Nationaal Cyber Security Centrum (NCSC) van de Nederlandse overheid wordt opgesteld.
Aan deze lijst van actoren zijn specifiek voor de context van verkiezingen een viertal actoren toegevoegd: de eigen overheid, politieke groeperingen, het stembureau en de kiezer. Hieruit mag niet worden afgeleid dat deze actoren in het verleden ook daadwerkelijk een dreiging hebben uitgeoefend op het verkiezingsproces. Het is echter onverstandig om de actoren met een belang alleen in de buitenwereld te zoeken, de dreiging kan ook vanuit de zittende bestuurders, de politiek, het stembureau of individuele kiezers komen. Een solide internetstemsysteem moet dusdanig ontworpen zijn dat weerstand geboden wordt tegen dreigingen van binnenuit.

	Actor	Belangen / drijfveer in geval van bewust handelen
A1	Staten	Vormen onderdeel van de overheid van een ander land (synoniem: vreemde mogendheid). Intentie geopolitieke positie verbeteren of invloed uitoefenen op dissidenten/oppositiegroeperingen.
A2	Terroristen	Handelend vanuit ideologische motieven. Intentie maatschappelijke verandering, veiligheidsgevoel aantasten of beïnvloeden politieke besluitvorming.
A3	Beroepscriminelen	Criminele activiteiten ontplooien t.b.v. geld verdienen (synoniem: cybercriminelen).
A4	Cybervandalen en Scriptkiddies	Handelend vanuit technologische uitdagingen, baldadigheid en ego.
A5	Hacktivisten	Handelend vanuit ideologische motieven (diverse motieven, snel wisselende groeperingen).
A6	Interne actor	Medewerkers, (voormalig) personeel en leveranciers, handelend vanuit wraak, financieel gewin en/of politiek onvrede (synoniem: 'insiders').
A8	Cyberonderzoekers	Onderzoeker(s) handelend vanuit ideële-, financiering- of wetenschappelijke motieven (en ego).
A9	Private organisaties	Bedrijven, organisatie handelend vanuit concurrentiepositie verbetering.
A10	Eigen overheid	Handelend vanuit de intentie invloed uit te oefenen op de uitslag van de stemming of om invloed uit te oefenen op dissidenten / oppositiegroeperingen.
A11	Kiezer	Handelend vanuit onvrede met de zittende regering. Intentie om invloed uit te oefenen op de uitslag van de stemming.
A12	Politieke groepering	Handelend vanuit de intentie invloed uit te oefenen op de uitslag van de stemming om zo meer stemmen te verkrijgen.
A13	Stembureau	Handelend vanuit de intentie invloed uit te oefenen op de uitslag van de

[19] Zie voor de meest actuele versie van het CSBN de website van het NCSC: www.ncsc.nl

Actor	Belangen / drijfveer in geval van bewust handelen
	stemming of om bevriende personen / organisaties te bevoordelen.

5.5 Overzicht dreigingsscenario's

In onderstaande tabel zijn de dreigingsscenario's beschreven die zich kunnen voordoen bij internetstemmen voor kiezers buiten Nederland.

De dreigingsscenario's zijn in detail beschreven in bijlage A. In de bijlage is per dreigingsscenario aangegeven welke actor een belang heeft bij de dreiging, hoe het dreigingsscenario kan optreden, of het een nieuwe dreiging betreft of één die ook bij briefstemmen reeds bestaat en op welke waarborgen en processtappen het dreigingsscenario betrekking heeft.

De lijst van dreigingsscenario's is niet uitputtend in de beschrijving van de manieren waarop een dreiging zich kan voordoen. Dat zou ondoenlijk en speculatief zijn, gelet op het feit dat deze risicoanalyse niet op een specifiek ontwerp of implementatie betrekking heeft.

In Bijlage B is per dreigingsscenario weergegeven in welke processtap(pen) deze kan optreden.

In het overzicht zijn de dreigingsscenario's ingedeeld in vier categorieën:

I. *Bewust menselijk handelen*: dreigingsscenario die wordt veroorzaakt door één of meerdere actoren die handelen om een specifiek belang te realiseren;
II. *Onbewust menselijk handelen*: dreigingsscenario's waarbij één of meerdere actoren een rol speelt zonder dat een specifiek belang is;
III. *Systeemfalen of technisch falen*: dreigingsscenario's die voorvloeien uit het niet correct functioneren van het internetstemsysteem; en
IV. *Force Majeur*: dreigingsscenario's die het gevolg zijn van overmacht situaties zoals natuurrampen, pandemiën, et cetera.

Categorie	DS	Dreigingsscenario's
Bewust menselijk handelen	1	Publiceren informatie over beveiliging internetstemsysteem
	2	Verkopen stem
	3	Dwang / beïnvloeding van kiezer
	4	Niet-kiesgerechtigde brengt stem uit
	5	Manipuleren van de stem of uitslag
	6	Kiezer brengt meer dan één stem uit
	7	Chantage
	8	Relatie tussen kiezer en inhoud stem (doorbreken stemgeheim)
	9	Doelbewust verstoren van de verkiezing

Categorie	DS	Dreigingsscenario's
	10	Defacing / bekladding internetstemsysteem
	11	Springplank: misbruik systeem voor andere aanvallen
	12	Voortijdige publicatie uitslag
	13	Onvoldoende inzicht en begrip kiezers
Onbewust menselijk handelen	14	Bedienfouten kiezer
	15	Incorrecte installatie
	16	Incorrecte beheer/bediening
	17	Incorrecte de-installatie
Systeemfalen of technisch falen	18	Stembescheiden komen niet aan bij kiezer of zijn onjuist
	19	Functionele, technische of beveiligingsgebreken
	20	Ontoegankelijkheid
Force Majeur	21	Onbeschikbaarheid

5.6 Maatregelen

Het risico van de dreigingsscenario's is eerst ingeschat op basis van een situatie zonder dat er maatregelen zijn genomen. Hiervoor is gekozen omdat dit een zuivere inschatting geeft van het risico, zonder in een ontwerpmodus van een internetstemsysteem te geraken. Tegelijkertijd is het niet realistisch om een internetstemsysteem te beschouwen zonder enige maatregelen. In bijlage A is daarom per dreigingsscenario ook aangegeven welke maatregen mogelijk zijn om deze dreigingsscenario's te voorkomen. Dit is per dreigingsscenario aangegeven onder het kopje 'Preventief'. Ook is aangegeven welke maatregelen mogelijk zijn om, in de situatie dat de dreiging zich daadwerkelijk heeft voorgedaan, het effect te beperken of te repareren. Dit is per dreigingsscenario aangegeven onder het kopje 'Correctief'.

Evenzo dat deze risicoanalyse niet alle mogelijke manieren beschrijft waarop een dreigingsscenario zich kan voordoen, is geen poging gedaan om een uitputtend overzicht op te stellen van alle denkbare maatregelen om dreigingen te voorkomen of te verhelpen. Een dergelijke uitputtende set van maatregelen dient in de ontwerpfase van een internetstemsysteem uitgevoerd te worden. Daarbij verdient het aanbeveling om, naast de preventieve en correctieve maatregelen ook aandacht te geven aan maatregelen om dreigingen te detecteren en maatregelen om het effect te mitigeren.

In bijlage A is per dreigingsscenario ook aangegeven wat het risico is indien de mogelijke maatregelen in ogenschouw worden genomen. Dit is aangegeven onder het kopje 'Risico inschatting na maatregelen'.

De beveiliging van de informatiesystemen in het Server domein van het internetstemsysteem vereist bijzondere aandacht. In de opsomming van mogelijke preventieve maatregelen bij een

aantal dreigingsscenario's wordt met de maatregel "beveiliging internetstemsysteem" verwezen naar een aantal richtlijnen en maatregelen die zijn opgenomen in bijlage E. De exacte set van maatregelen moet bepaald worden in de ontwerpfase van het internetstemsysteem.

6 RISICO'S INTERNETSTEMMEN

6.1 Risico-inschatting van de dreigingsscenario's

In onderstaande tabel zijn de dreigingsscenario's weergegeven, gerangschikt naar de risico-inschatting Groot, Middel en Klein. Voor de risico-inschatting is gebruik gemaakt van de wegingstabel uit 5.3. Hierbij is het effect van mogelijke preventieve en correctieve maatregelen meegewogen. Binnen de indeling G, M en K is geen verdere weging of prioritering aangebracht.

Risico	DS	Dreigingsscenario's
G	4	Niet-kiesgerechtigde brengt stem uit
G	5	Manipuleren van de stem of uitslag
G	8	Relatie tussen kiezer en inhoud stem (doorbreken stemgeheim)
G	15	Incorrecte installatie
G	16	Incorrecte beheer/bediening
G	19	Functionele, technische of beveiligingsgebreken
M	1	Publiceren informatie over beveiliging internetstemsysteem
M	2	Verkopen stem
M	3	Dwang / beïnvloeding van kiezer
M	6	Kiezer brengt meer dan één stem uit
M	7	Chantage
M	9	Doelbewust verstoren van de verkiezing
M	10	Defacing / bekladding internetstemsysteem
M	13	Onvoldoende inzicht en begrip kiezers
M	17	Incorrecte de-installatie
M	21	Onbeschikbaarheid
K	11	Springplank: misbruik systeem voor andere aanvallen
K	12	Voortijdige publicatie uitslag
K	14	Bedienfouten kiezer
K	18	Stembescheiden komen niet aan bij kiezer of zijn onjuist
K	20	Ontoegankelijkheid

6.2 Risico's per waarborg in vergelijking tot briefstemmen

In deze paragraaf is per waarborg aangegeven welke dreigingsscenario's een middel of groot risico kennen. Hierbij is ook waar mogelijk ook de vergelijking gemaakt met de risico's van het huidige proces van briefstemmen.

TRANSPARANTIE

De mate waarin internetstemmen voldoet aan de waarborg van transparantie wordt in belangrijke mate bepaald door het ontwerp en de implementatie van het internetstemsysteem.
Uit internationale ervaringen en uit de eerdere Kiezen op Afstand projecten, is naar voren gekomen dat eenvoud, communicatie / voorlichting en een intuïtieve gebruikersinterface de bepalende factoren zijn in de mate waarin de kiezer het verkiezingsproces doorgrond. Door het internetstemsysteem in de ontwerpfase te testen met representatieve groepen gebruikers kan de gebruikersinterface en de documentatie / voorlichting verbeterd worden.
Het begrip van kiezer van het stemproces en de stemmethode hangt ook samen met de frequentie van gebruik en de daarmee optredende gewenning.

Om dreigingsscenario's zoals het doorbreken van het stemgeheim of het manipuleren van de stem te voorkomen worden technische maatregelen voorzien zoals cryptografie. Op conceptueel niveau is zoiets als versleuteling voor veel mensen nog begrijpelijk, maar het doorgronden van de exacte werking en kunnen beoordelen van de implementatie is alleen voorbehouden aan specialisten. Los van de toepassing van deze specialistische technologie geldt in algemene zin dat door het gebruik van ICT het voor mensen minder goed mogelijk is om de werking te beoordelen vanuit directe eigen waarneming. Zie ook paragraaf 4.5.

In die zin is een internetstemsysteem, door haar gebruik van technologie zowel voor kiezers als voor het stembureau, minder transparant dan de briefstemmethode.

CONTROLEERBAARHEID

De verminderde transparantie heeft ook een relatie met de waarborg van controleerbaarheid. Voor het stembureau geldt dat het verloop van het verkiezingsproces niet te volgen en te sturen is, tenzij in het internetstemsysteem daartoe specifieke functionaliteit is opgenomen. Tot op zekere hoogte is dit niet anders dan in de situatie van briefstemmen; ook daar moet het briefstembureau afwachten welke stemmen binnenkomen. Wel heeft het briefstembureau directe controle over de stappen die daarna volgen: het verifiëren van de briefstembewijzen en het op grond daarvan 'toelaten' van stemmen van kiezers, het deponeren van de stemmen in de stembus en de stemopneming. Ook zijn deze stappen door waarnemers in volledige openheid te volgen en daarmee te controleren.

Voor de kiezer is internetstemmen niet meer of minder te controleren dan in geval gestemd wordt per brief. De kiezer zou in principe kunnen afreizen naar het briefstembureau om te controleren dat zijn briefstembewijs wordt geaccepteerd en daarmee zijn stem wordt gedeponeerd in de stembus. In de praktijk zal dit door de geografische afstand zelden gebeuren, hetgeen betekent dat in de praktijk ook de kiezer die per brief stemt niet in staat is om te controleren of zijn stem is aangekomen en of deze (correct) is meegeteld. Zoals beschreven in paragraaf 2.8 van Deel I - Internationale inventarisatie internetstemmen zijn er vanuit de wetenschap en bedrijfsleven verschillende technieken ontwikkeld om aanvullende controles mogelijk te maken voor kiezers ('individual verifiability') en voor derden ('universal verifiability'). Een deel van deze technieken biedt een verdergaande controle aan de kiezer, doordat niet alleen gecontroleerd kan worden of

de stem goed is ontvangen, maar ook of deze is 'opgeslagen zoals ontvangen', 'geteld zoals opgeslagen' of zelfs 'geteld zoals bedoeld'.

INTEGRITEIT

In de risicoanalyse zijn meerdere dreigingsscenario's onderkend die de waarborg van integriteit raken, waaronder de twee dreigingsscenario's *Niet-kiesgerechtigde brengt stem uit* en *Manipuleren van de stem of uitslag* waarvan het risico als groot is ingeschat. De mate waarin aan de waarborg van integriteit kan worden voldaan hangt primair af van het ontwerp van het internetstemsysteem en de mate waarin dit ontwerp correct is geïmplementeerd. Met de juiste technische maatregelen zoals hashing en encryptie zijn maatregelen mogelijk om manipulatie tijdens het transport van de stem te ontdekken en te voorkomen. Het is onmogelijk om vanuit de overheid de computer van de kiezer te beschermen tegen manipulatie. Deze manipulatie (in een scenario waarbij een aanvaller heimelijk malware heeft weten te installeren op de computer van de kiezer en daarmee de uitgebrachte stem wijzigt) is daarnaast ook bijzonder lastig te detecteren. Het is alleen de kiezer zelf die kan verifiëren of zijn stem wordt gemanipuleerd, mits gebruik gemaakt wordt van een vorm van controle waarbij de kiezer kan zien of zijn stem correct is aangekomen (zie ook hierboven onder controleerbaarheid).
Manipulatie van de stem kan zich in theorie ook voordoen in geval van briefstemmen, bijvoorbeeld tijdens het transport. Daar zijn nu geen maatregelen voor getroffen, zie ook paragraaf 4.3.1.

KIESGERECHTIGDHEID

Of een kiezer kiesgerechtigd is wordt vastgesteld in het registratieproces bij het beoordelen van het registratieverzoek. Dit is ongeacht of de kiezer aangeeft of hij per brief of via internet wil stemmen. Het registratieproces staat los van het stemmen via internet en is door de opdrachtgever buiten de reikwijdte van de risicoanalyse naar internetstemmen geplaatst. Het stemmen via internet levert derhalve geen risico's op ten aanzien van het vaststellen van de kiesgerechtigdheid.
Een direct aan de registratie gerelateerd proces is dat van de authenticatie van de kiezer. Zoals ook al in paragraaf 3.3.1 is geconstateerd, zal de authenticatie van de kiezer die via internet stemt anders verlopen dan bij briefstemmen. In de risicoanalyse zijn dreigingsscenario's onderkend waarin een derde de authenticatiegegevens van de kiezer onderschept en (heimelijk) een stem uitbrengt alvorens de kiezer dit kan doen. Ook het authenticatiemiddel zelf kent risico's. Een onvoldoende betrouwbaar authenticatiemiddel kan bijvoorbeeld worden geraden, nagespeeld worden of via een zgn. 'man in the middle' aanval worden omzeild. Hierdoor kan de situatie ontstaan dat een niet-kiesgerechtigde kiezer toch een stem kan uitbrengen.

Dit kan zich ook voordoen als een kiezer zijn authenticatiemiddel doorgeeft of verkoopt aan een ander. Dit is niet volledig te voorkomen en ook in de huidige situatie van briefstemmen mogelijk. De kans en daarmee het risico dat een kiezer dit doet wordt naar verwachting wel kleiner naarmate het te gebruiken authenticatiemiddel ook voor andere diensten, transacties en toepassingen wordt gebruikt. De kiezer zal zijn authenticatiemiddel dan naar verwachting minder snel weggeven omdat het risico op misbruik in andere situaties dan toeneemt.

STEMVRIJHEID

Aan de waarborg van stemvrijheid kan niet worden voldaan. Internetstemmen vindt plaats vanuit een omgeving die niet door het stembureau (of door een andere overheidsorganisatie) kan worden gecontroleerd.
In andere landen, zoals Estland en Noorwegen, is besloten om een systematiek in te voeren waarin de kiezer meerdere keren kan stemmen via internet en waarbij alleen de laatste stem geldt. Dit vanuit de gedachte dat een onder druk gezette kiezer later zijn stem kan herzien. Dit biedt naar onze mening bescherming, maar niet in absolute zin. Immers als er sprake is van echte dwang kan de dreiger ook de stembescheiden afnemen of de kiezer fysiek belemmeren om deel te nemen aan de stemming.
Het risico dat dwang of beïnvloeding plaatsvindt op de kiezer is een van de restrisico's van stemmen door kiezers buiten Nederland, of dat nu internetstemmen, briefstemmen of volmachtstemmen betreft. De kans dat dit op massale schaal plaatsvindt wordt overigens als klein ingeschat. Het is lastig voor één actor om deze dreiging op grote schaal uit te oefenen op een groep geografische verspreidde kiezers.

STEMGEHEIM

Doordat niet kan worden voldaan aan de waarborg van stemvrijheid geldt ook voor de waarborg van het stemgeheim dat dit niet door de overheid kan worden gegarandeerd aan de kant van de kiezer. Dit is overigens niet anders dan bij briefstemmen. Ook daar kan deze waarborg *aan de kant van de kiezer* niet door de overheid worden gegarandeerd. Daarnaast zijn er in het geval van stemmen via internet ook dreigingsscenario's, die eerder ook al zijn genoemd onder de waarborg van integriteit, die er toe kunnen leiden dat aanvallers met malware heimelijk op de computer van de kiezer afluisteren wat de kiezer stemt.

Voor het transport van de stem en aan de kant van de stembus / het stembureau is het wel mogelijk om te voldoen aan de waarborg van het stemgeheim, er vanuit gaande dat de gebruikte methode van versleuteling niet wordt doorbroken[20]. Of daadwerkelijk aan de waarborg wordt voldaan hangt echter af van het ontwerp van het internetstemsysteem en of het ontwerp correct is geïmplementeerd. Er zijn meerdere technische maatregelen beschikbaar waarmee de stem kan worden versleuteld zodat een tijdens het transport van kiezer naar stembus onderschepte stem niet kan worden ingezien. Ten aanzien van het transport van de stem zijn er voor internetstemmen betere middelen voorhanden om aan de waarborg te voldoen dan voor een stem die per brief in de reguliere post wordt verstuurd.
Op de plek waar de uitgebrachte stemmen worden ontvangen en worden opgeslagen in de stembus zijn aanvullende maatregelen nodig om te voorkomen dat voorafgaand, tijdens of na de stemopneming een relatie gelegd kan worden tussen de kiezer en de inhoud van de stem. Ook

[20] Het kan niet worden uitgesloten dat sommige actoren (bijvoorbeeld Staten) beschikken over de middelen om versleutelde stemmen te ontsleutelen. Ook kan een encryptietechnologie die nu als veilig wordt beschouwd in de toekomst 'gekraakt' worden.

hiervoor geldt dat het ontwerp en implementatie doorslaggevend zijn of daadwerkelijk aan de waarborg kan worden voldaan. Deze dreiging kan zowel komen van buitenstaanders als insiders (zoals stembureauleden, beheerders, auditors).

UNICITEIT

Ook de mate waarin aan de waarborg van uniciteit van de stem kan worden voldaan hangt af van het ontwerp van het internetstemsysteem en de mate waarin dit ontwerp correct is geïmplementeerd. Er zijn verschillende 'plekken' denkbaar waar gebreken in het internetstemsysteem kunnen leiden tot het meervoudig stemmen door een kiesgerechtigde kiezer: de stemprogrammatuur voor de kiezer, de programmatuur aan de serverzijde van het internetstemsysteem, et cetera.
De vraag is of deze waarborg zo letterlijk moet worden geïnterpreteerd dat een kiezer maar één keer zijn stem mag uitbrengen. In het huidige kiesstelsel is dat wel het geval. Het kan voordelen hebben om een kiezer meerdere keren te laten stemmen, bijvoorbeeld als hij zijn stem wil herzien of als hij twijfelt of zijn stem goed is aangekomen. In dat geval moet (wettelijk) geregeld worden welke van de uitgebrachte stemmen dan meegeteld moet worden.

TOEGANKELIJKHEID

De toegankelijkheid van het internetstemsysteem is niet minder goed dan de toegankelijkheid van het briefstemproces. De voorwaarde dat een kiezer beschikt over een computer was wellicht vroeger een beperkende factor, maar is dat nu en in de toekomst zeker niet meer. De toegankelijkheid wordt verder beïnvloedt door ontwerpkeuzes op het vlak van de authenticatiemethode en specifieke vereisten aan hardware en software.
Vanuit het oogpunt van toegankelijkheid (en beschikbaarheid) is het wenselijk dat de kiezer tot op het moment van stemmen (en niet al bij het indienen van het registratieverzoek) kan beslissen of hij per internet of per brief wil stemmen. Om te voorkomen dat dit leidt tot het meetellen van meerdere stemmen per kiezer (waarborg uniciteit), zal bij de stemopneming van de internetstemmen rekening gehouden moet worden met eventuele per brief uitgebrachte stemmen. De briefstembureaus dienen daartoe door te geven aan het internetstembureau welke kiezers per brief hebben gestemd, opdat in het internetstembureau kan worden bepaald of diezelfde kiezer ook via internet heeft gestemd. De consequentie van deze terugvaloptie is ook dat er een nieuwe fout-kans ontstaat, die mogelijk afbreuk doet aan de waarborg van uniciteit. Indien er geen of een onjuiste relatie wordt gelegd tussen de kiezer die per brief een stem uitbrengt en de stem of stemmen die deze kiezer via internet uitbrengt kan dit leiden tot het ten onrechte meetellen van meerdere stemmen van één en dezelfde kiezer of tot het ten onrechte niet meetellen van een internetstem van een kiezer. Ook creëert het een nieuwe tijdsafhankelijkheid tussen de stemopneming in het briefstembureau en de stemopneming in het internetstembureau.

BESCHIKBAARHEID

Een internetstemsysteem is kwetsbaar voor dreigingsscenario's die er opgericht zijn het verkiezingsproces te verstoren. In het bijzonder DDoS aanvallen op de servers van een internetstemsysteem hebben potentieel een groot effect doordat het internetstemsysteem onbeschikbaar raakt voor de kiezer. Met deze dreiging zal nadrukkelijk in het ontwerp van het

internetstemsysteem rekening gehouden moeten worden. Daarnaast zijn aanvullende maatregelen nodig in samenwerking met andere organisaties zoals Internet Service Providers, operators, netwerk exchanges en opsporingsdiensten om een DDoS aanval vroegtijdig te kunnen detecteren, af te weren en de daders op te sporen.

TIJDIGHEID

De problematiek van de trage en onbetrouwbare postverzending heeft minder effect bij internetstemmen dan bij briefstemmen, doordat de postzending van de stem naar het stembureau komt te vervallen. Als ook de stembescheiden in elektronische vorm aan de kiezer worden toegestuurd dan neemt de problematiek verder af. Of een elektronische verzending passend en betrouwbaar genoeg is hangt onder meer af van de wijze waarop de authenticatie van de kiezer plaatsvindt (moet er een PIN code o.i.d. naar de kiezer worden gestuurd of wordt er gebruik gemaakt van een authenticatiemiddel dat de kiezer reeds eerder heeft verkregen?) en of er voor wordt gekozen om de kiezer pas bij het uitbrengen van de stem te laten bepalen of hij dit per brief of via internet wil doen. In dat laatste geval moet verder nagedacht worden hoe de kiezer dan tijdig aan een briefstembewijs komt; bijvoorbeeld door deze uit te printen.

VERGELIJKING PER WAARBORG

In onderstaande tabel is per waarborg aangegeven in welke mate internetstemmen voldoet aan de waarborg *ten opzichte* van het huidige proces van briefstemmen.

Waarborg	Voldoet Minder of Meer	Korte toelichting
Transparantie	Minder	Door gebruik van ICT is het voor mensen minder goed mogelijk om de werking te beoordelen vanuit directe eigen waarneming.
Controleerbaarheid	Minder	Correcte verloop van stemming is alleen indirect te controleren, met behulp van ICT
Integriteit	Minder tot Gelijk	Is afhankelijk van goed ontwerp en implementatie van internetstemsysteem.
Kiesgerechtigdheid	Gelijk	Wordt bepaald door registratieproces.
Stemvrijheid	Gelijk	Zowel bij briefstemmen als bij internetstemmen kan niet aan deze waarborg worden voldaan.
Stemgeheim	Minder tot Gelijk	Aan de kant van de kiezer kan niet aan deze waarborg worden voldaan. Voor het transport van de stem en aan de zijde van het stembureau is het afhankelijk van een goed ontwerp en foutloze implementatie van internetstemsysteem. Bij gebruik van specifieke cryptografische maatregelen is stemgeheim beter te waarborgen dan in briefstembureau.

Waarborg	Voldoet Minder of Meer	Korte toelichting
Uniciteit	Minder tot Gelijk	Is afhankelijk van goed ontwerp en implementatie van internetstemsysteem.
Toegankelijkheid	Minder tot Meer	Is afhankelijk van ontwerp van internetstemsysteem. Indien specifieke middelen vereist worden neemt de toegankelijkheid af, bij geschiktheid voor minder validen neemt de toegankelijkheid toe
Beschikbaarheid	Minder	Kwetsbaarheid centrale Server domein
Tijdigheid	Gelijk tot Meer	Is afhankelijk van ontwerp van internetstemsysteem. Geen vertraging bij elektronische verzending stembescheiden / gebruik bestaand authenticatiemiddel.

6.3 Observaties uit de risicoanalyse

6.3.1 Internetstemsysteem is complex, maar niet door functionaliteit

Een internetstemsysteem is een complex informatiesysteem. De complexiteit wordt niet bepaald door de functionaliteit van het internetstemsysteem, die is namelijk relatief eenvoudig. Wat het complex maakt zijn de stringente eisen die voortvloeien uit de waarborgen controleerbaarheid, integriteit, stemgeheim, uniciteit en beschikbaarheid die maken dat het systeem geen enkele gebreken mag bevatten, de exacte werking gegarandeerd en controleerbaar moet zijn, het systeem intensief beheerd en beveiligd moet worden en dat het systeem niet alleen sterk beschermd moet zijn tegen dreigingen van buitenaf, maar ook tegen misbruik en dreigingen van binnenuit (zoals beheerders). Het ontwerpen, ontwikkelen en testen van deze, veelal ook technische, maatregelen maakt het systeem uiterst complex, mede omdat het geen routine werkzaamheden betreft maar een innovatief en niet in de praktijk beproefd systeem.

6.3.2 Ontwerp en implementatie zijn sterk bepalend voor mate waarin aan de waarborgen wordt voldaan

Of internetstemmen voldoet aan de waarborgen is in sterke mate afhankelijk van het internetstemsysteem en de daarin gebruikte technologie. Het kan niet gesteld worden dat internetstemmen in haar aard niet voldoet aan de waarborgen, met uitzondering van de waarborgen van stemvrijheid en stemgeheim.
Maar om aan de overige waarborgen te voldoen is een uitgebreide set van maatregelen, procedures en aanvullende systemen nodig om bestand te zijn tegen alle dreigingsscenario's en om de belangrijkste kwetsbaarheden in het proces en het systeem te elimineren. Naast een kwalitatief goed en doordacht ontwerp is ook de wijze waarop het internetstemsysteem wordt ontwikkeld, geïnstalleerd, beheerd, bediend en ontmanteld bepalend of in de praktijk aan de waarborgen wordt voldaan.

6.3.3 Maatregelen leiden tot aanvullende maatregelen

Uit de risicoanalyse is gebleken dat voor het voorkomen van dreigingen maatregelen genomen moeten worden die op zich zelf nieuwe dreigingen introduceren. En ook voor die afgeleide dreigingen dienen aanvullende maatregelen te worden genomen.

Als voorbeeld geven we hier een serie van maatregelen die noodzakelijk zijn rondom de versleuteling van de stem. Aanname hierbij is dat de versleuteling plaatsvindt op basis van een asymmetrisch cryptografisch algoritme, als bescherming tegen de dreiging van afluisteren en / of manipulatie van de stem. De generatie van het sleutelpaar en de veilige opslag van de sleutels en certificaten vereist aanvullende maatregelen, zoals bijvoorbeeld een Hardware Security Module. En om de kiezer zekerheid te geven dat hij de stem met de juiste publieke sleutel versleuteld, zal de authenticiteit en integriteit van de publieke sleutel aangetoond moeten worden door deze te certificeren via een Public Key Infrastructure. Dit kan een bestaande PKI zijn (zoals PKI Overheid), of een eigen PKI. In het laatste geval moet de fysieke en logisch inrichting van de PKI aan zware beveiligingseisen voldoen om te voorkomen dat niet-geautoriseerden een eigen publieke sleutel ten onrechte kunnen waarmerken met het certificaat behorende bij het internetstemsysteem.

Een ander voorbeeld zijn controlemaatregelen voor de kiezer. Zo is in Noorwegen een systeem toegepast waarbij de kiezer kan verifiëren dat de inhoud van de stem correct is ontvangen. Na het uitbrengen van de stem ontving de kiezer een SMS bericht op zijn mobiele telefoon met een ‘return code’ en informatie over het aantal keren dat door hem is gestemd. De return code moet overeenkomen met de informatie op de stemkaart. Om deze controle maatregel mogelijk te maken is een uitgebreide set van functionaliteiten én daarop van toepassing zijnde aanvullende (beveiligings)maatregelen nodig om die return codes te genereren en om gepersonaliseerde stembescheiden te drukken en te versturen.

De voorbeelden laten zien dat het ontwerpproces van het internetstemsysteem in meerdere iteratieslagen moeten worden uitgevoerd, waarbij steeds opnieuw de risico’s moeten worden beoordeeld na elke ontwerpslag. Dit geldt niet alleen voor alle maatregelen die genomen worden op het gebied van beveiliging van het internetstemsysteem, maar ook voor ontwerpkeuzes in andere processtappen en voor maatregelen die tot doel hebben om de beschikbaarheid te vergroten.

6.3.4 De beperkte omvang van de doelgroep verkleint het risico op manipulatie van de uitslag

Uit het overzicht van actoren is af te leiden dat er een aantal actoren een belang kunnen hebben bij het manipuleren van de uitslag van een verkiezing in Nederland. Een scenario is denkbaar dat politieke partijen, leden van een stembureau, andere staten en private organisaties er een belang bij hebben dat specifieke kandidaten / politieke partijen in het Nederlandse parlement of het Europese parlement worden verkozen of juist niet worden verkozen, vanwege (geo)politieke, economische of militaire belangen.

Het effect van één stem meer of minder is in Nederlandse kiesstelsel echter beperkt. In tegenstelling tot andere landen waar een 'first past the post' systeem geldt, kennen we in Nederland het systeem van evenredige vertegenwoordiging. Een kandidaat van een politieke partij kan pas verkozen worden tot het parlement indien deze een minimaal aantal stemmen heeft gekregen, de zgn. kiesdrempel. Bij de meest recente TK verkiezingen in 2012 werden er ruim 9,4 miljoen stemmen uitgebracht en was de kiesdrempel/kiesdeler 62.828.
Het merendeel van de stemmen wordt in Nederland uitgebracht op de eerste kandidaat van de lijst. Kiezers kunnen zelf invloed uitoefenen op welke kandidaten zetels toegewezen krijgen door op een specifieke kandidaat te stemmen. Een kandidaat wordt met voorkeurstemmen gekozen als hij ten minste een aantal van 25% van de kiesdeler aan stemmen gehaald heeft, en de laagst geplaatste kandidaat die een zetel zou zijn toegewezen minder voorkeurstemmen heeft. De kiesdeler is gelijk aan de kiesdrempel. Voor de verkiezing van de leden van het Europees parlement is dit percentage 10%.

Bij de verkiezingen voor de Tweede Kamer en het Europees parlement is in de afgelopen tien jaar het aantal vanuit het buitenland uitgebrachte stemmen nooit boven de kiesdrempel gekomen. Bij de laatste TK-verkiezingen in september 2012 waren in totaal 48.374 niet-ingezetene kiezers geregistreerd. Uiteindelijk hebben 35.898 kiezers een geldige stem hebben uitgebracht per brief.

Zelfs in het geval dat van alle internetkiezers de stem zou zijn gemanipuleerd dan nog leidt dat bij deze aantallen niet tot een directe zeteltoewijzing, hoogstens een voorkeursstem voor één of twee kandidaten of een wijziging van de restzetelverdeling.

De omvang van het aantal kiezers dat vanuit het buitenland stemt was in de afgelopen jaren relatief stabiel. Het kabinet heeft aangekondigd een permanente kiezersregistratie te willen invoeren. Dat betekent dat kiezers zich niet meer per verkiezing registeren, maar dat een eenmalige registratie volstaat. Ook wordt daarbij aansluiting gezocht bij de registratie van niet-ingezetenen die onderdeel uitmaakt van de basisadministratie personen. Hierdoor kan het aantal kiezers in de komende jaren aanzienlijk stijgen. Als het aantal kiezers stijgt dan neemt het reële effect op de uitslag uiteraard toe. Uit internationale ervaringen in andere landen waar internetstemmen wordt toegepast blijkt overigens dat de invoering van internetstemmen als nieuwe stemmethode niet direct leidt tot een hogere opkomst.

Zoals in dreigingsscenario DS4 is beschreven is er een dreiging denkbaar waarin heimelijk uit naam van in het buitenland wonende Nederlanders personen gepoogd wordt te gaan stemmen. Het registratieproces vormt een cruciale factor om die dreiging te voorkomen. Echter, dan moet het registratieproces zelf dusdanig zijn ingericht dat de dreiging kan worden gedetecteerd. Dit vergt een onderzoekscapaciteit bij de organisatie die de registratieverzoeken afhandelt om te kunnen onderzoeken of registratieverzoek overeenkomt met de intentie van een bonafide kiezer komt.

7 INTERNATIONALE AFWEGING VAN RISICO'S

De internationale inventarisatie van internetstemmen[21] laat zien dat er in elf landen experimenten zijn gehouden met internetstemmen, en dat stemmen via internet nu is toegestaan in zeven landen. Zonder uitzondering is in deze landen uitvoerig stilgestaan bij de risico's van internetstemmen. Ook in andere landen is er intensief gediscussieerd en geëxperimenteerd met internetstemmen, maar is uiteindelijk een andere afweging gemaakt die er toe heeft geleid om internetstemmen niet in te voeren. Dit geldt bijvoorbeeld voor de Verenigde Staten, voor delen van Canada, voor Oostenrijk, Finland en Duitsland.

In dit hoofdstuk is een beknopte uiteenzetting opgenomen van de risico's die in een tweetal Europese landen (Estland en Noorwegen) zijn onderkend, de afweging die daarbij is gemaakt, de maatregelen die zijn getroffen en de ervaringen uit de praktijk. In bijlage D zijn verwijzingen te vinden naar risicoanalyses en rapporten uit andere landen, zoals de Verenigde Staten, Canada en Zwitserland.

7.1 Estland

In Estland is bij de start van het e-voting project in opdracht van het National Electoral Committee een document[22] opgesteld waarin op basis van een eerste ontwerp de risico's, eisen en maatregelen van het beoogde internstemsysteem werden beschreven. In het document wordt onderscheid gemaakt tussen een aantal 'fundamental problems' en technische risico's.

Eén van de fundamentele problemen die wordt onderkend is de dreiging dat de computer van de kiezer wordt blootgesteld aan malware die heimelijk de handelingen van de kiezer vastlegt, de stemapplicatie vervangt, de ID kaart vervangt of de stem blokkeert. De Estse NEC vond deze risico's acceptabel om de volgende redenen:

- het heeft geen zin om de computer van een enkele kiezer te hacken om de uitslag te beïnvloeden, alleen een massale aanval heeft werkelijk effect;
- een massale aanval blijft niet onopgemerkt, juist door de diversiteit in de computer configuraties van kiezers zullen sommige kiezers de aanval opmerken, waarna de aanvaller kan worden opgespoord. Dit voorkomt dat politieke groeperingen als opdrachtgever zullen optreden voor een dergelijke aanval
- het ligt niet voor de hand dat een specifieke computer van een specifieke kiezer wordt aangevallen, de meeste aanvallen zijn geautomatiseerd en ongericht;
- de server is een aantrekkelijker doelwit dan een computer van een individuele kiezer.

[21] Zie Rapport Deel I – Internationale Inventarisatie internetstemmen

[22] Zie "E-voting conception security: analysis and measures"; National Election Committee Estonia, 15-12-2003. Dit document is geactualiseerd in 2010.

Verder adresseert de NEC dat een aantal problemen simpelweg geaccepteerd moeten worden: het internet zelf moet worden vertrouwd (als de kiezer start op de verkeerde webpagina, dan zijn overige maatregelen zinloos), er kan geen uitputtende inspectie plaatsvinden van alle standaard (hardware of software) onderdelen van het centrale deel van het internetstemsysteem en niet elke kiezer kan worden ondersteund als gevolg van technische keuzes. Tenslotte noemt de NEC in haar rapport dat de twee hoogste risico's van elk informatiesysteem liggen in de kwaliteit van de ontwikkeling en de kwaliteit van het beheer. Dit geldt specifiek voor een internetstemsysteem omdat dit een gedistribueerd systeem is dat weinig frequent gebruikt wordt, lastig is te testen en een strikte opleverdata heeft.

