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:

Our experiences depend on the sort of crime. In organised crime and cases related to cybercrime, child exploitation cases we see in almost every case examples of various forms of encryption. The communication between suspects will be encrypted (VPN, SSH, end to end encryption in messenger apps, encrypted PGP messages by special crypthofoons and/or special blackberries)

Besides that we encounter more and more encryption of the static information on devices (computers, telephones, servers etc.)

Last but not least we encounter more and more security measures which makes it very hard to get access to a device (upgrade of security by producers of phones and other hardware)

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:

We see a combination of VPN, SSH, PGP and TOR as well as Telegram, Signal and WhattsApp as choices of the suspect to communicate safely. Same tools are being used by companies and consumers as well. Question remains if there are possibilities to (for instance) get information of certain parties. That depends on the scripts and protocols used to encrypt the data.

HTTPS isn't a choice of the suspects.
SFTP is also very important for the business market

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:

Companies make it very hard to get access to the data stored on the hardware, by also encrypting the password information. In short that means that also when hardware is confiscated, it turns out to be very hard to get access to the information on the computer. When you get access, then you encounter encrypted containers.

The encryption cannot be broken with brute force, **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.**

X yes

o no

Please specify:

For non-suspects there is an obligation to help with decrypting information. It's an order that the public prosecutor decides on. There is no obligation for a suspect of a crime to share that information, at least not in cases where you want to extract evidence of that device that can be used against the suspect.

Neither is there a ground for prosecution when the suspects refuses to give the requested information. It has been a topic of debate en will (again) be a topic of debate when the new proposed Computer Crimes Act (CCIII) is discussed in Parliament.

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.

X yes

o no

Please specify: Only when service providesrs have access to information that is necessary to decrypt information, they can be obliged to do so. There is no obligation the change any process to make it possible for law enforcement to do so. In practice, only a few big companies providing the normal telephone calls are obliged to make it possible to intercept the data (sound).

Companies can be obliged to give access to law enforcement to their location to place tools to intercept the data under:

Dutch Telecommunications Act Chapter 13.

Chapter 13. Authorized tapping and application of other powers pursuant to the Code of Criminal Procedure and the Intelligence and Security Services Act 2002 in connection with telecommunications

Article 13.1

1. Providers of public telecommunications networks and publicly available telecommunications services shall only make their telecommunications networks and telecommunications services available to users if these can be tapped.

2. Rules may be set by or pursuant to a general administrative order regarding the technical susceptibility to tapping of public telecommunications networks and publicly available telecommunications services.

Article 13.2

1. Providers of public telecommunications networks shall be obliged to cooperate with the enforcement of an order pursuant to the Code of Criminal Procedure or consent pursuant to the Intelligence and Security Services Act 2002 for the tapping or recording of telecommunication that takes place via their telecommunications networks.
2. Providers of public telecommunications networks shall be obliged to cooperate with the enforcement of an order pursuant to the Code of Criminal Procedure or consent pursuant to the Intelligence and Security Services Act 2002 for the tapping or recording of telecommunication handled by them.
3. Rules may be set by or pursuant to a general administrative order regarding the organisational or personnel measures to be taken and arrangements to be made regarding tapping.

Article 13.2b

Providers of public telecommunications networks and publicly available telecommunications services shall comply with a demand pursuant to Articles 126hh, 126ii, 126nc to 126ni and 126uc to 126ui of the Code of Criminal Procedure.

Dutch Code of Criminal Procedure

Section 126m sub 6 (on organized crime)

6.Insofar as is specifically required in the interest of the investigation, the person, who may be reasonably presumed to have knowledge of the manner of encryption of the communications, may be requested, if subsection (1) is applied, to assist in decrypting the data by either providing this knowledge, or undoing the encryption.

Section 126zg (on terrorism)

1. In the case of indications of a terrorist offence, the public prosecutor may, if urgently required by the investigation, order an investigating officer to record by means of a technical device non-public communications which are conducted by use of the services of a provider of a communication service within the meaning of section 126la.

