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 - 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.**

ANNEX

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?

- o almost always
- o **often (in many cases)**
- o rarely (in some cases)
- o 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?

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

- o offline encryption
  - o **encrypted digital devices (mobile phone / tablet /computer)**
  - o **encrypting applications (TrueCrypt / VeraCrypt / DiskCryptor, etc)**
  - o 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: Pursuant to Article 215 of the Criminal Procedure Code, investigative authorities and prosecutor's offices can order the production of data from any person. Suspect and accused person do not have to disclose encyption keys/passwords.

§ 215. Obligation to comply with orders and demands of investigative bodies and prosecutors' offices

(1) The orders and demands issued by investigative bodies and prosecutors' offices in the criminal proceedings conducted thereby are binding on everyone and shall be complied with throughout the territory of the Republic of Estonia. The orders and demands issued by investigative bodies and prosecutor's offices are binding on the members of Defence Forces engaged in missions abroad, if the object of the criminal proceeding is an act of a person serving in the Defence Forces. Costs incurred for compliance with a claim or ruling shall not be compensated for.

(2) An investigative body conducting a criminal proceeding has the right to submit written requests to other investigative bodies for the performance of specific procedural acts and for other assistance. Such requests of investigative bodies shall be complied with immediately.

(3) A preliminary investigation judge may impose a fine on a participant in a proceeding, other persons participating in criminal proceedings or persons not participating in the proceedings who have failed to perform an obligation provided for in subsection (1) of this section by a court ruling at the request of a prosecutor's office. The suspect and accused shall not be fined.

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:

Not directly regulated.

§ 215. Obligation to comply with orders and demands of investigative bodies and prosecutors' offices

(1) The orders and demands issued by investigative bodies and prosecutors' offices in the criminal proceedings conducted thereby are binding on everyone and shall be complied with throughout the territory of the Republic of Estonia. The orders and demands issued by investigative bodies and prosecutor's offices are binding on the members of Defence Forces engaged in missions abroad, if the object of the criminal proceeding is an act of a person serving in the Defence Forces. Costs incurred for compliance with a claim or ruling shall not be compensated for.

(2) An investigative body conducting a criminal proceeding has the right to submit written requests to other investigative bodies for the performance of specific procedural acts and for other assistance. Such requests of investigative bodies shall be complied with immediately.

(3) A preliminary investigation judge may impose a fine on a participant in a proceeding, other persons participating in criminal proceedings or persons not participating in the proceedings who have failed to perform an obligation provided for in subsection (1) of this section by a court ruling at the request of a prosecutor's office. The suspect and accused shall not be fined.

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:

§ 126[7]. Wire-tapping or covert observation of information

(1) Information obtained by wire-tapping or covert observation of messages or other information transmitted by the public electronic communications network or communicated by any other means shall be recorded.

(2) Information communicated by a person specified in § 72 of this Code or information communicated to such person by another person which is subject to wire-tapping or covert observation shall not be used as evidence if such information contains facts which have become known to the person in his or her professional activities, unless:
1) the person specified in § 72 of this Code has already given testimony with regard to the same facts or if the facts have been disclosed in any other manner;
2) a permission has been granted with respect to such person for wire-tapping or covert observation; or
3) it is evident on the basis of wire-tapping or covert observation of another person that the specified person commits or has committed a criminal offence.

(3) A preliminary investigation judge grants permission for the surveillance activities specified in this section for up to two months. After expiry of the specified term, the preliminary investigation judge may extent this term by up to two months.

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

Please specify: The main problem is that communication or data are encrypted and if key is not available, it is not possible to decrypt them.

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: During the decryption procedure, an examination report is created indicating the programs used for decryption and information found.

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: Current legislation to gather evidence can be considered sufficient. The challenges related to encryption as more or less of technical nature.

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.