Aan de technische kant heeft het NEC vele dreigingen onderkend die voortvloeien uit het gebruik van technologie, zoals gebreken in de software, man-in-the-middle attacks, gebreken in webservers, problemen met cryptografische sleutels, etc. Opvallend genoeg eindigt de risico-analyse met de samenvatting dat "*risks of e-voting are in fact very similar to the risks of conventional voting, most technical attacks and threats have analogies in the material world. IT-systems are replaced by people and organisations, but schemes and processes remain the same. (…) E-voting only adds dependency on technical equipment into the equation. In addition, the use of technical equipment serves to seemingly magnify the general problems: frequency of errors is reduced but their scope extended.*"

In de geactualiseerde versie van de risico-analyse uit 2010 is in meer detail aandacht besteed aan de technische risico's. Opvallend is dat de dreiging van een doelbewuste verstoring van de verkiezing middels een DDoS aanval niet als een realistisch scenario wordt beschouwd, enerzijds omdat er vanuit wordt gegaan dat geen enkele politieke partij hiertoe opdracht zal geven, anderzijds omdat een aanval vanuit een buitenlandse entiteit gemakkelijker kan worden weg gefilterd. Deze maatregel is niet geschikt voor de Nederlandse situatie, aangezien het juist de kiezers zijn die in het buitenland verblijven.
In Estland wordt een meerdaagse stemperiode gehanteerd om het effect te verkleinen van een tijdelijke onbeschikbaarheid van het internetstemsysteem. Daarnaast is het voor kiezers mogelijk om alsnog te stemmen in een regulier stemlokaal, de via internet uitgebrachte stem wordt dan niet meegeteld.

Een belangrijk ontwerpprincipe voor de Estse regering was eenvoud. Eenvoud in de technische uitvoering én eenvoud door het zoveel mogelijk volgen van de opzet en structuur van bestaande kiesmethoden, zodat het systeem aansloot bij methoden die de kiezer al kende en vertrouwde. Het model van briefstemmen met het dubbele envelop principe stond daarbij centraal. Het gebruik van de nationale elektronische identiteitskaart was daarvoor een belangrijke randvoorwaarde, omdat daarmee zowel een aantal authenticatie gerelateerde dreigingen kon worden gepareerd als een elektronische handtekening kon worden gezet over de versleutelde stem. Mede doordat de elektronische identiteitskaart door burgers gebruikt wordt voor andere e-overheidsdiensten is de kans verkleind dat de kiezer zijn stem verkoopt door zijn ID card aan een ander te overhandigen.

Ten aanzien van de waarborg van toegankelijkheid is de discussie interessant die ontstond toen in 2005 het wetsvoorstel werd behandeld om internetstemmen mogelijk te maken. Politieke partijen (alsmede de president) debatteerden over de vermeende ongelijke behandeling van groepen kiezers. Dit had te maken met de mogelijkheid die was voorzien voor internetkiezers om hun stem gedurende de stemperiode te herzien, terwijl dit voor kiezers in een stemlokaal niet mogelijk was. Pas nadat het constitutionele hof had geoordeeld dat dit geen schending van de grondwet inhield, ging de president overstag en ondertekende hij de wet.

7.2 Noorwegen

In Noorwegen besloot het voor verkiezingen verantwoordelijke ministerie van lokale overheid en regionale ontwikkeling bij aanvang van haar internetstemproject (voor kiezers in Noorwegen uit een 9 tal gemeenten) tot zo compleet mogelijke transparantie. Dit vanuit de overtuiging dat volledige openheid bijdraagt aan het vertrouwen in internetstemmen, of minimaal wantrouwen in internetstemmen helpt te voorkomen. De transparantie is tot in vele details doorgevoerd, waarbij veel documentatie uit zowel aanbestedings-, ontwerp-, ontwikkel- en testfasen is gepubliceerd, evenals het cryptografisch protocol en de broncode. Belangrijke momenten zoals de sleutelgeneratie zijn uitgevoerd in openbare sessies waarvan video opnamen op het internet zijn geplaatst.

In haar ontwerp heeft de Noorse overheid nadrukkelijk gezocht naar maatregelen tegen de risico's van *dwang / beïnvloeding van de kiezer* en *manipulatie van de stem of uitslag*. Om dwang / beïnvloeding tegen te gaan is in Noorwegen voor een vergelijkbare systematiek gekozen als in Estland, waarin de kiezer meerdere keren mag stemmen via internet, waarbij alleen de laatste stem wordt meegeteld. En indien daarna nogmaals gestemd wordt in een stemlokaal dan dient die stem meegeteld te worden en niet de elektronische stem.
In haar pakket van eisen had zij daarom opgenomen dat kiezers moeten kunnen vaststellen of er geknoeid is met hun stembiljet zonder daarbij gebruik te moeten maken van computers. Hiertoe ontvangt de kiezer via een ander kanaal (SMS) een ontvangstcode die overeen moet komen met de vooraf toegestuurde stemkaart. Dit biedt een 'ontvangen zoals bedoeld' verificatie mogelijkheid aan de kiezer. De achterliggende doelstelling van de overheid was echter ook om te kunnen detecteren *of* er sprake was van grootschalige manipulatie van de stem. Zolang een klein (2%) percentage kiezers de verificatie uitvoert kan met een zeer grote waarschijnlijkheid een manipulatie worden gedetecteerd. Het ingevoerde verificatiesysteem heeft op zichzelf geleid tot nieuwe complexiteit in het internetstemsysteem en ook nieuwe dreigingen. Zo zijn fouten opgetreden bij de productie van de stemkaarten met de ontvangstcodes en is een nieuwe man-in-the-middle dreigingsscenario uitgedacht en aangetoond in een penetratietest, die de via SMS verstuurde ontvangstcode manipuleert.

Bij de meest recente verkiezingen van 2013 is het internetstemsysteem uitgebreid met de functionaliteit om wiskundig te kunnen bewijzen dat alle ontvangen stemmen correct zijn geteld. Dit als maatregel tegen het dreigingsscenario waarin de uitslag gemanipuleerd wordt of dat

gebreken in de stemdienst leiden tot een onjuiste uitslag. De Noorse overheid heeft aangegeven dat de verificatie eigenschappen van het internetstemsysteem als positief bijeffect hadden dat er minder stringente inspanningen nodig waren om de correcte werking aan te tonen.

De consequentie van het hebben van dergelijke controlemaatregelen is dat indien geconstateerd wordt dat er onregelmatigheden zijn opgetreden, er ook naar gehandeld moet worden. In het Noorse kiessysteem kan worden besloten tot een herstemming indien de problemen een effect zouden hebben gehad op de uitslag. De afweging is nadrukkelijk gemaakt dat manipulatie of het falen van het internetstemsysteem weliswaar zeer vervelend zijn, maar dat een onrechtmatige uitslag volstrekt onacceptabel is.

A Bijlage: Dreigingsscenario's

A1. DS1: Publiceren informatie over beveiliging internetstemsysteem tijdens stemming

BESCHRIJVING

In dit scenario wordt bewust informatie gepubliceerd over het internetstemsysteem en eventuele kwetsbaarheden daarin gedurende de stemming. De informatie kan zowel feitelijke informatie zijn uit bijvoorbeeld (gelekte) ontwerpdocumentatie, testrapporten, configuratiebestanden, beveiligingsmaatregelen, broncode, als ook meer speculatief zoals een opiniërend mediabericht. Met feitelijke informatie kunnen kwaadwillende actoren aan de slag om aanvallen uit te voeren op het internetstemsysteem.

Goed beschouwd mag het openbaar worden van informatie die de werking van een stemsysteem beschrijft niet als dreiging worden gezien, zeker niet als dit gebeurd in een periode voorafgaand aan de opening van de stemming. Vanuit het oogpunt van de waarborgen van transparantie en controleerbaarheid is openbaar making juist zeer gewenst.
Als de informatie openbaar wordt gemaakt gedurende de stemming kan dit allerlei aanvallen uitlokken, maar ook het publieke vertrouwen in de verkiezing en de verkiezingsuitslag schaden. Ongeacht of de informatie juist is, ligt de bewijslast bij de organisator van de verkiezing. Deze moet uitleggen of aantonen of de informatie juist is en als dat zo is of en in welke mate de kwetsbaarheid een effect heeft op de integriteit van de stemming, of een van de andere waarborgen. Ultiem heeft de organisator bij een serieus beveiligingsprobleem en een daadwerkelijk impact op een van de waarborgen de keuze tot het schorsen van de stemming of het ongeldig verklaren van de uitgebrachte stemmen.

ACTOREN EN BELANG

	Actor	Intentie
A4	Cybervandalen en Scriptkiddies	Technologische uitdaging en statusverhogend.
A5	Hacktivisten	Publiekelijk verstoren van de verkiezingen vanuit ideologische motieven.
A6	Interne actor, (voormalig) medewerker, beheerder	In diskrediet brengen van de verkiezingsorganisatie vanuit wraak of ideologische motieven.
A8	Cyberonderzoekers	Vanuit wetenschappelijke motieven onderzoeken van de (on)veiligheid van het internetstemsysteem.
A9	Private organisaties, concurrenten	In diskrediet brengen van internetstemsysteem om concurrentiepositie te verbeteren.
A13	Stembureau	In diskrediet brengen van de verkiezingsorganisatie vanuit wraak of ideologische motieven.

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, dan wel middelen waarmee de dreiging kan worden uitgevoerd.

	Dreiging
1	Hacken van het internetstemsysteem (ongeautoriseerde toegang verschaffen) en/of malverseren, en daarvan bewijs leveren aan de verkiezingsorganisatie en/of de media.
2	Lekken van vertrouwelijke informatie door (ex)medewerkers, leden van het stembureau of beheerders. Eventueel door samen te spannen.
3	Publiceren van (speculatieve) informatie of een opinie over de beveiliging van het internetstemsysteem zonder feitelijke onderbouwing.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op GROOT.

De kans wordt ingeschat op GROOT. Zoals aangegeven in hoofdstuk 4 wijkt internetstemmen in die zin af van briefstemmen dat de aandacht zeer groot zal zijn. Vanuit diverse actoren zal de internetstemdienst op haar merites onderzocht worden. De kans is GROOT.
Het effect hangt sterk af van het soort informatie en de reactie van de organisator van de verkiezingen. Indien op een transparante en zoveel mogelijk proactieve wijze informatie openbaar wordt gemaakt is het nadelig effect te beperken. Als het (publiek) vertrouwen in het internetstemsysteem eenmaal is geschaad dan is dit vertrouwen moeilijk terug te winnen. Het effect wordt om die reden ingeschat op MIDDEL.

BESTAANDE OF NIEUWE DREIGING

Dit is een nieuwe dreiging, die niet voorkomt bij het briefstemmen.

WAARBORGEN EN PROCESSTAP

Waarborgen: Transparantie, integriteit, controleerbaarheid
Processtappen:

- Stemuitbrenging
- Stemopneming
- Bepalen uitslag verkiezing

MAATREGELEN

Preventief	Correctief
• Proactief zelf openbaarheid betrachten. • Betrekken van belangengroeperingen / actoren bij het ontwerp en ontwikkeling van het internetstemsysteem om de kwaliteit van de beveiligingsmaatregelen te verbeteren en de kans van de dreiging van (betrokken) actoren te verkleinen. • Hoogwaardige softwareontwikkeling waarin beveiliging als belangrijk ontwerpfocus wordt meegenomen (“Security by design”).	• Onderzoeken van (geclaimde) kwetsbaarheden. • Indien incorrecte informatie over kwetsbaarheiden wordt gedeeld direct publiekelijk corrigeren om publiek vertrouwen terug te winnen.

Preventief	Correctief
• Zeer uitvoerig testen, inclusief broncode reviews, penetratietesten / Red teams etc.	

RISICO INSCHATTING NA MAATREGELEN

Door zelf proactief openbaarheid te betrachten is veel informatie reeds openbaar gemaakt, hierdoor wordt de kans gereduceerd naar MIDDEL. Door het betrekken van belangengroeperingen en deskundigen in het ontwerp en de ontwikkeling van het internetstemsysteem kan de kwaliteit van het internetstemsysteem mogelijk worden verhoogd. Het betrekken van partijen verkleint ook de kans dat onjuiste informatie wordt gepubliceerd.
Het effect op het vertrouwen hangt sterk samen met de aard van de gepubliceerde informatie en de wijze waarop daar mee omgegaan wordt. Het effect is niet eenvoudig te beperken en blijft daarom op MIDDEL staan.
Het risico wordt ingeschat op **MIDDEL**.

A2. DS2: Verkopen stem

BESCHRIJVING

In dit scenario verkoopt de kiezer zijn stembescheiden, of laat hij zich in ruil voor een tegenprestatie overhalen om een stem uit te brengen op een andere kandidaat.

ACTOREN EN BELANG

	Actor	Intentie
A11	Kiezer	Verkopen stem vanuit financiële motieven.
A12	Politieke partijen	Kopen van stemmen met de intentie vergroten van politieke invloed.

Een interne actor zou ook stemmen kunnen verkopen, bijvoorbeeld door de authenticatiegegevens door te spelen. Dit dreigingsscenario is ondergebracht bij DS4.

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, en middelen waarmee de dreiging kan worden uitgevoerd.

	Dreiging
1	Doorspelen van authenticatie gegevens door kiezer.
2	Indien het internetstemsysteem een bewijs afgeeft aan de kiezer waarmee deze richting derden kan aantonen wat hij heeft gestemd.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op MIDDEL.

Deze dreiging is ook aanwezig in het huidige proces van briefstemmen. In die zin is de kans aanwezig dat dit zich ook voordoet bij internetstemmen. Tegelijkertijd is het complexer om in massaliteit kiezers om te kopen gelet op de geografische verspreiding van de doelgroep. Ook mag worden verwacht dat bij het benaderen van kiezers er ook altijd kiezers zullen zijn die melding zullen maken van dergelijke (strafbare) praktijken waarna de koper kan worden opgespoord. Het risico wordt ingeschat op KLEIN.
Het effect hangt sterk samen met de schaal waarop het kopen / verkopen van stemmen plaatsvindt. Als het zich voordoet heeft het een effect op de waarborg kiesgerechtigdheid en uiteindelijk ook op de uitslag, de mate waarin hangt wederom af van de schaal. Het effect wordt ingeschat op MIDDEL.

BESTAANDE OF NIEUWE DREIGING

De dreiging van koop / verkoop van een stem is niet nieuw en is ook mogelijk in geval van briefstemmen.

WAARBORGEN EN PROCESSTAP

Waarborgen: Stemgeheim en kiesgerechtigdheid

Processtappen:

- Uitreiken stembescheiden
- Stemuitbrenging

MAATREGELEN

Preventief	Correctief
• Strafbaarstelling in Kieswet. • Invoeren van systematiek waarin kiezer meerdere keren kan stemmen via internet en waarbij alleen de laatste stem geldt. Dit kan mogelijk de aantrekkelijkheid voor de koper doen afnemen aangezien deze niet zeker weet dat de kiezer niet zelf alsnog stemt.	• Opsporing en vervolging. • Bij detectie voorafgaand aan de stemopneming intrekken van stembewijs / authenticatie middel dat is uitgereikt aan de kiezer waardoor stem ongeldig wordt.

RISICO INSCHATTING NA MAATREGELEN

Er zijn niet veel maatregelen mogelijk om te voorkomen dat een kiezer zijn stem verkoopt, de kans was echter klein, en blijft dat ook. Het effect kan door de maatregelen niet significant worden ingeperkt, alleen bij detectie voorafgaand aan de stemopneming kan de stem ongeldig worden verklaard.

Het risico wordt ingeschat op **MIDDEL**.

A3. DS3: Dwang / beïnvloeding van kiezer

BESCHRIJVING

De kiezer wordt door een derde gedwongen om een stem uit te brengen op een wijze die niet overeenstemt met de wil van de kiezer. Beïnvloeding kan plaatsvinden in de familie sfeer en/of vrienden groep en kan ook plaatsvinden bij verenigingen, gemeenschappen en (private) organisaties.

ACTOREN EN BELANG

	Actor	Intentie
A9	Private organisaties	Handelend vanuit ideologische motieven met de intentie maatschappelijke verandering of beïnvloeden politieke besluitvorming.
A11	Kiezer	Sociale druk vanuit sociaal milieu (familie en/of vrienden).
A12	Politieke partij	Vergroten politieke machtspositie.

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, dan wel middelen waarmee de dreiging kan worden uitgevoerd.

	Dreiging
1	Onder psychische of fysieke druk zetten van kiezer of dreigen daarmee (expliciete dwang / beïnvloeding).
2	Family voting: meer subtiel doordat de dwang / beïnvloeding in de familiaire sfeer plaats vind, of waar een lid van de familie stemt met gebruik van de stembescheiden van de andere familieleden (impliciete dwang / beïnvloeding).

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op MIDDEL**.**

De mate waarin deze dreiging zich voordoet bij Nederlandse verkiezingen is niet bekend. Aangenomen wordt dat family voting op enige schaal voorkomt, maar dat het aantal gevallen van dwang beperkt is. Het is lastig voor één actor om de dreiging op grote schaal uit te oefenen, gelet op de geografische spreiding van de kiezer. De kans wordt ingeschat op KLEIN.
Het effect hangt sterk samen met de schaal waarop deze dreiging zich manifesteert. Als het zich voordoet heeft het een effect op de waarborg kiesgerechtigdheid en uiteindelijk ook op de uitslag, de mate waarin hangt wederom af van de schaal. Het effect wordt ingeschat op MIDDEL.

BESTAANDE OF NIEUWE DREIGING

De dreiging van dwang / beïnvloeden van de kiezer is niet nieuw en is ook mogelijk in geval van briefstemmen.

WAARBORGEN EN PROCESSTAP

Waarborgen: Stemvrijheid en stemgeheim

Processtappen:

- Uitreiken stembescheiden
- Stemuitbrenging

MAATREGELEN

Preventief
• Een optie is om een systematiek in te voeren zoals in Noorwegen en Estland waarin kiezer meerdere keren kan stemmen via internet en waarbij alleen de laatste stem geldt. Dit biedt een beperkte bescherming, als er sprake is van fysieke bedreiging dan zal dit weinig effect hebben omdat de dreiger dan ook de stembescheiden kan afnemen of zelfs de kiezer fysiek kan belemmeren om deel te nemen aan de stemming.

RISICO INSCHATTING NA MAATREGELEN

Inherent aan het stemmen op afstand buiten een gecontroleerde omgeving, zijn er maar zeer beperkt maatregelen mogelijk om dwang / beïnvloeding tegen te gaan. Detectie aan de hand van de uitgebrachte stem is niet mogelijk. De systematiek van meervoudig stemmen is een ontwerpkeuze. Het preventieve of mitigerende effect hiervan is niet bekend.

Het risico wordt ingeschat op **MIDDEL.**

A4. DS4: Niet-kiesgerechtigde brengt stem uit

BESCHRIJVING

Een persoon die niet kiesgerechtigd is brengt een stem uit die wordt meegeteld voor de verkiezingsuitslag. Het doel van deze dreiging is om op een oneigenlijk manier de uitslag te beïnvloeden door onrechtmatig stemmen uit te brengen.

Deze dreiging is een inbreuk op waarborg kiesgerechtigdheid en integriteit en kan zich op meerdere manieren voordoen. Ten eerste door het onderscheppen van het authenticatiemiddel dat de kiezer gebruikt om zichzelf te op afstand identificeren. De onderschepping kan op verschillende momenten en locaties plaatsvinden, afhankelijk van de gebruikte authenticatiemethode en de wijze waarop het authenticatiemiddel wordt uitgereikt. Misbruik is alleen te detecteren indien de geregistreerde kiesgerechtigde op tijd meldt dat zijn stembescheiden niet zijn aangekomen en andere oorzaken tijdig zijn uit te sluiten (zoals DS18 en DS22).

Een andere mogelijkheid is dat het authenticatiemechanisme onvoldoende betrouwbaar blijkt of faalt zodat het uitbrengen van een stem ook mogelijk wordt voor overige niet kiesgerechtigde personen. Hierbij maakt een actor doelbewust misbruik van functioneel-, technisch- of beveiligingsgebreken zoals beschreven in scenario DS 23.

De authenticatiemiddelen kunnen ook aan de bron worden ontvreemd, bij de generatie in het internetstemsysteem, bij het drukken van de stembescheiden, of doordat malware de authenticatiegegevens onderschept zodra de kiezer ze invoert.

Het toevoegen van stemmen voorafgaand of tijdens de stemming middels onbevoegde toegang of andere malversaties in het internetstemsysteem wordt beschreven in scenario DS 7.

ACTOREN EN BELANG

	Actor	Intentie
A1	Staten	Intentie geopolitieke positie verbeteren door verkiezingsuitslag te beïnvloeden.
A5	Hacktivisten	Handelend vanuit ideologische motieven en vergroten van politieke invloed.
A6	Interne actor, (voormalig) medewerker	Handelend vanuit ideologische, financiële of politieke motieven.
A12	Politieke groepering	Handelend vanuit de intentie invloed uit te oefenen op de uitslag van de stemming om zo meer stemmen te verkrijgen. Kan de dreiging niet zelfstandig uitoefenen.

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, dan wel middelen waarmee de dreiging kan worden uitgevoerd.

	Dreiging
1	Ontvreemden van identiteitsgegevens van kiesgerechtigde (zie manieren zoals genoemd in DS 1).
2	Onderscheppen van de stembescheiden (fraude postverzending).
3	Malware[23] plaatsen op het internetstemsysteem die de authenticatie omzeilt of uitschakelt.
4	Backdoor aanbrengen tijdens de ontwikkeling of installatie van het internetstemsysteem die de authenticatie omzeilt of uitschakelt.
5	Manieren waarop functionele-, technische- of beveiligingsgebreken kunnen ontstaan (zie scenario DS19.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op GROOT.

Uitgaande van het versturen van stembescheiden per post, is de kans dat de stembescheiden voor een enkele kiezer worden onderschept aanwezig. De kans dat zich dit op grote schaal voordoet achten we KLEIN vanwege de benodigde inspanning om grootschalige te frauderen met postverzending. Het belang om deze fraude te plegen is alleen voor politieke groeperingen aanwezig, maar de kans dat die zich met identiteitsfraude en/of fraude van postverzending inlaten wordt gering geacht.

Indien een actor in staat is om de aanval op grote schaal uit te voeren worden vele stemmen ten onrechte uitgebracht. Zeker in geval de uitwisseling van de authenticatiegegevens volledig elektronisch wordt uitgevoerd – langs één en hetzelfde kanaal – zijn gegevens relatief eenvoudig te onderscheppen. Het effect wordt ingeschat op GROOT

BESTAANDE OF NIEUWE DREIGING

De dreiging dat een niet-kiesgerechtigde een stem uitbrengt is niet nieuw en is ook mogelijk in geval van briefstemmen.

WAARBORGEN EN PROCESSTAP

Waarborgen: Kiesgerechtigdheid en Integriteit

Processtappen:

- Stemuitbrenging

[23] Malware is een samenvoeging van de begrippen ‘malicious’ en ‘software’, en betekent kwaadaardige software. Het is een verzamelbegrip voor computervirussen, worms, trojan horses, ransomware, spyware, keyloggers, backdoor, rootkit, etc.

- Uitreiken stembescheiden

MAATREGELEN

Preventief	Correctief
• Gebruik van een voldoende betrouwbaar sterk authenticatiemiddel (bijvoorbeeld two-factor middel, waardoor het onderscheppen van de stembescheiden alleen onvoldoende is). • Gebruik van een ander authenticatie middel dan de huidige stembescheiden (stembewijs); een authenticatiemiddel dat door Nederlandse overheid geaccepteerd wordt en dat in een breder verband (ook buiten de verkiezingscontext) gebruikt wordt (waardoor kiezers dit niet snel weggeven vanwege het persoonlijk belang). • Functionaliteit in het internetstemsysteem die voorkomt dat bij een brute-force attack op de authenticatiegegevens deze pogingen worden afgewend. Bijvoorbeeld na detectie van vele pogingen vanaf één IP-adres. • Bij gebruik van stemcodes deze zo genereren dat de kans dat de stemcode geraad of herleid kan worden extreem klein is. • Uitreiken van stembescheiden / authenticatiemiddelen niet via hetzelfde kanaal als waarlangs het registratieverzoek is ingediend.	• Bij detectie voorafgaand aan de stemopneming intrekken van stembewijs / authenticatie gegeven dat is uitgereikt aan de kiezer waardoor stem ongeldig wordt. • Bij detectie na stemopneming is geen maatregel meer mogelijk.

RISICO INSCHATTING NA MAATREGELEN

De methode van authenticatie, het gebruikte authenticatiemiddel en de wijze waarop dit middel wordt uitgereikt aan de kiezer is sterk bepalend voor de kans dat authenticatiefraude optreedt. Met de genoemde maatregelen kan de kans tot KLEIN worden gereduceerd. Zeer sterke vormen van authenticatie, zoals bijvoorbeeld een smart card die persoonlijk afgehaald moet worden, reduceren de kans in grote mate, echter hiermee wordt ook afbreuk gedaan aan de waarborg van toegankelijkheid.
Het effect kan alleen teruggebracht worden in geval van vroegtijdige detectie. Het effect blijft GROOT.

Het risico wordt ingeschat op **GROOT**.

A5. DS5: Manipuleren van de stem of uitslag

BESCHRIJVING

In dit scenario wordt de integriteit van de stemming aangetast doordat stemmen worden gewijzigd, worden toegevoegd of worden verwijderd. Het doel van het manipuleren van stemmen is beïnvloeding van de verkiezingsuitslag.

Dit kan op verschillende manieren, zoals:

- het wijzigen of verwijderen van een stem tijdens de stemuitbrenging, het transport en/of de opslag in het internetstemsysteem;
- het in de stembus injecteren van stemmen voorafgaand aan de stemming (zogenaamde 'ballot stuffing');
- het in de stembus injecteren van geldige stemmen (van niet bestaande kiezers);
- het ontvreemden van stembescheiden ten einde zelf een stem te kunnen uitbrengen;
- het manipuleren van de programmatuur van het stemsysteem of de telprogrammatuur.

Actoren en belang

	Actor	Intentie
A1	Staten	Intentie geopolitieke positie verbeteren door verkiezingsuitslag te beïnvloeden.
A4	Cybervandalen en Scriptkiddies	Technologische uitdaging en statusverhogend.
A5	Hacktivisten	Handelend vanuit ideologische motieven en vergroten van politieke invloed.
A6	Interne actor, (voormalig) medewerker, beheerder	Handelend vanuit ideologische, financiële of politieke motieven.
A10	Eigen overheid	intentie beïnvloeden politieke besluitvorming door de verkiezingsuitslag te beïnvloeden.
A11	Kiezer	Onderscheppen van stembescheiden van familieleden, vrienden of kennissen met als doel om zelf de stem uit te brengen en zo de uitslag van de stemming te beïnvloeden.
A12	Politieke partij	Vergroten politieke machtspositie.

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, dan wel middelen waarmee de dreiging kan worden uitgevoerd.

	Dreiging
1	Malware plaatsen op de computer van de kiesgerechtigde. De malware verandert of verwijdert de uitgebrachte stem voordat deze wordt verzonden naar de verkiezingsorganisatie.
2	Malware plaatsen op het internetstemsysteem bij de verkiezingsorganisatie. De malware verandert

	Dreiging
	of verwijdert de ontvangen/geregistreerde stem voordat deze wordt meegenomen in de telling.
3	Man-in-the-middle-attack: onderscheppen van uitgebrachte stemmen en deze aangepast doorsturen naar de verkiezingsorganisatie.
4	Onderscheppen en blokkeren van uitgebrachte stemmen op internet.
5	Backdoor aanbrengen tijdens de ontwikkeling of installatie van het internetstemsysteem. Met deze backdoor kan tijdens stemming de controle over het internetstemsysteem worden verkregen om de uitgebrachte stemmen te wijzigen, verwijderen of nieuwe stemmen te introduceren.
6	Hacken van het internetstemsysteem (ongeautoriseerde toegang) tijdens de stemming om de ontvangen/geregistreerde stemmen te veranderen of te verwijderen, of nieuwe stemmen te introduceren.
7	Spoofing: de kiesgerechtigde wordt verleid zijn/haar stem uit te brengen op een malafide site die lijkt het internetstemsysteem. De uitgebrachte stem wordt verwijderd, of veranderd en doorgestuurd naar de verkiezingsorganisatie.
8	Omzeilen functiescheiding door samenspannen van beheerders (ongeautoriseerd toegang) om geregistreerde stemmen te wijzigen of te verwijderen of nieuwe stemmen te introduceren.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat als GROOT.

Voor diverse actoren voorziet het manipuleren van het stemproces in een duidelijk belang. Indien er geen maatregelen worden getroffen in de opzet van het internetstemsysteem en in de controlemaatregelen ter voorkoming van deze dreiging, dan wordt de kans dat er manipulatie plaats vindt op GROOT ingeschat.
Het effect hangt sterk samen met de schaal waarop deze dreiging zich manifesteert. Als het zich voordoet heeft het een effect op de waarborg Kiesgerechtigdheid, Integriteit en Uniciteit en uiteindelijk ook op de verkiezingsuitslag, de mate waarin hangt wederom af van de schaal. Het effect wordt ingeschat op GROOT.

BESTAANDE OF NIEUWE DREIGING

Strikt genomen is het manipuleren van een briefstem ook mogelijk, bijvoorbeeld door de envelop open te stomen en het stembiljet aan te passen. In de praktijk is dit echter lastig op grote schaal uit te voeren zonder dat het opgemerkt wordt. Malversaties van interne actoren wordt tegengegaan door het openbare karakter van de telling en de onderlinge controle in het briefstembureau.
Deze dreiging wordt als een nieuwe dreiging beschouwd.

WAARBORGEN EN PROCESSTAP

Waarborgen: Controleerbaarheid, Integriteit, Kiesgerechtigdheid en Uniciteit
Processtappen:

- Uitreiken stembiljet

- Stemuitbrenging
- Stemopneming

MAATREGELEN

Preventief	Correctief
• Beveiligingsmaatregelen internetstemsysteem. • Informeren van kiezers op vlak van beveiligingsmaatregelen eigen computer (bv Digibewust[24]). • Controle van opzet en werking van alle componenten van internetstemsysteem. • AO / IC maatregelen, zoals toepassen van het vier-ogen principe, functiescheiding, etc. • Verificatie door de kiezer: of hij met de echte stemdienst contact heeft, of hij zijn stem is ontvangen als uitgebracht, of zijn stem is geteld als uitgebracht etc. • Controle instrumenten voor de leden van het stembureau. • Beveiligde verbindingen voor overdracht van de uitgebrachte stem over het internet. • Cryptografische maatregelen (zoals hash algoritmes) om wijzigingen te detecteren of te voorkomen (encryptie). • Controle van programmatuur op ongewenste code.	• Hertellen. Het hangt van het ontwerp van het stemsysteem af of een hertelling überhaupt mogelijk is, en of het zinvol is. Een hertelling heeft zin als er een vermoeden is dat niet alle ontvangen stemmen zijn meegeteld in de uitslag. • Herstemmen. Het is aan het vertegenwoordigend orgaan om, op basis van de proces verbalen van de stembureaus, te bepalen of de manipulatie op dermate ernstig was of op een schaal heeft plaatsgevonden dat een herstemming noodzakelijk is.

RISICO INSCHATTING NA MAATREGELEN

Met de preventieve maatregelen kan de kans dat de stem wordt gemanipuleerd worden gereduceerd, maar niet worden voorkomen. Met name de malware dreiging tegen de computer van de kiezers blijft moeilijk te ondervangen. De kans wordt ingeschat op MIDDEL. Het effect blijft GROOT.

Het risico wordt ingeschat op **GROOT**.

[24] Digibewust is een onderdeel van het programma Digivaardig & Digiveilig dat een samenwerkingsverband is tussen overheid, bedrijfsleven en maatschappelijke organisaties, gericht op het voorlichten van burgers over het veilig en verantwoord gebruik van internet.

A6. DS6: Kiezer brengt meer dan één stem uit

BESCHRIJVING

Een (bonafide) kiezer brengt meerdere stemmen uit. Met het uitbrengen van meerdere stemmen die ook allemaal worden meegenomen in de telling, wordt de waarborg Uniciteit geschonden. Met dit scenario wordt de uitslag op een oneigenlijke manier beïnvloed met onrechtmatig uitgebrachte stemmen, dus een inbreuk op de integriteit van de verkiezingen.

Dat een kiezer meer dan één stem kan uitbrengen kan het gevolg zijn van een functioneel gebrek of het technisch falen van het internetstemsysteem. Het kan zijn dat de kiezer merkt dat er meer dan één stem wordt uitgebracht, maar het gebrek / falen kan zich ook op een dusdanige manier manifesteren dat een kiezer het niet zal merken.

Er zijn in het buitenland (bijvoorbeeld Estland en Noorwegen) implementaties bekend van internetstemsystemen waarbij het kunnen uitbrengen van meerdere stemmen juist een expliciete gewenste functionaliteit is. Deze functie wordt gezien als terugvalmaatregel in het geval van ongewenste dwang / beïnvloeding van de kiezer. In die landen wordt alleen de laatst uitgebrachte internetstem meegeteld. Een kiezer kan in deze systematiek (onbewust) meer dan één stem uitbrengen als gevolg van technisch falen waardoor niet alleen de laatste uitgebrachte stem, maar iedere stem wordt meegeteld. In individuele gevallen is dit voor de kiezer of het stembureau niet te detecteren, en valt het pas op als het aantal getelde stemmen uitstijgt boven het aantal geregistreerde kiezers.

In geval van de verkiezingen voor het Europees parlement kan de kiezer zelf bepalen waar hij zijn stem uitbrengt: of in de lidstaat waar hij woont, of in de lidstaat wiens nationaliteit hij heeft. De situatie is denkbaar dat een kiezer zich in meerdere lidstaten inschrijft in de bevolkingsregistratie en zo meerdere keren opgeroepen wordt om te stemmen. De Nederlandse kiezer die in een andere lidstaat woont kan ook een registratieverzoek doen om als kiezer buiten Nederland te worden ingeschreven, hij zou dan zowel voor de lidstaat waar hij woont als voor het Nederlandse deel van het EP kunnen stemmen. Deze dreiging valt wel onder de noemer ‘Kiezer brengt meer dan één stem uit’, maar wordt in deze risicoanalyse verder buiten beschouwing gelaten, aangezien dit risico ook nu bestaat en niet specifiek gerelateerd is aan internetstemmen maar inherent is aan het kiesstelsel.

ACTOREN EN BELANG

	Actor	Intentie
A11	Kiezer	Sociale druk vanuit sociaal milieu (familie en/of vrienden).

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, dan wel middelen waarmee de dreiging kan worden uitgevoerd.

	Dreiging
1	Functionele-, technische-, beveiligingsgebreken (zie DS19) die worden misbruikt door de kiezer.
2	Misbruik van bestaande mogelijkheid om te mogen stemmen in Nederland en het land waar de kiezer woont.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat als MIDDEL

Deze dreiging is theoretisch aanwezig in het huidige proces bij verkiezingen voor het Europese parlement, maar komt in de praktijk zelden voor (voor zover bekend). De waarschijnlijkheid dat het internetstemsysteem als gevolg van gebreken tot deze ongewenste situatie leidt, wordt KLEIN geacht.
De dreiging van een kiezer die meerdere stemmen uitbrengt, heeft effect op de waarborgen Uniciteit en Integriteit. Bij een gebrek in de stemdienst die het mogelijk maakt dat een (bonafide) kiezer meerdere keren stemt kan er een verschil ontstaan tussen het aantal geregistreerde kiezers en het aantal uitgebrachte stemmen (mits het aantal uitgebrachte stemmen hoger is dan het aantal registraties). Dit kan pas gedetecteerd worden als het te laat is dus is het effect op de uitslag van de verkiezing is MIDDEL.

BESTAANDE OF NIEUWE DREIGING

Dit is een nieuwe dreiging.

WAARBORGEN EN PROCESSTAP

Waarborgen: Uniciteit en Integriteit
Processtappen:

- Stemuitbrenging

MAATREGELEN

Preventief	Correctief
• Beveiligingsmaatregelen internetstemsysteem. • Bij ontwerp en ontwikkeling van internetstemsysteem toepassen van principes van defensief programmeren, waardoor het internetstemsysteem minder kwetsbaar wordt voor onverwachte situaties of falen van onderdelen. • Uitvoeren van rigoureuze en uitputtende testscenario's : maximale belasting, ketentesten, penetratietesten etc. • Kritische componenten (zoals uitslagberekening)	• Foutherstel / correctie van telprogrammatuur.

Preventief	Correctief
laten ontwikkelen door verschillende teams van programmeurs.	

RISICO INSCHATTING NA MAATREGELEN

De waarschijnlijkheid dat het internetstemsysteem als gevolg van gebreken tot deze ongewenste situatie leidt wordt KLEIN geacht, onder de aanname dat het internetstemsysteem uitvoerig wordt getest. Het effect is lastig te detecteren en niet te mitigeren, dus blijft MIDDEL.

Het risico wordt ingeschat op **MIDDEL**.

