Council of the
European Union

Brussels, 21 October 2016
(OR. en)

13434/16

LIMITE

CYBER 115
COPEN 304
ENFOPOL 364

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	12368/16
Subject:	Encryption of data: Mapping of the problem - orientation debate

Delegations will find in annex a discussion paper to facilitate the debate on the issues related to encryption following the answers to the questionnaire provided by Member-States.

ANNEX

Encryption: mapping of the problem

1. The internet has changed the way the world communicates today where encryption technologies are becoming globally part of these new communication models. The use of encryption serves both the legitimate needs for privacy and security and the exercise of the fundamental rights of individuals as well as those needs of business and governments for a safe and secure cyberspace. Businesses have started investing and/or are developing tools to offer the best possible protection using strong encryption for their customers' privacy and to increase cyber security. Any effort to weaken encryption or security protocols in general may not only expose people's private or sensitive business information to the abuse by other parties, but can also introduce major cyber security risks.

2. In practice, anyone can use encryption in order to secure and protect his or her personal data and/or communications. Secure processing is an important element of personal data protection, and encryption is recognised as one of the security measures in the recently adopted General Data Protection Regulation. Companies, public administrations and individuals are encouraged to use encryption to protect their data and electronic communication. The e-Privacy Directive also encourages the use of encryption technologies to protect users' communications. However, the opportunities offered by the encryption technologies are also exploited by criminals in order to hide their data and potential evidence, protect their communications and mystify their financial transactions.

3. According to the Europol iOCTA 2016 strong encryption is highly important to e-commerce and other cyberspace activities, but adequate security depends on law enforcement authorities having the ability to investigate successfully criminal activity. The use of encryption deprives law enforcement of crucial evidential opportunities, especially given the fact that it is no longer restricted to desktop computers but increasingly available on mobile devices and many commercially available communication platforms have now encryption-by-default (increasingly by way of end-to-end encryption leading to situations where services are not interceptable).

4. On 2 June 2016 Eurojust organised a strategic seminar on the topic "Keys to Cyberspace", where experts exchanged information on various issues, including encryption. Discussion focussed mainly on access to locked mobile devices and in particular on the opportunity to use previously collected fingerprints of a suspect person to open a locked device in order to access data. There was an overall agreement on the need to protect privacy of citizens including by means of encryption, but a careful balance should be struck between this need and the need to fight crime ensuring thereby a higher level of security of all citizens.

5. Given the increasing relevance of the matter, the informal meeting of the Justice Ministers in July this year held a political discussion dedicated to encryption. It resulted in recognition of the problems posed by it and a mandate to continue to explore it. Different opinions on what approach to be used were expressed ranging from preserving the status quo in respect to privacy and business standards to finding more efficient tools for law enforcement authorities and even expanding the solutions to other areas, beyond the criminal justice.

6. To follow-up the political discussion outcome, the Presidency decided to gather more in-depth information though a questionnaire in order to assess the current situation from the perspective of law enforcement authorities in the Member States and on that basis consider possible lines for further steps.

7. Replies were received from 25 Member States and Europol. They reveal the following features commonly shared by the majority of Member States:

- encryption is encountered often or almost always in the context of criminal investigations. (Only 5 delegations stated to encounter it rarely);

- experience is present both with regard to online (in the form of encrypted emails or other forms of e-communication and/or commercial applications such as Facebook, Skype, WhatsApp or Telegram) and offline encryption (most often criminal investigation involving encrypted digital devices and encrypting applications).

- neither the suspect, nor the accused who is in possession of a digital device/electronic data are under the legal obligation to provide to the law enforcement authorities the encryption keys/passwords, in most cases due to the right against self-incrimination. However, in some Member States different legislative approaches have been taken providing such possibilities either with respect to the suspect and/or third persons.

- service providers are obliged according to national law to provide law enforcement authorities with encryption keys/passwords; a judicial order is not always required. However, in general, the answers do not make a distinction whether this obligation applies only to the providers of electronic communications services or encompasses also the providers of information society services.

- interception/monitoring of encrypted data flows is possible under certain conditions prescribed in the national law with the aim of obtaining decrypted data; a prior judicial order is often required.

- the national legal framework aimed at securing of electronic evidence when encrypted is considered sufficiently effective [in contrast to the general legal provisions on e-evidence].

- the lack of sufficient technical capacity both in terms of efficient technical solutions to decrypt and respective equipment is among the top 3 challenges, followed by the lack of sufficient financial resources and personal capacity (both in terms of numbers and training of staff).

- the need for practically orientated measures prevailed over the need for adoption of new legislation on EU level (with the exception of one delegation that identified such need in the areas of data retention and lawful interception).

8. Any steps taken in the future should consider the political setting defined by the Council Conclusions on improving criminal justice in cyberspace and on the European Judicial Cyber Network, both adopted by the June (JHA) Council under the NL Presidency, and the respective ongoing processes stemming from them:

- on e-evidence given that fact that a significant amount of electronic data is encrypted;

- on establishing a cooperation framework with service providers given their pivotal role;

- on operationalising the judiciary dealing with cyber/cyber-enabled cases or investigations in cyberspace by providing them with a special forum for exchange of specialised expertise in support of execution of their functions.

9. The European Judicial Cybercrime Network (EJCN) will start its work on 24 November 2016 and encryption is one of the main topics of the meeting. It is presumed that the EJCN will closely analyse the obstacles to effective cybercrime investigations, including various aspects of encryption and to share best practices in this field.

10. Against this background the Presidency would like to propose the following steps to be considered by delegations as possible approach to be taken in the future with regard to encryption:

A. *Launch a reflection process on the issues related to encryption, taking into account the progress and integrating the outcome, where relevant, of the*:

- ongoing expert process on e-evidence launched by the Commission as a follow-up to the June Council Conclusions on improving criminal justice in cyberspace due their interlinkages and interdependencies as well as the need for cooperation with the service providers; and

- process for developing a common framework for cooperation with the service providers for the purpose of obtaining specific categories of data;

in order to define practical solutions that would allow for the possible disclosure of encrypted data/devices through an integrated EU approach and framework.

B. *Explore further the possibilities for improving the technical expertise both at national and EU level, inter alia by enhancing the technical capabilities already available within Europol and encouraging their use by Member States in the respective limits of its mandate as well as Europol's further development as an European Centre of expertise on encryption. The assistance of the other relevant EU entities, as for example ENISA, could also be considered.*

C. *Encourage the members of the European Judicial Cybercrime Network (EJCN) to bring to its forum also the practical aspects related to encryption for discussion, exchange of information, good practices and expertise. Close cooperation and consultations with Europol, Eurojust and EJCN seems to be vital to meet the challenges stemming from encryption.*

D. *Deepen the practical aspects of the encryption related trainings for law enforcement authorities provided by EU entities and increase the capacity building efforts to ensure that practitioners have an appropriate and up-to-date knowledge and resources to obtain and handle digital evidence.*

After fine-tuning the outcome to reflect the Member States' views expressed during the FOP meeting, the Presidency intends to present these steps to CATS in preparation for the (JHA) Council in December.