



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  
- 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
- often (in many cases)
- rarely (in some cases)
- never

Please provide other relevant information:

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

**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:

**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: No obligation for suspects/accused. For other persons, se question 4.

**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: Witnesses can be heard in court during the preliminary investigation in order to obtain encryption keys/passwords. Chapter 23, section 13, paragraph 1 "If a person refuses to make a statement concerning a matter of importance to the inquiry, and that person would be required to give testimony as a witness in the event of a prosecution, or if it is otherwise of extraordinary importance to the inquiry that a person who is obliged to testify as a witness be questioned as a witness already while the preliminary investigation is still in progress, a witness examination may be held before the court at the request of the leader of the investigation "

**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: Secret interception of electronic communications is allowed if there is a judicial order, but it is difficult to achieve the purpose of obtaining decrypted data

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

Please specify: Trying to get password information from the suspect. Sometimes this information can be obtained during interviews with the suspect, sometimes not. The necessity of speed during search and seizure operations is evident.  
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: The principle of free submission of evidence applies in Sweden, so the question of admissibility does not cause any problems.

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:

**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:

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:

**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.**