A7. DS7: Chantage

BESCHRIJVING

Een actor chanteert een kiezer, de organisator van de verkiezing of een leverancier met als doel geld of een tegenprestatie. Te denken valt aan:

- Het chanteren van de **kiezer** door het afluisteren/inzien van de uitgebrachte stem en dreigen met publieke onthulling. Onthulling van de uitgebrachte stem heeft met name effect indien de kiezer een 'VIP' is, zoals een bekende Nederlander, een bewindspersoon of iemand die prominent actief is in een politieke partij.
- Het chanteren van (medewerkers van) de **verkiezingsorganisatie** door te dreigen met bijvoorbeeld het onbeschikbaar maken van het internetstemsysteem waardoor kiezers geen stem meer kunnen uitbrengen, door er voor te zorgen dat het stembureau of de verkiezingsorganisatie geen controle meer heeft over het internetstemsysteem of door te dreigen met de verstoring van de verkiezingen. De chantage kan ook plaatsvinden door te dreigen met de publicatie van vertrouwelijke (beveiligings)informatie en eventuele kwetsbaarheden in het internetstemsysteem (zie DS1).
- Het chanteren van (medewerkers van) de **leverancier** van het internetstemsysteem door te dreigen met publicatie van vertrouwelijke informatie over het internetstemsysteem (onder de aanname dat er een leverancier is).

ACTOREN EN BELANG

	Actor	Intentie
A1	Staten, via stroman	Staten zullen niet direct chanteren, maar meer waarschijnlijk hiervoor een stroman in zetten. Intentie kan zijn het uitoefenen van invloed op een specifieke persoon of een groep personen (bijvoorbeeld dissidenten).
A3	Beroepscriminelen	Financieel gewin.
A4	Cybervandalen en Scriptkiddies	Technologische uitdaging en statusverhogend.
A6	Interne actor, (voormalig) medewerker, beheerder	Financieel gewin.
A9	Private organisatie, concurrerende organisaties	Concurrentie voordeel.

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, dan wel middelen waarmee de dreiging kan worden uitgevoerd.

	Dreiging
1	Malware plaatsen op de computer van de kiesgerechtigde. De malware - bijvoorbeeld een keylogger of wachtwoordsniffer - luistert de uitgebrachte stem af of ontzegt de kiesgerechtigde de toegang tot

	Dreiging
	het internetstemsysteem.
3	Malware plaatsen op of hacken van het internetstemsysteem bij de verkiezingsorganisatie. De malware luistert de ontvangen/geregistreerde stem af of ontzegt medewerkers en kiesgerechtigden de toegang tot het internetstemsysteem.
5	Backdoor aanbrengen tijdens de ontwikkeling of installatie van het internetstemsysteem. Met deze backdoor kan tijdens stemming de uitgebrachte stemmen worden ingezien of de controle over het systeem worden overgenomen ('Hijacking').
6	Onderscheppen en afluisteren van uitgebrachte stemmen op internet.
7	Onderscheppen en blokkeren van uitgebrachte stemmen op internet.
10	Malware plaatsen op de computer van de medewerker van de verkiezingsorganisatie. De malware ontzegt de medewerker de toegang tot het internetstemsysteem.
11	'Phishing' aanval: De kiesgerechtigde wordt verleid haar/zijn stem uit brengen op een malafide site die lijkt op het internetstemsysteem ('Spoofing'). De uitgebrachte stem wordt afgeluisterd.
12	DDoS aanval op het internetstemsysteem zodat deze niet meer beschikbaar is voor de kiesgerechtigden.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op **MIDDEL**

De kans dat een kiezer of een verkiezingsorganisator daadwerkelijk wordt gechanteerd wordt KLEIN geacht. Het is niet ondenkbeeldig, maar er zijn geen voorbeelden publiekelijk bekend.
Het effect hangt sterk samen met de schaal waarop deze dreiging wordt toegepast. Als het zich voordoet heeft het een effect op de waarborg Kiesgerechtigdheid en uiteindelijk ook op de uitslag. De mate waarin hangt wederom af van de schaal. Het effect wordt ingeschat op MIDDEL.

BESTAANDE OF NIEUWE DREIGING

Chantage van individuele personen is niet nieuw en is ook mogelijk in geval van briefstemmen. Wel is het aantal mogelijkheden om de dreiging uit te voeren in het geval van internetstemmen groter.
Deze dreiging wordt als een nieuwe dreiging beschouwd.

WAARBORGEN EN PROCESSTAP

Waarborgen: Integriteit, Kiesgerechtigdheid, Stemgeheim en Beschikbaarheid
Processtappen:

- Stemuitbrenging
- Stemopneming
- Bepalen uitslag verkiezing

MAATREGELEN

Preventief	Correctief
• Voorkomen dat medewerkers die chantabel zijn 'vertrouwensfuncties' verkrijgen in het stemproces. • Kwetsbaarheden in het internetstemsysteem zoveel mogelijk beperken met beveiligingsmaatregelen. • Maatregelen om minder kwetsbaar te zijn voor verstoringen, zoals meerdaagse stemperiode, anti-DDoS maatregelen, etc. • Stemperiode afsluiten ruim voor dag van stemming om alternatief briefstemmen mogelijk te maken. • Controle van programmatuur op ongewenste code. • Informeren van kiezers op vlak van beveiligingsmaatregelen eigen computer (bv Digibewust).	• Opsporing en vervolging. • Actieve monitoring op DDoS aanvallen en upstream maatregelen in samenwerking met leveranciers, ISP's, CERT's en Politie. • Kiezers alsnog per brief laten stemmen (beperkt effect afhankelijk van moment waarop dit gebeurt). • Kiezers actief informeren in geval van verstoring.

RISICO INSCHATTING NA MAATREGELEN

In algemene zin is chantage niet te voorkomen. De preventieve maatregelen kunnen de kwetsbaarheden bij de kiezer, leverancier of het stembureau/verkiezingsorganisatie verminderen en de kans op chantage verkleinen. Het effect van chantage is echter niet te beperken en blijft MIDDEL.

Het risico wordt ingeschat op **MIDDEL**.

A8. DS8: Relatie tussen kiezer en inhoud stem (doorbreken stemgeheim)

BESCHRIJVING

Achterhalen / inzien van de uitgebrachte stem(men) en relateren aan de kiezer. Dit is een inbreuk op de waarborg van het stemgeheim en kan vanuit verschillende intenties plaatvinden:

Het achterhalen van de stem met de intentie de kiezer, een groep kiezers, een organisatie of een politieke partij in verlegenheid te brengen door deze te publiceren. Publicatie van stemmen kan ook een middel zijn voor het uitoefenen van sociale controle binnen een groep gelijkgestemden zoals een politieke partij, vereniging of geloofsgenootschap. Deze dreiging heeft direct invloed op het resultaat van de verkiezing.

Het achterhalen van de uitgebrachte stem kan ook een latent doel hebben, bijvoorbeeld om een informatiepositie op te bouwen over een bepaalde persoon. Dit heeft geen direct effect op de kiezer, het verkiezingsproces of de uitslag. De dreiging is met name indirect en kan zich in de toekomst en/of in een heel andere context manifesteren, als bijvoorbeeld het stemgedrag wordt gecombineerd met andere gegevens.

ACTOREN EN BELANG

	Actor	Intentie
A1	Staten	Invloed uit oefenen op een specifiek persoon of een groep personen (bijvoorbeeld dissidenten).
A4	Cybervandalen en Scriptkiddies	Uitdaging en statusverhogend.
A6	Interne actor, (voormalig) medewerker, beheerder	Wraak jegens werkgever.
A10	Eigen overheid	Invloed uit oefenen op een specifiek persoon of een groep personen (bijvoorbeeld dissidenten).
A12	Politieke partij	Invloed uit oefenen op een specifiek persoon of een groep personen/politieke partij.

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, dan wel middelen waarmee de dreiging kan worden uitgevoerd.

	Dreiging
1	Malware plaatsen op de computer van de kiesgerechtigde. De malware – bijvoorbeeld een keylogger of andere spyware - luistert de uitgebrachte stem af.
2	Malware plaatsen op het internetstemsysteem bij de verkiezingsorganisatie. De malware luistert de ontvangen/geregistreerde stemmen af.
3	Backdoor aanbrengen tijdens de ontwikkeling of installatie van het internetstemsysteem. Met deze

	Dreiging
	backdoor kan tijdens stemming de uitgebrachte stemmen worden ingezien.
4	Onderscheppen en afluisteren van uitgebrachte stemmen op internet.
5	Hacken van het internetstemsysteem (ongeautoriseerde toegang) tijdens de stemming om de ontvangen/geregistreerde stem af te luisteren.
6	'Phishing' aanval: De kiesgerechtigde wordt verleid haar/zijn stem uit te brengen op een malafide website die lijkt op het internetstemsysteem ('Spoofing'). De uitgebrachte stem wordt afgeluisterd en ongewijzigd doorgestuurd naar de verkiezingsorganisatie.
7	Omzeilen functiescheiding door samenspannen van beheerders (ongeautoriseerd toegang) tijdens de stemming om de ontvangen/geregistreerde stem af te luisteren.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op **GROOT**

Indien er geen maatregelen worden getroffen in de opzet van het internetstemsysteem en in de controlemaatregelen ter voorkoming van deze dreiging, dan wordt de kans dat het stemgeheim wordt doorbroken op GROOT ingeschat. Het effect wordt ingeschat op GROOT.

BESTAANDE OF NIEUWE DREIGING

De dreiging van het doorbreken van het stemgeheim is strikt genomen niet nieuw en is ook mogelijk in geval van briefstemmen. Malversaties van interne actoren wordt echter tegengegaan door het openbare karakter van het briefstembureau en de onderlinge controle daarbinnen.

De wijze waarop de dreiging zich voor kan doen is echter wel nieuw, en de mogelijkheden tot detectie zijn een stuk beperkter. Deze dreiging wordt om die reden als een nieuwe dreiging beschouwd.

WAARBORGEN EN PROCESSTAP

Waarborg: Stemgeheim

Processtappen:

- Stemuitbrenging
- Stemopneming

MAATREGELEN

Preventief	Correctief
• Versleuteling van de uitgebrachte stem. • Dusdanig ontwerpen van het internetstemsysteem dat er geen relatie gelegd kan worden tussen een stem en een kiezer. Bijvoorbeeld door geen persoonsgegevens van kiezers in het internetstemsysteem te gebruiken,	• Geen maatregel mogelijk.

Preventief	Correctief
door de stem te versleutelen, door de ontvangen stemmen te anonimiseren en door uitgebrachte stemmen in een willekeurige volgorde opslaan zonder indirect identificerende gegevens zoals IP-adres, tijdstip of volgorde van ontvangst etc. • Beveiliging / versleuteling van transport van de uitgebrachte stem. • AO / IC maatregelen, zoals toepassen van het vier-ogen principe, functiescheiding, etc. • Beveiliging van het internetstemsysteem tegen ongeautoriseerde toegang. • Informeren van kiezers op vlak van beveiligingsmaatregelen eigen computer (bv Digibewust). • Controle van de programmatuur van het internetstemsysteem op ongewenste code. • Cryptografische maatregelen (zoals hash algoritmes) om wijzigingen te detecteren of te voorkomen (encryptie).	

RISICO INSCHATTING NA MAATREGELEN

De preventieve maatregelen kunnen de kans reduceren naar KLEIN. Het effect blijft onverminderd van invloed op een waarborg uit de Grondwet en wordt daarmee nog steeds ingeschat op GROOT.

Het risico wordt ingeschat op **GROOT**.

A9. DS9: Doelbewust verstoren van de verkiezing

BESCHRIJVING

Heimelijk of publiekelijk verstoren van de verkiezingen door of het internetstemsysteem of één of meerdere stappen van het verkiezingsproces te verstoren. Doel kan zijn het verhinderen van de stemming en/of het (betrouwbaar) vaststellen van de verkiezingsuitslag.
Een bekende en veel gebruikte dreiging is om een DDoS aanval uit te voeren op de website van het internetstemsysteem. Maar ook (dreiging met) bomaanslagen, brandstichting etc. zijn (vergaande) manieren om de verkiezing te verstoren.

ACTOREN EN BELANG

	Actor	Intentie
A1	Staten	Heimelijk verstoren van de verkiezingen vanuit de intentie verbeteren van machtspositie.
A2	Terroristen	Publiekelijk verstoren van de verkiezingen om angst aan te jagen of om politieke besluitvorming te beïnvloeden.
A4	Cybervandalen en Scriptkiddies	Publiekelijk verstoren van de verkiezingen vanuit de technologische uitdaging en/of statusverhogend.
A5	Hacktivisten	Publiekelijk verstoren van de verkiezingen vanuit ideologische motieven.
A6	Interne actor, beheerders, medewerkers	In diskrediet brengen van de verkiezingsorganisatie vanuit wraak of publiek verstoren van de verkiezing vanuit politieke onvrede.
A9	Private organisaties, concurrenten	Verstoren van het internetstemsysteem om concurrentiepositie te verbeteren.

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, dan wel middelen waarmee de dreiging wordt uitgevoerd.

	Dreiging
1	DDoS aanval op het internetstemsysteem zodat deze niet meer toegankelijk is voor de kiesgerechtigden.
2	Malware plaatsen op de computer van de kiesgerechtigde. De malware verhindert het uitbrengen van een stem.
3	Malware plaatsen op het internetstemsysteem bij de verkiezingsorganisatie. De malware ontzegt medewerkers en kiesgerechtigden de toegang tot het internetstemsysteem.
4	Backdoor aanbrengen tijdens de ontwikkeling of installatie van het internetstemsysteem. Met deze backdoor kan tijdens stemming de controle over het systeem worden overgenomen (‘Hijacking’).

	Dreiging
5	Blokkeren van uitgebrachte stemmen op internet.
6	Hacken van het internetstemsysteem (ongeautoriseerde toegang) tijdens de stemming om geregistreerde stemmen te verwijderen.
7	Hacken van het internetstemsysteem (ongeautoriseerde toegang) om de toegang tot het internetstemsysteem voor kiesgerechtigden en medewerkers te blokkeren.
8	Malware plaatsen op de computer van de medewerker van de verkiezingsorganisatie. De malware ontzegt de medewerker de toegang tot het internetstemsysteem.
9	Spoofing : de kiesgerechtigde wordt toegeleid naar een andere (malafide) website die lijkt op het internetstemsysteem en wordt de toegang tot de echte site ontzegt.
10	Onderscheppen van de stembescheiden om de kiezer te verhinderen een stem uit te brengen.
11	Omzeilen functiescheiding door samenspannen van beheerders (ongeautoriseerd toegang) met als doel malversatie uit te voeren op het internetstemsysteem.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op **GROOT**.

De in het voorjaar van 2013 uitgevoerde DDoS aanvallen op onder meer Nederlandse banken heeft duidelijk gemaakt dat DDoS aanvallen een aanzienlijke verstoring kunnen opleveren, vrijwel niet te voorkomen zijn én uiterst lastig op te lossen zijn. Een internetverkiezing is voor actoren zoals hacktivisten en cybervandalen een aantrekkelijk doelwit dat veel publiciteit (en daarmee status) genereert. De kans op een verstoring wordt GROOT geacht.
Indien de verstoring lang aanhoudt kan het effect op de beschikbaarheid van het internetstemsysteem groot zijn. Het effect van een verstoring wordt GROOT geacht.

BESTAANDE OF NIEUWE DREIGING

Deze dreiging wordt als een nieuwe dreiging beschouwd. Het equivalent van deze dreiging in het briefstemproces zou zoiets als een ‘poederbrief’ of bommelding zijn bij het briefstembureau[25]. Dit heeft zich in Nederland niet eerder voorgedaan.

WAARBORGEN EN PROCESSTAP

Waarborgen: Integriteit en Beschikbaarheid
Processtappen:

- Authenticatie en bepalen kiesgerechtigheid
- Uitreiken stembescheiden

[25] Een dergelijke situatie leidt niet tot het verhinderen dat de kiezer zijn stem uitbrengt, maar mogelijk wel tot een vertraging bij de stemopneming. Door het verplaatsen van het briefstembureau kunnen dergelijke dreigingen relatief eenvoudig worden omzeild.

- Stemuitbrenging
- Stemopneming
- Bepalen uitslag verkiezing

MAATREGELEN

Preventief	Correctief
• Internetstemsysteem ingericht op zeer hoge capaciteitsbelasting. • Meerdaagse stemperiode om minder kwetsbaar te zijn voor een verstoring. • Stemperiode afsluiten ruim voor dag van stemming om alternatief briefstemmen mogelijk te maken. • Redundantie van kritieke componenten. • Beveiligingsmaatregelen internetstemsysteem up-to-date houden tijdens de verkiezingen. • Controle van programmatuur op ongewenste code. • Cryptografische maatregelen (zoals hash algoritmes) om wijzigingen te detecteren of te voorkomen (encryptie)Informeren van kiezers op vlak van beveiligingsmaatregelen eigen computer (bv Digibewust). • Beveiliging / versleuteling van transport van de uitgebrachte stem.	• Actieve monitoring op DDoS aanvallen en upstream maatregelen in samenwerking met leveranciers, ISP's, CERT's en High Tech Crime unit van de politie. • Kiezers actief informeren in geval van verstoring. • Kiezers alsnog per brief laten stemmen (beperkt effect afhankelijk van moment waarop dit gebeurt).

RISICO INSCHATTING NA MAATREGELEN

De kans op doelbewust verstoren van de verkiezingen is vrijwel niet te verkleinen. Deze blijft GROOT. De gevolgen van het doelbewust verstoren van de verkiezingen zijn wel te beperken met doordachte maatregelen. Het effect wordt teruggebracht naar KLEIN.

Het risico wordt ingeschat op **MIDDEL**.

A10. DS10: Defacing/bekladden internetstemsysteem

BESCHRIJVING

Misbruiken van het internetstemsysteem voor publicitaire doeleinden, veelal door het tonen van een ideologische, persoonlijke of politieke boodschap. Hierbij is het niet direct de bedoeling kiezers te verhinderen een stem uit te brengen, zoals in scenario DS9: Doelbewust verstoren van de verkiezingen. Met het tonen van de boodschap kunnen kiezers indirect worden beïnvloed in het uitbrengen van een stem.
Niet alleen het internetstemsysteem is kwetsbaar voor deze dreiging, dit geldt juist ook voor aanpalende websites zoals die voor de registratie of voorlichting. De aandacht voor de beveiliging van die websites zal waarschijnlijk minder groot zijn dan de aandacht voor de beveiliging van het internetstemsysteem.

ACTOREN EN BELANG

	Actor	Intentie
A2	Terroristen	Handelend vanuit ideologische motieven met de intentie maatschappelijke verandering of beïnvloeden politieke besluitvorming, door de verkiezingsuitslag te beïnvloeden.
A4	Cybervandalen en Scriptkiddies	Uitdaging en statusverhogend.
A5	Hacktivisten	Publiekelijk verstoren van de verkiezingen vanuit ideologische motieven. De boodschap is niet noodzakelijkerwijs specifiek op Nederlanders in het buitenland gericht, eerder op de verkiezingsorganisatie en de media.
A6	Interne actor, (voormalig) medewerker, beheerder	In diskrediet brengen van verkiezingsorganisatie of vanuit politieke onvrede.

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, dan wel middelen waarmee de dreiging wordt uitgevoerd.

	Dreiging
1	De kiezer wordt verleid haar/zijn stem uit brengen op een malafide site die lijkt op het internetstemsysteem (‘Spoofing’). De malafide site toont een (ideologische) boodschap.
2	Bekladden (‘Defacen’) van het internetstemsysteem met een (ideologische) boodschap.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op **MIDDEL**.

Defacing heeft in het verleden plaatsgevonden en vindt nu ook veelvuldig plaats, buiten de context van verkiezingen. Het is veelal het werk van Hacktivisten, Cybervandalen of Scriptkiddies. Het

belang voor deze actoren wordt vooral bepaald door de aard van de doelgroep en de publicitaire waarde van de website. In de situatie van internetstemmen achten we met name de publicitaire waarde groot en daardoor de kans dat er pogingen tot defacing worden gedaan aanwezig: kans MIDDEL.
Het effect is MIDDEL, want ondanks dat het imagoschade oplevert, blijft het internetstemsysteem zelf beschikbaar. De situatie dat het de functionaliteit van het internetstemsysteem niet meer beschikbaar is voor de kiezers is reeds beschreven onder dreigingsscenario DS9.

BESTAANDE OF NIEUWE DREIGING

De dreiging van defacing/bekladden is nieuw.

WAARBORGEN EN PROCESSTAP

Waarborgen: Toegankelijkheid en Beschikbaarheid
Processtappen:

- Registratie kiesgerechtigden (is geen onderdeel van internetstemsysteem)
- Informeren kiesgerechtigden (is geen onderdeel van internetstemsysteem)
- Stemuitbrenging

MAATREGELEN

Preventief	Correctief
• Beveiliging internetstemsysteem. • Informeren van kiezers op vlak van beveiligingsmaatregelen eigen computer (bv Digibewust).	• PR : informatie verschaffen, reageren op berichtgeving in de media.

RISICO INSCHATTING NA MAATREGELEN

De belangrijkste preventieve maatregel om de kans op een geslaagde poging van defacing te reduceren is een goede beveiliging van het internetstemsysteem. De kans is daarmee terug te brengen tot KLEIN. Het effect van een defacement, imagoschade, is slechts beperkt te mitigeren en blijft MIDDEL.

Het risico wordt ingeschat op **MIDDEL**.

A11. DS11: Springplank: misbruik systeem voor andere aanvallen

BESCHRIJVING

Een actor maakt misbruik van het internetstemsysteem door computers van kiezers en/of medewerkers te infecteren met malware. Deze malware heeft als doel om een andere cyberaanval mogelijk te maken. Het internetstemsysteem zelf is dus niet het doelwit van de dreiging maar het middel, 'de springplank', voor verdere verspreiding.

De besmetting van de computer van een kiezer heeft geen direct verstorend effect op het verkiezingsproces en het bepalen van de uitslag. Mogelijk dat de geïnfecteerde computer trager reageert of anderszins minder bruikbaar is om zijn stem uit te brengen. Anderzijds kan een kiezer worden afgeschrikt om zijn stem via internet uit te brengen. Dit scenario kan gevolgen hebben voor de toegankelijkheid van het internetstemsysteem.

De doelgroep kiezers in het buitenland vormt als zodanig geen logisch doelwit voor deze dreiging, daarvoor is de doelgroep te klein en te wijd verspreid over de wereld. Echter, specifieke subgroepen of personen kunnen interessant zijn vanuit de intentie van de andere aanval. Hierbij valt te denken aan ambassadepersoneel (intentie infiltreren in ambassadenetwerk), pensionado's (intentie financieel gewin) en expatriates van grote multinationals (spionage).

Naast het internetstemsysteem zelf is de voorlichtingssite voor deze doelgroep (en andere eventueel specifieke websites) ook een doelwit voor deze dreiging.

ACTOREN EN BELANG

	Actor	Intentie
A1	Staten	Heimelijke cyberaanval op andere (Nederlandse) organisaties om via spionage een informatiepositie op te bouwen.
A3	Beroepscriminelen	Cyberaanval op specifieke (Nederlandse) organisatie vanuit financiële motieven.
A4	Cybervandalen en Scriptkiddies	Opzetten van cyberaanval naar andere organisaties/personen.

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, dan wel middelen waarmee de dreiging wordt uitgevoerd.

	Dreiging
1	Malware plaatsen op het internetstemsysteem bij de verkiezingsorganisatie. De malware besmet de computer van de kiezer zodra deze de programmatuur installeert/gebruikt.
2	Backdoor aanbrengen tijdens de ontwikkeling of installatie van het internetstemsysteem. Met deze

	Dreiging
	backdoor kunnen de kiezer die een stem uitbrengen doelgericht besmet worden met malware.
3	Spoofing: de kiezer wordt verleid zijn stem uit te brengen op een malafide site die lijkt op het internetstemsysteem en wordt gelijktijdig besmet met malware. Om de besmetting niet te laten opvallen wordt de uitgebrachte stem zonder wijzigingen doorgestuurd naar de verkiezingsorganisatie.

INSCHATTING RISICO ZONDER MAATREGELEN

Besmetting van computers van burgers met malware komt zeer veel voor. De manieren waarop malware zich verspreid en hoe het opereert wordt steeds geavanceerder. Niet alleen het aanklikken van een verkeerde link in een e-mail bericht kan leiden tot besmetting, ook via speciale advertenties die op algemene nieuwswebsites stonden is besmetting mogelijk. Hierbij waren de achterliggende advertentienetwerken gecorrumpeerd.
De doelgroep is echter beperkt. De dreiging is voornamelijk afkomstig van Staten met de intentie van bedrijfsspionage en Beroepscriminelen met financiële motieven. We schatten de kans dat Nederlanders in buitenland een *specifiek* doelwit vormen in op KLEIN.

Het effect van deze dreiging voor het verkiezingsproces en het bepalen van de uitslag is beperkt, aangezien het in dit dreigingsscenario gaat om andere doelwitten. Gezien de capaciteit en vaardigheden van de voornaamste dreigingsactoren, Staten en Beroepscriminelen, is de verwachting dat indien specifieke malware wordt ontwikkeld voor deze doelgroep met als doel om andere aanvallen mogelijk te maken, de malware zo wordt ontworpen dat het geen merkbaar effect heeft op het kunnen stemmen. Het effect *op het verkiezingsproces* wordt derhalve ingeschat op KLEIN; het effect elders kan uiteraard groot zijn.

BESTAANDE OF NIEUWE DREIGING

Dit is een nieuwe dreiging, uniek voor het digitale domein, die niet voorkomt bij het briefstemmen.

WAARBORGEN EN PROCESSTAP

Waarborg: is niet gerelateerd aan het verkiezingsproces
Processtappen:

- Informeren kiesgerechtigde (geen onderdeel van internetstemsysteem)
- Stemuitbrenging

MAATREGELEN

Preventief	Correctief
• Beveiliging van internetstemsysteem. • Informeren van kiezers op vlak van beveiligingsmaatregelen eigen computer (bv Digibewust). • Controle van programmatuur op ongewenste code.	• PR : informatie verschaffen, reageren op berichtgeving in de media.

Preventief	Correctief
• Cryptografische maatregelen (zoals hash algoritmes) om wijzigingen te detecteren of te voorkomen (encryptie).	

RISICO INSCHATTING NA MAATREGELEN

De preventieve maatregelen beperken de kans op manifesteren van de dreiging, maar deze is nooit helemaal te voorkomen. Inschatting van de dreiging was en blijft KLEIN. Het effect voor het verkiezingsproces wordt ingeschat op KLEIN.

Het risico wordt ingeschat op KLEIN.

A12. DS12: Voortijdige publicatie uitslag

BESCHRIJVING

De uitslag of een deel van de uitslag wordt openbaar gemaakt voor het moment dat de stemming is gesloten en de stemopneming is aangevangen door het stembureau. Het is bij wet geregeld (zie hoofdstuk N in Kieswet) dat de publicatie van de stemmen aan het eind van de verkiezing plaatsvindt. Het is niet wenselijk dat (een deel van de) uitslag voortijdige publicatie wordt gepubliceerd omdat dit kan leiden tot een beïnvloeding van de kiezers die nog moeten stemmen.

In dit dreigingsscenario wordt uitgegaan van bewust menselijk handelen. Publicatie/uitlekken van tussenuitslagen door onbewust (en onkundig) menselijk handelen vallen onder dreigingsscenario DS16 – Onkundig bediening en beheer.

ACTOREN EN BELANG

	Actor	Intentie
A1	Staten	Invloed uitoefenen om een specifieke partij of kandidaat verkozen te krijgen.
A4	Cybervandalen en Scriptkiddies	Uitdaging en statusverhogend.
A5	Hacktivisten	Handelend vanuit ideologische motieven.
A6	Interne actor, (voormalig) medewerker, beheerder	In diskrediet brengen van verkiezingsorganisatie of vanuit politiek onvrede.
A10	Eigen overheid	Invloed uitoefenen om een specifieke partij of kandidaat verkozen te krijgen.
A12	Politieke groepering	Invloed uitoefenen om een specifieke partij of kandidaat verkozen te krijgen.

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, dan wel middelen waarmee de dreiging wordt uitgevoerd.

	Dreiging
1	Malware plaatsen op de computer van de kiesgerechtigde die de uitgebrachte stem afluistert (bijvoorbeeld een keylogger of wachtwoordsniffer).
2	Malware plaatsen op het internetstemsysteem bij de verkiezingsorganisatie die de ontvangen/geregistreerde stem afluistert.
3	Backdoor aanbrengen tijdens de ontwikkeling of installatie van het internetstemsysteem. Met deze backdoor kan tijdens stemming de uitgebrachte stemmen worden ingezien.
4	Afluisteren van uitgebrachte stemmen op internet.
5	Ongeautoriseerde toegang tot het internetstemsysteem tijdens de stemming om de ontvangen /

	Dreiging
	opgeslagen stemmen af te luisteren.
6	Ongeautoriseerde toegang tot het internetstemsysteem om tussentijdse telling uit te voeren.
7	Omzeilen functiescheiding door samenspannen van beheerders (ongeautoriseerd toegang) en/of medewerkers om stemmen af te luisteren of een tussentijdse telling uit te voeren.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op **KLEIN**.

De kans dat deze dreiging optreedt wordt als KLEIN ingeschat. De actoren die in staat moeten worden geacht deze dreiging uit te oefenen zijn de leden van het stembureau of beheerders van het internetstemsysteem.
Het effect van voortijdig publiceren heeft een beperkt indirect effect op de uitslag van de stemming. Een voortijdige publicatie is niet toegestaan en ongewenst, maar leidt op zichzelf niet direct tot een andere uitslag. Alleen als andere kiezers zich in hun stemgedrag laten beïnvloeden door de voortijdige (tussen) uitslag is er sprake van een effect. Juist omdat de kiezers in het buitenland wonen en ze gedurende een meerdaagse stemperiode kunnen stemmen is ook de kans dat ze beïnvloed worden KLEIN.

BESTAANDE OF NIEUWE DREIGING

Dit is een nieuwe dreiging.

WAARBORGEN EN PROCESSTAP

Waarborgen: Integriteit en Tijdigheid
Processtappen:

- Stemuitbrenging

MAATREGELEN

Preventief	Correctief
• Beveiliging van internetstemsysteem. • AO / IC maatregelen die verhinderen dat één persoon te ruime bevoegdheden heeft. • Beveiliging / versleuteling van transport van de uitgebrachte stem. • Informeren van kiezers op vlak van beveiligingsmaatregelen eigen computer (bv Digibewust). • Controle van programmatuur op ongewenste code. • Cryptografische maatregelen (zoals hash algoritmes) om wijzigingen te detecteren of te voorkomen (encryptie).	• PR : informatie verschaffen, reageren op berichtgeving in de media.

RISICO INSCHATTING NA MAATREGELEN

De preventieve maatregelen verlagen de kans op voortijdige publicatie van de uitslag. Deze was en blijft KLEIN. De maatregelen hebben geen impact op het effect.

Het risico wordt ingeschat op **KLEIN**.

A13. DS13: Onvoldoende inzicht en begrip kiezers

De kiezer begrijpt de opzet en werking van het internetstemsysteem niet. Deze dreiging komt niet voort uit bewust menselijk handelen maar ontstaat als gevolg van het ontbreken van inzicht en begrip in het verloop van het verkiezingsproces en de werking van het internetstemsysteem. Onvoldoende inzicht en begrip bij kiezers kan leiden tot een verminderd vertrouwen in de verkiezingen en de uitslag van de verkiezingen, en mogelijk ook consequenties hebben voor de opkomst.

De complexiteit van het internetstemsysteem vereist aandacht voor de communicatie over de opzet en werking aan de kiezer. De kiezer moet de werking kunnen begrijpen zodat hij weet hoe hij moet stemmen. Uit buitenlandse ervaringen is gebleken dat een eenvoudige opzet helpt in het verkrijgen van publiek vertrouwen in deze wijze van stemmen, bijvoorbeeld door niet te veel af te wijken van bij bestaande procesinrichtingen (zoals briefstemmen). Zodra de complexiteit toeneemt, bijvoorbeeld doordat de kiezer ingewikkelde handelingen moet verrichten of indien hij cryptografische controles kan uitvoeren neemt het begrip af en daardoor ook het vertrouwen.

ACTOREN EN BELANG

	Actor	Intentie
A11	Kiezer	Geen opzet, dreiging komt voort uit onbewust handelen.

MANIEREN WAAROP DREIGING KAN WORDEN UITGEVOERD

In onderstaande tabel zijn voorbeelden opgenomen van manieren waarop de dreiging zich kan voordoen, dan wel middelen waarmee de dreiging wordt uitgevoerd.

	Dreiging
1	Verminderd vertrouwen in verkiezing en uitslag van de verkiezing.
2	Verminderde opkomst verkiezingen.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op **MIDDEL**.

De complexiteit van het internetstemsysteem is groot. Een volledig begrip en inzicht van de opzet en werking is alleen voorbehouden aan technisch experts. Voor de gemiddelde gebruiker is wel een globaal inzicht en begrip haalbaar. Ervaringen in andere domeinen van elektronische dienstverlening (bijvoorbeeld elektronisch bankieren) tonen aan dat dit geen hinder vormt voor het gebruik. Voor stemmen via internet wordt de kans op KLEIN ingeschat.
Onvoldoende inzicht en begrip in het internetstemsysteem leidt mogelijk tot een gebrek aan vertrouwen in de verkiezingen en de verkiezingsuitslag, en leidt mogelijk ook tot een lagere opkomst. Omdat het hier individuele kiezers betreft, wordt het effect ingeschat op MIDDEL.

BESTAANDE OF NIEUWE DREIGING

Dit is een nieuwe dreiging in verband met de introductie van een nieuwe wijze van stemmen.

WAARBORGEN EN PROCESSTAP

Waarborgen: Transparantie

Processtappen:

- Informeren kiesgerechtigden
- Authenticatie
- Uitreiken stembescheiden
- Stemuitbrenging

MAATREGELEN

Preventief	Correctief
• Procesinrichting internetstemsysteem zoveel mogelijk gelijk houden aan (bekende) proces van briefstemmen. • Gebruiksvriendelijk ontwerp van internetstemsysteem welke kiezer meeneem in de te doorlopen stappen. • Voldoende aandacht aan publieke communicatie over internetstemsysteem.	• PR : informatie verschaffen, reageren op berichtgeving en mogelijk foutieve informatie in de media om vertrouwen te behouden.

RISICO INSCHATTING NA MAATREGELEN

De genoemde preventieve maatregelen verkleinen de kans nog verder maar er zullen altijd kiezers blijven die de werking van het internetstemsysteem niet begrijpen. Het effect blijft gelijk, MIDDEL.

Het risico wordt ingeschat op **MIDDEL**.

A14. DS14: Bedienfouten kiezer

BESCHRIJVING

Er zijn veel verschillende (soorten) fouten die kunnen optreden doordat de kiezer het internetstemsysteem of de computer onjuist bedient. Te denken valt aan installatiefouten, per ongeluk wissen van bestanden of programma's, onjuist inloggen (authenticeren), verkeerde keuze voor kandidaten maken, verbinding verbreken met het internet, etc.

Door bedienfouten van de kiezer kan hij mogelijk een verkeerde keuze maken en een stem uitbrengen die niet overeenkomst met zijn intentie. Ook is het mogelijk dat door bedienfouten een kiezer zijn stem helemaal niet kan uitbrengen.
Bedienfouten grijpen in op de waarborg Toegankelijkheid.

ACTOREN EN BELANG

	Actor	Intentie
A11	Kiezer	Geen opzet, dreiging komt voort uit onbewust handelen.

AANLEIDING

Voorbeelden van oorzaken en gebeurtenissen die de reden kunnen zijn voor de dreiging.

	Aanleiding
1	Onvoldoende computervaardigheden kiesgerechtigde.
2	Lastig bedienbaar, niet intuïtieve, gebruikersinterface internetstemsysteem.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op **KLEIN**.

De kans op een bedienfout van de programmatuur is afhankelijk van de eenvoud van de gebruikersinterface. Deze afhankelijkheid is in eigen hand. De kans op bedienfouten aan de kant van de computer van de kiezer zijn groter. Mocht dit leiden tot problemen dan is het internetstemsysteem vanaf een willekeurige andere geschikte computer te benaderen. De kans op een bedienfout wordt daarom ingeschaald op KLEIN.
Bedienfouten kunnen leiden tot ontoegankelijkheid of verkeerd uitgebrachte stemmen. Beide hebben een effect op uitslag van de verkiezingen. Omdat het hier om individuele gevallen gaat wordt het effect ingeschat op KLEIN.

BESTAANDE OF NIEUWE DREIGING

Deze dreiging bestaat ook in het huidige proces van briefstemmen. In geval van briefstemmen kunnen ook (bedien)fouten worden gemaakt zoals het niet dichtplakken van de oranje envelop, het niet (goed) invullen van het briefstembewijs etc.

WAARBORGEN EN PROCESSTAP

Waarborgen: Transparantie

Processtappen:

- Stemuitbrenging

MAATREGELEN

Preventief	Correctief
• Ontwerp intuïtieve gebruikersinterface. • Uitgebreid testen op gebruiksvriendelijkheid (usability lab). • Duidelijke gebruiksinstructies.	• Helpdesk voor kiezer.

RISICO INSCHATTING NA MAATREGELEN

Met een simpele, duidelijke en intuïtieve gebruikersinterface kunnen bedienfouten worden beperkt, maar niet worden voorkomen. Met de maatregelen kan de kans verder worden verkleind. De genoemde maatregelen beperken niet het effect.

Het risico wordt ingeschat op **KLEIN**.

