



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 27 June 2002

10394/02

**ENFOPOL 99
COMIX 426**

NOTE

from :	incoming Danish Presidency
to :	Police Cooperation Working Party
No. prev. doc. :	OJ C 19, 23.1.1999, p.1
Subject :	Electronic exchange of information between law enforcement authorities of the Member States

1. Background.

At the meeting of the European Council in Vienna 11 – 12 December 1998 the Heads of State and Government approved a five-year action plan for the implementation of an area of freedom, security and justice. The action plan sets out a number of measures to be adopted within a two-year period and a five-year period respectively from the entry into force of the Amsterdam Treaty on 1 May 1999 (OJ C 19, 23.1.1999, p.1).

The European Council in Tampere 15 – 16 October 1999 furthermore decided on a number of political guidelines and priorities concerning the co-operation on justice and home affairs, including the implementation of the Vienna Action Plan from 1998 (SN 200/99).

At the European Council in Laeken 14 – 15 December 2001 the Heads of State and Government had an in depth discussion on the results achieved regarding the implementation of the conclusions from the European Council in Tampere. In that connection the European Council set out further guidelines in relation to the implementation of the Tampere conclusions (SN 300/01).

The incoming Danish Presidency intends to continue the implementation of the Vienna Action Plan based on the political priorities and guidelines decided by the European Council and results achieved during previous presidencies.

One of the priorities of the incoming Danish Presidency will be **electronic exchange of information between law enforcement authorities of the Member States**.

2. A Danish proposal for a Council decision regarding electronic exchange of information between law enforcement authorities of the Member States.

In order to continue the implementation of the Vienna Action Plan based on the political priorities and guidelines decided by the European Council and results achieved during previous presidencies, Denmark will table a proposal for a Council decision regarding electronic exchange of information between law enforcement authorities of the Member States to be discussed in the Police Co-operation Working Group during the second half of 2002.

The Council decision will be a further development of the Schengen Agreement - in particular Article 39 – and will be based on the Treaty on European Union (TEU), article 30(1)(a)(b) and article 34(2)(c). In accordance with TEU, article 39(1), the European Parliament will be asked for its opinion on the Danish proposal (OJ L 239, 22.9.2000, p.19).

When relevant for a specific investigation or prosecution a Member State in accordance with national law, should be able to ask other Member States by electronic means if information is available, e.g. concerning criminal records, finger prints or DNA profiles (**hit/no-hit system**). The purpose of the Danish initiative is to facilitate the exchange of this kind of information.

In case information is available in another Member State this information can be requested subsequently by forwarding a formal request in accordance with relevant international instruments and national law.

It is the intention that the proposal will create the legal basis for Member States to be able to ask other Member States by electronic means if information is available. In that connection Member States should be asked to appoint or designate contact points for communication of information between law enforcement authorities in Member States. Contact points should be able to cover all relevant law enforcement files in Member States.

At the same time it is the intention of the proposal that Member States – when requested – should be able to reply within a certain time limit, e.g. 24 hours. The question of a so called “silent procedure” could also be explored.

The proposal should be seen as a first step towards the establishment of a central European criminal record, including records on fingerprints and DNA profiles (see OJ C 187, 3.7.2001, p.1).

It is the intention of the incoming Danish Presidency to table the initiative in the beginning of the Danish Presidency in order for the proposal to be published in the Official Journal and send to the European Parliament before 1 September 2002.

3. Possible electronic systems to be used for electronic exchange of information between law enforcement authorities of the Member States.

As appropriate the possible involvement of Europol should be explored as well as the possibility of using other already existing means for exchanging information, e.g. within the framework of the Schengen co-operation and Interpol.

A number of electronic systems for the exchange of information between law enforcement authorities of Member States are already in place:

a) Interpol

Interpol currently has 179 member countries with very different levels of technological equipment. However, the European member countries all meet the same requirements in connection with the processing and communication of international police information.

The physical structure of the network is based on National Central Bureaus (NCB) of the member countries. NCB's constitute the interface between national police authorities and Interpol.

The Central Station at the General Secretariat of Interpol at Lyon manages the flow of traffic between the different Regional Stations and at the same time serves as Regional Station for Europe.

The technical solution is a mail system based on the international message-handling standard **X.400**. All EU Member States have installed X.400 equipment and the message server at the General Secretariat conforms to the X.400 standard.

The network is secured by an encryption system that can be adapted to all microcomputer-based equipment. It does not require any modifications to the X.400 server.

This telecommunications network can handle information in various forms such as typed texts, texts with graphs, diagrams and tables, images (i.e. counterfeit notes, fingerprints, photographs), combinations of texts and images (notices). In accordance with national law and international instruments the information can subsequently be used for consultation of centrally stored data and criminal records including data on previous convictions.

