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.**

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: Encryption is increasingly present due to the trend of the default data encryption on newer devices

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: Both types of encryption (online and offline) represents a challenge for the gathering of electronic data during criminal investigations in cyberspace.

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: Persons who are in possession of such devices are obligated to provide access to the data as prescribed under our national law, but suspects and accused are excluded from this obligation. Court order (or personal consent) is required to investigate the device and this also consumes the obligation to provide access (i.e. encryption keys). Failure to comply with this obligation can be sanctioned by the court.

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: Yes, but only if service providers are not also suspects or accused in the case. Judicial order from the judge (or personal consent from data owner) is required to investigate the device/hosted data.

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: This is possible under our national law, but judicial order from the judge is required.

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

Please specify: The main issue typically encountered during mentioned operations are the use of advanced cryptographic protocols and algorithms. Encrypted data is technologically hard to decrypt, therefore we have limited capabilities to obtain decrypted data.

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 mainly use specialized tools for decrypting data (different kinds of attack on encrypted data - i.e. brute force attach, dictionary attack, etc).

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: Data encryption can be a serious obstacle in the investigation. One of possible measures is a covert installation of specialized software on the suspect's device, which could potentially obtain the encryption keys and/or unencrypted data. But this option is not prescribed under our national law.

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

- o financial
- o personal
- o technical
- o legal/legislative
- o others

Describe in more detail the issues identified above: Technical and financial aspect is the main issue in these cases, since capable decrypting solutions are very expensive.

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

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

Please give examples: Dedicated and unified legislation, with established legislative framework, would improve conditions of communications with service providers. While practical tools for authorities and improved exchange of relevant information would also improve technical expertise at EU level.

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.

Technically, a powerful solution for brute-force decryption of data ("decrypting cluster") on EU-level could be a great contribution for investigations of some criminal cases.