A15. DS15: Incorrecte installatie van internetstemsysteem

BESCHRIJVING

Door een fout bij het installeren of configureren van de programmatuur en apparatuur kan de functioneel correcte werking van het internetstemsysteem worden aangetast. Deze fout is een gevolg van onbewust en onkundig menselijk handelen. Daarbij kunnen ook nieuwe kwetsbaarheden worden geïntroduceerd. De verminderde functionaliteit kan directe gevolgen hebben voor het verkiezingsproces en het bepalen van de uitslag. (zie DS19)

Het is in dit stadium niet mogelijk een uitputtende lijst van dreigingen op te stellen die vallen onder dit dreigingsscenario, bij gebrek aan een specifiek internetstemsysteem. Hier wordt nu volstaan met een aantal voorbeelden van dreigingen die kunnen ontstaan als gevolg van fouten bij de installatie van informatiesystemen:

- Verkeerde of oude versies van de programmatuur of configuratiebestanden wordt geïnstalleerd of niet geïnstalleerd.
- Fouten in de configuratie van netwerkapparatuur (zoals routers, firewalls, switches, servers) zorgt ervoor dat beveiligingskwetsbaarheden ontstaan.
- Servers worden voorzien van verkeerde beveiligingscertificaten waardoor deze elkaar niet herkennen.
- Logbestanden worden overschreven of niet aangemaakt.
- etc.

ACTOREN EN BELANG

	Actor	Intentie
A6	Interne actor, medewerker, beheerder	Deze dreiging komt voor uit onachtzaamheid en onkunde, er is geen achterliggend belang.
A9	Private organisatie, leverancier[26]	Deze dreiging komt voor uit onachtzaamheid en onkunde, er is geen achterliggend belang.

AANLEIDING

Voorbeelden van oorzaken en gebeurtenissen die de reden kunnen zijn voor de dreiging.

	Aanleiding
1	Fouten in instructie/handleiding.
2	Onachtzaamheid en/of onkundige medewerker.
3	Complexiteit internetstemsysteem.

[26] Een leverancier (private organisatie) is een Actor in dit dreigingsscenario indien deze activiteit is uitbesteed aan een leverancier.

	Aanleiding
4	Krappe tijdsplanning.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op **GROOT**.

De complexiteit van het internetstemsysteem, de veelal krappe tijdsvensters waarbinnen gewerkt wordt en de ketenafhankelijkheden tussen verschillende onderdelen van een internetstemsysteem maakt dat de kans op MIDDEL wordt geschat. Een voordeel is dat de installatie volledig voorbereid, getest en geprotocolleerd kan worden.
Het effect van een installatiefout is niet op voorhand te zeggen aangezien het volledig afhangt van het soort fout. Sommige fouten hebben wellicht alleen een effect in situaties van extreme belasting, andere fouten kunnen kritiek en blokkerend zijn voor alle kiezers. Voor de risicoanalyse wordt het effect op GROOT ingeschaald.

BESTAANDE OF NIEUWE DREIGING

De dreiging van een Incorrecte installatie is nieuw ten opzichte van het bestaande proces van briefstemmen, aangezien in laatstgenoemde geen computers worden ingezet.

WAARBORGEN EN PROCESSTAP

Waarborgen: Beschikbaarheid, Kiesgerechtigdheid en Integriteit
Processtappen:

- Opbouw stemsysteem

MAATREGELEN

Preventief	Correctief
• Duidelijke en goed gecommuniceerde procedures, planningen, richtlijnen en handleidingen. • Vooraf testen van configuratie. • Elimineren / beperken van handmatige acties in installatieprocedure(s). • Testen werking internetstemsysteem voorafgaand aan opening verkiezing.	• Opnieuw installeren (bij detectie voorafgaand aan opening stemperiode).

RISICO INSCHATTING NA MAATREGELEN

De genoemde preventieve maatregelen verkleinen de kans aanzienlijk maar detectie van fouten blijft lastig. Blokkerende installatiefouten kunnen met een test voorafgaand aan ingebruikname worden gedetecteerd. Andere fouten kunnen pas later tijdens het verkiezingsproces een effect hebben, in een specifieke situatie of doordat beveiligingskwetsbaarheden geïntroduceerd worden. Het effect van deze fouten is niet met maatregelen te beperken en kan gevolgen hebben voor de uitslag. Het effect blijft GROOT.

Het risico wordt ingeschat op **GROOT**.

A16. DS16: Incorrecte bediening en beheer van internetstemsysteem

BESCHRIJVING

De functioneel correcte werking van het internetstemsysteem wordt aangetast door een onjuiste bediening door medewerkers van de verkiezingsorganisatie, of door handelingen door de functioneel- of technische beheerders van het internetstemsysteem. Dit scenario is een gevolg van onbewust en onkundig menselijk handelen.

Het is waarschijnlijk dat het internetstemsysteem uit meerdere onderdelen bestaat die op verschillende locaties en/of door verschillende personen worden beheerd. Het is in dit stadium niet mogelijk een uitputtende lijst van dreigingen op te stellen bij gebrek aan een specifiek internetstemsysteem. Hier wordt nu volstaan met een aantal voorbeelden van onkundige bediening en beheer:

- Voortijdig openen, schorsen of sluiten van de stemming.
- Invoeren van onjuiste cryptografische sleutels.
- Rondslingeren van cryptografische sleutels.
- Aanpassen van configuratiebestanden.
- Wissen van logbestanden.
- Onbewust inbreuk op stemgeheim (relateren geregistreerde stem en kiezer).
- Onbevoegde toegang tot apparatuur internetstemsysteem (locatie).
- Falen programmatuur, apparatuur of netwerk wordt niet tijdig gedetecteerd.
- etc.

ACTOREN EN BELANG

	Actor	Intentie
A6	Interne actor, medewerker, beheerder	Deze dreiging komt voor uit onachtzaamheid en onkunde, er is geen achterliggend belang.
A9	Private organisatie, leverancier[27]	Deze dreiging komt voor uit onachtzaamheid en onkunde, er is geen achterliggend belang.

AANLEIDING

Voorbeelden van oorzaken en gebeurtenissen die de reden kunnen zijn voor de dreiging.

	Aanleiding
1	Fouten in instructie/handleiding.
2	Onachtzaamheid en/of onkundige medewerker.

[27] Een leverancier (private organisatie) is een Actor in dit dreigingsscenario indien deze activiteit is uitbesteed aan een leverancier.

	Aanleiding
3	Complexiteit internetstemsysteem.
4	Wisselen van personen tijdens de verkiezing.

INSCHATTING RISICO ZONDER MAATREGELEN

Het internetstemsysteem is een complex informatiesysteem dat een grote beheerinspanning vergt. Mede door de veelal krappe tijdsvensters waarbinnen gewerkt wordt en de ketenafhankelijkheden tussen verschillende onderdelen van het internetstemsysteem wordt de kans op beheer- of bedieningsfouten ingeschat op MIDDEL.
Het effect van een bedieningsfout en/of een beheerfout is niet op voorhand te zeggen aangezien dit volledig afhangt van het soort fout. Sommige fouten hebben wellicht alleen een effect in situaties van extreme belasting, andere fouten kunnen kritiek en blokkerend zijn voor alle kiezers en het verkiezingsproces. Omdat deze fouten zich tijdens het verkiezingsproces kunnen voordoen wordt het effect op GROOT ingeschaald.
Het risico wordt ingeschat op GROOT.

BESTAANDE OF NIEUWE DREIGING

De dreiging van onkundig beheer en/of bediening is nieuw ten opzichte van het bestaande proces van briefstemmen, aangezien in laatstgenoemde geen computers worden ingezet.

WAARBORGEN EN PROCESSTAP

Waarborgen: Controleerbaarheid, Kiesgerechtigdheid, Integriteit, Stemgeheim, Beschikbaarheid en Tijdigheid
Processtappen:

- Beheer
- Registratie kiesgerechtigden
- Authenticatie en bepalen kiesgerechtigdheid
- Uitreiken stembescheiden
- Stemuitbrenging
- Stemopneming
- Bepalen uitslag verkiezing

MAATREGELEN

Preventief	Correctief
• Duidelijke en goed gecommuniceerde procedures, richtlijnen en handleidingen. • Opleidingen / examineren van beheerders en medewerkers verkiezingsorganisatie. • Minimaliseren technische beheer (handelingen). • Toezicht / Hanteren van vier-ogen (of meer) principes in beheer en bediening. • Ontwerp van internetstemsysteem dient kritieke	• Fail-over zonder transactie verlies.

Preventief	Correctief
functies te beschermen tegen fouten van individuen. • Oefeningen.	

RISICO INSCHATTING NA MAATREGELEN

Automatiseren van beheer vermindert de kans op beheerfouten. Het effect van beheerfouten kan echter nog steeds GROOT zijn en zodanig ingrijpend dat er geen beperkende maatregelen mogelijk zijn. De kans op bedienfouten is met bovenstaande maatregelen te verlagen naar KLEIN. Het effect van bedienfouten is vaak minder ingrijpend en eventueel met maatregelen te verkleinen.

Het risico wordt ingeschat op **GROOT**.

A17. DS17: Incorrecte de-installatie van internetstemsysteem

BESCHRIJVING

Door een niet goed uitgevoerde de-installatie of vanwege een foutieve procedure, blijven (sporen van) digitale gegevens achter in de apparatuur en programmatuur. Dit is inherent aan de werking van computers en programmatuur. Een andere manier waarop deze dreiging kan optreden kan zijn als gevolg van onbewust en onkundig menselijk handelen.
Gevolg van de dreiging zou kunnen zijn dat het mogelijk wordt om inzage te krijgen in gegevens van kiezers en eventueel (afhankelijk van het ontwerp) ook de inhoud van de geregistreerde stemmen in relatie tot de kiezers. Een ander effect kan zijn dat het stemgeheim in een volgende verkiezing niet goed wordt geborgd of dat achtergebleven stemmen opnieuw worden meegeteld (onbedoeld “ballot stuffing”).

ACTOREN EN BELANG

	Actor	Intentie
A6	Interne actor, medewerker	Deze dreiging komt voor uit onachtzaamheid en onkunde, er is geen achterliggend belang.
A9	Private organisatie, leverancier[28]	Deze dreiging komt voor uit onachtzaamheid en onkunde, er is geen achterliggend belang.

AANLEIDING

Voorbeelden van oorzaken en gebeurtenissen die de reden kunnen zijn voor de dreiging.

	Aanleiding
1	Fouten in instructie/handleiding.
2	Onachtzaamheid en/of onkundige medewerker.
3	Complexiteit internetstemsysteem.
4	Krappe tijdsplanning.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op **MIDDEL**.

De de-installatie van het internetstemsysteem vergt specifieke kennis en vaardigheden en is zeer complex als echt alle digitale sporen gewist moeten worden. Dit zal in de ontwerp fase nader onderzocht moeten worden. In een aantal gevallen kan fysieke vernietiging volstaan.
We schatten de kans een incorrecte de-installatie op MIDDEL.

[28] Een leverancier (private organisatie) is een Actor in dit dreigingsscenario indien deze activiteit is uitbesteed aan een leverancier.

Het effect van een foutieve de-installatie kan ernstig zijn. Vertrouwelijke gegevens, persoonsgegevens eventueel in combinatie met stemgegevens (stemgeheim), kunnen bekend raken na afloop van de verkiezing. Ook kan de correcte werking van het internetstemsysteem (integriteit) in een volgende verkiezing in het geding komen. Voor de risicoanalyse wordt het effect op MIDDEL ingeschaald.

BESTAANDE OF NIEUWE DREIGING

De dreiging van een onkundige de-installatie is nieuw ten opzichte van het bestaande proces van briefstemmen, aangezien in laatstgenoemde geen computers worden ingezet.

WAARBORGEN EN PROCESSTAP

Waarborgen: Kiesgerechtigdheid, Stemgeheim en Integriteit

Processtappen:

- Afbouw internetstemsysteem

MAATREGELEN

Preventief	Correctief
• Fysieke vernietiging van apparatuur en gegevensdragers. • Specifieke (forensische) software voor wissen van gegevens. • Duidelijke en goed gecommuniceerde procedures, planningen, richtlijnen en handleidingen. • Opleidingen / examineren beheerders. • Vooraf procedure oefenen. • Toezicht / Hanteren van vier-ogen (of meer) principes in afbouw.	

RISICO INSCHATTING NA MAATREGELEN

Met de genoemde maatregelen is de kans effectief te verlagen naar KLEIN. Ondanks de kleine kans is het mogelijke effect ernstig. Bovendien is het effect niet te beperken met correctieve maatregelen. Het effect blijft op MIDDEL.

Het risico wordt ingeschat op **MIDDEL**.

A18. DS18: Stembescheiden komen niet of te laat aan bij kiezer of zijn onjuist

BESCHRIJVING

In dit dreigingsscenario heeft de kiezer geen stembescheiden ontvangen of zijn de gegevens op de stembescheiden niet correct, waardoor de kiezer geen stem kan uitbrengen. Dit onder de aanname dat op de stembescheiden gegevens staan die de kiezer nodig heeft om zich te kunnen authenticeren bij het internetstemsysteem.

Het grootste risico op vertraging doet zich voor bij de verzending van de stembescheiden. De stembescheiden werden in het verleden geproduceerd zodra de kandidatenlijst definitief is vastgesteld en daarmee een stembiljet kan worden geproduceerd. Pas op dat moment werden de (brief)stembewijzen worden verzonden naar de kiezers. De doorlooptijd van de internationale post verschilt sterk per land, maar kan voor sommige landen enkele weken bedragen. Deze dreiging speelt in mindere mate voor internetstemmers aangezien daar geen stembiljet toegestuurd hoeft te worden. Voor deze doelgroep kunnen de stembescheiden al eerder worden verstuurd.

Er zijn meerdere situaties denkbaar waardoor dit dreigingsscenario kan optreden. De stembescheiden kunnen verkeerd geadresseerd zijn (verkeerde bestemming), verkeerd of niet bezorgd zijn, verloren gegaan of foutief samengesteld zijn. Incorrecte informatie kan ontstaan omdat verkeerde bestanden zijn aangeleverd aan de drukker, of doordat bij de drukker fouten worden gemaakt.

Optreden van dit scenario kan mogelijk een aanwijzing zijn voor manifestatie van een andere dreiging, namelijk één die het gevolg is van bewust menselijk handelen, zoals beschreven in scenario DS4 of DS5.

ACTOREN EN BELANG

	Actor	Intentie
A6	Interne actor	Medewerkers of toeleveranciers (zoals drukkerij) die fouten maken.
A9	Private organisaties	Postbedrijven in binnen- en buitenland, geen belang tot structureel (laten) verliezen van stembescheiden.

AANLEIDING

Voorbeelden van oorzaken en gebeurtenissen die de reden kunnen zijn voor de dreiging.

	Aanleiding
1	Foutieve adressering kiesgerechtigde.
2	Foutieve stem bescheiden zijn toegestuurd.
3	Stembescheiden zijn niet bezorgd (bijvoorbeeld omdat het e-mailadres op een blacklist staat of onjuist is).

	Aanleiding
4	Stembescheiden zijn verkeerd bezorgd (verkeerd e-mailadres).
5	Stembescheiden zijn verkeerd samengesteld (foutieve informatie).
6	Stembescheiden worden verlaat verstuurd.
7	Fouten bij drukprocedé.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op **MIDDEL**.

In de afgelopen jaren is bij eerdere verkiezingen het regelmatig voorgekomen dat een aantal kiezers hun stembescheiden niet of te laat ontvingen. Meestal was vertraging en/of fouten in de bezorging van de post de oorzaak. Het risico is in mindere mate aanwezig bij internetstemmen omdat het stembewijs al eerder kan worden verstuurd, direct na de dag van kandidaatstelling. Ervaringen uit de Kiezen op Afstand projecten en andere landen heeft laten zien dat met de productie van de stembescheiden veel mis kan gaan, zeker als het gepersonaliseerde stembescheiden betreft. De kans wordt ingeschat op MIDDEL.
Het effect hangt sterk samen met de schaal waarop deze dreiging zich voordoet, dat bepaalt in welke mate het een effect heeft op het aantal kiezers dat niet kan stemmen. Het effect wordt ingeschat op MIDDEL.

BESTAANDE OF NIEUWE DREIGING

Deze dreiging bestaat ook in het huidige proces. Ook bij briefstemmen is het mogelijk dat stembescheiden verloren gaan.

WAARBORGEN EN PROCESSTAP

Waarborg: Kiesgerechtigheid, Toegankelijkheid, Integriteit en Tijdigheid
Processtappen:

- Authenticatie en bepalen kiesgerechtigdheid
- Uitreiken stembescheiden

MAATREGELEN

Preventief	Correctief
• Vroegtijdig toesturen van het deel van de stembescheiden dat dient ter authenticatie. • Elektronisch versturen van de stembescheiden. • Kiezer zelf gegevens elektronisch laten invullen zodat er geen overname-fouten worden gemaakt. • Invoeren permanente registratie. • Gebruik van generiek authenticatiemiddel dat kiezer reeds heeft, waardoor toezending stembescheiden niet meer nodig is.	• Toesturen van vervangende stembescheiden (en tegelijkertijd ongeldig verklaren van ingetrokken stembescheiden).

RISICO INSCHATTING NA MAATREGELEN

De invoering van een generiek authenticatiemiddel voor de kiezer is een maatregel die verder gaat dan de scope van het verkiezingsproces, maar die, indien aanwezig, dit risico sterk doet afnemen.

De kans dat de stembescheiden niet op tijd aankomen bij de kiezer is verder alleen te verkleinen door óf de stembescheiden vroegtijdig te versturen óf door deze elektronisch toe te sturen. Met de automatisering van de productie van stembescheiden (zoals de overdracht van gegevens naar de drukker) kunnen fouten worden verminderd. De kans wordt met deze maatregelen KLEIN.

Het effect is verder te beperken door vervangende stembescheiden uit te reiken. De mogelijkheid om vervangende stembescheiden te kunnen uitreiken vergt specifieke beveiligingsmaatregelen, om te voorkomen dat kiezers alsnog meerdere keren kunnen stemmen. Zo moeten de reeds eerder uitgereikte stembescheiden ongeldig worden verklaard en niet alsnog kunnen leiden tot een stem die wordt meegeteld. Ook moet het uitgifteproces aan strenge regels voldoen om te voorkomen dat vervangende stembescheiden ten onrechte worden verstrekt en om te voorkomen dat een interne actor kennis kan nemen van authenticatiegegevens op de stembescheiden.

Met de maatregelen kan het effect worden gereduceerd tot KLEIN. Het risico wordt ingeschat op **KLEIN**.

A19. DS19 : Functionele-, technische- of beveiligingsgebreken

BESCHRIJVING

Dit dreigingsscenario omvat diverse situaties waarin het internetstemsysteem gebreken vertoond. Met gebreken wordt bedoeld dat de werking niet gelijk is aan de gespecificeerde werking. Dit uit zich doordat het internetstemsysteem onjuiste of ongevraagde eigenschappen vertoond of juist eigenschappen niet vertoond. Onder dit dreigingsscenario worden verschillende gebreken verstaan, zoals:

- Kandidaten worden niet of niet correct weergegeven
- Uitgebrachte stemmen worden niet opgeslagen, worden niet meegeteld, of worden niet incorrect meegeteld.
- Er blijkt een relatie gelegd te kunnen worden tussen kiezer en stem
- Ongeautoriseerde toegang tot het Server domein van het internetstemsysteem
- Logbestanden zijn niet beschikbaar of bevatten incorrecte informatie

Dit dreigingsscenario kan zich voor doen vanaf het moment dat het internetstemsysteem in gebruik wordt genomen (hetgeen ruim voor de daadwerkelijke stemuitbrenging kan zijn).

Het blijkt in de praktijk dat het bijzonder complex en zeer (arbeids-)intensief is om een informatiesysteem uitputtend te testen. Die complexiteit is groter naar mate het informatiesysteem zelf complex is en naar mate deze gebruik maakt van andere componenten, services, libraries etc.
Daarnaast wordt de werking van een informatiesysteem tijdens het gebruik beïnvloed door onvoorspelbare gebeurtenissen van buitenaf, door een onvoorziene combinatie van factoren (zoals de diversiteit in de computerconfiguraties van de kiezers) of door gebreken die aanwezig zijn in standaard software modules waar het internetstemsysteem gebruik van maakt.

Een bijzondere categorie van gebreken betreft de beveiliging van het internetstemsysteem. Op basis van het grote aantal beveiligingsincidenten en cyberaanvallen mag worden gesteld dat er een reële dreiging is dat kwetsbaarheden in de programmatuur ook daadwerkelijk worden misbruikt.

De gebreken kunnen het systeem geheel of gedeeltelijk onbruikbaar maken, voor zowel de kiezer als voor de medewerkers van het stembureau/verkiezingsorganisatie.

ACTOREN EN BELANG

Niet van toepassing.

AANLEIDING

Voorbeelden van oorzaken en gebeurtenissen die de reden kunnen zijn voor de dreiging.

	Aanleiding
1	Onachtzaamheid of ontwerpkeuzes in het proces van specificeren van functionele- technische en

	Aanleiding
	beveiligingseisen kunnen leiden tot gebreken.
2	Onachtzaamheid, ontwerpkeuzes, programmeerfouten, gebruik van niet geteste libraries of modules kunnen leiden tot gebreken.
3	Niet uitputtend testen tijdens de ontwikkeling.
3	Onvoldoende kwaliteitscontrole bij oplevering.
4	Fouten in configuratie of opbouwproces van het internetstemsysteem (‘in productie brengen’) kunnen gebreken introduceren in het internetstemsysteem.
5	Fouten in beheerproces van het internetstemsysteem.
6	Door het hacken van de ontwikkelomgeving van de leverancier kan een backdoor worden aangebracht in het internetstemsysteem.
7	Door een technisch gebrek kan de uitslag niet worden berekend, waardoor de termijn waarbinnen het procesverbaal bij het hoofdstembureau moet zijn wordt overschreden.

INSCHATTING RISICO ZONDER MAATREGELEN

Een internetstemsysteem is een complex en kritisch informatiesysteem. De bijzondere vereisten vanuit beveiliging (zoals maximale controleerbaarheid zonder dat stemgeheim wordt doorbroken) maken dat het ontwerp, de ontwikkeling en het testen van een internetstemsysteem anders moet worden aangepakt, omdat de kans anders groot is dat er gebreken worden geïntroduceerd. Het is bijzonder lastig om met testinspanningen alle gebreken vooraf te ontdekken. De kans op gebreken zonder maatregelen te nemen is GROOT.
Het effect van functionele- of technische gebreken is niet op voorhand te zeggen aangezien dat afhangt van het soort gebrek, waar in het systeem deze aangrijpt en wat het effect is voor de werking van het systeem. Voorbeeld: Gebreken kunnen aangrijpen op de gebruikersinterface, en hebben daarmee slechts een cosmetisch effect hebben voor een beperkt deel van de kiezers. Een gebrek in de module die zorgt voor de ontsleuteling van stemmen kan een effect hebben op alle stemmen. Het effect wordt ingeschat op GROOT.

Het risico wordt ingeschat op GROOT.

BESTAANDE OF NIEUWE DREIGING

Nieuwe dreiging

WAARBORGEN EN PROCESSTAP

Waarborgen: Controleerbaarheid, Integriteit, Kiesgerechtigdheid, Stemgeheim, Uniciteit, Toegankelijkheid, Beschikbaarheid, Tijdigheid
Processtappen:

- Ontwikkelen/verwerving internetstemsysteem
- Opbouw internetstemsysteem
- Beheer
- Registratie kiezers

- Authenticatie en bepalen kiesgerechtigdheid
- Uitreiken stembiljet
- Stemuitbrenging
- Stemopneming
- Bepalen uitslag verkiezing

MAATREGELEN

Preventief	Correctief
• Bij ontwerp en ontwikkeling van internetstemsysteem toepassen van principes van defensief programmeren, waardoor het internetstemsysteem minder kwetsbaar wordt voor onverwachte situaties of falen van onderdelen. • Uitvoeren van rigoureuze testscenario's : maximale belasting, ketentesten, penetratietesten etc. • Uitvoerig testen van internetstemsysteem op grote diversiteit van Client omgevingen. • Compartimenteren van internetstemsysteem • Voorkomen van tijdsdruk bij het ontwerp, ontwikkeling en testen van het internetstemsysteem. • Kritische componenten (zoals uitslagberekening) meervoudig ontwikkelen door verschillende teams van programmeurs. • Controle van programmatuur op ongewenste code. • Cryptografische maatregelen (zoals hash algoritmes) om wijzigingen te detecteren of te voorkomen (encryptie).	• Controle door stembureau op correcte werking voorafgaand en tijdens stemming. • Audit op correcte werking, bijvoorbeeld door analyse van logbestanden. • Individuele verificatie door kiezer 'ontvangen zoals uitgebracht', of 'geteld zoals ontvangen' of 'geteld zoals uitgebracht'. • Universele verificatie door kiezers of derden dat alle stemmen correct geteld zijn.

RISICO INSCHATTING NA MAATREGELEN

De genoemde maatregelen kunnen de kans op gebreken in het internetstemsysteem sterk verkleinen. De noodzakelijke inspanning hiervoor is echter bijzonder groot en wordt in de praktijk altijd beperkt in geld, tijd en middelen. In het meest optimale geval zullen de praktisch uitvoerbare maatregelen de kans op gebreken reduceren tot MIDDEL.
Het effect van gebreken kan zeer groot zijn, zoals ernstige beveiligingsgebreken of de integriteit van het verkiezingsproces aantasten. Eerder genoemde maatregelen kunnen de effecten niet beperken, maar wel detecteren. Echter sommige maatregelen zoals verificatie door de kiezer of stembureau op het correct verwerken van de stem introduceren op zichzelf weer nieuwe complexe functionaliteit in het internetstemsysteem waarin ook gebreken kunnen voorkomen. Het effect blijft daarom GROOT.

Het risico wordt ingeschat op **GROOT.**

A20. DS20: Ontoegankelijkheid

BESCHRIJVING

Ontoegankelijkheid is een dreiging die een kiezer hindert of uitsluit van het gebruik van het internetstemsysteem.

Ontoegankelijkheid kan ontstaan doordat in de gebruikersinterface of opzet van het internetstemsysteem niet voldoende rekening is gehouden met personen met lichamelijke beperkingen, of factoren zoals woonplaats, taal, leeftijd, opleidingsniveau etc.
De gebruikersinterface grijpt ook in op de waarborg van transparantie.

Een andere oorzaak van ontoegankelijkheid heeft te maken met specifieke eisen die gesteld worden aan de kiezer en specifieke middelen die hij moet hebben om een registratieverzoek in te dienen of om te kunnen stemmen. Bijvoorbeeld de eis van een specifiek authenticatiemiddel (bijvoorbeeld een E-ID op een smartcard), specifieke hardware of software eisen (zoals type operating systeem, type of versie van browser, rechten tot installatie van software, encryptie technologie etc.). De ontoegankelijkheid neemt toe als de kiezer niet aan deze eisen kan voldoen (bijvoorbeeld omdat hij in een bepaald land woont waar een export restrictie geldt op bepaalde encryptietechnologie) of waar de kiezer additionele kosten moet maken om aan deze eisen te voldoen.

ACTOREN EN BELANG

Niet van toepassing.

AANLEIDING

Voorbeelden van oorzaken en gebeurtenissen die de reden kunnen zijn voor de dreiging

	Aanleiding
1	Onachtzaamheid of ontwerpkeuzes in het proces van specificeren van functionele- technische en beveiligingseisen leidt tot verminderde functionaliteit m.b.t. toegankelijkheid.
2	Onachtzaamheid, ontwerpkeuzes of fouten in het software ontwikkelproces – in een aantal fasen vertalen van de functionele eisen en wensen naar een correct werkend internetstemsysteem - kunnen leiden tot verminderde functionaliteit m.b.t. toegankelijkheid.

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op **MIDDEL**.

Het ontwerp van een internetstemsysteem is een complex proces waarin afwegingen moeten worden gemaakt tussen verschillende waarborgen. Zo kan vanuit oogpunt van beveiliging een zeer betrouwbaar registratieproces worden ingericht waarin de kiezer zich persoonlijk moet identificeren bij een ambassade. De toegankelijkheid tot het stemproces neemt dan echter af. Veel van de oorzaken van ontoegankelijkheid liggen daarmee echter in eigen hand. De grote onbekende

is de diversiteit van de computer configuratie van de kiezer heeft. Om die reden wordt de kans op ontoegankelijkheid ingeschat op MIDDEL.
Het effect van ontoegankelijkheid wordt op KLEIN ingeschat omdat het naar verwachting enkele kiezers zal betreffen die door ontoegankelijkheidsredenen niet deel kunnen nemen aan de stemming.

BESTAANDE OF NIEUWE DREIGING

Ontoegankelijkheid wordt beschouwd als een nieuwe dreiging gelet op de sterkere mate waarin gebruik gemaakt wordt van technologie.

WAARBORGEN EN PROCESSTAP

Waarborgen: Toegankelijkheid
Processtappen:

- Registreren kiesgerechtigdheid
- Authenticatie en bepalen kiesgerechtigdheid
- Stemuitbrenging

MAATREGELEN

Preventief	Correctief
• Bij ontwerp van internetstemsysteem rekening houden met personen met een lichamelijke beperking, meertaligheid en laag opleidingsniveau. Voldoen aan webrichtlijnen[29]. • Bij ontwerp van internetstemsysteem rekening houden met wereldwijde (on)beschikbaarheid van specifieke middelen (zoals authenticatiemiddel, vereiste software, encryptietechnologie etc.) • Onderzoek usability / gebruikersinterface onder testgroepen. • Uitvoerige testen van internetstemsysteem op grote diversiteit van client-omgevingen.	• Alternatief briefstemmen.

RISICO INSCHATTING NA MAATREGELEN

De preventieve maatregelen verlagen de kans op ontoegankelijkheid. Door het internetstemsysteem tegen veel voorkomende computerconfiguraties te testen kan ontoegankelijkheid voor de kiezer worden gereduceerd naar KLEIN.

[29] Zie https://lijsten.forumstandaardisatie.nl/open-standaard/webrichtlijnen

De maatregelen hebben geen impact op het effect. Het alternatief van briefstemmen blijft voorhanden onder de voorwaarden dit nog mogelijk is in de beschikbare tijd. Het effect blijft KLEIN.
Het risico wordt ingeschat op **KLEIN**.

A21. DS21: Onbeschikbaarheid

BESCHRIJVING

In dit scenario is het internetstemsysteem onbeschikbaar voor de kiezer als gevolg van uitval van (delen van) het systeem. Afhankelijk van de exacte onderdelen die uitvallen heeft dit gevolgen voor de kiezers, het stembureau of beheerders van het systeem.

Onbeschikbaarheid kan het gevolg zijn van een force majeur, zoals brand, stroomuitval, bommelding, natuurramp of andere calamiteiten. De uitval van het systeem is niet het gevolg van gebreken (zie DS19), incorrecte bediening (zie DS16) of doelbewust verstoren (zie DS9).

Onbeschikbaarheid kenmerkt zich niet alleen in een onbereikbaarheid van het internetstemsysteem, maar ook in een dusdanige uitval van functionaliteit dat het systeem niet meer bruikbaar is voor het beoogde doel en dus onbedienbaar is geworden.

Calamiteiten treden vaak lokaal op maar kunnen afhankelijk van de locatie van optreden een groot effect hebben op de beschikbaarheid van het internetstemsysteem. Een stroomstoring bij een kiesgerechtigde ter plaatse sluit één kiezer uit. Dezelfde storing op locatie van het stembureau/verkiezingsorganisatie of op een belangrijk internetknooppunt, kan iedereen uitsluiten van gebruik.

Een calamiteit kan op zich zelf weer gevolgen (schade) hebben met nog meer impact het internetstemsysteem. Zo kan een kleine brand als gevolg van blikseminslag zorgen voor stroomuitval. Het blussen van de brand kan op haar beurt mogelijk het overschakelen op noodstroom weer verhinderen, met een ongecontroleerde ‘powerdown’ van het systeem en mogelijk verlies van gegevens tot gevolg.

ACTOREN EN BELANG

Niet van toepassing.

AANLEIDING

Voorbeelden van oorzaken en gebeurtenissen die de reden kunnen zijn voor de dreiging:

	Aanleiding
1	Weersinvloeden
2	Brand
3	Overstroming
4	Pandemie
5	Stroomuitval
6	Ongeval

INSCHATTING RISICO ZONDER MAATREGELEN

Het risico wordt ingeschat op **GROOT**.

De kans dat er ergens op de wereld een force majeur optreedt is aanzienlijk. Kiezers zitten verspreid over de wereld waaronder landen waar geen betrouwbare stroomvoorziening is. De kans dat een kiezer last ondervindt van onbeschikbaarheid van het internetstemsysteem is daarom aanzienlijk. De kans dat een force majeur optreedt op locatie van het stembureau of de locatie van de Server of in het internet, wordt als klein ingeschat, mede door de hoge betrouwbaarheid van de infrastructuur in Nederland en het zelf-routerende karakter van het internet. De kans op onbeschikbaarheid van het internetstemsysteem als geheel wordt geschat op MIDDEL.

Het effect van het optreden van een force majeur is volledig afhankelijk van de locatie waar dreiging zich voordoet. Bij een enkele kiezer is het effect klein, ook omdat deze meerdere dagen de tijd heeft om te stemmen. Als het een dreigingsscenario betreft met een destructief effect op de Server dan is het effect groot aangezien alle kiezers worden getroffen. Afhankelijk van het moment dat zich de dreiging voordoet is er een terugvaloptie naar briefstemmen. Het effect wordt op GROOT ingeschat.

BESTAANDE OF NIEUWE DREIGING

De dreiging van onbeschikbaarheid is nieuw ten opzichte van het bestaande proces van briefstemmen.

WAARBORGEN EN PROCESSTAP

Waarborgen: Beschikbaarheid

Processtappen:

- Registratie kiesgerechtigden
- Authenticeren en bepalen kiesgerechtigdheid
- Uitreiken stembescheiden
- Stemuitbrenging
- Stemopneming
- Bepalen uitslag verkiezing

MAATREGELEN

Preventief	Correctief
• Meerdaagse stemperiode. • Mogelijkheid voor kiezer om alsnog per brief te stemmen bij onbeschikbaarheid internetstemmen (al is de resterende tijd dan wel zeer kort). • Keuze van locatie voor Server domein die minder gevoelig is voor invloeden van natuurrampen of ongevallen. • Uitwijklocatie inrichten.	• Vervangen / repareren van door ramp getroffen / beschadigde onderdelen. • Uitwijklocatie betrekken. • Afhankelijk van processtap: overgaan op handmatige verwerking (bv bij registratie kiesgerechtigdheid, bepalen uitslag).

Preventief	Correctief
• Redundant en multi-site uitvoeren van kritieke componenten in het Server en Toezicht domein. • Continuïteit verhogende voorzieningen zoals noodstroom, brandblusinstallatie etc. • Beveiligingsmaatregelen internetstemsysteem.	

RISICO INSCHATTING NA MAATREGELEN

Door in het ontwerp van het internetstemsysteem rekening te houden met hoge beschikbaarheid ('high availability') wordt de kans op onbeschikbaarheid aan de kant van de server sterk verkleind. Invoer van een meerdaagse stemperiode reduceert de kans aan de kant van de kiezer. De kans wordt daarmee KLEIN.
Maatregelen aan de serverkant kunnen het effect van een force majeur verminderen. Aan de kant van de kiezer zijn geen maatregelen te treffen, echter door het lokale voorkomen van een force majeur is het effect beperkt tot een kleine(re) groep kiezers. Het effect wordt MIDDEL.

Het risico wordt ingeschat op **MIDDEL**.

