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

CZ - DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (21.11.2016)

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?

○ almost always
○ often (in many cases)
☑**rarely** (in some cases)
○ never

Please provide other relevant information:

In many cases perpetrators combine Linux distro and anonymous services like TOR.

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:

Additional intentional encryption is quite rare in most cases although encrypted mobile phones are more and more popular among members of certain organized crime groups.

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**

There is no such an obligation for the suspects or accused persons. In our opinion, if the suspected or accused persons are concerned, such a provision would be clearly contrary to the right not to incriminate oneself and therefore contrary to the Constitution of the Czech Republic.

In case other persons are concerned than the suspects and accused persons, the application of Section 8 (1) of the Act No. 141/1961 Coll., the Code of Criminal Procedure, as amended might be considered, therefore they might be obliged to provide the requested information to law enforcement authorities. In case the information would be subject to a duty of non-disclosure, Section 8 (5) of the Code of Criminal Procedure would also apply.

Section 8 - Cooperation of Public Authorities, Natural Persons and Legal Entities

(1) Public authorities, legal entities and natural persons are obliged to comply without undue delay, and unless a special legal regulation provides otherwise, also without a consideration, with request of authorities involved in criminal proceedings in the performance of their tasks. Furthermore, public authorities are also obliged to immediately notify the public prosecutor or police authorities of facts indicating that a criminal offence has been committed.

(5) Unless a special Act stipulates the conditions under which information may be disclosed for the purpose of criminal proceedings that are deemed classified pursuant to such Act or which is subject to an obligation of secrecy, such information may be requested for criminal proceedings upon the prior consent of the judge. This does not affect the obligation of confidentiality of an attorney under the Advocacy Act.

In case a person would not cooperate without a justified reason, then they might be subject to a procedural fine according to Section 66 of the Code of Criminal Procedure.

See also answer related to service providers below.

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

In general, all subjects are obliged to cooperate with the law enforcement authorities. In addition, service providers are obliged to cooperate in a specific way specified in the Act on Electronic Communications (Act No. 127/2005 Coll., on Electronic Communications, as amended). Therefore, they are also obliged to provide data in a readable, decrypted way, if they are able to do so. There is different legislation for e.g. interceptions (judicial order required), search of an e-mail box (judicial order required) etc.

If solely the encryption keys/passwords were requested, such a request would be based on Section 8 (1) of the Code of Criminal Procedure. In practice, the encryption keys/passwords could be provided together with the content data (see above a mention of the obligation to provide readable, decrypted data – or eventually the encryption key/password) upon the request for content data. Such a request could be based on Section 158d (3) or Section 88 of the Code of Criminal Procedure.

Relevant provisions of the Act No. 141/1961 Coll., the Code of Criminal Procedure, as amended:

Section 8 - Cooperation of Public Authorities, Natural Persons and Legal Entities

(1) Public authorities, legal entities and natural persons are obliged to comply without undue delay, and unless a special legal regulation provides otherwise, also without a consideration, with request of authorities involved in criminal proceedings in the performance of their tasks. Furthermore, public authorities are also obliged to immediately notify the public prosecutor or police authorities of facts indicating that a criminal offence has been committed.

In case the information would be subject to a duty of non-disclosure, Section 8 (5) of the Code of Criminal Procedure would also apply (see above).

Section 158d - Surveillance of Persons and Items

(3) If the surveillance should interfere with inviolability of residence, inviolability of letters or if it should investigate the contents of other documents and records kept in privacy by use of technical means, it can be performed solely on the basis of a prior authorization of a judge. When entering residences, only steps related to placement of technical devices may be made.

Section 88 - Interception and Recording of Telecommunications

(2) Only the presiding judge and in pre-trial proceedings the judge upon a motion of the public prosecutor is entitled to order interception and recording of telecommunication traffic. The order to intercept and record telecommunication traffic must be issued in writing and must be justified, including a specific reference to a promulgated international treaty, if the criminal proceeding is conducted for a criminal offence, to prosecution of which is the Czech Republic bound by this international treaty. (...)

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

A judicial order is required depending on the nature of “monitoring/interception”, or, in other words, rights interfered. Please see the relevant provisions listed above. The Section 158d (3) of the Code of Criminal Procedure applies to cases of finished communication, Section 88 of the Code of Criminal Procedure applies to the cases of “live” communication (real time communication).

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

DELETED

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.

DELETED

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

DELETED

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

DELETED

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

DELETED

DELETED

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.

We strongly believe there will be a possibility for the relevant police authorities to find appropriate forum or platform for sharing sensitive information on the challenges related to encryption and decryption of data.