A new communication standard intended to replace the international message-handling standard X.400 is currently being developed. At the moment it cannot be foreseen when the new standard will be available to Member States.

The Automated Search Facility (ASF) has been developed with a view to establish a computer-based system, which allows connected NCB's to consult a database automatically via a server located at the General Secretariat.

Information sent by the NCB's is – with the prior consent of the sending country – introduced into the database on a daily basis.

Connected NCB's can search in the database with a view to identify suspected individuals based on several criteria including phonetic, known aliases, passports and identity documents. The system also allows for the transmission of photographs and fingerprints together with an international notice in English, French, Spanish or Arabic.

Information on stolen vehicles and stolen objects of art is also stored in the database.

Access to the central ASF server may be obtained using public switched telephone networks, packet-switching data networks (X.25) or an integrated services digital network.

All EU Member States are connected to ASF.

Automated Fingerprint Identification System (AFIS) is a system of national electronic databases on fingerprints at the national central units for the identification of fingerprints and one at the General Secretariat. AFIS allows for an electronic search for fingerprints. Fingerprints are forwarded electronically via the NCB's. A computer "hit" will subsequently have to be analysed manually and visually for positive identification.

All EU Member States have acquired the system.

b) Co-operation within the framework of the Schengen Agreement

Schengen Information System (SIS) is a computerised information system for storage and search of structured data on certain individuals and stolen goods, documents in blanc and counterfeit notes. SIS consists of a central reference database (C.SIS), a technical support facility, placed at Strasbourg and national databases (N.SIS) in Member States. SIS is part of systems of national authorities of Member States for entries and searches.

The current version of the SIS can only handle structured text and figures in formats. Photos and fingerprints cannot be exchanged electronically. The information is exchanged in the original language and another appropriate language chosen by Member States concerned.

A special electronic network connects SIRENE bureaus of Member States.

In accordance with **article 39 of the Schengen Agreement** Member States undertake to ensure that their police authorities shall, in compliance with national legislation and within the limits of their responsibilities, assist each other for the purposes of preventing and detecting criminal offences. Member States exchange information via the central units. However, information exchange with reference to article 39 can take place through direct contact between competent authorities of Member States and with parallel notification of the central unit of the Member State.

In some Member States the SIRENE bureau handles the information exchange. In other Member States a separate office handles information exchange with reference to article 39. The technical solution used for the exchange of information with reference to article 39 is the mail system based on the international message-handling standard X.400. As mentioned all EU Member States have installed X.400 equipment. However, some Member States handle information exchange with reference to article 39 by other means.

c) Europol

The physical structure of the Europol information network is based on Europol National Units and Europol headquarters via the national desks at Europol.

In order to achieve its purpose Europol maintains three systems for the storage and exchange of information.

The Information Exchange System (InfoEx) connects the national desks at Europol with their respective National Units and Europol. The system is a mail system based on a Virtual Private Network (VPN).

This information exchange system can handle information in various forms such as text-files, text with graphs, diagrams and tables, images (i.e. counterfeit notes, fingerprints, photographs), combinations of text and images and requests for consultation of centrally stored data.

The system consists of an exchange form, a Word document and attached files in any format.

It follows from the Europol Convention that **the Europol Information System (EIS)** is a computerised information system for storage and search of data concerning certain individuals, crimes and convictions (OJ C 316, 27.11.1995, p.1).

EIS consists of central servers at Europol head quarters connected to the National Units. National Units, liaison officers at the desks, the director, deputy directors and duly empowered officials have direct access to enter and search information in the EIS.

4. Presidency proposal regarding possible electronic systems to be used for electronic exchange of information between law enforcement authorities of the Member States.

Under reference to the above a feasible solution would be to create the legal basis for Member States to facilitate the exchange of information in question based on the international message-handling standard X.400 since this standard is already in place in all Member States. Thus enhancing the electronic exchange of information between law enforcement authorities of the Member States does not require the setting up of a new system.

To enable electronic exchange of fingerprints between Member States, national law enforcement authorities should send fingerprints as an attached file via the international message-handling standard X.400.

In order to exchange the information in question Member States could use already existing templates.

Since a new standard is being developed to replace the international message-handling standard X.400 and since a system for electronic exchange of fingerprints is being developed within the framework of the Schengen co-operation (SIRPIT, 9450/02 SIRENE 41 COMIX 374) , a Council Decision should be flexible regarding the technical details.

Against this background a Council Decision – as a first step – could base the electronic exchange of information between law enforcement authorities of the Member States on the international message-handling standard X.400 as described above.