B Bijlage: Dreigingsscenario's en processtappen

		Ontwikkeling/verwerving	Opbouw stemsysteem	Beheer	Registratie kiesgerechtigden	Authenticatie en	Uitreiken stembescheiden	Stemuitbrenging	Stemopneming	Bepalen uitslag verkiezing	Afbouw stemsysteem
1	**Publiceren informatie over beveiliging internetstemsysteem**							√	√	√	
2	Verkopen stem				√		√	√			
3	Dwang / beïnvloeding van kiezer						√	√			
4	Niet-kiesgerechtigde brengt stem uit							√			
5	**Manipuleren van de stem of uitslag**						√	√	√		
6	Kiezer brengt meer dan één stem uit							√			
7	**Chantage**							√	√	√	
8	**Relatie tussen kiezer en inhoud stem (doorbreken stemgeheim)**							√	√		
9	**Doelbewust verstoren van de verkiezing**				√	√	√	√	√	√	
10	**Defacing / bekladding internetstemsysteem**				√			√			
11	**Springplank: misbruik systeem voor andere aanvallen**							√			
12	Voortijdige publicatie uitslag							√			
13	**Onvoldoende inzicht en begrip kiezers**				√	√	√	√	√	√	
14	Bedienfouten kiezer							√			
15	**Incorrecte installatie van internetstemsysteem**		√								
16	**Incorrecte bediening en beheer van internetstemsysteem**			√	√	√	√	√	√	√	
17	**Incorrect de-installatie van internetstemsysteem**										√
18	Stembescheiden komen niet aan bij kiezer of zijn onjuist				√	√	√				
19	**Functionele-, technische- of beveiligingsgebreken**	√	√	√	√	√	√	√	√	√	√

		Ontwikkeling/verwerving	Opbouw stemsysteem	Beheer	Registratie kiesgerechtigden	Authenticatie en	Uitreiken stembescheiden	Stemuitbrenging	Stemopneming	Bepalen uitslag verkiezing	Afbouw stemsysteem
20	**Ontoegankelijkheid**				√	√		√			
21	**Onbeschikbaarheid**				√	√	√	√	√	√	

Vetgedrukte dreigingsscenario's zijn nieuw ten opzichte van briefstemmen

C Bijlage: Dreigingsscenario's en waarborgen

		Transparantie	Controleerbaarheid	Integriteit	Kiesgerechtigdheid	Stemvrijheid	Stemgeheim	Uniciteit	Toegankelijkheid	Beschikbaarheid	Tijdigheid
1	**Publiceren informatie over beveiliging internetstemsysteem**	√	√	√							
2	Verkopen stem				√		√				
3	Dwang / beïnvloeding van kiezer					√	√				
4	Niet-kiesgerechtigde brengt stem uit			√	√						
5	**Manipuleren van de stem of uitslag**		√	√	√			√			
6	Kiezer brengt meer dan één stem uit			√				√			
7	**Chantage**			√	√		√			√	
8	**Relatie tussen kiezer en inhoud stem (doorbreken stemgeheim)**						√				
9	**Doelbewust verstoren van de verkiezing**			√						√	
10	**Defacing / bekladding internetstemsysteem**								√	√	
11	**Springplank: misbruik systeem voor andere aanvallen**										
12	Voortijdige publicatie uitslag			√							√
13	**Onvoldoende inzicht en begrip kiezers**	√									
14	Bedienfouten kiezer	√									
15	**Incorrecte installatie van internetstemsysteem**			√	√					√	
16	**Incorrecte bediening en beheer van internetstemsysteem**		√	√	√		√			√	√
17	**Incorrecte de-installatie van internetstemsysteem**			√	√		√				
18	Stembescheiden komen niet aan bij kiezer of zijn onjuist			√	√				√		V
19	**Functionele-, technische- of beveiligingsgebreken**		√	√	√		√	√	√	√	√
20	**Ontoegankelijkheid**								√		

	Transparantie	Controleerbaarheid	Integriteit	Kiesgerechtigdheid	Stemvrijheid	Stemgeheim	Uniciteit	Toegankelijkheid	Beschikbaarheid	Tijdigheid
21 **Onbeschikbaarheid**									√	

Vetgedrukte dreigingsscenario's zijn nieuw ten opzichte van briefstemmen

D Bijlage: Geraadpleegde bronnen

1.	Adviescommissie inrichting verkiezingsproces, Stemmen met vertrouwen, 2007.
2.	Risicoanalyse kiezen op afstand, Kiezers in het buitenland, Ministerie van BZK, 2003
3.	Risicoanalyse kiezen op afstand, Kiezers in het buitenland, Ministerie van BZK, 2007
4.	OVSE/ODIHR, The Netherlands parliamentary elections 22 November 2006 Election Assessment
5.	Cybersecuritybeeld Nederland CSBN-3, NCSC
6.	Informatiebeveiliging onder controle, Paul Overbeek e.a. 2006
7.	EAC, Voluntary Voting Systems Guidelines, 2009.
8.	EAC, A Survey of Internet Voting 2011
9.	OVSE, Norway internet voting pilot project local government elections, September 2011
10.	Raad van Europa, Certification of e-voting systems. Guidelines for developing processes that confirm compliance with prescribed requirements and standards, 2011.
11.	Raad van Europa, Code of good practices in electoral matters, 2013.
12.	Raad van Europa, legal, operational and technical standards for e-voting, Recommendation Rec (2004) 11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum.
13.	Verification and Validation Issues in Electronic Voting, Orhan Cetinkaya, and Deniz Cetinkaya 2007
14.	Electronic Voting: Essential Considerations, IDEA December 2011
15.	When Reality Comes Knocking. Norwegian Experiences with Verifiable Electronic Voting, Ida Sofie Gebhardt Stenerud and Christian Bull
16.	Technical report Source code audit of Norwegian electronic voting system, Ministry of Local Government and Regional Development Norway. 2013
17.	International Experience with E-Voting, Norwegian E-Vote Project, IFES, 2012
18.	e-Vote 2011 Security Objectives, Ministry of Local Government and Regional Development Norway.
19.	Electronic voting – challenges and opportunities, Ministry of Local Government and Regional Development Norway. 2006
20.	Compliance with International Standards, Norwegian E-Vote Project, IFES, 2012
21.	eValg2011 platform – 1.4 update for 2013 Parliamentary elections Electronic Voting Software – Security Target, Scytl 2013
22.	E-voting conception security: analysis and measures. National Electoral Committee Estland, 2003
23.	E-voting conception security: analysis and measures. National Electoral Committee Estland, 2010
24.	Observing electronic voting, Kåre Vollan, Norwegian Centre for Human Rights/NORDEM, 2005
25.	A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), David Jefferson, et al 2004

26. Analyzing internet voting security, David Jefferson, et al 2004
27. Jones, Douglas W. en Simons, Barbara, Broken Ballots. Will your vote count? (Stanford 2012).
28. Issues Guide: Internet Voting, The Centre for Public Involvement, University of Alberta, 2012
29. Discussion Paper: Internet Voting, Elections BC, Canada, 2011
30. Independent panel on internet voting, British Columbia, Preliminary Report - October 2013
31. iVote Strategy for the NSW State General Election 2015, NSW Electoral Commission, 2013
32. Internet voting in Australian election systems, 2013

E Bijlage: Richtlijnen en maatregelen voor veilige informatiesystemen

In deze bijlage wordt een nadere uiteenzetting gegeven van maatregelen die genomen kunnen (en moeten) worden om een internetstemsysteem te beveiligen. Deze lijst van maatregelen is niet opgesteld met de intentie om uitputtend te zijn, de lijst is bedoeld om inzicht te geven in de mogelijke maatregelen, vanuit het oogpunt van de risico-analyse. In de (technische) ontwerpfase van de ontwikkeling van een internetstemsysteem moeten de exacte maatregelen worden bepaald.

Vooropgesteld moet zijn dat de veiligheid van een informatiesysteem geen absoluut begrip is. Wel kunnen onderstaande maatregelen bijdragen aan een informatiesysteem dat, onder alle omstandigheden, exact doet wat het geacht wordt te doen en dat haar functionaliteit en gegevens alleen ter beschikking staan aan die personen of systemen die daartoe gerechtigd zijn.

De maatregelen hebben betrekking op het ontwerp, de ontwikkeling, het internetstemsysteem zelf, het gebruik en beheer en de organisatie.

ONTWERP

- Definieer de exacte specificaties van de beoogde werking van het systeem, waar relevant en mogelijk in een formele taal.
- Hanteer ontwerpprincipes van eenvoud, security bij design, modulaire opbouw en defensief programmeren.
- Automatiseer kwetsbare / gevoelige taken om menselijke fouten uit te sluiten.
- Ontwerp beschermingsmaatregelen om uitval van componenten op te vangen (meervoudig uitvoeren, high availability maatregelen, spreiding over locaties, etc.).
- Ga uit van volledige transparantie en openbaarheid. Publiceer alle documentatie, zoals offertes en contracten met leveranciers, functioneel en technisch ontwerp.
- Gebruik waar mogelijk open source systemen, zodat inspectie van code mogelijk is door derden.
- Pas zoveel mogelijk universele en open standaarden en security protocollen toe.
- Ontwerp controle mogelijkheden om correcte werking van het systeem te kunnen bepalen, gedurende en na afloop van de verkiezing.
- Bemoeilijk afluisterbaarheid door in ontwerp communicatie met kiezer te spreiden over meerdere kanalen uit te voeren.

ONTWIKKELING

- Screening van alle personen die werken aan de ontwikkeling van de programmatuur.
- Fysieke en logische toegangsbeveiliging op de softwareontwikkelomgeving.
- Verplicht gebruik versiebeheersysteem, met audittrail op alle bewerkingen.

- Uitvoerig testprogramma dat parallel loopt met ontwikkeling. Type testen: unittesten tegen functionele specificaties, testen van extremen, loadtesten, broncode review, integratietesten, duurtesten, red team & white hat hacking.
- Inzet van cryptografische middelen om integriteit van broncode te borgen.
- Gebruik van betrouwbare en geteste compilers.
- Verplichte documentatie van alle broncode, geschikt voor formele audit processen (en eventueel Common Criteria evaluatie tegen nader vast te stellen EAL).
- Kritische componenten (zoals uitslagberekening) laten ontwikkelen door verschillende onafhankelijke teams van programmeurs.
- Betrekken van belangengroeperingen / actoren bij het ontwerp en ontwikkeling van het internetstemsysteem om de kwaliteit van de beveiligingsmaatregelen te verbeteren en de kans van de dreiging van (betrokken) actoren te verkleinen.

INTERNETSTEMSYSTEEM

- Betrek alle apparatuur van betrouwbare leveranciers.
- Gebruik van “geharde” operating systemen voor computers en netwerk componenten (zoals routers, firewalls etc.). Geharde operating systemen zijn operating systemen waarvan niet-gebruikte functionaliteit is verwijderd of uitgezet, waardoor de kwetsbaarheid van het systeem afneemt.
- Gebruik van netwerk apparatuur zoals routers en firewalls die internetverkeer routeren en filteren zodat de ongewenst internetverkeer kan worden gefilterd.
- Gebruik Intrusion Detection Systems om a-typisch netwerkverkeer te detecteren.
- Gebruik fysieke en logische toegangsbeveiligingsmaatregelen om de toegang tot servers en netwerkapparatuur te beschermen.
- Gebruik een separaat audit / logsysteem om de werking van een systeem, alsook toegang(spogingen) en bediening en beheeracties kan vastleggen.
- Gebruik van speciale Hardware Security Modules voor de generatie en veilige opslag van cryptografische sleutels.
- Gebruik van cryptografische technieken zoals certificaten, handtekeningen om de authenticiteit van systemen vast te stellen.
- Maak gebruik van versleutelde verbindingen voor transport over internet (SSL/TLS, minimale sleutellengte 2048 bits).
- Gebruik van threshold encryptie voor cryptografische sleutels.
- Compartimentering van server netwerkinfrastructuur. Gebruik van ‘air gaps’ om systemen daadwerkelijk van elkaar te scheiden.
- Controle functionaliteit die het mogelijk maakt om de correcte werking van het internetstemsysteem te controleren onafhankelijk van het internetstemsysteem zelf.

INSTALLATIE, GEBRUIK EN BEHEER

- Administratieve en organisatorische maatregelen, zoals toepassen van meer-ogen principe, functiescheiding, het opdelen en verspreiden van gegevens of systemen onder meerdere onafhankelijke partijen, openbaarheid en audit.

- Installatie vanaf aantoonbaar lege / schone computers, volgens exact script dat vooraf is getest.
- Sleutelgeneratie in apart proces door andere personen, los van de ontwikkelaars of beheerders van het internetstemsysteem.
- Minimaliseer beheerwerkzaamheden, beperk deze tot strikt noodzakelijke activiteiten onder toezicht.
- Beveiligingsbeheer uit laten voeren door andere personen dan beheerders vanuit onafhankelijke organisatie.
- Fysieke en logische toegangscontrole van gebruikers (stembureau), en eventuele beheerders.
- Beheerwerkzaamheden uitgeschreven conform COBIT

ORGANISATIE

- Leverancier is gecertificeerd tegen ISO9001:2008 en die werkt volgens Code voor Informatiebeveiliging (met norm obv ISO27001 en code of practice NEN/ISO 17799:2005)
- Screening / Verklaring omtrent Gedrag van medewerkers en toeleveranciers

VERDONCK KLOOSTER & ASSOCIATES

DEEL III - EISEN AAN EEN INTERNETSTEMSYSTEEM

VERDONCK KLOOSTER & ASSOCIATES

DEEL III - EISEN AAN EEN INTERNETSTEMSYSTEEM

DATUM	28 januari 2014
STATUS	Definitief
VERSIE	1.0

INHOUDSOPGAVE

1 INLEIDING

1.1 Algemeen

In dit derde deel van het onderzoek naar internetstemmen worden eisen beschreven die bepalend zijn voor een betrouwbare vorm van internetstemmen. In opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) zijn functionele, technische en beveiligingseisen opgesteld waar een internetstemsysteem aan dient te voldoen. Deze eisen kunnen gebruikt worden voor het vormgeven van wet- en regelgeving, voor het opstellen van functionele- en technische ontwerpen en als onderdeel van de norm bij certificatie.

Tevens is onderzocht hoe de kiezers in het buitenland op een veilige en betrouwbare wijze kunnen worden voorzien van de stembescheiden die men nodig heeft om via internet te stemmen. In het onderzoek is ook onderzocht welke eisen gesteld moeten worden om het stembureau een zinvolle taakinvulling te geven in het geval van internetstemmen.

In de aanpak om de eisen op te stellen is uitgegaan van de dreigingsscenario's uit de risico-analyse naar internetstemmen (deel II). Hierbij is met name gekeken naar de dreigingsscenario's met een risico-inschatting op het niveau Hoog of Middel.

In het proces om eisen op te stellen wordt de grens geraakt van het maken van een ontwerp van een internetstemsysteem. Het stellen van bepaalde eisen kan immers het ontwerp sterk in een bepaalde richting sturen of juist het aantal vrijheidsgraden van de ontwerpers beperken. Gepoogd is om de grens van het maken van een ontwerp niet te overschrijden, aangezien dit buiten de reikwijdte van de opdracht viel. Wel zijn een aantal *ontwerpprincipes* opgesteld, welke gebaseerd zijn op internationale ervaringen, de eerdere ervaringen van Kiezen op Afstand, en welke zijn afgeleid van de risico-analyse.

De in dit document opgenomen eisen zijn niet uitputtend. In de ontwerpfase van het internetstemsysteem zullen nieuwe eisen ontstaan, welke toegevoegd moeten worden aan dit programma van eisen.

In de opdracht is gevraagd om functionele, technische en beveiligingseisen. Naar de mening van de auteurs is het ook nodig om eisen te stellen aan het proces en de organisatie en om een aantal algemene eisen te stellen aan de invoering van internetstemmen.

1.2 Afbakening

Dit document beschrijft de eisen die gesteld worden aan een internetstemsysteem.

Een internetstemsysteem is hierbij gedefinieerd als: *een wijze van stemmen waarbij de kiezer op elektronische wijze zijn stemvoorkeur kenbaar maakt, op een locatie waar geen toezicht wordt gehouden, en waarbij hij de stem overdraagt aan het stembureau via het openbare internet*.

In dit document worden alleen eisen gesteld aan het internetstemsysteem zelf. In dit document zijn geen eisen opgenomen aan de wijze waarop het internetstemsysteem moet worden ontworpen, ontwikkeld, beheerd of afgebouwd.

1.3 Leeswijzer

In hoofdstuk 2 is een algemene introductie van de eisen opgenomen en is een overzicht gegeven van de aanbevelingen en eisen die in andere landen zijn opgesteld. In hoofdstuk 3 zijn de algemene waarborgen opgenomen die de algemene beginselen vormen waar een internetstemsysteem aan moet voldoen. In de hoofdstukken 4, 5, 6 en 7 zijn achtereenvolgens de proces-, functionele, technische en beveiligingseisen beschreven. In hoofdstuk 8 zijn de eisen beschreven om een betrouwbare distributie van stembescheiden mogelijk te maken. In hoofdstuk 9 is de taak en functie van het stembureau in de context van een internetstemming gedefinieerd. Tenslotte zijn in hoofdstuk 10 een aantal algemene aanbevelingen geformuleerd voor de invoering van internetstemmen.

1.4 Legenda

Elke eis is voorzien van een letter en een nummer. De letter definieert het soort eis.

A	Algemene eis
B	Beveiligingseis
F	Functionele eis
P	Proceseis
T	Technische eis
W	Waarborg

2 EISEN

2.1 Algemeen

Een internetstemsysteem dient te voldoen aan de algemene beginselen die gesteld worden aan elk verkiezingssysteem. In internationaal verband wordt dit vaak aangeduid met de vijf principes universal, equal, free, secret en direct elections. De beginselen zijn in Nederland vervat in de waarborgen zoals die in 2007 beschreven zijn door de commissie *Stemmen met vertrouwen*. De waarborgen zijn opgenomen in hoofdstuk 3.

De waarborgen vormen de algemene beginselen waar een internetstemsysteem aan moet voldoen. Van de waarborgen kunnen nadere eigenschappen worden afgeleid die een internetstemsysteem dient te bezitten. Deze eigenschappen hebben betrekking op zowel de gebruikte middelen (zoals computerapparatuur, programmatuur, netwerk apparatuur, authenticatiemiddelen, et cetera) als op het proces. De vereiste eigenschappen worden in dit document aangeduid als eisen. Het totaal aan eisen wordt het programma van eisen genoemd (PvE). Het PvE is onderverdeeld in functionele eisen, technische eisen, proceseisen en beveiligingseisen.

De functionele eisen beschrijven de gewenste functionaliteit van het internetstemsysteem, zoals de wijze waarop de kiezer zijn keuze kan maken, de berekening van de uitslag, et cetera. De technische eisen hebben betrekking op de technologie die gebruikt wordt in het internetstemsysteem en enkele prestatie-eisen die hieraan gesteld worden. De proceseisen hebben betrekking op de organisatie en inrichting van het stemproces. De beveiligingseisen tenslotte geven aan welke eigenschappen het systeem *moet hebben* én welke eigenschappen het internetstemsysteem *niet mag hebben* om weerstand te bieden aan de dreigingen die worden onderkend. De beveiligingseisen hebben betrekking op zowel de gebruikte (ICT-) middelen, het proces als de organisatie.

De eisen dienen twee doelen. Allereerst hebben de eisen een dwingende functie richting de ontwerper / leverancier van het internetstemsysteem. Ten tweede vormen de eisen een maatstaf voor zowel de gebruikers als voor certificatie instanties om tegen te beoordelen of het internetstemsysteem doet wat het moet doen. Dit laatste doel helpt in het verkrijgen van vertrouwen onder kiezers om een nieuwe stemmethode te gebruiken.

2.2 Internationale normenkaders

Door verschillende wetenschappelijke instellingen en door overheden uit diverse landen zijn in het verleden normen en eisen geformuleerd waar een internetstemsysteem aan moet voldoen. Voor een deel zijn deze eisen opgesteld met een specifieke toepassing of aanbesteding op het oog, en voor een deel zijn deze eisen vanuit een meer generieke invalshoek opgesteld. In de laatste categorie vallen de aanbevelingen zoals die door de Raad van Europa zijn opgesteld in 2004.

In de aanpak is gebruik gemaakt van deze normenkaders en sets van eisen zoals die eerder zijn opgesteld. Steeds is daarbij afgewogen of de eis integraal overgenomen kon worden met inachtneming van de toepassing van het internetstemsysteem, het beveiligingsdoel en eventuele wettelijke kaders.

Bij het opstellen van de eisen in dit document is gebruikt gemaakt van:

a. Raad van Europa – Recommendation Rec (2004) 11.
b. Programma van eisen geformuleerd bij de Kiezen op afstand experimenten met internetstemmen in 2004 (verkiezing leden van het Europees Parlement).
c. Hoofdlijnenontwerp van een basisvoorziening internetstemmen (BVIS) door ICTU in opdracht van BZK.
d. Eisen zoals geformuleerd door Noorwegen[1], Estland[2] en Zwitserland[3] welke mede gebruikt zijn voor aanbestedingen en selectie van leveranciers.
e. Eisen aan internetstemsystemen opgesteld door het Duitse Gesellschaft für Informatik[4].

2.2.1 Common Criteria

Idealiter zijn eisen dusdanig geformuleerd dat ze maar op één manier geïnterpreteerd kunnen worden. Dit voorkomt begripsverwarring bij de ontwikkelaar / leverancier waardoor mogelijk een internetstemsysteem wordt ontwikkeld dat niet alle gewenste eigenschappen bezit of dat juist ongewenste eigenschappen bezit. Voor een onafhankelijke beoordelaar geldt hetzelfde, ook zijn interpretatie van de eisen mag niet afwijken van dat van de opdrachtgever of de leverancier.

De Common Criteria for Information Technology Security Evaluation (afgekort CC, vastgelegd in ISO/IEC 15408) zijn ontwikkeld als gestandaardiseerd raamwerk voor de evaluatie van computer beveiliging. Met de CC kunnen de gewenste eigenschappen van een specifiek systeem worden gedefinieerd. In de standaard is vastgelegd hoe de eigenschappen / eisen gespecificeerd moeten worden en met welk betrouwbaarheidsniveau de certificatie tegen de eisen plaats moet vinden ('Evaluation Assurance Level'). De eigenschappen worden beschreven in een zgn. Protection Profile (PP). Een PP ondergaat een formele evaluatie door een aangestelde certificatie instantie om te toetsen of het document voldoet aan (onder meer) syntactische eisen. Goedgekeurde PPs worden gepubliceerd op http://www.commoncriteriaportal.org/.

Door de Duitse Bundesamt für Sicherheit in de Informationstechnik is in 2008 een Protection Profile[5] opgesteld voor Online Voting Products conform de Common Criteria versie 3.1 Rev 2. Voor

---

[1] e-Vote 2011 Security Objectives, Ministry of Local Government and Regional Development, Norway

[2] E-voting conception security: analysis and measures. National Electoral Committee Estland, 2010

[3] Rapport van kanton Geneve. http://www.ge.ch/evoting/doc/rapports/RD00639.pdf

[4] "Gi-anforderungen an internetbasierte vereinswahlen", Gesellschaft für Informatik http://www.gi.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf

zover bekend is dit PP de enige die is opgesteld voor internetstemsystemen. Dit PP is opgesteld voor verkiezingen die plaatsvinden binnen verenigingen, besturen, universiteiten en alle andere niet-politieke officiële verkiezingen. Het PP is niet opgesteld met het oog op officiële verkiezingen voor vertegenwoordigende organen. De beveiligingseisen in het PP zijn afgeleid van onder meer de Recommendation van de Raad van Europa.

Het maken van een PP voor een Nederlands internetstemsysteem maakte geen onderdeel uit van de opdracht.

Aanbeveling 01 *In overweging wordt gegeven aan het ministerie van BZK om wel een dergelijk PP op te (laten) stellen als onderdeel van de ontwerpfase van het internetstemsysteem. Mogelijk kan hierbij gebruik gemaakt kan worden van het eerdere werk dat in Duitsland is verricht.*

2.3 Basisniveau beveiliging minimaal gelijk aan briefstemmen

In dit programma van eisen is als uitgangspunt gehanteerd dat het internetstemsysteem een beveiligingsniveau moet hebben dat minimaal gelijk is aan het systeem van briefstemmen. Op een aantal onderdelen wordt een hoger beveiligingsniveau vereist.

2.4 Aanname architectuur internetstemsysteem

Bij het opstellen van dit programma van eisen zijn de volgende aannames gedaan:

- Het internetstemsysteem bestaat minimaal uit de volgende onderdelen:
  - Een stemapplicatie die een kiezer op zijn eigen computer gebruikt.
  - Een website die gebruikt wordt voor voorlichting aan de kiezer en van waar uit de stemapplicatie wordt gedistribueerd.
  - Een stemserver: één of meerdere centraal opgestelde servers voor de authenticatie van de kiezer, voor de ontvangst van de stemmen van de stemapplicatie en voor de opslag van de stemmen in een stembus.
  - Een voorziening voor de leden van het stembureau voor het bedienen van de servers, voor het tellen van de stemmen en het verkrijgen van rapportages.
  - Een voorziening voor generatie en veilige opslag van cryptografische sleutels.
  - Een voorziening voor logging / auditing doeleinden.
- De registratie van kiezers en het vaststellen van de kiesgerechtigdheid vindt plaats buiten het internetstemsysteem.
- Het internetstemsysteem bevat geen register met persoonsgegevens van de kiezer. De persoonsgegevens zijn opgenomen in het registratiesysteem. In het internetstemsysteem wordt de kiezer gerepresenteerd door een geanonimiseerd gegeven (de gegevens worden omgezet naar een vorm die identificatie van de kiezer niet langer mogelijk maakt).

---

[5] "Common Criteria Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte", BSI-CC-PP-0037, version 1.0 18 april 2008. http://www.commoncriteriaportal.org/files/ppfiles/pp0037b.pdf

2.5 Kunnen herroepen van eerder uitgebrachte stem

In dit programma van eisen is als uitgangspunt genomen dat een kiezer meerdere pogingen mag doen om een stem uit te brengen, maar dat slechts één stem wordt meegeteld. Hiermee wordt een maatregel voorzien die het dreigingsscenario van "dwang / beïnvloeding van de kiezer" kan beperken. De kiezer kan een eerder onder dwang uitgebrachte stem herroepen door een nieuw stem uit te brengen. De mogelijkheid om meerdere stempogingen te doen maakt het ook mogelijk voor de kiezer die twijfelt of het internetstemsysteem goed heeft gefunctioneerd 'voor de zekerheid' nogmaals een stem uit te brengen.
Zoals in de risicoanalyse is beschreven biedt de maatregel geen absolute bescherming tegen vergaande vormen van dwang, zeker indien die geperkt gaan met fysieke bedreigingen of belemmeringen.

Deze systematiek is overgenomen van de inrichting van het internetstemproces zoals dat in Noorwegen en Estland wordt toegepast. Ook daar kan de kiezer meerdere keren stemmen via internet, waarbij alleen de laatste stem wordt meegeteld. Dit betekent dat het internetstemsysteem moet beschikken over de functionaliteit om te bepalen welke ontvangen stemmen moeten worden meegeteld. Hiervoor is het nodig dat er wettelijk wordt vastgelegd welke van de ontvangen stem moet worden geteld. Het meest voor de hand liggend is om de laatst ontvangen stem te tellen.

2.6 Terugvaloptie briefstemmen

In het programma van eisen is er voor gekozen om de kiezer de mogelijkheid te geven om pas op het moment van stemmen te bepalen of hij per brief of via internet wil stemmen. Bij eerdere experimenten met Kiezen op Afstand in 2004 en 2006 diende de kiezer reeds bij de registratie aan te geven of hij via internet of per brief wilde stemmen. Dit is opgenomen in de eisen P002 en P003.

Deze keuze maakt het mogelijk om kiezers bij een eventuele (langdurige) uitval van het internetstemsysteem een terugvaloptie aan te bieden: het alsnog per brief uitbrengen van de stem. Ook voorkomt deze werkwijze dat, in de situatie van de voorgenomen invoering van de permanente registratie, de kiezer per verkiezing alsnog moet aangeven op welke wijze hij wil stemmen.

De consequentie van dit uitgangspunt is dat kiezers niet alleen meerdere keren via internet kunnen stemmen (zie vorige paragraaf) maar naast hun internetstem ook een briefstem kunnen uitbrengen. Indien een kiezer zowel via internet als per brief stemt wordt alleen de per brief uitgebrachte stem meegeteld. Een kiezer kan overigens niet meerdere briefstemmen uitbrengen.

Om te voorkomen dat dit leidt tot het meetellen van meerdere stemmen per kiezer (waarborg uniciteit), zal bij de stemopneming van de internetstemmen rekening gehouden moet worden met eventuele per brief uitgebrachte stemmen. De briefstembureaus dienen daartoe door te geven aan het internetstembureau welke kiezers per brief hebben gestemd, opdat in het internetstembureau kan worden bepaald of diezelfde kiezer ook via internet heeft gestemd. De

internetstemmen van die kiezers dienen vervolgens door het internetstembureau ter zijde te worden gelegd bij het tellen van de stemmen.

Deze terugvaloptie betekent dat ook eisen gesteld moeten worden aan de stembescheiden die aan de kiezer worden toegestuurd. Deze moeten geschikt zijn voor zowel internetstemmen als briefstemmen. Het briefstembewijs moet worden voorzien van gegevens waarmee een relatie kan worden gelegd met een kiezer die ook via internet heeft gestemd.

De consequentie van deze terugvaloptie is ook dat er een nieuwe fout-kans ontstaat die mogelijk afbreuk doet aan de waarborg van uniciteit. Indien er geen of een onjuiste relatie wordt gelegd tussen de kiezer die per brief een stem uitbrengt en de stem of stemmen die deze kiezer via internet uitbrengt kan dit leiden tot het ten onrechte meetellen van meerdere stemmen van één en dezelfde kiezer of tot het ten onrechte niet meetellen van een internetstem van een kiezer. Ook creëert het een nieuwe tijdsafhankelijkheid tussen de stemopneming in het briefstembureau en de stemopneming in het internetstembureau.

3 ALGEMENE EISEN EN WAARBORGEN

3.1 Wet- en regelgeving

A001 *Het internetstemsysteem moet voldoen aan de Nederlandse wet- en regelgeving.*

In het bijzonder dient het internetstemsysteem te voldoen aan de Kieswet (en lagere regelgeving zoals het Kiesbesluit en Ministeriële regelingen). Noot: de Kieswetgeving zal aangepast moeten worden om internetstemmen mogelijk te maken.

A002 *Het internetstemsysteem dient te voldoen aan de aanbevelingen van de Raad van Europa ("Council of Europe e-vote Recommendation Rec(2004) 11").*

De aanbevelingen van de Raad van Europa zijn niet vervat in een interstatelijk verdrag. In geval van een tegenstrijdigheid tussen de aanbevelingen prevaleert de Nederlandse wet- en regelgeving en een nog op te stellen programma van eisen boven de aanbevelingen van de Raad van Europa.

3.2 Waarborgen

Het internetstemsysteem moet voldoen aan de volgende waarborgen:

3.2.1 Stemgeheim

W001 *Elke uitgebrachte stem is geheim. Het moet onmogelijk zijn om een verband te leggen tussen de identiteit van de persoon die de stem uitbrengt en de inhoud van de uitgebrachte stem.*

3.2.2 Stemvrijheid

W002 *Iedere kiesgerechtigde moet bij het uitbrengen van zijn of haar stem zijn of haar keuze in alle vrijheid, vrij van beïnvloeding, kunnen bepalen.*

3.2.3 Transparant

W003 *Het verkiezingsproces moet zo zijn ingericht, dat het helder van structuur en opzet is, zodat in beginsel iedereen inzicht in de structuur en werking ervan kan hebben.*

3.2.4 Controleerbaar

W004 *Het verkiezingsproces moet objectief controleerbaar zijn. De controle instrumenten kunnen, afhankelijk van de vorm van stemmen waartoe wordt besloten, verschillen.*

3.2.5 Integriteit

W005 *Het verkiezingsproces moet correct verlopen en de uitkomst mag niet beïnvloedbaar zijn anders dan door het uitbrengen van rechtmatige stemmen.*

3.2.6 Kiesgerechtigdheid

W006 *Alleen kiesgerechtigde personen mogen aan de verkiezing deelnemen. Kiezers dienen hun identiteit aan te tonen alvorens zij toegang krijgen tot de stemming.*

3.2.7 Uniciteit

W007 *Van iedere kiesgerechtigde mag, gegeven het Nederlandse kiesstelsel, niet meer dan één stem worden meegeteld bij de stemopneming.*

3.2.8 Toegankelijkheid

W008 *Kiesgerechtigden moeten zoveel mogelijk in de gelegenheid gesteld worden om direct deel te nemen aan het verkiezingsproces. Indien dat onmogelijk is, moet de mogelijkheid openstaan om indirect – door het verlenen van een volmacht – aan de verkiezing deel te nemen.*

3.2.9 Beschikbaarheid

W009 *Indien in het verkiezingsproces gebruik gemaakt wordt van (technische) voorzieningen dan moeten deze dusdanig beschikbaar zijn dat een tijdelijke verstoring van de voorziening niet betekent dat een kiezer niet meer zijn stem kan uitbrengen. Bij complete uitval dient de kiezer via een andere stemmethode te kunnen stemmen.*

3.2.10 Tijdigheid

W010 *De kiezer wordt tijdig voorzien van middelen om te kunnen stemmen zodat deze zijn stem tijdig kan uitbrengen en de stemmen tijdig kunnen worden geteld. De termijnen moet in wet- en regelgeving worden gedefinieerd.*

4 PROCESEISEN

4.1 Stemming

P001 *Internetstemmen wordt aangeboden aan kiezers als alternatief naast de bestaande stemmethoden.*

Toelichting: De huidige stemmethoden (briefstemmen, stemmen bij volmacht en stemmen via een kiezerspas) blijven bestaan.

P002 *Kiezers kunnen tot op het moment van stemmen bepalen of zij per brief of via internet willen stemmen.*

P003 *Indien een kiezer zowel via internet als per brief stemt wordt alleen de per brief uitgebrachte stem meegeteld.*

Toelichting: Dit maakt het mogelijk om bij eventuele (langdurige) uitval van het internetstemsysteem alsnog een stem per brief uit te brengen. Deze eis heeft als consequentie dat kiezers niet alleen meerdere keren via internet kunnen stemmen (zie ook eis F014) maar naast hun internetstem ook een briefstem kunnen uitbrengen. Om te voorkomen dat dit leidt tot het meetellen van meerdere stemmen per kiezer (waarborg uniciteit), zal bij de stemopneming van de internetstemmen rekening gehouden moet worden met eventuele per brief uitgebrachte stemmen. Zie hiervoor ook de eerdere toelichting in hoofdstuk 2.

P004 *Gedurende de stemperiode is het internetstemsysteem 18 uur per dag toegankelijk tussen 0:600u en 0:00 uur Nederlandse tijd.*

Toelichting: De doelgroep kiezers in het buitenland woont verspreid over de hele wereld. Een deel van de doelgroep leeft daardoor in andere tijdzones dan het stembureau. De 18-uurs openstelling is zo gekozen dat kiezers uit alle tijdzones gedurende minimaal 9 (niet aaneengesloten) uren kunnen stemmen tussen 08:00 en 23:00 uur lokale tijd. Er is niet gekozen voor een 24-uurs opening om de personele belasting van het stembureau te verminderen en dagelijks de mogelijkheid te scheppen om onderhoud te plegen op het internetstemsysteem. Uit eerdere ervaringen in de Kiezen op Afstand projecten en uit andere landen blijkt overigens dat het aantal stemmen dat ’s nachts wordt uitgebracht zeer gering is.

P005 *Internetstemmen vindt plaats gedurende een stemperiode van minimaal 5 en maximaal 10 kalenderdagen.*

Toelichting: Uit eerdere ervaringen is gebleken dat het wenselijk is dat de kiezer in het buitenland gedurende meerdere dagen de gelegenheid heeft om een stem uit te kunnen brengen.

De daadwerkelijke lengte van de stemperiode kan later worden vastgesteld. Het aantal verwachte stemmen kan daarbij een factor zijn, om te grote piekbelasting van het internetstemsysteem te voorkomen. Een periode langer dan 10 dagen wordt afgeraden, gelet op de implicaties voor het aantal benodigde medewerkers en stembureauleden.

P006 *De stemperiode eindigt uiterlijk 7 kalenderdagen voor de dag van stemming.*

Toelichting: Mocht het zo zijn dat het internetstemsysteem onbeschikbaar of onbruikbaar is door een force majeur, een DDoS aanval of een technisch gebrek, dan hebben de kiezers alsnog minimaal 7 dagen de tijd om een stem per brief uit te brengen.

5 FUNCTIONELE EISEN

5.1 Algemeen

F001 *Het internetstemsysteem moet over een configuratiefunctie beschikken waarmee het internetstemsysteem voor een specifieke verkiezing kan worden ingesteld.*

Toelichting: Het internetstemsysteem moet zonder wijzigingen in de programmatuur bruikbaar zijn voor meerdere (soorten) verkiezingen. Hiertoe is een configuratiefunctie vereist zodat het internetstemsysteem instelbaar is per verkiezing.

F002 *Het internetstemsysteem dient een overzicht van kandidaten te kunnen inlezen op basis van een EML_NL bericht.*

Toelichting: De politieke partijen sturen de persoonsgegevens van de kandidaten op hun lijsten aan het centraal stembureau in een elektronisch bericht of bestand dat voldoet aan de EML_NL standaard. Hiertoe heeft de Kiesraad een programma Ondersteunende Software Verkiezingen [6] beschikbaar gesteld. Het is vereist dat het internetstemsysteem de gegevens van de kandidaten direct kan inlezen, zodat geen handmatig invoer vereist is. EML_NL is de open standaard voor de uitwisseling van gegevens tussen systemen die gebruikt worden bij formele verkiezingen. De EML_NL standaard is afgeleid van de internationale Election Markup Language en is opgenomen op de “Pas toe of leg uit” lijst van het Bureau Forum Standaardisatie.

F003 *Het internetstemsysteem moet geschikt zijn voor verkiezingen voor de leden van de Tweede Kamer en de verkiezingen voor de leden van het Europees Parlement.*

Toelichting: Kiezers in het buitenland mogen op grond van de Nederlandse Kieswet meedoen aan deze twee verkiezingen.

5.2 Kiezer

F004 *Het internetstemsysteem kent een intuïtieve gebruikersinterface, die specifiek ontworpen is voor de taak om een stem uit te brengen. Op de schermen is geen enkele andere informatie weergegeven dan noodzakelijk voor het uitbrengen van een stem. De gebruikersinterface toont de kiezer steeds in welke stap van het stemproces hij zich bevindt.*

[6] De Ondersteunende Software Verkiezingen (OSV) is programmatuur die in opdracht van de Kiesraad is ontwikkeld en die gebruikt wordt voor de kandidaatstelling en de berekening en vaststelling van de uitslag.

Toelichting: De kiezer moet beschouwd worden als onervaren met stemmen via internet. De gebruikersinterface dient dusdanig ontworpen te zijn dat het overgrote merendeel van de kiezers direct, zonder het doornemen van een handleiding, begrijpt wat van hem verwacht wordt en weet welke stappen in het stemproces hij reeds heeft doorlopen en welke stappen hij nog moet doorlopen. Een intuïtieve gebruikersinterface draagt bij aan het vertrouwen van de kiezer en daarmee aan de waarborg transparantie.

