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?

- ○ almost always
- ☒ often (in many cases)
- ○ rarely (in some cases)
- ○ never

Suspects are increasingly using technologies to encrypt their communications and their stored data. We encounter encryption especially in cybercrime cases but also in normal cases where digital communication is used. During forensic analysis we recognise encryption also increasingly in companies. In the past, encryption and masking tools were found (Tails, TrueCrypt etc.).

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: Bitlocker, FileVault, Lux, DM-Crypt

The marked points are encountered primarily. All other techniques are also used but not as often.

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

Cf. Annex 1 at page 7.

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

No, service providers are not obliged to provide law enforcement authorities with encryption keys/passwords. Because of the principle of confidentiality of the communication and data protection reasons, service providers are only obliged to provide the law enforcement authorities certain data. For more detailed information pls see Annex 1 at page 8.

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

Austrian legal provisions per se do not distinguish between encrypted and decrypted data. However, due to technical reasons, at the present moment it is not possible to intercept/monitor encrypted data flow to obtain decrypted data for the purposes of criminal proceedings. The Federal Ministry of Justice is currently working on a draft for a new investigative measure, that would allow law enforcement authorities the interception and monitoring of (encrypted) data that is transmitted over a computer system (e.g. WhatsApp, Skype).

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

With our possibilities we are not able to decrypt, encrypted data flows in most cases.

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.

We try to decrypt seized data by doing dictionary- or brutforce-attacks. Therefore we have dedicated hardware available. We can do this for files like zip, rar, truecrypt and some other formats. In cases with high sophisticated decrypted files we ask Europol for assistance. There is also a “social approach” by questioning affected persons. So far, no assistance from external companies has been sought.

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

- ☒ yes
- ○ no

We regard seized encrypted evidence less a legal than a technical problem. However, there is a draft for a new investigative measure currently underway (cf. Question 5).

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

- ○ financial
- ○ personal
- ☒ technical
- ☒ legal/legislative
- ☒ others: time constraints

Describe in more detail the issues identified above: The keys are usually very strong. It's impossible to decrypt them in an adequate time (= technical + time issues). A legal/legislative issues exists in so far that there is no possibility to force suspects/accused persons to provide keys or passwords.

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.

-

ANNEX 1 – Questionnaire „Encryption of data“

Question 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.

Under Austrian law, suspects or accused persons are not obliged to provide law enforcement authorities with a device/e-data relevant for the criminal proceedings or encryption keys/passwords, as it is considered that such obligation would interfere with the principle of nemo-tenetur-se-ipsum-accusare (Article 90 of the Austrian Constitution, Article 6 of the European Convention on Human Rights as well as Section 7 of the Austrian Code of Criminal Procedure).
Other persons who are in possession of a device/e-data relevant for the criminal proceedings or encryption keys/passwords can be obliged to provide such devices, e-data or keys/passwords in accordance to the relevant provisions for seizures under **Section 111 of the Austrian Code of Criminal Procedure**.
Generally, the seizure is to be ordered by the public prosecutor and executed by the criminal police.

Relevant excerpt of the Austrian Code of Criminal Procedure

Under **Section 110 para 3 of the Austrian Code of Criminal Procedure**, the criminal police is entitled to seize objects at their own discretion
1. if they
    a. are under nobody’s authority to dispose
    b. have been taken from a victim of a criminal act,
    c. have been found on the crime scene and could have been used or determined to be used for committing the criminal act, or
    d. are of low value or can be easily substituted for a limited period of time,
2. if their possession is generally prohibited (section 445a para. 1),
3. that are in the possession of a person arrested for reasons of section 170 para. 1 n° 1 when arrested or that are found during a search according section 120 para. 1, or
4. in the cases of article 4 of the Council Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights.

Note: If the obtainment of relevant devices, e-data or keys/passwords requires a search of premises, a judicial approval of the issued order is needed.

Section 111
(1) Every person who possesses objects or assets to be seized is obliged (section 93 para. 2) to hand them over to the criminal police if requested so or to ensure the seizure in

any other way. This obligation can be executed by force if necessary by searching the persons or domiciles. In this case sections 119 to 122 are to be applied analogously.
(2) If information stored on data carriers is to be seized anyone has to grant access to this information and on request hand over or produce an electronic data storage medium in a file format commonly used. Moreover he/she has to abide the creation of a backup copy of the data stored on the data storage medium.
(3) To persons that are not accused of the criminal act themselves the appropriate and common costs necessarily incurred to them by the separation of documents or other objects of evidence from other things or by handing over copies have to be refunded on their application.
(4) In any case the person affected by the seizure has to be given or served a confirmation of the seizure immediately or at the latest within 24 hours that also informs them about their right to object (section 106). In case of a seizure in order to secure civil rights claims (section 110 para. 1 n° 2) the victim has to be informed if this is possible.

Question 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.