2.The warrant shall also state in addition to the information referred to in section 126za:
a. where possible, the number or another indication by means of which the individual user of the communication service is identified as well as, insofar as is known, the name and the address of the user;
b. the term of validity of the warrant; and
c. a description of the nature of the technical device or the technical devices by means of which the communications are recorded.
3.If the warrant relates to communications which are conducted through a public telecommunication network or by use of a public telecommunication service within the meaning of the Telecommunications Act, the warrant shall –unless such is impossible or is not permitted in the interest of the criminal proceedings –be executed with the assistance of the provider of the public telecommunication network or the public telecommunication service and the warrant shall be accompanied by a request for assistance from the public prosecutor to the provider.
4. If the warrantrelates to communications other than the communications referred to in subsection (3), the provider shall –unless such is impossible or is not permitted in the interest of the criminal proceedings – be given the opportunity to assist in the execution of the warrant.
5.Section 126m(5) to (9) inclusive shall apply mutatis mutandis.

Section 126nh
1. The public prosecutor may, if required in the interest of the investigation, in or immediately after the application of section 126nd(1), 126ne(1) or (3), or 126nf(1), order the person who may be reasonably presumed to have knowledge of the manner of encryption of the data referred to in these sections to assist in decrypting the data by either undoing the encryption, or providing this knowledge.
2.The order shall not be given to the suspect. Section 96a(3) shall apply mutatis mutandis.

Section 125k
1. Insofar as is specifically required in the interest of the investigation, the person who may be reasonably believed to have knowledge of the security system of a computerised device or system may be ordered, if section 125i or section 125j is applied, to provide access to the computerised devices or systems present or parts thereof. The person who is ordered to do so must comply with this order, if requested, by providing the knowledge about the security system.

2. Subsection (1) shall apply mutatis mutandis if encrypted data is found in a computerised device or system. The order shall be directed to the person who may be reasonably believed to have knowledge of the manner of encryption of this data.
3.The order, referred to in subsection (1), shall not be given to the suspect. Section 96a(3) shall apply mutatis mutandis.

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?

X yes

o no

On the basis of article 126m (and 126t/126zg) an order can be given to intercept both encrypted and non-encrypted data. The order is given by the prosecutor after authorisation from an investigative judge.

It is possible to intercept encrypted information and law enforcement is also free to try to decrypt that information. But we cannot force everybody to work with law enforcement especially the companies who don't have any access themselves.

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

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

Companies that encrypt the data do not have access to the decryption keys (end to end encryption, like Telegram, WhatsApp, Skype (at this moment).

In most cases the companies that offer their services are located outside the Netherlands or Europe, which makes it very difficult to communicate with those companies or to oblige them to decrypt information (international cooperation in these matters is hard).

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

Law Enforcement has a lot of freedom to decrypt the information and can use the experience of (foreign) companies for that. But to present the gathered information in court, it has to be clear who can be questioned about the decryption of the information, to give the defence the possibility to challenge the evidence. In practice that makes it difficult, because when it becomes clear that we got access to some information, the company offering the platform will take additional safety measures.

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

o yes

X no

Please specify:

It is not possible to intercept information on the device itself before it is encrypted and for that purpose getting access to that device without physically having access to the device. Nor is it possible to adept the dataflow in a way that you alter only the safety measures, without changing anything in the information being exchanged.

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

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

Describe in more detail the issues identified above:

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

Information that is encrypted cannot be decrypted by calculating the keys. The level of encryption is too good for that. What we see is that other means to get access to devices is also getting harder and harder, because that information on the device itself is also encrypted in the new types of devices.

In legal terms, the applicable laws need modernisation to fully face these problems. Obliging companies to work with law enforcement in the country where they offer their services (see article 18 of the Budapest Convention for instance) raise a lot of legal questions and also political questions that have to be solved.

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
  - X practical (e. g. development of practical tools for police and judicial authorities)
  - X improve exchange of information and best practices between police and judicial authorities
- o create conditions for improving technical expertise at EU level
- X improve the (legislative) conditions of communication with service providers, including through the establishment of a legislative framework.

Other, give a clear legal framework to intercept e-evidence on a device before it is encrypted and how law enforcement may access that device (from a distance, or only physical). In short what most people refer to as hacking

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.

The Netherlands has developed a government-wide position on encryption. This has been enclosed with this email.

It is important that Politicians give their view on the interrelation between the right of privacy and the measures needed in a democratic society