F005 *Het internetstemsysteem toont de lijsten en kandidaten op een wijze die bepaald wordt door wet- en regelgeving.*

Toelichting: De wijze waarop lijsten en kandidaten op het scherm worden getoond moet tijdens de ontwerpfase nader worden vastgesteld. In Nederland moeten 80 kandidaten per partij getoond kunnen worden, waarbij scrollen, swipen of onderverdeling in meerdere pagina's noodzakelijk is.

F006 *De kiezer bedient het internetstemsysteem met een stemapplicatie op zijn eigen computer. De stemapplicatie voorziet minimaal in de volgende functies:*
- tonen overzicht van kandidaten waaruit kan worden gekozen;
- mogelijkheid tot selectie van kandidaat;
- inzien van gemaakte keuze alvorens definitief uitbrengen van stem;
- definitief uitbrengen van stem.

F007 *Het internetstemsysteem biedt de kiezer de mogelijkheid om blanco te stemmen, hiertoe wordt naast de keuzemogelijkheid voor kandidaten ook een keuzemogelijkheid voor blanco geboden.*

Toelichting: De Nederlandse Kieswet (art. N7, T8 Kw) staat het kiezers toe om te stemmen zonder op een specifieke kandidaat te stemmen. Het aantal blanco stemmen wordt ook op het proces-verbaal vermeld.

F008 *Alle lijsten en kandidaten worden op een identieke en neutrale manier gepresenteerd. Iedere kiezer krijgt in het keuzeproces een zoveel mogelijk gelijke opmaak van de schermen.*

Toelichting: Doordat kiezers niet beschikken over een identieke computerconfiguratie (verschillende hardware, operating systemen, browsers, etc.) moet er rekening mee worden gehouden dat er verschillen kunnen optreden in de gebruikersinterface en presentatie (schermformaat, vormgeving, kleur etc.) van de stemapplicatie. Desondanks moet het internetstemsysteem zo ontworpen worden dat dit niet mag leiden tot een ongewenste beïnvloeding van de wijze waarop de kiezer een keuze maakt of zijn stem uitbrengt. Bevoordeling van één of meerdere specifieke lijsten of kandidaten moet worden voorkomen.

F009 *Om een definitieve keuze te maken, moet een kiezer zijn stem expliciet bevestigen.*

Toelichting: De kiezer moet zijn keuze van kandidaat expliciet bevestigen alvorens deze keuze als stem wordt uitgebracht. Hiermee kan worden voorkomen dat de kiezer abusievelijk op een andere kandidaat een stem uitbrengt dan zijn intentie is.

F010 *Tot het moment van de bevestiging mag de kiezer zijn stem nog wijzigen of het stemproces afbreken. Het internetstemsysteem wordt niet geacht de voorlopige, niet-bevestigde, keuze te onthouden en bij een volgende poging weer te tonen.*

Toelichting: De kiezer moet op elk moment in het stemproces zijn keuze kunnen aanpassen tot aan het moment dat hij zijn keuze expliciet als stem deponeert. Het is vanuit de waarborg van het stemgeheim niet gewenst dat het internetstemsysteem tussentijdse keuzes opslaat; bij een hervatting of nieuwe stempoging dient de kiezer 'van voren af aan' te beginnen.

F011 *Het internetstemsysteem moet duidelijk aangeven dat met succes een stem is uitgebracht en dat daarmee de procedure voor de kiezer is voltooid.*

Toelichting: De kiezer moet een bevestiging ontvangen dat de stem daadwerkelijk is ontvangen door het internetstemsysteem, zodat de kiezer in geval de stem niet is ontvangen een nieuwe poging kan doen om zijn stem uit te brengen.

F012 *Het moet onmogelijk zijn om een verband te leggen tussen de identiteit van een kiezer en de inhoud van zijn stem.*

Toelichting: Deze eis ziet toe op het grondwettelijk vereiste dat de stemming een geheim karakter dient te hebben.

F013 *Een kiezer mag geen (overdraagbaar) bewijs van de inhoud van zijn stem krijgen van het internetstemsysteem.*

Toelichting: Met een (overdraagbaar) bewijs van de inhoud van de stem zou de kiezer aan een derde kunnen aantonen wat hij heeft gestemd. Dit is wettelijk niet toegestaan.

F014 *Een kiezer kan meerdere stemmen uitbrengen, en daarmee zijn eerdere keuze herroepen. Van elke kiezer wordt slechts één stem meegeteld, dat is de laatste stem die is ontvangen.*

Toelichting: zie paragraaf 2.5. De regels omtrent de stemopneming zullen tevens in de wet- en regelgeving moeten worden vastgelegd.

F015 *Een kiezer krijgt geen bericht over de inhoud van eerdere uitgebrachte stemmen.*

Toelichting: Het is toegestaan dat het internetstemsysteem aan de kiezer meldt dat hij al eerder een stem heeft uitgebracht, maar over de inhoud van die stem mag niet worden bericht om doorbreken van het stemgeheim te voorkomen.

5.3 Stemserver / Stembureau

F016 *Het internetstemsysteem moet het stembureau en/of waarnemers de mogelijkheid geven voorafgaand aan de opening van de stemming de configuratie van de verkiezing te controleren.*

Toelichting: Het stembureau moet kunnen vaststellen dat het internetstemsysteem correct is ingesteld voor de betreffende verkiezing. Hierbij kan gedacht worden aan de juiste datum en omschrijving van de verkiezing, juiste kandidaten, cryptografische sleutels, et cetera.

F017 *Het internetstemsysteem moet het stembureau en/of waarnemers de mogelijkheid geven voorafgaand aan de opening van de stemming te controleren dat er geen stemmen in de stembus opgeslagen zijn.*

Toelichting: Door het stembureau en / of waarnemers moet kunnen worden vastgesteld dat de stembus bij aanvang van de stemming leeg is.

F018 *Het internetstemsysteem moet het stembureau de mogelijkheid geven de stemming te openen. Vanaf het moment van openen kunnen kiezers een stem uitbrengen. Het aanroepen van deze functie kent een verzwaarde autorisatieprocedure.*

Toelichting: Om te voorkomen dat één van de leden van het stembureau onbewust of bewust de stemming eerder opent is een verzwaarde autorisatieprocedure van kracht waardoor deze functionaliteit alleen kan worden aangeroepen indien twee stembureauleden hiertoe opdracht geven.

F019 *Het internetstemsysteem moet het stembureau de mogelijkheid geven om de stemming tijdelijk te onderbreken (schorsen). Gedurende de schorsing kunnen kiezers geen stem uitbrengen en worden geen nieuwe stemmen in de stembus opgeslagen. Kiezers die bezig waren met het uitbrengen van een stem krijgen een melding dat de stemming geschorst is. Eventuele stemmen die reeds zijn uitgebracht door een kiezer, maar nog niet zijn opgeslagen in de stembus worden geweigerd. Deze kiezers dienen hiervan een bericht te krijgen zodat zij weten dat ze nog niet hebben gestemd. Het aanroepen van deze functie kent een verzwaarde autorisatieprocedure.*

Toelichting: Het moet mogelijk zijn voor het stembureau om de stemming te onderbreken ('schorsen'), bijvoorbeeld in een situatie dat er een vermoeden is dat de stemdienst niet correct functioneert, of omdat er sprake is van een ordeverstoring o.i.d. Dit geeft het stembureau de mogelijkheid om onderzoek te (laten) doen en eventueel (herstel)maatregelen te treffen. Ook kan het stembureau besluiten om de reeds uitgebrachte stemmen veilig te stellen.

In functionele zin betekent schorsing dat het internetstemsysteem geen stem meer mag opslaan in de stembus (en dus ook geen bewijs van correcte ontvangst mag afgeven). Een bericht van de schorsing zal zowel op de website van het internetstembureau getoond worden, als via de stemapplicatie van de kiezer. Om te voorkomen dat één van de leden van het stembureau onbewust of bewust de stemming schorst is een verzwaarde autorisatieprocedure van kracht waardoor deze functionaliteit alleen kan worden aangeroepen indien twee stembureauleden hiertoe opdracht geven.

F020 *Het internetstemsysteem moet het stembureau de mogelijkheid geven om de stemming weer te hervatten na een schorsing. Het aanroepen van deze functie kent een verzwaarde autorisatieprocedure.*

Toelichting: Na een schorsing kan het stembureau besluiten de stemming weer te hervatten. Het internetstemsysteem biedt hiertoe deze functionaliteit. Vanaf dat moment accepteert het internetstemsysteem weer de opslag van stemmen in de stembus. Via de website en de stemapplicatie van de kiezer worden de kiezers geïnformeerd over de status van de stemming.

Om te voorkomen dat één van de leden van het stembureau onbewust of bewust de stemming schorst is een verzwaarde autorisatieprocedure van kracht waardoor deze functionaliteit alleen kan worden aangeroepen indien twee stembureauleden hiertoe opdracht geven.

F021 *Het internetstemsysteem moet het stembureau de mogelijkheid geven de stemming te sluiten. Het aanroepen van deze functie kent een verzwaarde autorisatieprocedure en een dubbele bevestigingsfunctie om abusievelijk sluiten te voorkomen.*

F022 *Een gesloten stemming kan niet worden heropend.*

F023 *Na sluiting van de stemming kunnen nieuwe kiezers zich niet meer aanmelden en kunnen geen stemmen meer worden uitgebracht. Kiezers die bezig waren met het uitbrengen van een stem krijgen een melding dat de stemming gesloten is. Eventuele stemmen die reeds zijn uitgebracht door een kiezer, maar nog niet zijn opgeslagen in de stembus worden geweigerd. Deze kiezers dienen hiervan een bericht te krijgen zodat zij weten dat ze nog niet hebben gestemd.*

Toelichting: Direct na het sluiten van de stemming mag het internetstemsysteem geen nieuwe stemmen accepteren.

Om te voorkomen dat één van de leden van het stembureau onbewust of bewust de stemming sluit is een verzwaarde autorisatieprocedure van kracht waardoor deze functionaliteit alleen kan worden aangeroepen indien twee stembureauleden hiertoe opdracht geven. Omdat deze functie onherroepelijk is moet het internetstemsysteem om een bevestiging te vragen van het aanroepen van deze functie.

F024 *De functionaliteit tot openen, schorsen, hervatten en sluiten is exclusief voorbehouden aan het stembureau.*

Toelichting: Het is de exclusieve bevoegdheid van het stembureau om te bepalen of en wanneer een stemming wordt geopend, geschorst, hervat of gesloten.

F025 *Het internetstemsysteem dient gedurende de periode dat het operationeel is actuele informatie verstrekken aan het stembureau over het functioneren van het internetstemsysteem.*

Toelichting: Het stembureau dient inzicht te kunnen krijgen in het (correct) functioneren van het internetstemsysteem, om op grond daarvan eventueel te kunnen besluiten tot het schorsen of sluiten van de stemming. Welke informatie dit betreft dient in een later ontwerpstadium te worden bepaald.

F026 *Het tellen van de uitgebrachte stemmen mag alleen indien de stemming gesloten is.*

Toelichting: Het is (wettelijk) niet toegestaan om tijdens de stemming een telling van de reeds uitgebrachte stemmen uit te voeren.

F027 *Het internetstemsysteem genereert de wettelijk voorgeschreven verantwoordingsinformatie, onder andere ten behoeve van het proces-verbaal van het internetstembureau.*

5.4 Onafhankelijk toezicht en waarnemers

F028 *Het internetstemsysteem dient te beschikken over een log-functionaliteit die het voor een onafhankelijke auditors en / of waarnemers mogelijk maakt om gedurende de stemming én na afloop van de stemming het correcte functioneren van het internetstemsysteem te kunnen vaststellen.*

F029 *In de log-functionaliteit mogen geen gegevens worden bewaard die, op zichzelf of in combinatie met andere gegevens binnen het internetstemsysteem, kunnen leiden tot het doorbreken van het stemgeheim.*

Toelichting: Het is gewenst dat het correct functioneren van het internetstemsysteem niet alleen voorafgaand aan de verkiezing wordt vastgesteld in een uitgebreid test- en certificatietraject, maar ook feitelijk wordt vastgesteld ten tijde van de verkiezing. Om dit te kunnen doen is een log-functionaliteit vereist waarmee de werking van het internetstemsysteem kan worden geanalyseerd. Tegelijkertijd moet voorkomen worden dat er met behulp van de gegevens uit de log-functionaliteit een relatie gelegd kan worden tussen de inhoud van de stem en naar een individuele kiezer herleidbare (persoons)gegevens.

F030 *De log-functionaliteit is gescheiden van, en niet te beïnvloeden door, de rest van het internetstemsysteem en is beschermd tegen wijziging en verwijdering van gegevens.*

Toelichting: Door scheiding van de log-functionaliteit van de rest van het internetstemsysteem kan worden voorkomen dat een technisch gebrek in het internetstemsysteem leidt tot het uitvallen of niet correct functioneren van de log-functionaliteit. De log-functionaliteit is immers bedoeld om faalsituaties en gebreken in het internetstemsysteem vast te stellen. De log-functionaliteit moet beschermd zijn tegen wijziging of verwijdering van gegevens om te voorkomen dat sporen van niet toegestane handelingen worden gewist.

6 TECHNISCHE EISEN

6.1 Stemapplicatie

T001 *De kiezer stemt met een stemapplicatie die geschikt is voor algemeen gangbare computer systemen.*

Toelichting: De eis dat de stemapplicatie moet functioneren op algemeen gangbare computer operating systemen is ingegeven vanuit de wens om een zo groot mogelijke groep kiezers toegang te geven tot het stemmen via internet. Tegelijkertijd is het onhaalbaar en vanuit het oogpunt van kosten en beheersbaarheid ook ongewenst om alle mogelijke computerconfiguraties (hardware platformen, operating systemen et cetera) te ondersteunen.
Per verkiezing zal moeten worden vastgesteld of voor welke computer systemen en operating systemen de stemapplicatie geschikt moet zijn. Hieronder worden zowel personal computers verstaan als mobiele devices zoals tablets en smartphones.

T002 *De stemapplicatie moet verkrijgbaar zijn vanaf een website van de overheid of een gecertificeerde app store die is toegerust op het verwerken van grote aantallen gelijktijdige downloads.*

Toelichting: Het is gewenst dat het downloaden van de stemapplicatie vlot verloopt. Aan de downloadtijd kunnen in dit stadium nog geen nadere eisen worden gesteld aangezien dit (o.a.) afhangt van de omvang van de applicatie, de distributiewijze en het verwachte aantal kiezers. De downloadsnelheid wordt verder in de praktijk beïnvloed door de snelheid van de internetverbinding van de kiezer.

T003 *Het installeren van de applicatie moet kunnen geschieden zonder dat de kiezer over speciale rechten of programmatuur moet beschikken.*

T004 *De applicatie werkt zoveel als mogelijk “stand-alone”, de afhankelijkheid van de aanwezigheid van andere programma’s wordt zoveel mogelijk beperkt, met uitzondering van het operating system en eventueel een internet browser.*

Toelichting: Het functioneren van de stemapplicatie moet zo min mogelijk afhankelijk zijn van de aanwezigheid van andere programmatuur, enerzijds om te voorkomen dat de kiezer naast de stemapplicatie ook andere programmatuur moet aanschaffen of downloaden, anderszijds om zoveel mogelijk te waarborgen dat de correcte werking van de stemapplicatie niet wordt beïnvloed door andere programmatuur (of malware).

T005 *De stemapplicatie van het internetstemsysteem dient zoveel mogelijk te voldoen aan de eisen van het Web Accessibility Initiative*[7]*. Het WAI streeft toegankelijkheid voor gehandicapten na.*

Toelichting: In het ontwerp van de stemapplicatie moet zoveel mogelijk rekening worden gehouden met mogelijke lichamelijke beperkingen (zoals bijvoorbeeld kleurenblindheid, een motorische handicap of anders) van kiezers.

6.2 Stemserver

T006 *De toegang tot het internetstemsysteem voor de kiezer dient te voldoen aan een beschikbaarheidseis van 99,8% gedurende de stemperiode. Dit betekent een maximale aaneengesloten periode van onbeschikbaarheid als gevolg van technisch falen of gebreken van het internetstemsysteem van (afgerond) 15 tot 30 minuten bij respectievelijk een 5 daagse of 10 daagse stemperiode.*

T007 *Het internetstemsysteem dient binnen 1 uur na sluiting van de stemming door het stembureau de stemmen verwerkt en geteld te hebben.*

T008 *Het internetstemsysteem maakt gebruik van de EML-NL standaard voor berichtuitwisseling.*

Toelichting: EML_NL is de open standaard voor de uitwisseling van gegevens tussen systemen die gebruikt worden bij formele verkiezingen. De EML_NL standaard is afgeleid van de internationale Election Markup Language en is opgenomen op de “Pas toe of leg uit” lijst van het Bureau Forum Standaardisatie.

[7] De richtlijnen zijn te vinden op www.w3.org/WAI

7 BEVEILIGINGSEISEN

7.1 Stemapplicatie

B001 *De kiezer moet de integriteit en authenticiteit van zowel de website of appstore waar hij de stemapplicatie downloadt als van de stemapplicatie kunnen controleren.*

Toelichting: De kiezer moet kunnen vaststellen dat hij de authentieke stemapplicatie van het ministerie van BZK downloadt en niet een gemanipuleerde of gehackte stemapplicatie.

B002 *Het internetstemsysteem moet kiezers de mogelijkheid geven om te controleren dat zij met het authentieke internetstemsysteem verbinding hebben.*

Toelichting: De kiezer moet kunnen vaststellen dat hij de authentieke website van het ministerie van BZK verbinding heeft en niet met een nep-website.

B003 *Het internetstemsysteem dient voorzien te zijn van een systematiek waarmee de integriteit van het overzicht van kandidaten kan worden vastgesteld.*

Toelichting: De kiezer moet kunnen vaststellen dat de kandidaten waaruit hij kan kiezen in de stemapplicatie overeenkomt met de officiële lijst van kandidaten, bijvoorbeeld doordat er een hashwaarde (controlegetal) kan worden gecontroleerd.
Dit kan ook worden bewerkstelligd met een niet-technische maatregel door een overzicht van kandidaten er post of e-mail toe te sturen aan de kiezer of deze te publiceren op de website.

B004 *De stemapplicatie moet voorzien zijn van maatregelen tegen het afluisteren, onderscheppen, wijzigen, verwijderen en/of anderszins manipuleren van de communicatie tussen de stemapplicatie op de computer van de kiezer en de stemserver. Onder de communicatie wordt verstaan alle identificerende gegevens, authenticatiegegevens, eventuele sessie data, cryptografische sleutels, de stem et cetera.*

Toelichting: De stemapplicatie moet dusdanig worden ontworpen en communiceren met de stemserver dat genoemde dreigingen zoveel mogelijk worden uitgesloten. Ook de communicatie tussen kiezer en stemapplicatie moet beveiligd worden, tegen bijvoorbeeld keylogging malware die toetsenbordaanslagen registreert en zo probeert om gegevens van de kiezer (zoals zijn inlog- / authenticatiegegevens of zijn stemkeuze) te verkrijgen. Hiertoe kan gedacht worden aan maatregelen als een virtueel toetsenbord op het scherm binnen de stemapplicatie waarmee de kiezer zijn gegevens kan invoeren.

B005 *Bij het toepassen van cryptografische technieken worden alle gangbare voorzorgsmaatregelen toegepast zoals goed ingericht sleutelbeheer en het gebruik van minimale sleutellengten en*

versleutelingstechnieken / algoritmen die in overeenstemming zijn met de actuele stand van de techniek.

Toelichting: De keuze voor een encryptie of hashing algoritme is onderdeel van het technisch ontwerp. In generieke zin wordt hier als eis gesteld dat gekozen wordt voor cryptografische technieken en implementaties daarvan (b.v. sleutellengte) die in de markt als veilig worden beschouwd.

B006 *Kiezers moeten de mogelijkheid hebben om te controleren dat de uitgebrachte stem ook daadwerkelijk is opgeslagen in de officiële stembus. Deze controle dient plaats te kunnen vinden via een controlegegeven of controlemechanisme dat gebruik maakt van een ander kanaal dan de computer van de kiezer.*

Toelichting: De kiezer moet kunnen vaststellen dat zijn stem is ontvangen en opgeslagen in de officiële stembus zonder daarbij afhankelijk te zijn van de stemapplicatie. Deze kan immers gemanipuleerd zijn. Hiertoe verstrekt het internetstemsysteem een ontvangstbevestiging aan de kiezer. Om een man-in-the-middle aanval tegen te gaan dient in de controlemethodiek gebruik gemaakt te worden van een ander kanaal dan de computer waarmee de kiezer stemt. Dit kan bijvoorbeeld een gepersonaliseerde controlecode zijn die op reeds stond op de toegestuurde stembescheiden, of het toesturen van de ontvangstbevestiging via een e-mail of SMS bericht.

B007 *Het internetstemsysteem biedt geen functionaliteit aan kiezers om te controleren of hun stem correct is meegeteld.*

Toelichting: Alhoewel er in de wetenschappelijke wereld geavanceerde cryptografische mogelijkheden zijn uitgedacht om het mogelijk te maken dat een kiezer kan controleren dat zijn stem correct is meegeteld (conform zijn intentie) zonder dat daarbij het stemgeheim wordt doorbroken, is er voor gekozen deze functionaliteit niet toe te staan. Dit om geen andere waarborgen en eigenschappen te introduceren in vergelijking tot het briefstemsysteem en om te voorkomen dat de complexiteit van de stemdienst sterk toeneemt (cryptografische protocol, additionele maatregelen om het cryptografische protocol en de bij behorende voorzieningen en procedures te beveiligen.

7.2 Stemserver

B008 *De programmatuur van de modules aan de serverzijde van het internetstemsysteem bevatten alleen die functies die strikt noodzakelijk zijn voor de taak.*

Toelichting: De programmatuur van de stemserver alsook het gebruikte operating systeem moet worden ontdaan van functionaliteit die niet wordt gebruikt in de verkiezingstaak van de stemserver, om zo het risico uit te sluiten dat deze ongebruikte functionaliteit misbruikt wordt door hackers of kan leiden tot onvoorziene gebreken of foutsituaties.

B009 *Het internetstemsysteem dient de eigen toestand en beschikbare statusinformatie zelf constant te analyseren om aanvallen en andere problemen te detecteren. In het geval van problemen dient het systeem het stembureau en de beheerders te alarmeren.*

Toelichting: De programmatuur van de stemserver moet zo worden ontworpen dat deze weerbaar is tegen (on)voorziene foutsituaties en aanvallen van hackers. In dergelijke situaties moet direct het stembureau en beheerders worden gealarmeerd.

B010 *Het internetstemsysteem moet voorzien in de mogelijkheid om per object (modules, databestanden, functies, invoervelden etc.) in het systeem verschillende soorten rechten (zoals lees, schrijf, wijzig, etc.) te kunnen instellen.*

B011 *Het internetstemsysteem moet voorzien in de mogelijkheid om deze rechten te groeperen in rollen en in de mogelijkheid om rollen toe te kennen aan specifieke gebruikers.*

B012 *Het internetstemsysteem moet voorzien in maatregelen om de logische toegang tot het systeem en tot objecten per rol en per gebruiker te regelen.*

Toelichting: De eisen B010 tot en met B012 zijn opgesteld om het mogelijk te maken dat in het internetstemsysteem rechten op een fijnmazige manier kunnen worden toebedeeld aan specifieke personen in specifieke rollen.

B013 *Het internetstemsysteem moet ontworpen zijn volgens de richtlijnen van secure software development.*

Toelichting: De exacte richtlijn moet in een later stadium worden vastgesteld. Relevante richtlijnen zijn de ISO/IEC 27034-1 richtlijn voor Secure Software Development, de 'secure programming' richtlijnen voor webapplicaties (www.owasp.org) en de aanbevelingen voor Secure Software Development van het Centrum voor Informatiebeveiliging en Privacybescherming (www.cip-overheid.nl).

B014 *De stemserver van het internetstemsysteem dient voorzien te zijn van maatregelen tegen het afluisteren, onderscheppen, wijzigen, verwijderen en/of anderszins manipuleren van de communicatie tussen internetstemsysteem en de stemapplicatie op de computer van de kiezer. Onder de communicatie wordt verstaan alle identificerende gegevens, authenticatiegegevens, eventuele sessie data, cryptografische sleutels, de stem et cetera.*

Toelichting: De stemserver moet dusdanig worden ontworpen en communiceren met de stemapplicatie van de kiezer dat genoemde dreigingen zoveel mogelijk worden uitgesloten. Hierbij wordt minimaal gedacht aan de toepassing van SSL/TLS v 1.2.

B015 *Het internetstemsysteem is voorzien van maatregelen om cyberaanvallen zoals hacking, manipulatie, defacing en DDoS aanvallen te detecteren en te mitigeren.*

Toelichting: Een van de grootste risico's van een internetstemsysteem is dat de stemserver wordt aangevallen. Het internetstemsysteem moet worden ontworpen vanuit een defensief principe waarbij beveiliging centraal staat. In een later ontwerpstadium dienen alle beveiligingsmaatregelen gedefinieerd te worden.

B016 *De gebruikte authenticatiemiddelen voor toegang tot server modules van het internetstemsysteem dienen aan Stork level QAA4 te voldoen.*

Toelichting: De (logische) toegang tot de server modules moet dusdanig zijn ingericht dat alleen geautoriseerde personen toegang mogen verkrijgen. De methode van authenticatie dient te voldoen aan een zeer hoog betrouwbaarheidsniveau (zie voor een toelichting op Stork betrouwbaarheidsniveau QAA4 verderop paragraaf 8.3).

B017 *Het internetstemsysteem moet dusdanig zijn ontworpen dat er, vanaf het moment dat de stemmen ontsleuteld worden, geen relatie gelegd kan worden tussen de inhoud van de stem en gegevens die de identiteit van de kiezer kunnen duiden. Gegevens die indirect kunnen leiden naar de identiteit van een kiezer, zoals IP adressen, logfiles, tijdstempel, volgordelijkheid etc. moeten voorafgaand aan de telling gewist worden.*

Toelichting: Volgend uit eis F014 moet het internetstemsysteem kunnen bepalen welke ontvangen stemmen toebehoren aan dezelfde kiezer. Hiertoe zullen de stemmen voorzien zijn van identificerende gegevens (bijvoorbeeld een digitale handtekening, een unieke code etc.) die het mogelijk maken om een relatie te leggen tussen de versleutelde stem met een kiezer. Noot: de identificerende gegevens mogen geen persoonsgegevens zijn. Zolang de stemmen versleuteld zijn is het stemgeheim gewaarborgd. Alvorens de stemmen ontsleuteld en daarna geteld worden moeten de stemmen worden ontdaan van deze identificerende gegevens.

B018 *Het internetstemsysteem moet beschermd zijn tegen insider attacks, door toegang tot gevoelige onderdelen voorafgaand aan de stemming alleen toe te staan volgens een goedgekeurd autorisatieprotocol vanuit het ministerie van BZK. Toegang en werkzaamheden dienen plaats te vinden onder toezicht van minimaal 1 andere persoon.*

B019 *Het internetstemsysteem moet beschermd zijn tegen insider attacks, door toegang tot gevoelige onderdelen tijdens de stemming alleen toe te staan na goedkeuring door het stembureau en onder toezicht van minimaal 1 andere persoon.*

B020 *Het mag niet mogelijk zijn om de in het internetstemsysteem opgeslagen stemmen te wijzigen of te verwijderen danwel om stemmen toe te voegen. Pogingen daartoe moeten worden gedetecteerd en worden gemeld aan het stembureau.*

Toelichting: Het internetstemsysteem moet voorzien zijn van maatregelen om de integriteit van de stembus te waarborgen.

B021 *De toegang tot het internetstemsysteem voor kiezer is gescheiden van de toegang voor het stembureau en beheerders.*

B022 *De toegang tot het internetstemsysteem voor het stembureau loopt niet via het internet of een ander publiek netwerk.*

Toelichting: Door de toegang tot het internetstemsysteem voor het stembureau te scheiden van de toegang door kiezers én deze via een niet-publiek netwerk te laten verlopen wordt voorkomen dat bij een DDoS aanval het internetstemsysteem ook voor het stembureau onbeschikbaar wordt.

B023 *Sleutelgeneratie wordt uitgevoerd in apart proces en apart systeem voorafgaand aan de opening van de stemming.*

Toelichting: De generatie van de cryptografische sleutels die gebruikt worden in het internetstemsysteem wordt uitgevoerd voorafgaand aan de opening van de stemming.

B024 *De cryptografische sleutels worden beschermd door deze op te delen (threshold encryptie) en onder te brengen bij verschillende functionarissen / organisaties*

Toelichting: De toepassing van threshold-encryptie maakt het mogelijk om de toegang tot de cryptografische sleutels (bijvoorbeeld de sleutel die nodig is voor de ontsleuteling van de stemmen) zo te regelen dat er meerdere partijen samen moeten werken, maar dat niet alle partijen nodig zijn om toegang te krijgen tot de sleutel. Het minimaal aantal vereiste partijen wordt de threshold genoemd. Door deze threshold systematiek kan de sleutel bijvoorbeeld verdeeld worden over 7 personen, waarvan er minimaal 5 sleuteldelen moeten worden samengebracht om een volledige sleutel te krijgen.

B025 *Cryptografische sleutels worden opgeslagen in een Hardware Security Module (HSM) die voldoet aan FIPS 140-2 level 3 niveau of beter.*

Toelichting: Het gebruik van een HSM is vereiste om de cryptografische sleutels veilig op te slaan. De FIPS 140-2[8] standaard definieert aan welke eisen een HSM moet voldoen gegeven een bepaald betrouwbaarheidsniveau (level). Voor deze toepassing is level 3 vereist.

[8] FIPS 140-2 is een internationale standaard die opgesteld is door het Amerikaanse National Institute for Standards and Technology. Zie ook http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

B026 *Het internetstemsysteem kan, na opening van de stemming, niet worden teruggebracht naar de oorspronkelijke status zoals die was voorafgaand aan de opening van de stemming. Een herstart mag niet leiden tot het wissen van de reeds uitgebrachte stemmen.*

Toelichting: Deze eis ziet er op toe dat het internetstemsysteem zo ontworpen en geïmplementeerd wordt dat voorkomen wordt dat, bewust of onbewust, gedurende de stemming het internetstemsysteem gereset kan worden waardoor alle uitgebrachte stemmen gewist worden.

B027 *Medewerkers met een vertrouwensfunctie worden voorafgaand gescreend. Voor medewerkers van externe leveranciers geldt dat deze alleen een arbeidscontract aangeboden mag zijn als de medewerker met positief gevolg een screening c.q. een antecedentenonderzoek heeft ondergaan waaruit is gebleken dat betrokkene geen strafblad heeft. Voor zover medewerkers die woonachtig zijn in een ander land dan Nederland niet aan een onderzoek onderworpen kan worden dat gericht is op hetzelfde resultaat, zal genoegen worden genomen met een onderzoek dat de bedoelde screening c.q. het antecedentenonderzoek zoveel mogelijk benadert.*

Toelichting: In een later stadium moet bepaald worden welke functies geclassificeerd worden als vertrouwensfuncties. Doel van de screening is om te onderzoeken of deze medewerkers eerder strafbare feiten hebben gepleegd, of ze vatbaar zijn voor chantage of anderszins ongeschikt zijn voor de taak. Voor medewerkers van buitenlandse leveranciers kunnen niet automatisch de Nederlandse screeningsregels van toepassing worden verklaard, vandaar dat in de laatste zin van de eis wordt gespecificeerd dat een alternatief vergelijkbaar onderzoek acceptabel is.

7.3 Beheer

B028 *Functioneel of applicatiebeheer van het internetstemsysteem is tijdens een verkiezing alleen toegestaan na instemming van het stembureau en uitvoering onder toezicht. Elke wijziging dient een formele procedure te doorlopen.*

Toelichting: Het is ongewenst dat tijdens de stemming beheerwerkzaamheden plaatsvinden op het internetstemsysteem. Er kan zich echter een situatie voordoen die het noodzakelijk maakt dat er beheerwerkzaamheden worden uitgevoerd, bijvoorbeeld in verband met een beveiligingsincident. Voor die situaties is de instemming van het stembureau vereist, waarbij vooraf via een wijzigingsprocedure wordt ingestemd met de uit te voeren beheeractiviteiten of wijzigingen. Het beheer zelf dient plaats te vinden onder toezicht om te voorkomen dat één persoon onbewust of bewust niet-toegestane beheerhandelingen verricht.

B029 *Systeembeheer van de computer infrastructuur is tijdens een verkiezing alleen toegestaan onder toezicht.*

Toelichting: Tijdens de stemming zal permanent systeembeheer (waaronder security operations) uitgevoerd moeten worden om de juiste werking van de infrastructuur waarop het internetstemsysteem draait te bewerkstelligen. Het beheer zelf dient plaats te vinden onder toezicht om te voorkomen dat één persoon onbewust of bewust niet toegestane beheerhandelingen verricht.

B030 *Het beheer van de beveiliging is ondergebracht bij andere personen dan de functioneel / applicatie beheerders, systeembeheerders, stembureauleden of waarnemers.*

Toelichting: Vanuit het oogmerk van functiescheiding moet de taak van beveiligingsbeheerder gescheiden zijn van de overige uitvoerings-, toezichts- of beheertaken.

8 DISTRIBUTIE VAN STEMBESCHEIDEN EN AUTHENTICATIE

8.1 Inleiding

In het huidige systeem van briefstemmen worden stembescheiden toegestuurd aan de kiezers die zich hebben laten registreren als kiezer buiten Nederland. Deze verzending vindt plaats per reguliere post en vindt plaats zo snel als mogelijk nadat de definitieve kandidatenlijsten zijn vastgesteld. De stembescheiden bestaan uit een stembiljet, een envelop voor het stembiljet, een briefstembewijs en een retourenvelop.

Fysieke biljetten of enveloppen zijn bij internetstemmen niet meer nodig. De 'stembescheiden' in geval van internetstemmen bestaan uit vier onderdelen:

a. een website of applicatie om de stem mee uit te brengen, en
b. een authenticatiemiddel (optioneel), en
c. een brief / aankondiging waarmee de kiezer geïnformeerd wordt over de wijze van stemmen, over de installatie van de programmatuur, wijze van authenticatie, de openingstijden, contactgegevens helpdesk etc.

Een van de ontwerpvraagstukken is hoe de kiezers in het buitenland op een veilige en betrouwbare wijze kunnen worden voorzien van de stembescheiden. In dit hoofdstuk worden eisen gedefinieerd aan de distributie van de stemapplicatie en aan het authenticatiemiddel.

8.2 Stemapplicatie

De stemapplicatie vervult een cruciale rol in het stemproces aangezien de applicatie het enige middel is waarmee de kiezer zijn stem kan uitbrengen. Vanuit beveiligingsoogpunt is de stemapplicatie daarnaast ook een kwetsbaar object, omdat het een aantrekkelijke doelwit is om aanvallen op of mee uit te voeren. Dit betekent dat aanvullende eisen gesteld moeten worden aan de distributie van de stemapplicatie die zorgen dat de stemapplicatie wereldwijd goed beschikbaar is én dat de kiezer de enige juiste stemapplicatie gebruikt.

In praktische zin is alleen distributie van de applicatie over het internet een reële optie. Distributie van de stemapplicatie via de reguliere post (op CD of memory stick) duurt te lang, is onbetrouwbaar én kostbaar. Distributie via internet kent ook nadelen. Zoals in de risicoanalyse ook is aangegeven is één van de risico's het infecteren van de computer van de kiezer met malware. Een voor de hand liggende methode om dat te doen is om een nep website te maken die lijkt op de verkiezingswebsite en zo kiezers te verleiden om een nep stemapplicatie te downloaden en te installeren. Er zijn inmiddels diverse technieken beschikbaar, zoals het EV certificaat (groen balk in browser), die de kiezer kan helpen om vast te stellen of hij verbinding heeft met de authentieke verkiezingswebsite.

Ten aanzien van de distributie zelf is er een afhankelijkheid van het technisch ontwerp van de stemapplicatie: bestaat deze uit HTML pagina's met een scripttaal, uit een java applet dat draait op

een java virtual machine op de computer of bestaat de stemapplicatie uit een afzonderlijke executable die geïnstalleerd moet worden? Die keuze wordt bepaald door de gewenste functionaliteit, mogelijkheden van de programmeertaal en door beveiligingsoverwegingen.

Voor de distributie kan eventueel gebruik gemaakt worden van zgn. content distribution netwerken (CDN). Door een CDN in te zetten kan de stemapplicatie worden gedownload via een netwerk van gedistribueerde servers. Het voordeel is dat de afhankelijkheid van de beschikbaarheid van één website sterk afneemt, waardoor dit ook een populaire maatregel is tegen DDOS aanvallen. Aangeraden wordt om een CDN te kiezen die valt onder de Nederlandse wetgeving en niet onder de reikwijdte van (bij voorbeeld) de Amerikaanse Patriot Act.

Als de keuze gemaakt wordt voor het aanbieden van een stemapplicatie op een mobiel platform dat ligt het gebruik van een app store (Apple App Store / Google Play / Windows Phone) voor de hand. Het voordeel van deze app stores is dat dit een voor de kiezer herkenbare en vertrouwde manier is van softwaredistributie. De authenticiteit van de programmatuur wordt daarbij geborgd door ingebouwde digitale handtekeningen van de app store. Het nadeel is dat er een (kleine) afhankelijkheid ontstaat van de app store beheerder voor de ondertekening en acceptatie van de applicatie.

Ook zullen maatregelen genomen moeten worden om de integriteit van de applicatie te borgen. Er zijn zowel maatregelen voorhanden waarin de applicatie zelf detecteert of de eigen code is veranderd als maatregelen waarin de gebruiker deze controle uitvoert (bijvoorbeeld door een certificaat te controleren).