According to **Section 76a Austrian Code of Criminal Procedure** providers of communication services are obliged to provide master data upon request of the police responsible for criminal investigations, public prosecutor's offices or the competent courts. The request has to be related to investigations that are based on a concrete suspicion of an offence. Master data under **Section 93 para 3 item 3 of the Telecommunications Act** means all personal data required for the establishment, processing, modification or termination of the legal relations between the user and the provider or for the production and publication of subscriber directories, including name, academic degree, address, subscriber number and other contact information for the message, information about manner and content of the contractual relationship and credit-worthiness.

Furthermore, providers of communication services are obliged to provide the following data of the owner of technical equipment upon request of the public prosecutor's office (Section 76a para 2 Austrian Code of Criminal Procedure):

1. the name, address and terminal identification of a subscriber, who was assigned a public IP-address on a definite date, unless it would determine a large number of people;
2. the terminal identification , that is assigned by using e-mail-services;
3. the name and address of a subscriber who was assigned an e-mail-address on a definite date;
4. the e-mail-address and the public IP-address of the sender of an e-mail.

Correspondingly, the duty of communication providers to provide the relevant data is also stipulated in **Section 90 para 7 Telecommunications Act**: At the written request of the competent courts, public prosecutor's offices or the police responsible for criminal investigations (Section 76a para 1 Austrian Code of Criminal Procedure), providers of communications services are obliged to provide those authorities with information on

master data (Section 92 para 3 item 3) on subscribers for the investigation and prosecution of actual suspicions of a criminal offence. […] In urgent cases, such requests may be conveyed orally on a preliminary basis.

Definitions and requirements for obtaining information about the data of a message transmission and the surveillance of messages are regulated **in Sections 134 and 135 Austrian Code of Criminal Procedure**.

According to **Section 138 para 2 Austrian Code of Criminal Procedure**, providers (Section 92 para 3 item 1 of the Telecommunications Act: operator of public communications services) and other providers of services (Sections 13, 16 and 18 para 2 of the E-Commerce Act) are obliged to provide information about data of a message transmission and to cooperate in the surveillance of messages (Section 135 para 2 and 3 Austrian Code of Criminal Procedure).

Relevant excerpt of the Austrian Code of Criminal Procedure for obtaining data of a message transmission and the surveillance of messages:

Definitions
Section 134. For the purposes of the present law, the following terms shall mean:
[…]
2. "information about the data of a message transmission" is information that is provided about communication data (Section 92 para 3 item 4 of the Telecommunications Act), access data (Section 92 para 3 item 4a of the Telecommunications Act) and position data (Section 92 para 3 item 6 of the Telecommunications Act) of a telecommunications service, or a service of the information society (Section 1 para 1 item 2 of the Notification Act),
3. "surveillance of messages" is the determination of the contents of messages (Section 92 para 3 item 7 of the Telecommunications Act), which are exchanged or forwarded via a communications network (Section 3 item 11 of the Telecommunications Act), or a service of the information society (Section 1 para 1 item 2 of the Notification Act),

[…]

Confiscation of Letters, Information about Data of a Message Transmission, as well as Surveillance of Messages

Section 135.
[…]
(2) Information about the data of a message transmission shall be admissible
1. if and as long as it is urgently suspected that one of the persons concerned by the information has kidnapped or otherwise seized another person, and that the information about data is restricted to such a message of which it has to be assumed that it was communicated, received or sent by the accused at the time when the person was deprived of his/her liberty,
2. if it is to be expected that this can promote the clearing up of a punishable act, committed with intent, which carries a prison term of more than six months, and if the owner of the technical equipment, which was or will be the source or the target of a message transmission, expressly agrees to it, or

3. if it is to be expected that this can promote the clearing up of a punishable act, committed with intent, which carries a prison term of more than one year, and if it is to be assumed, on account of certain facts, that data concerning the accused can thus be obtained.

(3) The surveillance of messages shall be admissible

1. in the cases of paragraph (2) item 1,
2. in the cases of paragraph (2) item 2, whenever the owner of the technical equipment, which was or will be the source or target of the message transmission agrees to the surveillance,
3. if this appears to be required to clear up a punishable act, committed with intent, that carries a prison term of more than one year, or if the clearing up or prevention of a punishable act, committed or planned within the framework of a criminal or terrorist association or a criminal organisation (Section 278 to Section 278b of the Criminal Law Code) would otherwise be essentially impeded, and
   a. the owner of the technical equipment, which was or will be the source or target of messages is urgently suspected of a punishable act, committed with intent, that carries a prison term of more than one year, or of a punishable act pursuant to Section 278 to Section 278b of the Criminal Law Code, or
   b. it is to be expected, on account of certain facts, that a person urgently suspected of the offence (letter a) will use the technical equipment or will establish contact with it;

4. if it is to be expected, on account of certain facts, that the whereabouts of a fugitive or absent accused may be determined, who is urgently suspected of a punishable act, committed with intent, that carries a prison term of more than one year."