Council of the
European Union

**Brussels, 20 September 2016**
**(OR. en)**

**12368/16**

**LIMITE**

**CYBER 102**
**JAI 764**
**ENFOPOL 295**
**GENVAL 95**
**COSI 138**
**COPEN 269**

**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Delegations |
| Subject: | Encryption of data<br>- Questionnaire |

Over lunch during the informal meeting of the Justice Ministers (Bratislava, 8 July 2016) the issue of encryption was discussed in the context of the fight against crime. Apart from an exchange on the national approaches, and the possible benefits of an EU or even global approach, the challenges which encryption poses to criminal proceedings were also debated. The Member States' positions varied mostly between those which have recently suffered terrorist attacks and those which have not. In general, the existence of problems stemming from data/device encryption was recognised as well as the need for further discussion.

To prepare the follow-up in line with the Justice Ministers' discussion, the Presidency has prepared a questionnaire to map the situation and identify the obstacles faced by law enforcement authorities when gathering or securing encrypted e-evidence for the purposes of criminal proceedings.

On the basis of the information be gathered from Member States' replies, the Presidency will prepare the discussion that will take place in the Friends of the Presidency Group on Cyber Issues and consequently in CATS in preparation for the JHA Council in December 2016.

Delegations are kindly invited to fill in the questionnaire as set out in the Annex and return it by **October 3, 2016** to the following e-mail address: **cyber@consilium.europa.eu.**

**1. How often do you encounter encryption in your operational activities and while gathering electronic evidence/evidence in cyber space in the course of criminal procedures?**

○ almost always<br>
⊗ often (in many cases)<br>
○ rarely (in some cases)<br>
○ never

Please provide other relevant information:

If you have different experiences in cross-border cases, please specify:

Almost all modern phones, computers and cloud-data-spaces have some encrypted information stored in them. Many software products have automatic decryption of certain kinds of data, like credentials, passwords etc. Usually the investigation focuses on non-encrypted data. In case of full-disk encryption, which is rare, we have to either use brute force -attacks, or try to obtain the credentials some other way.

**2. What are the main types of encryption mostly encountered during criminal investigations in cyberspace?**

○ online encryption

- ○ e-mail (PGP/GPG)
- ○ SFTP
- ○ HTTPS
- ○ SSH Tunnelling
- ○ TOR
- ○ P2P / I2P
- ○ e-data stored in the cloud
- ○ e-communications (through applications such as Skype, WhatsApp, Facebook, etc.)
- ○ others? Please specify:

○ offline encryption

- ○ encrypted digital devices (mobile phone / tablet /computer)
- ○ encrypting applications (TrueCrypt / VeraCrypt / DiskCryptor, etc)
- ○ others? Please specify:

Please provide other relevant information:

If you have different experiences in cross-border cases, please specify:

We have experience in all of the abovementioned data-types, but most often we encounter encrypted data in the form of mobile devices and computer hard drives. Other encryption techniques/programs we have encouncered are Bitlocker, LUKS, EPM, Endpoint Security and Filevault.
Also, banking trojans' configuration files and command&control server communication is usually encrypted.

**3. Under your national law, is there an obligation for the suspects or accused, or persons who are in possession of a device/e-data relevant for the criminal proceedings, or any other person to provide law enforcement authorities with encryption keys/passwords? If so, is a judicial order (from a prosecutor or a judge) required? Please provide the text of the relevant provisions of your national law.**

☒ yes
○ no

Please specify: This obligation doesn't cover suspects or accused persons. A judicial order is not required.

Chapter 8, Section 23 of the Coercive Measures Act

(1) A person possessing or maintaining an information system or other person is required to provide to a criminal investigation authority at its request the passwords and other corresponding information necessary to conduct the search of data contained in a device. On request, a written certificate shall be given to the person to whom the request was made.

(2) If a person refuses to provide the information referred to in subsection 1, he or she may be heard in court in the manner provided in Chapter 7, section 9 of the Criminal Investigation Act.

(3) The provisions above in subsection 1 do not apply to the suspect in the offence nor to a person referred to in Chapter 7, section 3, subsection 1 or 2 who has the right or the obligation to refuse to testify.

**4. Under your national law, are service providers obliged to provide law enforcement authorities with encryption keys/passwords? If so, is a judicial order (from a prosecutor or a judge) required? Please provide the text of the relevant provisions.**

☒ yes
○ no

Please specify: See the answer to question 3 above.

**5. Under your national law, is it possible to intercept/monitor encrypted data flow to obtain decrypted data for the purposes of criminal proceedings? If so, is a judicial order (from a prosecutor or a judge) required?**

○ yes
○ no

Please specify: The meaning of the phrase "data flow" is unclear. According to the provisions of Chapter 10 of the Coercive Measures Act it's possible to use as covert coercive measures telecommunications interception, traffic data monitoring, on-site interception and technical surveillance of a device in criminal investigations. A judicial order from a judge is required in most cases. .

**6. What are the main issues typically encountered while intercepting/monitoring encrypted data flow in order to obtain decrypted data?**

Retrieving a decryption key is a problem. It could be acquired from the online/offline memory dump of a command & control server. However, in addition to clearing out of its location, a problem is how to take the server into possession. Server storage could be disseminated to third parties which makes locating it even more difficult. Moreover, large international service providers are not willing to disseminate the decryption keys to LEAs.

Please specify:

If you have different experiences in cross-border cases, please specify:

**7. What other approaches/techniques do you use for decrypting encrypted e-evidence and securing it so that it is admissible as evidence in the criminal proceedings? Do your authorities use e.g. the services of foreign companies or assistance from Europol for the purposes of decryption? If so, please provide examples of assistance.**

Please specify: We have collaborative efforts with other agencies of the Finnish public sector. We do not usually use private sector companies for decryption purposes, but of course a large part of the software/hardware used are commercial products.

If you have different experiences in cross-border cases, please specify:

**8. Do you consider that your current national law allows sufficiently effective securing of e-evidence when encrypted? If not, why?**

☒ yes
○ no

Please specify:

Wireless criminal intelligence gathering can be challenging, because the LE sector has limited legal rights to gather for example WIFI data.
There are usually no legal issues that would limit us in trying to decrypt any criminal case related data material that we have obtained.
The legislation offers no sanction measures to try to persuade a suspect to hand over passwords.

**9. What main issues do you typically encounter when seizing encrypted evidence and decrypting it?**

○ financial
○ personal
☒ technical
○ legal/legislative
○ others

Describe in more detail the issues identified above:

Sometimes insufficient computational capacity of our password-breaking platforms make the decrypting process too lengthy.

If you have different experiences in cross-border cases, please specify:

**10. In your view, will measures in this regard need to be adopted at EU level in the future?**

○ no EU measures are necessary
○ dedicated new legislation
☒ practical (e. g. development of practical tools for police and judicial authorities)
☒ improve exchange of information and best practices between police and judicial authorities
☒ create conditions for improving technical expertise at EU level
○ improve the (legislative) conditions of communication with service providers, including through the establishment of a legislative framework.
○ other

Please give examples: At this early stage of the discussions it's not possible to draw far-reaching conclusions concerning for example the need of legislative measures. Many diverging interests have to be taken into account and more information is needed.

**11. Are there other issues that you would like to raise in relation to encryption and the possible approach to these issues? Please share any relevant national experience or considerations arising from your practice that need to be taken into account.**