Aanbevolen wordt om tevens via voorlichting aan de kiezers duidelijk te maken hoe de stemapplicatie verkregen kan worden, hoe de authenticiteit kan worden vastgesteld en hoe men waakzaam kan zijn tegen malware, spoofing of phising pogingen.

8.3 Authenticatiemiddel

Een tweede onderdeel van de stembescheiden is het authenticatiemiddel. De distributie van een authenticatiemiddel als onderdeel van de verkiezing is overigens niet noodzakelijk indien de kiezer reeds beschikt over een betrouwbaar authenticatiemiddel. Zo wordt in Estland en Noorwegen gebruik gemaakt van een elektronische identiteit op een smart card die wordt uitgegeven door de overheid en/of private instanties. Een dergelijk, door de Nederlandse overheid erkent, authenticatiemiddel was op het moment van schrijven van dit rapport (december 2013) niet beschikbaar voor de doelgroep kiezers buiten Nederland.

De betrouwbaarheid van een authenticatiemiddel wordt niet alleen bepaald door het authenticatiemiddel zelf (wachtwoord, 2-factor met soft certificaat of token, smart card etc.) maar ook door i) de identificatieprocedure van de aanvrager/gebruiker bij aanvraag van het middel, ii) de procedure waarin het middel wordt uitgereikt, iii) de kwaliteit van de organisatie die het middel

uitreikt, en iv) de bescherming van het authenticatiemechanisme zelf tegen manipulatie en inbreuken.

In Europees verband is een interoperabiliteitsmethodiek[9] ontwikkeld voor de uitwisselbaarheid van elektronische identiteiten (STORK project). Als onderdeel van de het STORK project zijn vier referentieniveaus ontwikkeld die het betrouwbaarheidsniveau van de authenticatie aangeven. Om een referentieniveau te bepalen is een framework opgezet met eisen aan het registratieproces en aan de elektronische authenticatie. In onderstaande tabel is de inschaling gegeven voor het authenticatiemodel bij internetstemmen, voor de definitie van de kwaliteitsniveaus wordt verwezen naar de Stork methodiek.

	Stap	Kwaliteitsniveau
Registratieproces	Identificatie procedure	ID3
	Uitgifte proces authenticatiemiddel	IC3
	Uitgifteorganisatie	IE3
Authenticatie	Robuustheid authenticatiemiddel	RC3
	Robuustheid tegen aanvallen[10]	AM3

Bij deze inschaling is uitgegaan van de uitgevoerde risicoanalyse internetstemmen in deel II van dit rapport. Op grond van de risicoanalyse en het daarin onderkende dreigingsscenario dat een niet-kiesgerechtigde een stem uitbrengt zou het wenselijk zijn dat ergens in het uitreikproces van het authenticatiemiddel een persoonlijke identificatie van de kiezer plaatsvindt, om zo een hogere betrouwbaarheid te verkrijgen. Het uitreikproces van het authenticatiemiddel kan (maar hoeft niet) gecombineerd worden met het registratieproces (hetgeen buiten de scope van het internetstemsysteem valt).

Gelet op de doelgroep van kiezers buiten Nederland levert de persoonlijke identificatie mogelijk praktische bezwaren op indien deze kiezers hun authenticatiemiddel in persoon moeten ophalen in Nederland of bij een ambassade of consulaat in het land. Tegelijkertijd levert dit wel een betrouwbaarder uitgifteproces en daardoor een betrouwbaarder authenticatie op. Er zijn een paar oplossingen denkbaar voor dit probleem.

Eén daarvan is het gebruik van een authenticatiemiddel, uitgegeven door de Staat der Nederlanden, dat de kiezer ook voor andere elektronische diensten kan (of moet) gebruiken. Het praktische bezwaar van het afhalen blijft weliswaar bestaan, maar de bereidheid van de kiezer om

[9] Zie D2.3 Quality authenticator scheme, Stork project. https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

[10] In STORK worden vijf dreigingen onderkend: Raden, Afluisteren, Kapen, Naspelen en 'Man-in-the-middle'

dit te doen neemt toe doordat ook het belang toeneemt. Onderzocht moet worden of het DigiD Buitenland authenticatiemiddel, dat nu beproefd wordt voor de authenticatie van in het buitenland wonende Nederlanders in hun communicatie met SVB en Belastingdienst voldoende geschikt is in de verkiezingscontext.

Het praktische bezwaar kan verder worden verlaagd door het registratieproces of het uitgifteproces een eenmalige karakter te geven, hetgeen ook voorzien is met de voorgenomen invoering van de permanente registratie.

Een andere oplossingsrichting is om gebruik te maken van andere private authenticatiemiddelen, mits deze een vergelijkbaar of hoger betrouwbaarheidsniveau hebben en mits de authenticatie een bruikbaar identiteitskenmerk oplevert dat gebruikt kan worden bij het bepalen van de kiesgerechtigdheid. Een andere oplossingsrichting is om de identiteitscontrole bij de uitgifte van het authenticatiemiddel toe te vertrouwen aan andere organisaties, zoals lokale postkantoren, internationale koeriers of banken. Het nadeel van de laatste twee opties is uiteraard dat het vertrouwen vergt in de juiste uitvoering van de controle tegen een legitimatiebewijs door deze partijen.

B031 *Het authenticatiemodel en het gebruikte authenticatiemiddel dient minimaal te voldoen aan Stork Quality Authentication Assurance niveau QAA3.*

Toelichting: zie boven.

N.B. In eis B016 worden eisen gesteld aan het authenticatiemiddel dat beheermedewerkers gebruiken om toegang te krijgen tot de stemserver modules van het internetstemsysteem.

9 HERZIENING FUNCTIE EN TAKEN STEMBUREAU

9.1 Inleiding

In de evaluatie van eerdere Kiezen op Afstand experimenten met internetstemmen uit 2004 en 2006 is aandacht gevraagd voor de rol van het stembureau. Bij die experimenten is, op grond van de Kieswet, de toen geldende experimentenwet Kiezen op Afstand en het toen geldende experimentenbesluit Kiezen op Afstand, een internetstembureau ingericht in analogie van een traditioneel stembureau zoals dat bij de reguliere verkiezing voor kiezer in Nederland zitting houdt in een stemlokaal per stemdistrict. Uit de evaluatie van 2006 onder de leden van het internetstembureau kwamen een aantal aandachtspunten naar voren die maken dat een herziening van de functie en taken van het stembureau bij een internetstemming gewenst is:

- Taken en handelingen stembureau
- Controle mogelijkheden op een geautomatiseerd proces
- Bewaken van orde en vaststellen van onregelmatigheden
- Afhankelijkheid stembureau van beheerders internetstemsysteem
- Het meerdaagse en 24 uurs karakter van de stemming
- Openbaarheid van het ‘stemlokaal’
- Vereiste deskundigheid
- Mogelijkheid van bezwaar

9.2 Taken stembureau

De taken van het stembureau zijn vastgelegd in de Kieswet (hoofdstukken J t/m N) lagere regelgeving (Kiesbesluit, ministeriële besluiten en modellen). Voor de stemmen die per brief worden uitgebracht is in hoofdstuk M en in een deel van hoofdstuk N beschreven hoe die stemming verloopt en wat de taken van het briefstembureau daarbij zijn.

In onderstaande tabel zijn de taken van een regulier stembureau weergegeven in vergelijking met de taken van een briefstembureau en een internetstembureau. Met ‘Nee’ of ‘Ja’ is aangegeven of de taak respectievelijk niet of wel vergelijkbaar is met een regulier stembureau. Voor de taken van het internetstembureau geldt dat deze afhankelijk zijn van het ontwerp / de functionaliteit van het internetstemsysteem.

	Taken regulier stembureau	Taken briefstembureau	Taken internetstembureau
1.	Controle inrichting stemlokaal en aanwezigheid alle materialen en voorzieningen voor kiezers om hun stem mee uit te brengen	Nee	Nee
2.	Controle stembus leeg	Ja	Ja

	Taken regulier stembureau	Taken briefstembureau	Taken internetstembureau
3.	Controle aanwezigheid materialen en documenten voor stembureau	Ja	Ja
4.	Openen stemming op dag van stemming	Nee, kiezers kunnen stemmen vanaf moment dat zij hun briefstembescheiden ontvangen	Ja, mogelijk gedurende meerdaagse periode voorafgaand aan de dag van stemming
5.	Controle identiteit kiezer a.d.h.v. identiteitsdocument, controle echtheid stempas van kiezer en tenaamstelling, controle of volgnummer stempas staat in met register van ongeldige stempassen	Equivalent: bij ontvangst van retourenvelop wordt controle uitgevoerd van handtekening op briefstembewijs met handtekening op registratieverzoek	Nee, is geautomatiseerd proces van authenticatie door internetstemsysteem of een third party authenticatiedienst
6.	Controle volmachtbewijs	Niet van toepassing	Niet van toepassing
7.	Controle kiezerspas	Niet van toepassing	Niet van toepassing
8.	Uitreiken stembiljet	Nee, gebeurt niet door stembureau maar door B&W Den Haag / Ministerie van BZK	Nee, is onderdeel van de functionaliteit van het de stemapplicatie
9.	Toezien op deponering stembiljet in stembus door kiezer	Nee, stembiljet (in gesloten envelop) wordt door lid briefstembureau in stembus gestoken	Nee, is onderdeel van de functionaliteit van het internetstemsysteem
10.	Aantekenen van weigering deponering stembiljet	Niet van toepassing	Niet van toepassing
11.	Onbruikbaar maken niet gebruikte en terugontvangen stembiljetten of ongeldige stembiljetten	Ja	Nee. Inherent aan het internetsysteem is er geen sprake van een (ongeldig) stembiljet, maar alleen van uitgebrachte stemmen. Wel kunnen er digitale gegevens / bestanden worden ontvangen waarvan het internetstemsysteem vaststelt dat het ongeldige stemmen betreft

	Taken regulier stembureau	Taken briefstembureau	Taken internetstembureau
	Toezicht op ordelijk verloop van stemming	Toezicht op ordelijk verloop van de stemopneming in het briefstembureau	Detectie van digitale ordeverstoringen (zoals DDoS) en toezicht op ordelijk verloop van de stemopneming
12.	Schorsing stemming	Ja	Ja
13.	Waarborgen geheime stemming door inrichting stemlokaal, door controle afwezigheid van aantekeningen op de gedeponeerde stembiljetten in de stembus	Ja, door toe te zien op correcte uitvoering dubbele envelop principe	Deels, is primair onderdeel van de functionaliteit van het internetstemsysteem
14.	Waarborgen stemvrijheid	Nee, niet mogelijk	Nee, niet mogelijk
15.	Sluiten stemming	Ja	Ja
16.	Stemopneming : tellen stemmen en evt hertellen	Ja	Nee, het internetstembureau telt niet zelf, maar geeft opdracht aan het internetstemsysteem tot het tellen van de stemmen.
17.	Aantekening bezwaren aanwezige kiezers in proces-verbaal	Ja	Nee, kiezers zijn niet aanwezig in stemlokaal.
18.	Invullen proces verbaal	Ja	Ja
19.	Afronden: verzegeling uitgebrachte stemmen en overige documenten in enveloppen, transport naar gemeente	Ja	Nee, het internetstembureau kan alleen opdracht geven tot een digitale equivalent van het veiligstellen van de stemmen

In de volgende paragrafen wordt op een aantal van deze taken een nadere verdieping gegeven.

9.3 Controlemogelijkheden op een geautomatiseerd proces

In een internetstemsysteem zijn een aantal bepalende processtappen (zoals controle identiteit kiezer, uitreiken stembiljet) geautomatiseerd, waardoor de daar aan gerelateerde (handmatige / visuele) taken van het stembureau komen te vervallen. De rol van het internetstembureau is het beste te vergelijken met de rol die operators vervullen in bijvoorbeeld een elektriciteitscentrale of

een chemische fabriek; zij bedienen en monitoren een (verregaand) geautomatiseerd proces waarbij ze niet zelf met eigen ogen het exacte verloop van het proces kunnen waarnemen. Voor de waarnemingen en daarop volgende beslissingen zijn de operators afhankelijk van de informatie die door het geautomatiseerde systeem wordt verstrekt.

Zo worden ook de mogelijkheden voor de leden van het internetstembureau om het stemproces te observeren vrijwel volledig bepaald door de aanwezigheid van controle- en monitorfunctionaliteiten van het internetstemsysteem zelf[11].

9.4 Afhankelijkheid stembureau van beheerders internetstemsysteem

Uit de eerder genoemde evaluatie bleek ook dat de leden van het stembureau voor de uitoefening van hun taak vrijwel volledig afhankelijk waren van een aantal ICT specialisten, die gedurende de stemming het technisch beheer uitvoerden van het internetstemsysteem. De afhankelijkheid bestond er uit dat voor de ondersteuning van kiezers en voor de interpretatie van zich voordoende (fout)situaties moest worden teruggevallen op de inhoudelijke en technische expertise van de specialisten. Alleen zij waren op de hoogte van de exacte werking van het internetstemsysteem en waren in staat om handelingen[12] uit te voeren op de servers en netwerkapparatuur van het internetstemsysteem. Deze handelingen werden uitgevoerd onder de verantwoordelijkheid van het stembureau, maar de leden waren niet deskundig genoeg om het handelen van de beheerders te kunnen controleren.

Aanbeveling 02 *Aanbevolen wordt dat beheeractiviteiten van het internetstemsysteem gedurende de stemperiode tot een absoluut minimum moet worden beperkt. Alle beheerhandelingen moeten plaatsvinden in opdracht van en onder de verantwoordelijkheid van het stembureau, welke daartoe geëquipeerd is. Zie ook de eisen in 7.3.*

9.5 Het meerdaagse karakter van de stemming

Onder aanname dat een meerdaagse stemming wordt gehouden, is het een vereiste dat gedurende de hele stemperiode het stembureau zitting heeft. In de eerdere experimenten in 2004 en 2006 waren dat respectievelijk tien en vijf dagen.

Om praktische en arbo redenen is het niet wenselijk om alle leden van het internetstembureau gedurende meerdere dagen en gedurende 18 uur per dag actief te laten zijn. In de praktijk (en ook in de andere landen) werd de functie van het stembureau ingevuld door meerdere teams van personen die elkaar afwisselden. Vanuit taak- en functiescheiding is het een vereiste dat het stembureau bestaat uit meerdere personen.

---

[11] Of een monitoringsysteem dat los van het internetstemsysteem staat.

[12] Het merendeel van de handelingen betrof controle werkzaamheden op de hardware, operating systeem of serverprocessen van de servers waarop de programmatuur van het internetstemsysteem draaide.

Aanbeveling 03 *Aanbevolen wordt om de functie van het internetstembureau vorm te geven door deze in 'ploegendiensten' te bemensen. In de aanstelling van de voorzitter en (reserve)leden van het stembureau dient hier rekening mee te worden gehouden, zodat er voldoende personen beschikbaar en opgeleid zijn om de taak te vervullen.*

Overwogen kan worden om gebruik te maken van piketdiensten, waarbij niet continue een voltallig stembureau actief is, maar slechts twee leden. In geval van bijzondere situaties kan dan het voltallige stembureau bijeen worden geroepen.

9.6 Openbaarheid van het 'stemlokaal'

Op grond van de Kieswet (art J35 lid 1) is het kiezers[13] toegestaan om aanwezig te zijn in het stemlokaal, zowel gedurende de stemming als de stemopneming. Het is de vraag wat het stemlokaal is bij een internetstemming, is dat de fysieke plek waar de servers van het internetstemsysteem staan opgesteld, of is dat de fysieke plek waar de leden van het stembureau bijeenkomen en hun taken uitvoeren? Aangenomen mag worden dat de servers fysiek in één of meerdere (i.v.m. redundantie) beveiligde en geconditioneerde hostinglocaties worden opgesteld, mede om te kunnen voldoen aan de waarborg van beschikbaarheid. Het verlenen van toegang aan kiezers (of derden) tot de fysieke locatie van de servers is in theorie mogelijk, maar is in de praktijk om beveiligings- en continuïteitsredenen zeer ongewenst. Daarnaast is met toegang tot de locatie waar de servers opgesteld staan nog geen openbaarheid gecreëerd in de zin dat een kiezer zelfstandig kan waarnemen dat het verkiezingsproces conform de wettelijke regels verloopt (J35 lid 2 Kw).

Inherent aan het gebruik van computers in het stemproces is het verloop van het stemproces voor mensen niet direct waarneembaar; het enige dat de kiezer ziet is de buitenkant van de server(s). Het vergt aanvullende maatregelen en systemen om dit verloop inzichtelijk te maken. Door de complexiteit van een internetstemsysteem is het ook maar de vraag of een gemiddelde kiezer in realistische zin inzicht *kan* verkrijgen in de werking van het internstemsysteem.

Aanbeveling 04 *Aanbevolen wordt om het openbare karakter op een andere wijze vorm te geven, langs de volgende principes:*

a. Als 'internetstemlokaal' wordt de locatie waar het internetstembureau zitting houdt aangewezen.

[13] Op grond van de formulering in de Kieswet is het niet-kiezers niet toegestaan om aanwezig te zijn in het stemlokaal, in de praktijk wordt deze regel niet of nauwelijks gehandhaafd. Daarnaast kan de minister toestemming verlenen aan (buitenlandse) waarnemers om getuige te zijn van het verloop van de verkiezingen, en toegang te hebben tot het stemlokaal.

b. Het is kiezers toegestaan hierbij aanwezig te zijn, voor zover het de orde en de voortgang van de zitting van het stembureau niet verstoord.
c. De controlerende functie die uitgaat van het openbare karakter en de mogelijke aanwezigheid van kiezers wordt daarnaast ingevuld door meerdere onafhankelijke deskundige waarnemers aan te wijzen. Deze waarnemers krijgen speciale bevoegdheden om naar eigen inzicht informatie op te vragen, voorzieningen te inspecteren en toezicht te houden op het functioneren van het stembureau. Deze waarnemers rapporteren aan het centraal stembureau en het vertegenwoordigend orgaan.
d. Voor specifieke handelingen, zoals bijvoorbeeld de cryptografische sleutelgeneratie, het openen of sluiten van de stemming, en de stemopneming, worden de onafhankelijke waarnemers, auditors en een aangestelde notaris uitgenodigd om toe te zien op het conform protocol uitvoeren van de vereiste handelingen door het stembureau.
e. Er wordt door het internetstembureau een proces-verbaal opgemaakt waarin zij verslag doet van de door haar verrichtte handelingen. Dit proces-verbaal wordt na afloop van de zitting gepubliceerd op internet.
f. In het openbare karakter wordt mede voorzien door openbaarmaking van alle informatie over de opzet en werking van het internetstemsysteem, en door het bieden van een controlemogelijkheid aan de kiezers (zie eis B006).

9.7 Bewaken van orde en vaststellen van onregelmatigheden

Het is het stembureau dat de wettelijke taak heeft om toe te zien op de orde in het stemlokaal. Indachtig het vorige punt betreft dit de orde in de locatie waar het internetstembureau zitting houdt. Echter de orde kan bij internetstemmen ook elders worden verstoord, bijvoorbeeld door het doelbewust verstoren van de toegang van kiezers tot het internetstemsysteem (DDoS aanval, aanval op tussenliggende internetverbindingen, malware bij de kiezer, etc.), het uitbrengen van stemmen door niet-kiesgerechtigden, etc.
De voorzitter van het stembureau kan bij een ordeverstoring in een traditioneel stemlokaal de burgemeester om bijstand verzoeken. De burgemeester kan in zo'n geval de orde laten handhaven door instructies te geven aan de politie.
In geval van een ordeverstoring bij een internetstemming kan de inzet van politie ook worden ingeroepen, zij het dat de lokale wijkagent hier beperkte toegevoegde waarde heeft. Omwille van de handelingssnelheid zal het internetstembureau direct, zonder tussenkomst van een burgemeester, een beroep moeten kunnen doen op gespecialiseerde teams die zich bezig houden met de bestrijding van cybercrime (zoals het Team High Tech Crime van KLPD en het Nationaal Cyber Security Center).

Aanbeveling 05 *Aanbevolen wordt dat het stembureau bij constatering van een ordeverstoring een direct beroep kan doen op deze gespecialiseerde teams, zonder tussenkomst van een burgemeester of minister.*

Aanbeveling 06 *Aanbevolen wordt dat het stembureau dit beroep kan doen gedurende de periode van stemming, alsook in een periode voorafgaand aan en volgend op de stemperiode.*

9.8 Vereiste deskundigheid

In de uitvoeringspraktijk van de reguliere verkiezingen zijn geen eisen gesteld aan de vereiste deskundigheid van het stembureau. In het geval van internetstemmen is, gelet op de complexiteit van een internetstemsysteem, specifieke deskundigheid vereist vanuit meerdere disciplines.

Aanbeveling 07 *Het verdient aanbeveling dat het stembureau beschikt over expertise op minimaal de volgende terreinen: kiesrecht, verkiezingspraktijk, cryptografie, informatiesystemen en informatie beveiliging / cybersecurity.*

9.9 Mogelijkheid van bezwaar

De in het stemlokaal aanwezige kiezers kunnen mondeling bezwaren inbrengen, indien de stemming niet overeenkomstig de wet geschiedt. Het stembureau vermeldt deze bewaren in het proces-verbaal van de zitting. Deze werkwijze kan evenzo worden toegepast voor de kiezers aanwezig in het internetstemlokaal (de locatie waar het internetstembureau zitting houdt).

Het is voor kiezers buiten Nederland in praktische zin lastig om zelf aanwezig te kunnen zijn in het internetstemlokaal. Het is om die reden dat er een aanvullende mogelijkheid moet worden getroffen voor deze groep kiezers om eventuele bezwaren te kunnen inbrengen.

Aanbeveling 08 *Aanbevolen wordt dat kiezers buiten Nederland de mogelijkheid krijgen om schriftelijk (via e-mail) een bezwaar in te dienen, hetgeen door het stembureau zal worden toegevoegd aan het proces-verbaal.*

9.10 Conclusie

Uit het overzicht van taken blijkt dat bij internetstemmen een groot aantal taken van het reguliere stembureau komt te vervallen, i) deels doordat taken die gerelateerd zijn aan de fysieke ruimte en inrichting niet van toepassing zijn, ii) deels doordat er taken gerelateerd zijn aan stemmethoden (volmachtstemmen en stemmen in een willekeurig stemlokaal) die geen toepassing kennen bij internetstemmen en iii) deels doordat de taken geautomatiseerd zijn en onderdeel van de functionaliteit van het internetstemsysteem.

Geconcludeerd moet worden dat het stembureau zoals bedacht is voor verkiezingen in een stemlokaal niet één op één vorm te geven is bij internetstemmen. Een internetstembureau kan niet op een vergelijkbare wijze de controlerende en sturende functie van het reguliere stembureau invullen.

Aanbeveling 09 *In overweging wordt gegeven om het internetstembureau een andere naam te geven, om zo het onderscheid met een regulier stembureau te benadrukken. In België is hiertoe een College van Deskundigen opgericht, in Estland een Electronic Voting Committee onder het National Election Committee. In dit document wordt vanuit het oogpunt van consistentie nog wel de term internetstembureau gebruikt.*

9.11 Voorgesteld mandaat en taken van internetstembureau

Het internetstembureau:

- Is ingesteld op grond van de Kieswet.
- De voorzitter(s) en leden worden door de minister van BZK benoemd.
- Opereert onafhankelijk van het ministerie van BZK.
- Is verantwoordelijk voor het correct uitvoeren van de internetstemming en stemopneming.
- Heeft mandaat om te beslissen tot het schorsen of sluiten van de stemming in geval van bijzondere onvoorziene omstandigheden.
- Rapporteert middels een proces-verbaal aan het hoofdstembureau en het centraal stembureau (en daarmee in openbaarheid) over het verloop van stemming.
- Is gedurende de stemperiode in piketdienst actief en komt voltallig bijeen bij de opening en sluiting van de stemming en in bijzondere situaties.
- Wordt bij voorkeur niet per verkiezing samengesteld, maar voor een langere periode van minimaal 3 verkiezingen. De voorzitter en leden ontvangen een vergoeding voor de dagen dat zij in functie zijn.
- Het mandaat om te besluiten tot een herstemming ligt bij het vertegenwoordigend orgaan (de Tweede Kamer).

TAKEN INTERNETSTEMBUREAU

- Maakt gebruik van de in het internetstemsysteem beschikbare functionaliteit (zie hoofdstuk 5.3) om de stemming te openen, schorsen, hervatten en sluiten en om rapportages te genereren (zonder afhankelijkheid van operators / beheerders van het internetstemsysteem of onderliggende infrastructuur).
- Stembureau heeft geen rol in voorbereidingen van de verkiezing, waaronder registratie van kiezers, cryptografische sleutelgeneratie, installatie van internetstemsysteem, etc.
- Dient ruim voor aanvang van de start van de internetstemperiode bijeen te komen voor training in de specifieke wettelijke taken en verantwoordelijkheden, de werking van het internetstemsysteem, operationele protocollen en beveiligingsinstructies.
- Instrueert de helpdesk / publieksvoorlichting van het ministerie van BZK in geval van bijzondere omstandigheden.
- Stembureau, beheerders en helpdesk zijn idealiter op één locatie gevestigd.
- Indien een systeem van kiezersverificatie wordt gehanteerd heeft het stembureau geen rol in de behandeling van claims van kiezers.

9.12 Overige partijen

Het mandaat en de taken van het internetstembureau kunnen niet los gezien worden van de taken en verantwoordelijkheden van de overige betrokken partijen.

MINISTERIE VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

- Is verantwoordelijkheid voor ontwerp, verwerving en ontwikkeling van internetstemsysteem en het correct functioneren daarvan.
- Laat het internetstemsysteem certificeren door een onafhankelijke certificatie instantie.
- Is verantwoordelijk voor de opbouw van het internetstemsysteem.

BEHEERDERS

- Beheerders van het internetstemsysteem werken voorafgaand en na afloop van de stemming op aanwijzing van het ministerie van BZK.
- Beheerders van het internetstemsysteem werken gedurende de stemming op aanwijzing van het internetstembureau en leggen over hun werkzaamheden verantwoording af aan internetstembureau.
- Beheerders voeren hun werkzaamheden uit vanuit dezelfde locatie als het internetstemlokaal.
- Beheerders staan in contact met instanties die waken over de beveiliging en continuïteit van de servers en het internet (NCSC, THTC Politie, Computer Emergency Response Teams van internet providers, etc.)

SLEUTELBEWAARDERS

- Sleutelbewaarders zijn door het ministerie van BZK benoemde onafhankelijke personen die de taak hebben om een deel van de cryptografische sleutels van het internetstemsysteem in bewaring te nemen en die ter beschikking te stellen conform strikte protocollen.

WAARNEMERS

- Waarnemers zijn onafhankelijke deskundigen die de taak hebben de correcte werking van het internetstemsysteem voorafgaand, tijdens en na afloop van de stemming te controleren én die de taak hebben om toe te zien op het correct handelen van het internetstembureau.
- Waarnemers worden door de minister van BZK benoemd. De functie wordt aangemerkt als een vertrouwensfunctie.
- Waarnemers opereren steeds gezamenlijk in een team van minimaal drie personen.
- Waarnemers hebben een wettelijk verankerd recht om informatie te vorderen van betrokken partijen, het ministerie, eventuele leveranciers van onderdelen van het internetstemsysteem, het stembureau en beheerders. Specifieke cryptografische sleutels en wachtwoorden zijn hiervan uitgezonderd.
- Waarnemers hebben het recht om onaangekondigd inspecties te houden.
- Waarnemers leggen verantwoording af aan het centraal stembureau en het vertegenwoordigend orgaan.

HELPDESK

- Het ministerie van BZK richt een helpdesk in voor de ondersteuning van kiezers buiten Nederland die vragen hebben of die problemen ondervinden bij de installatie of het gebruik van het internetstemsysteem.
- De helpdesk informeert het internetstembureau gedurende de stemming over mogelijke ordeverstoringen of signalen die wijzen op het niet functioneren of gebreken van het internetstemsysteem.

10 AANBEVELINGEN T.A.V. INVOERING

10.1 Beschouw internetstemmen als een langdurig proces van ontwikkeling, invoering en evaluatie

Uit de eerdere Kiezen op Afstand ervaringen én uit de ervaringen in het buitenland blijkt dat het ontwikkelen van een internetstemvoorziening niet als een eenmalige exercitie kan worden beschouwd. Zowel in Nederland, Noorwegen, Estland, Zwitserland (Geneve) als Frankrijk is de gebruikte internetstemvoorziening na toepassing in een verkiezing op onderdelen aangepast en in sommige gevallen zelfs volledig opnieuw ontwikkeld.

Het is dan ook niet realistisch om te veronderstellen dat een kant-en-klaar systeem aangeschaft kan worden dat ingezet kan worden voor bijvoorbeeld de eerstvolgende vier of vijf verkiezingen zonder dat er aanpassingen nodig zijn. Dit heeft verschillende oorzaken.

Allereerst zijn aanpassingen te verwachten gelet op het nieuwe, soms experimentele, karakter van internetstemmen. Een evaluatie is dan ook noodzakelijk en levert aanbevelingen op die leiden tot aanpassingen. Zo bleek in Nederland in 2006 dat het stembureau (te) sterk afhankelijk was van een aantal beheerders. In Noorwegen bleek in 2012 dat het drukken van de gepersonaliseerde oproepingskaarten veel foutgevoeliger was dan voorzien, waardoor enkele kiezers verkeerde controlecodes toegestuurd kregen. Eveneens in Noorwegen bleek dat de stemapplicatie voor de kiezer niet meer werkte toen er een wereldwijde update van de Java virtual machine werd uitgerold.

Ook zijn aanpassingen te verwachten doordat de ontwikkelingen op het gebied van internet- en computertechnologie elkaar in een hoog tempo opvolgen. Hierdoor is de levensduur en daarmee verkrijgbaarheid van computerapparatuur in praktische zin beperkt tot ongeveer vijf jaar. Veel componenten van het internetstemsysteem zullen dan ook tussentijds vervangen (moeten) worden. Ook zullen er in de loop der tijd nieuwe mogelijkheden ontstaan (bijvoorbeeld gebruik van smartphones en tablets, nieuwe encryptietechnologie, nieuwe authenticatiemiddelen etc.) waarvan het wenselijk is dat die ingepast worden in het internetstemsysteem. De ontwikkelingen op het gebied van cybercrime dreigingen kennen een zo mogelijk nog hogere snelheid. Dit betekent dat in continuïteit het internetstemsysteem voorzien moet worden van aanvullende maatregelen om nieuwe dreigingen het hoofd te bieden.

Indien besloten wordt tot invoering, dan moet worden gerealiseerd dat een internetstemsysteem een grote complexiteit kent en eerder als een langdurig proces van ontwikkeling, invoering en evaluatie beschouwd moet worden dan een systeem wat eenmaal aangeschaft ongewijzigd gebruikt kan worden in vele jaren daarna.

10.2 Invoering in stappen en met terugvalopties

In zowel Zwitserland, Australië, Canada, Frankrijk als Noorwegen is gekozen voor een stapsgewijze invoering van internetstemmen. Zonder uitzondering was in al deze landen steeds de overweging

hierbij dat mocht, om welke reden dan ook, het internetstemsysteem falen het effect op de totale uitslag beperkt zou zijn. In Zwitserland gold eerst een wettelijke limiet van 10% van het aantal kiezers dat mag stemmen via het internet. Na tien jaar toepassen, waarbij de formele status nog immer experimenteel is, is besloten deze grens op te trekken naar 30% van de kiezers woonachtig in Zwitserland (en alle Zwitsers woonachtig in het buitenland). In Noorwegen is ook nadrukkelijk gekozen voor eerst experimenteren bij een tiental gemeenten, hetgeen opgetrokken is naar 12 gemeenten bij de tweede toepassing in 2013. Ook vanuit het oogpunt van vertrouwen onder kiezers is het aan te bevelen om kiezers gedurende meerdere verkiezingen te laten wennen aan de nieuwe stemmethode, alvorens te besluiten tot een definitieve invoering.

In geen van de landen wordt internetstemmen als enige stemmethode aangeboden. Ook al zal het aantal personen dat geen toegang heeft tot internet in het komende decennium sterk afnemen, het is vanuit het oogpunt van toegankelijkheid niet haalbaar en ook niet gewenst om alle kiezers buiten Nederland via internet te laten stemmen. In Estland, Zwitserland en Noorwegen, waar kiezers woonachtig in het land zelf via internet mogen stemmen is er steeds voor gekozen om de kiezer ook een terugvaloptie aan te bieden; mocht internetstemmen falen dan kan de kiezer alsnog op de dag van stemming naar een stemlokaal gaan om daar te stemmen. Voor de doelgroep kiezers buiten Nederland is reizen naar een stemlokaal in Nederland praktisch gezien geen optie. Wel kan de kiezer alsnog de mogelijkheid worgen gegeven om alsnog per post te stemmen. Mogelijk treedt dan het probleem op dat niet alle briefstemmen tijdig binnenkomen. Overwogen kan worden om hier een wettelijke uitzondering voor te maken, door de minister de mogelijkheid te geven de termijn[14] waarop briefstemmen mogen worden ingestuurd te kunnen verlengen in geval er een grootschalige (ver)storing van het internetstemsysteem heeft plaatsgevonden. Een dergelijke uitzondering heeft uiteraard ook gevolgen voor de zitting van het hoofdstembureau en centraal stembureau.

10.3 Benut expertise van markt zonder afhankelijk te worden

In de risicoanalyse is geconcludeerd dat een internetstemsysteem een complex informatiesysteem is, niet zozeer door de functionaliteit, maar door de grote hoeveelheid maatregelen die noodzakelijk zijn om te kunnen voldoen aan de waarborgen. De expertise om een dergelijk systeem te ontwikkelen is schaars binnen de overheid.

Er zijn internationaal meerdere leveranciers actief die zich gespecialiseerd hebben in elektronische stemsystemen, waaronder internetstemmen. Het inschakelen van deze partijen (via een EU-aanbesteding) heeft als voordeel dat geprofiteerd kan worden van de specialistische expertise en de ervaringen die opgedaan zijn uit andere landen. Echter om een te grote afhankelijkheid van marktpartijen te voorkomen is het essentieel dat overheid zelf de expertise in huis haalt én houdt om als een goed opdrachtgever de regie te houden over het ontwerp en de (door)ontwikkeling van

[14] art. M8 lid 1 Kieswet

het internetstemsysteem. Dit is niet alleen in de projectfase van belang, maar ook wanneer internetstemmen definitief als stemmethode is ingevoerd. Door de democratische controle op de overheid kan het publieke belang van verkiezingen zo beter worden geborgd. En uiteindelijk ligt de verantwoordelijkheid voor het juiste verloop van de verkiezing niet bij een marktpartij, maar bij de overheid.

Deze rolverdeling dient ook in de juridische kaders van een EU-aanbesteding te worden meegenomen. Er is veel voor te zeggen om het internetstemsysteem als een dienst af te nemen van marktpartijen, aangezien hiermee de verantwoordelijkheid voor de systeemintegratie en het correct functioneren van het internetstemsysteem bij de leverancier kan worden belegd. Ook kan door een vaste prijs te bedingen meer (contractuele) zekerheid over de kosten worden verkregen. Echter aangezien te verwachten is dat het internetstemsysteem over de loop der jaren veelvuldig aangepast zal worden is het ongewenst als de overheid daarmee afhankelijk wordt van één specifieke leverancier.

10.4 Eigendom in handen van de Staat der Nederlanden

Specifieke aandacht is nodig voor de intellectuele eigendomsrechten. Er zijn diverse octrooien vergeven op specifieke vindingen die gebruikt worden in internetstemsystemen. Dit geldt onder meer voor bepaalde cryptografische technieken en voor verificatiesystemen. Bij het ontwerp van het internetstemsysteem zal hier rekening mee moeten gehouden.

A003 *Het eigendom en alle gerelateerde eigendomsrechten voor zaken die specifiek worden ontwikkeld voor het internetstemsysteem dienen te worden overgedragen aan de Staat der Nederlanden.*

A004 *Indien een octrooi is gevestigd op een onderdeel dat toegepast wordt in het internetstemsysteem dan dient de overheid een (niet-exclusief) eeuwigdurend gebruiksrecht te krijgen om de vinding te mogen toepassen in haar internetstemsysteem.*

A005 *Contractueel moet worden bedongen dat de overheid het recht heeft om alle documentatie, specificaties, bestanden en broncode openbaar te mogen (laten) inspecteren en openbaar te mogen maken.*

A006 *Bij gebruik van bestaande software(modules) dient deze bij voorkeur onder een open source licentie te zijn verkregen. Hiervoor geldt het "pas toe of leg uit"- principe; het gebruik van programmatuur die onder closed source licentie wordt geleverd is alleen toegestaan als er geen andere mogelijkheid is om de functionaliteit van deze programmatuur te verkrijgen. Hierbij dient nog steeds aan de vorige eis van broncode inspectie en openbaarmaking te worden voldaan.*

A Bijlage: Ontwerpprincipes

Op grond van de eerdere ervaringen uit de Kiezen op Afstand projecten en op grond van de ervaringen uit andere landen dient het ontwerp van een internetstemsysteem te voldoen aan de volgende principes:

	Principe	Toelichting
1.	Eenvoud	Hou het ontwerp zo simpel mogelijk. Eenvoud verkleint de omvang van het systeem en verkleint de kans op fouten.
2.	Aandacht voor risico's en (informatie)beveiliging	In het ontwerp van het internetstemsysteem dient continue een afweging gemaakt worden welke maatregelen en functionaliteit noodzakelijk zijn gegeven de dreigingen waartegen bescherming gezocht wordt. Het hele ontwerp- en ontwikkelproces moet uitgevoerd worden met een stringente focus op beveiliging.
3.	Defensief	Het internetstemsysteem dient uit te gaan van defensief programmeren: alle input dient gevalideerd te worden en het systeem dient zelf afwijkende condities te detecteren.
4.	Modulaire opbouw	Het ontwerp moet voorzien in een architectuur met gescheiden modules. Modules moeten los van elkaar opereren, zelfstandig kunnen worden getest en eenvoudig kunnen worden vervangen.
5.	Transparantie en openbaarheid	Het ontwerpproces moet transparant verlopen, zodat opdrachtgever en onafhankelijke deskundigen inzicht kunnen krijgen in alle gemaakte ontwerpkeuzes. Het eindproduct moet openbaar gemaakt kunnen worden, de beveiliging van het internetstemsysteem mag niet berusten op geheimhouding van delen van het systeem.
6.	Standaard verkrijgbare componenten	Gebruik zoveel mogelijk standaard componenten die breed verkrijgbaar zijn. Dit vergroot de levensduur van het systeem en verlaagt de kosten.
7.	Beperkte ondersteuning PCs kiezer	Beperk het aantal platformen aan de kant van de kiezer dat wordt ondersteund tot de twee of drie meest gebruikte. Dit reduceert de complexiteit van het internetstemsysteem en de benodigde ontwikkelcapaciteit.

VERDONCK KLOOSTER & ASSOCIATES

DEEL IV – TOETSMETHODE INTERNETSTEMSYSTEEM

VERDONCK KLOOSTER & ASSOCIATES

DEEL IV – TOETSMETHODE INTERNETSTEMSYSTEEM

DATUM	28 januari 2014
STATUS	
VERSIE	1.0

REVISIELIJST

Versie	Datum	Opgesteld door	Vastgesteld op	Toelichting revisie
1.0	24 jan 2014	VKA		Eerste opzet toetsmethode

INHOUDSOPGAVE

1 TOETSEN VAN EEN INTERNETSTEMSYSTEEM

1.1 Inleiding

Door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties is gevraagd een methode te schetsen waarmee kan worden gewaarborgd dat de internetvoorziening voor stemmen via internet op een transparante en controleerbare wijze aan de gestelde eisen voldoet, alsmede om te waarborgen dat de eisen voor het stemmen per internet worden onderhouden zodat het vertrouwen in het internetstemmen door de kiezers in het buitenland kan blijven bestaan.

Deze methode heeft als doel om te beschrijven aan welke norm een (internetstem)systeem moet voldoen, hoe de toetsing tegen de norm verloopt en wie beslissingsbevoegd is over het vaststellen van de norm, hoe de norm wordt onderhouden en de wijze waarop de toetsing verloopt. Onder het begrip 'de norm' wordt hier verstaan het geheel aan eisen, standaarden en wet- en regelgeving waar, in dit geval het internetstemsysteem, aan moet voldoen.

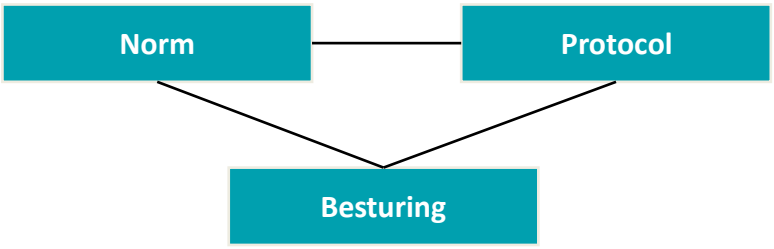
Er is anno 2013 nog geen norm opgesteld of vastgesteld door een nationale of internationale standaardisatieorganisatie of door de Nederlandse overheid. Dit document bevat een eerste aanzet van een toetsmethode voor een internetstemsysteem voor Nederlandse verkiezingen. Een dergelijke toetsmethode wordt ook wel een certificatieschema genoemd.

1.2 Opbouw toetsmethode

Dit document bevat een eerste aanzet tot een toetsmethode met aanbevelingen op de drie aspecten norm, protocol en besturing. Dit document het bevat niet de gevalideerde en goedgekeurde norm waar een internetstemsysteem aan moet voldoen, het bijbehorende protocol of de vastgestelde besturing. De inhoud van de toetsmethode zal in een later stadium moeten worden bepaald en vastgesteld.

De toetsmethode is opgebouwd uit drie onderdelen:

- Wat is de **norm**? Definitie van de eisen, standaarden en wet- en regelgeving waartegen de kwaliteit van het internetstemsysteem wordt vastgesteld;
- Hoe wordt getoetst tegen de norm? Een **protocol** dat de wijze beschrijft waarop wordt vastgesteld dat de het internetstemsysteem daadwerkelijk voldoet aan de gestelde norm(en);
- **Besturing**: wie bepaalt de norm en protocol? Een beschrijving van eigenaarschap, rollen en verantwoordelijkheden bij onderhoud van de toetsmethode, alsmede de te betrekken belanghebbenden.



Figuur 1 Vereenvoudigde weergave certificatieschema

Een certificatieschema moet worden beschouwd als een 'levend document'. Over de jaren heen zal wet- en regelgeving veranderen, (internationale) standaarden gewijzigd worden en zullen nieuwe eisen hun intrede doen en oude vervallen. Ook het protocol zal aangepast (moeten) worden aan vernieuwingen in het internetstemsysteem en aan vernieuwingen in testmethoden. In de toetsmethode is daarom specifieke aandacht ingeruimd voor de besturing, die er voor dient te zorgen dat de norm en het protocol in continuïteit actueel zijn.

In de hoofdstukken 2, 3 en 4 zijn de aspecten norm, protocol en besturing van de toetsmethode nader uitgewerkt.

1.3 Internationale standaardisatie / certificatieschema's

Ook in internationaal verband is en wordt gewerkt aan certificatie van systemen voor internetstemmen. Deze werkzaamheden zijn tot nu toe voornamelijk uitgevoerd door de landen die geëxperimenteerd hebben met internetstemmen of die internetstemmen als stemmethode hebben ingevoerd. Veelal is daarbij een beroep gedaan op universiteiten, onderzoeksinstellingen en onafhankelijke auditors. De opzet en inhoud van de certificatieschema's uit deze landen verschillen aanzienlijk, zowel in context waarin de eisen zijn opgesteld (hetzij vanuit een eigen ontwerp van een internetstemsysteem, hetzij vanuit generieke eisen) als de wijze waarop de eisen zijn verwoord.

Er is anno 2013 geen generiek certificatieschema voor internetstemsystemen vastgesteld door een internationale standaardisatie organisatie zoals ISO, IEC, ITU, IETF, IEEE of de CCRA.
Wel is door de Duitse Bundesamt für Sicherheit in de Informationstechnik in 2008 een Protection Profile opgesteld voor Online Voting Products conform de Common Criteria versie 3.1 Rev 2. Voor zover bekend is dit PP de enige die is opgesteld voor internetstemsystemen. Dit PP is opgesteld voor verkiezingen die plaatsvinden binnen verenigingen, besturen, universiteiten en alle andere niet-politieke officiële verkiezingen. Het PP is niet opgesteld met het oog op officiële verkiezingen voor vertegenwoordigende organen.

In overweging wordt gegeven aan het ministerie van BZK om wel een dergelijk PP op te (laten) stellen als onderdeel van de ontwerpfase van het internetstemsysteem. Mogelijk kan hierbij gebruik gemaakt kan worden van het eerdere werk dat in Duitsland is verricht.

In februari 2011 is door de Raad van Europa een rapport[1] uitgebracht met richtlijnen die door lidstaten kunnen worden gebruikt om hun eigen toetsmethode op te stellen. Bij het opstellen van deze toetsmethode is daar waar mogelijk invulling gegeven aan de aanbevelingen uit dit rapport.

Aanbevolen wordt om de definitieve versie van de toetsmethode tevens in het Engels op te stellen. Dit maakt het eenvoudiger om met andere landen kennis en ervaring uit te wisselen over de toetsmethode en het maakt de toetsmethode toegankelijker voor buitenlandse leveranciers en certificerende instanties.

1.4 Begrippen

Begrip	Toelichting
Internetstemsysteem	Een internetstemsysteem is het geheel van mensen, procedures en middelen (waaronder informatiesystemen) welke benodigd zijn om stemmen via internet mogelijk te maken.
Norm	De vastgestelde verzameling van specificaties waar het internetstemsysteem aan moet voldoen. De norm is opgebouwd uit eisen, standaarden, wet- en regelgeving en best practices.
Object	Een object is het voorwerp van de toetsing tegen de norm. Een internetstemsysteem is opgebouwd uit verschillende objecten.
Eisen	Specificaties die zijn vastgesteld door de opdrachtgever.
Standaarden	Specificaties die zijn vastgesteld door een erkend lichaam.
Best Practices	Een techniek, werkmethode, proces of activiteit die zich in de praktijk als effectief heeft bewezen en die de facto gebruikt wordt als kwaliteitsstandaard.

[1] "Certification of e-voting systems" GGIS (2010) 3 fin. E, Guidelines for Guidelines for developing processes that confirm compliance with prescribed requirements and standards. 16 februari 2011. Council of Europe, directorate general of democracy and political affairs.

2 NORM

2.1 Inleiding

De basis van de toetsmethode zijn de eisen waar het internetstemsysteem aan moet voldoen. Het totaal aan eisen wordt de norm genoemd.

Weliswaar wordt in de toetsmethode steeds gesproken over de norm waar het internetstemsysteem aan moet voldoen, maar deze is feitelijk opgebouwd uit verschillende eisen en wensen afkomstig uit wet- en regelgeving, bestekseisen, standaarden en best practices, die kunnen verschillen per object, per periode of per fase.

Dit hoofdstuk geeft aan wat minimaal vastgelegd moet worden in de norm:

a. het object waarop de norm van toepassing is;
b. de verzameling van wet- en regelgeving, (besteks-)eisen, algemene standaarden en best practices waar het object aan moet voldoen.

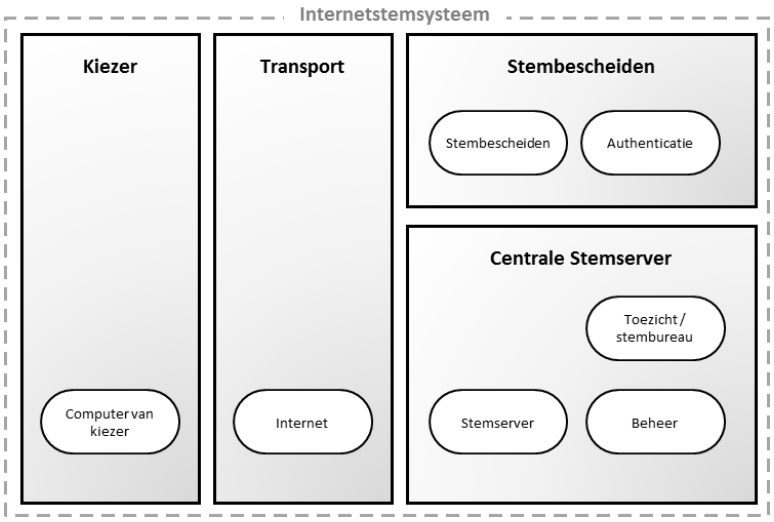
Daarnaast wordt stilgestaan bij specifieke kenmerken van de norm: de wijzigingsfrequentie en de actualiteit. Deze versie van de toetsmethode beschrijft niet uitputtend alle objecten of de inhoud van de norm zelf. Die invulling kan pas geschieden als het ontwerpproces van het internetstemsysteem afgerond is en dient te worden vastgesteld conform het besturingsproces (zie hoofdstuk 4).

2.2 Te toetsen objecten

In de toetsmethode moet duidelijk worden aangegeven of een norm van toepassing is op het gehele internetstemsysteem, of dat de norm alleen van toepassing is op een specifiek onderdeel.

Deze onderdelen worden in de toetsmethode aangeduid als *objecten* en *domeinen* (verzameling van objecten).

Een typische opbouw van een internetstemsysteem is weergegeven in figuur 2. Hierbij wordt onderscheid gemaakt naar de domeinen kiezer, transport, registratiesysteem en internetstemsysteem.



Figuur 2 Domeinmodel internetstemmen

In de navolgende paragrafen is per domein een nadere uitwerking gegeven en zijn voorbeelden van mogelijke normen geschetst.

2.2.1 Domein kiezer

Vanuit het oogpunt van normering vormt het domein van de kiezer een bijzondere uitdaging aangezien enerzijds het nodig is om eisen te stellen aan de middelen die de kiezer gebruikt bij het stemmen, maar anderzijds het vanuit het oogpunt van de waarborgen van toegankelijkheid en beschikbaarheid ongewenst is om eisen te stellen die de locatie, omgeving of de te gebruiken middelen te sterk inperken. Daarnaast is de computerconfiguratie die de kiezer gaat gebruiken vooraf niet bekend en is de variëteit van configuraties ook nog eens zeer groot.

2.2.2 Domein transport

De overdracht ('transport') van de stem van de kiezer naar het centrale deel van het internetstemsysteem verloopt via het publieke internet. Inherent aan de wijze waarop het internet functioneert is het op voorhand niet bekend welk deel van het internet gebruikt gaat worden voor het transport van de stem, dat is immers afhankelijk van de locatie van de kiezer en de routeringsprotocollen in de routers op het internet.

Aanbevolen wordt om geen specifieke eisen te stellen aan die delen van het internet die niet kunnen worden afgedwongen vanuit het centrale stemserver domein van het internetstemsysteem. Eisen aan tussenliggende internet service providers e.d. zijn in de praktijk niet af te dwingen.

Wel kunnen standaarden worden gekozen als onderdeel van het technische ontwerp van een internetstemsysteem, die bijvoorbeeld aansluiten bij algemene IETF of W3C internetstandaarden, zoals de te gebruiken protocolstack op transport of applicatie laag, specifieke beveiligings-protocollen zoals TLS/SSL, etc.

2.2.3 Domein stembescheiden

De productie en verzending van de stembescheiden wordt gezien als een separaat object binnen het internetstemsysteem waaraan specifieke eisen zullen worden gesteld.

Dit geldt ook voor het authenticatieproces, waarmee in dit domeinmodel zowel het aanvraagproces, de productie van het authenticatiemiddel als het uitgifteproces van het authenticatiemiddel wordt bedoeld. Hier is de aanname gedaan dat de authenticatie zelf onderdeel uitmaakt van het domein centrale stemserver. Het is overigens ook denkbaar dat in het ontwerp van het internetstemsysteem gekozen wordt voor een publiek authenticatiesysteem, waarbij de aanvraag en uitgifte van het authenticatiemiddel buiten het domein van het internetstemsysteem komt te liggen. In dat geval zal de centrale stemserver de authenticatie 'uitbesteden' aan het publieke authenticatiesysteem.

2.2.4 Domein Centrale Stemserver

Het centrale stemserverdomein van het internetstemsysteem bevat alle mensen, procedures en middelen (waaronder informatiesystemen) die aan de 'centrale kant' benodigd zijn voor onder andere de website van de internetstemming, voor de functionaliteit om kiezers te authenticeren en te autoriseren, voor het tonen van de kandidaten, voor het ontvangen van de uitgebrachte stemmen en tenslotte voor het tellen van de stemmen.

In dit domein worden (meest waarschijnlijk) meerdere informatiesystemen gebruikt voor verschillende functies van het verkiezingsproces. Sommige eisen uit de norm zullen van toepassing zijn op het geheel van objecten dat samen het internetstemsysteem vormt, andere eisen hebben betrekking op specifieke onderdelen. Juist omdat het internetstemsysteem gekoppeld is aan het internet, is het gewenst om het exacte demarcatiepunt[2] te bepalen waar het internetstemsysteem ophoudt, en waar het publieke internet begint.

2.3 Fasering

Bij het bepalen van de norm is niet een onderscheid naar objecten van belang, maar ook de fasering in de *levenscyclus* van deze objecten. Aanbevolen wordt om hierbij onderscheid te maken naar minimaal vier fasen:

i. Verwerving en ontwikkeling
ii. Installatie
iii. Productie
iv. Afbouw

[2] Bijvoorbeeld een ethernet koppelvlak in een router of firewall

VERWERVING EN ONTWIKKELING

In deze fase zijn normen van toepassing die in belangrijke mate op het object zelf betrekking hebben alsook op de *verwerving* of *ontwikkeling* van het object. Onder ontwikkeling wordt in deze context ook onderhoud en doorontwikkeling verstaan.

Het serverdomein bestaat uit diverse objecten die elk bepalend zijn voor de correcte werking van het totale systeem. Het betreft hier objecten zoals de 'stembus', de telprogrammatuur om de stemmen te tellen en de programmatuur voor de uitslagberekening.
Vanwege de grote impact op de kwaliteit van het totale internetstemsysteem dienen eisen gesteld te worden aan:

- Het **ontwikkelproces**. Dit begint bij de wijze waarop de specificaties tot stand komen en goedgekeurd worden, autorisatie van programmeurs, de gebruikte software ontwikkelomgeving, kwaliteitsmanagement, documentatieproces, compilatie en versiebeheer.
- Het **programmeren**. Hierbij zijn eisen relevant op het gebied van onder andere software architectuur, veilig programmeren, authenticatie, configuratie management, defensief programmeren (foutafhandeling, input validatie) etc.
- Het **testproces**. Interne procedures bij de ontwikkelorganisatie die maakt dat code getest en gecontroleerd wordt alvorens het wordt opgenomen in een build.
- **Beveiliging van de ontwikkeling**. Waarborgen dat de programmatuur geen ongewenste functionaliteit bevat die manipulatie van stemmen of uitslag mogelijk maakt, dat traceerbaar is wie welke code heeft geprogrammeerd / gewijzigd, toegangsbeveiliging tot de ontwikkelomgeving, borgen dat geen andere versie gebruikt later wordt in het productiestadium, back-up functionaliteit en procedures in het ontwikkelproces, organisatorische normen voor screening, geheimhouding en functiescheiding, etc.

Voor dit type eisen zijn diverse algemene standaarden voorhanden op het gebied van software kwaliteit, standaarden voor Secure Software Development (o.a. ISO/IEC 27034-1) en actuele 'secure programming' richtlijnen (bv. OWASP[3]). Ook vanuit het CIP zijn aanbevelingen opgesteld voor Secure Software Development, zie hiervoor onder andere het rapport "Grip op Secure Software Development"[4]
Deze standaarden ondersteunen bij het ontwikkelen en testen van programmatuur die moet voldoen aan zeer hoge integriteitseisen.

Indien de objecten worden verworven met een aanbesteding, dan is het aanbestedingsdocument en het bijbehorende (concept)contract de (juridische) plek om de leverancier de norm te laten accepteren en om later naleving van de norm te kunnen afdwingen. Hierbij zal een balans moeten

[3] Open Web Application Security Project, www.owasp.org

[4] Grip op Secure Software Development, jan 2014, http://www.cip-overheid.nl/wp-content/uploads/2014/01/Grip-op-SSD-Het-proces-v1-0.pdf

worden gevonden tussen het enerzijds strikt willen specificeren aan welke norm de programmatuur en het ontwikkelproces moet voldoen, en anderzijds het geven van enige speelruimte aan een leverancier om eigen methoden te kunnen gebruiken.

INSTALLATIE

Onder installatie wordt verstaan het inrichten van de servers waarop de programmatuur voor internetstemmen draait. Hierbij wordt ervan uit gegaan dat servers voor iedere verkiezing opnieuw worden geïnstalleerd en ingericht (met andere woorden: tussen twee verkiezingen in is er geen internetstemsysteem beschikbaar / online, anders dan voor ontwikkeling en testen).

Bij normering kan worden gedacht aan normen met betrekking tot:

- De ruimte waar de objecten worden opgesteld / gehost, zoals geografische locatie, afscherming van andere servers / personen in een hostinglocatie, fysieke toegangsbeveiliging, inbraakbeveiliging, brandbestrijding, et cetera.
- Procedures om te borgen dat de correcte versie van programmatuur wordt geïnstalleerd.
- Procedures om de wijze van installatie te kunnen testen, zónder daarmee invloed uit te oefenen op verkiezingen (als gevolg van bijvoorbeeld het uitbrengen van teststemmen).
- Procedures die de installatie en configuratie van de apparatuur en programmatuur beschrijven.

PRODUCTIE

Onder productie wordt de fase verstaan waarbij de objecten gebruikt worden voor een officiële verkiezing. De eisen die verband houden met deze fase zijn onder andere:

- Alle wettelijke, inhoudelijke / functionele, beveiligings- en kwalitatieve eisen aan het internetstemsysteem zelf.
- Eisen ten aanzien van het functionele en systeembeheer van het internetstemsysteem.
- Eisen ten aanzien van de beveiliging van de locaties en beveiliging van het functionele en systeembeheer van het internetstemsysteem.
- Procedures en alternatieven in geval van verstoringen / incidenten.

AFBOUW

Na afloop van het onherroepelijk vaststellen van de verkiezingsuitslag wordt het internetstemsysteem afgebouwd en ontmanteld. Relevante eisen voor die fase zijn:

- Procedure voor het veiligstellen van (log-)bestanden voor eventuele audits of forensisch onderzoek.
- Eisen voor het veilig afvoeren/vernietigen van gebruikte informatiedragers (harddisks, USB sticks, smart cards, back-ups).
- Eisen voor (niet) toegestaan hergebruik van programmatuur en apparatuur.
- Procedures voor evaluatie en vastlegging van leerpunten ten behoeve van de doorontwikkeling van programmatuur voor volgende verkiezingen.

2.3.1 Domein toezicht

De eisen aan het toezicht op het correcte verloop van de verkiezingen zijn vastgelegd in de Kieswet en mogelijk aanvullend in de Administratieve Organisatie / Interne Controle documentatie van het internetstemsysteem.

Aanvullend zijn eisen benodigd voor het toezicht op eventuele beheeractiviteiten in de installatie, productie en afbouw fasen.

Vanuit het oogpunt van transparantie, integriteit en controleerbaarheid kan overwogen worden om meerdere organisaties uit te nodigen om de uitslag te berekenen, met door hen zelf te ontwikkelen programmatuur.

2.4 Norm blijft in ontwikkeling

In de landen waar meerdere experimenten zijn gehouden met internetstemmen is de ontwikkeling van het internetstemsysteem eerder een continue proces geweest dan een eenmalige exercitie. In sommige landen is het internetstemsysteem na het eerste experiment zelfs volledig opnieuw ontwikkeld. Deze doorontwikkeling is deels het gevolg van wijzigingen van de norm, op grond van de evaluatie van eerdere experimenten / verkiezingen of van leerervaringen uit andere landen. De internationale uitwisseling van ervaringen met andere landen draagt bij aan het actualiseren en onderhouden van de normen. Uiteraard moet hierbij rekening worden gehouden met de verschillen in verkiezingswetgeving en verkiezingssystemen per land. Nieuwe inzichten op het gebied van informatiebeveiliging kunnen ook leiden tot nieuwe of aangescherpte normen. Denk bijvoorbeeld aan strengere eisen rondom cryptografische algoritmes.

Als de norm frequent wordt gewijzigd kan verwarring kan ontstaan bij zowel leverancier als toetsende instantie tegen welke norm het internetstemsysteem (of een deel daarvan) moet worden getoetst. Dit stelt in die zin ook eisen aan de toetsmethode zelf, dat onder strikt versiebeheer moet staan, en aan de communicatie over wijzigingen in de norm.

3 PROTOCOL

3.1 Inleiding

Dit hoofdstuk geeft aanbevelingen voor de wijze waarop de toetsing tegen de norm moet plaatsvinden.

3.2 Onafhankelijkheid van toetsing

De toetsende instantie dient onafhankelijk te zijn van zowel leverancier als overheid. Om die reden mag de organisatie geen onderdeel uitmaken van de organisatie van de leverancier of van de overheid. Ook is het vanuit het oogpunt van onafhankelijkheid ongewenst als er financiële of aandeelhoudersrelaties zijn tussen leverancier en de toetsende organisatie of daaraan gelieerde organisaties (zoals holding of dochterorganisaties).
Aanbevolen wordt dat de financiële compensatie voor de toetsing niet afhankelijk is van het oordeel van de toetsing.

De eisen waaraan een toetsende instantie en de personen die als auditor optreden moeten voldoen worden vooraf gespecificeerd en publiek gemaakt. Het protocol ziet er op toe dat selectie van de instantie en auditor plaatsvindt tegen deze eisen.

3.3 Certificatie

Voor de toetsing zijn meerdere methodes gangbaar;

- Eigen verklaring: de leverancier verklaart zelf dat hij voldoet aan een publieke norm,
- Certificatie: de leverancier geeft opdracht aan een certificerende instantie om zijn product te laten toetsen tegen de norm, of
- Acceptatieprocedure: de afnemer (de overheid) geeft opdracht aan een onafhankelijke instantie om het product te toetsen tegen de bestekeisen als onderdeel van de acceptatieprocedure.

De eerste methode is zeer gangbaar voor het goedkeuren van consumentenproducten, zoals het CE-keurmerk dat aangeeft dat een product voldoet aan de Europese richtlijnen voor veiligheid, gezondheid en milieu. Een bekend voorbeeld van de tweede methode is het Kema-keurmerk voor elektrische veiligheid tegen internationale normen. De derde methode wordt met name gebruikt in projecten of (eenmalige) producten die voor een specifiek doel ontworpen zijn. Maar ook op het vlak van geneesmiddelen wordt (een variant van) de derde methode gebruikt; alvorens een geneesmiddel in Nederland mag worden verhandeld dient een registratie (en daarmee een handelsvergunning) te worden verkregen van het College ter Beoordeling van Geneesmiddelen.

In het geval van een internetstemsysteem wordt aanbevolen om de acceptatieprocedure te kiezen. Een eigen verklaring geeft gelet op het belang en de risico's onvoldoende garantie dat aan de norm is voldaan. Certificatie in opdracht van een leverancier is in principe mogelijk, maar wordt meestal toegepast in situaties waar het afdoende is om een eenmalige type-certificering te verkrijgen (en niet alle exemplaren van het product getoetst hoeven te worden). Certificatie is in

feite een eenmalige toets, waar meerdere afnemers gebruik van maken zodat ze niet zelf hoeven te toetsen. Certificatie wordt bemoeilijkt doordat een internationale norm waartegen een internetstemsysteem kan worden gecertificeerd nog ontbreekt. Het is ook niet waarschijnlijk dat in een dergelijke norm de precieze Nederlandse situatie en alle specifiek door de Nederlandse overheid gestelde eisen zijn vervat.

De methode waarbij de afnemer (de overheid) opdracht geeft aan een onafhankelijke instantie om het internetstemsysteem te toetsen tegen de norm als onderdeel van de acceptatieprocedure is het meest geschikt..

3.4 Moment van toetsen

De verwachtte doorlooptijd van een toetsingstraject van een compleet internetstemsysteem is aanzienlijk en ligt in de ordegrootte van meerdere maanden. Dit betekent dat het traject ruim voor de verkiezing moet worden opgestart én worden afgerond, zodat er voldoende tijd is om gebreken te verhelpen en een herkeuring uit te voeren. De acceptatie kan ook in delen worden afgegeven, bijvoorbeeld per fase (verwerving en ontwikkeling, installatie, opbouw, afbouw). De doorlooptijd van de toetsing kan verder worden verkort door op onderdelen toe te staan om alleen een hertoetsing te doen van aangepaste onderdelen, of door het accepteren van deel-certificaten op onderdelen (die bijvoorbeeld in het buitenland al zijn gecertificeerd).

Tussentijdse verkiezingen

In geval het kabinet besluit om tussentijdse verkiezingen voor de Tweede Kamer uit te schrijven is de beschikbare tijd om een internetstemsysteem op dat moment nog te toetsen te kort. Indien op het moment van uitschrijven van de verkiezing geen reeds geaccepteerd (of gecertificeerd) internetstemsysteem voorhanden is, is stemmen via internet niet mogelijk. Dit probleem treedt met name op indien net besloten was om de norm aan te passen of indien om een andere reden besloten is tot doorontwikkeling van (onderdelen van) het internetstemsysteem.
Om toch internetstemmen mogelijk te maken bij tussentijdse verkiezingen zal gewerkt moeten worden met een parallel ontwikkelings- en toetsingstraject *naast* het bestaande, goedgekeurde, productiesysteem. Mochten er dan tussentijdse verkiezingen worden uitgeschreven dan kan altijd met het bestaande productiesysteem de verkiezing worden uitgevoerd. Hierbij geldt één kanttekening: als tussentijds de norm is aangepast om dwingende redenen (bijvoorbeeld vanwege wijzigingen in de kieswetgeving, of gegeven nieuwe betrouwbaarheidseisen), dan kan het bestaande systeem niet worden gebruikt (ook al voldoet deze aan de oude norm).

3.5 Frequentie

De Raad van Europa adviseert de internetstemvoorziening voorafgaand aan iedere verkiezing te beoordelen en daarnaast op het stemproces (vanaf het opbouwen van de voorziening tot en met de afbouw en rapportage) een procesaudit, validatie en evaluatie uit te voeren. Daarnaast dient de voorziening voor internetstemmen (specifiek de servers en applicatie) ook periodiek – bijvoorbeeld jaarlijks – beoordeeld te worden om extra toe te zien op tussentijdse ontwikkelingen en wijze waarop met verbeterpunten om wordt gegaan. De beoordeling voorafgaand aan

verkiezingen kan daarmee mogelijk met een kortere doorlooptijd worden uitgevoerd wanneer resultaten uit de periodieke beoordeling hierin worden meegenomen.

3.6 Diepgang

De te hanteren acceptatietesten en diepgang daarvan moeten per object en per fase van de levenscyclus vooraf bepaald worden, op basis van de aard van het object en de risico's die volgen uit een risicoanalyse. De wijze van toetsen en testen wordt bepaald door de organisatie die de acceptatietesten uitvoert in overleg met de opdrachtgever.

3.7 Rapportage

De bevindingen uit de beoordeling (waaronder de geconstateerde tekortkomingen en verbeterpunten) worden gerapporteerd aan de opdrachtgever. De rapportage dient ook al het bewijsmateriaal te bevatten, zodat een geïnteresseerde derde partij de bevindingen kan reproduceren en de conclusies kan verifiëren.

De opdrachtgever bepaalt binnen zijn verantwoordelijkheid en mandaat hoe hij omgaat met de bevindingen en welke consequenties hij hieraan verbindt in zijn besluit om een internetstemsysteem toe te staan.

3.8 Openbaarheid

In het protocol wordt vastgelegd of en welke informatie rondom de toetsing openbaar is. De rapportage van de toetsende instantie wordt opgeleverd aan zowel de leverancier die het systeem ontwikkelt als aan de overheid als opdrachtgever.

Aanbevolen wordt om de rapportage openbaar te maken voor zover het een object (en de versie van het object) betreft dat daadwerkelijk wordt ingezet in het internetstemsysteem. Aanbevolen wordt om (tussentijdse) bevindingen die betrekking hebben op niet definitieve versies van een object, en die geen onderdeel uitmaken van het internetstemsysteem, niet te openbaren.

Speciale aandacht is nodig voor onderdelen van het internetstemsysteem waarop intellectuele eigendomsrechten rusten, of waarvoor non-disclosure agreements gelden. Aanbevolen wordt om reeds in de contractering te regelen dat het finale rapport openbaar kan worden gemaakt.

4 BESTURING

4.1 Bevoegdheid tot opstellen en vaststellen van de norm en het protocol

Voor het verkrijgen van een algemeen vertrouwen in internetstemmen als stemmethode is het noodzakelijk dat het internetstemsysteem voldoet aan alle gestelde eisen. Dat vereist ook dat de norm en het protocol niet ter discussie staat en dus een brede acceptatie geniet.

Dit raakt het onderwerp van de besturing van de toetsmethode; wie gaat er over de norm en het protocol? Wie is bevoegd om deze vast te stellen en hoe wordt het gewenste brede draagvlak bereikt?

Het ligt voor de hand dat het ministerie van BZK als verantwoordelijk ministerie, als opdrachtgever voor de verwerving van een internetstemsysteem en als wetgever zeggenschap verkrijgt. Gelet op de complexiteit van een internetstemsysteem is het aannemelijk dat het ministerie een beroep doen op specifieke externe deskundigheid. Hierbij moet worden bewerkstelligd dat deze externe deskundigen in een positie worden gebracht waarin zij ook minimaal *mede-verantwoordelijkheid* dragen voor een kwalitatief hoogwaardige toetsmethode die ook in praktische zin implementeer is tegen redelijke kosten.

Idealiter zou ook de Tweede Kamer als vertegenwoordigend orgaan een rol moeten vervullen in de besturing. In het Nederlandse parlementaire stelsel en organisatie is het echter (nog) niet gebruikelijk dat de Tweede Kamer een eigen ondersteunend apparaat heeft die kan participeren in het opstellen van de toetsmethode. De Tweede Kamer heeft uiteraard vanuit haar functie als mede-wetgever wel invloed op die onderdelen van de norm die in wet- en regelgeving worden vastgelegd.

4.2 Instantie Normering Internetstemmen

Aanbevolen wordt om een instantie te creëren met als taak om de norm en het protocol op te stellen en te onderhouden. De leden van deze instantie moeten worden benoemd door de minister van BZK. Eventueel kan de taak van deze instantie worden verankerd in wet- en regelgeving. Dit heeft als bijkomend voordeel dat de taak in openbaarheid wordt uitgevoerd.

Voorgesteld wordt dat de instantie een aantal werkgroepen kent, waarin minimaal de volgende expertise is verenigd:

- Een Juridische werkgroep met experts op het gebied van verkiezingen, kiesrecht, (EU) aanbestedingen en civiele rechtsgebieden (IT contracten, intellectuele eigendomsrechten).
- Een Technische werkgroep met daarin experts op het gebied van softwareontwikkeling, testen, internet, ICT en informatiebeveiliging.
- Een Verkiezingspraktijk werkgroep met daarin deskundigen op het gebied van de verkiezingspraktijk. Deze commissie richt zich op de functionaliteit van het internetstemsysteem, de procesinrichting en de praktische uitvoerbaarheid.

- Een Certificatiewerkgroep, bestaande uit deskundigen op het gebied van auditing / assurance, certificatie en internationale normering.

Overwogen kan worden om, net als in andere landen zoals Noorwegen en Estland, ook leden van politieke partijen uit te nodigen om zitting te nemen in de werkgroepen, of om als toehoorder aan te zitten bij de bijeenkomsten.

De instantie staat onder leiding van een onafhankelijk voorzitter, welke zorg draagt voor het contact met het ministerie van BZK en de afstemming tussen de werkgroepen.

De bijeenkomsten van de instantie en werkgroepen en de verslagen van alle bijeenkomsten zijn openbaar.

De experts uit de werkgroepen worden geselecteerd uit de wetenschap (hoogleraren, gerenommeerde onderzoekers), overheid en bedrijfsleven. De instantie stelt op basis van eigen inzicht en onderzoek, eerdere evaluaties, internationaal overleg en eventueel marktconsultaties de norm en het protocol op.

De toetsmethode wordt uiteindelijk vastgesteld door de minister van BZK.

4.3 Aanstelling toetsende organisatie(s)

Aanbevolen wordt dat het ministerie van Binnenlandse Zaken en Koninkrijksrelaties de selectie uitvoert van de toetsende organisatie of organisaties. Conform de aanbevelingen van de Raad van Europa wordt een organisatie aangewezen voor een bepaalde termijn. Aanbevolen wordt om deze termijn op 6 jaar te zetten. In een periode van 6 jaar worden normaliter minimaal drie verkiezingen (TK en EP) gehouden.

In het contract met de toetsende instantie wordt de toetsmethode als basis gebruikt voor het specificeren van de werkzaamheden van de toetsende organisatie. Verder is het aan te bevelen om ook afspraken te maken over bewijslast, vertrouwelijkheid, toegang tot informatie, beschikbaarheid van personeel en aansprakelijkheid (bij onjuist uitvoeren van toetsing)

4.4 Kosten

4.4.1 Kosten Instantie Normering Internetstemmen

Aanbevolen wordt om de uitgaven voor het opstellen en onderhoud van de toetsmethode te bekostigen uit de begroting van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Aanbevolen wordt om aan het verkrijgen van de norm(en) en het protocol geen kosten te verbinden. Dit vergroot de toegankelijkheid en transparantie. Eventuele documentatie, (test)bestanden en/of (test)programmatuur kunnen via internet beschikbaar worden gesteld.

4.4.2 Kosten toetsing

Aangenomen wordt dat delen van het internetstemsysteem ontwikkeld en geleverd worden door private organisaties (leveranciers). Aanbevolen wordt om de kosten die de toetsende organisatie in rekening brengt voor het onderzoek en het verlenen van een goedkeurende verklaring voor rekening van de overheid te laten komen, daar deze onderdeel zijn van de acceptatieprocedure.

De kosten die de overheid (als afnemer van het product / dienst) maakt om eigen testen uit te voeren komen voor rekening van de overheid.

Indien de overheid het internetstemsysteem in eigen beheer ontwikkelt is ook zij gehouden een goedkeuring te verkrijgen en draagt zij de kosten zelf.

4.5 Evaluatie werking toetsmethode

Na afloop van iedere verkiezing wordt de werking van de toetsmethode geëvalueerd of zoveel vaker als door de Instantie Normering Internetstemmen wordt besloten. Zij betrekt bij de evaluatie relevante stakeholders, zoals het ministerie van BZK, betrokken leverancier(s) en de Kiesraad. De evaluatie wordt uitgevoerd door een onafhankelijke organisatie. Het evaluatierapport wordt openbaar gemaakt.