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

Answers for Germany

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: The police does not compile statistics as to the occurrence of encryption.

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:

Both for on- and offline encryption, police encounters all prevalent encryption methods/software, including the methods/software mentioned above.

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

[Beitrag BMJV]
- suspects or accused:

No, as suspects or accused have a right not to incriminate themselves.

- persons in possession of a device/e-data:

Yes, but only as witnesses, in case they have knowledge of the encryption key or passwords:

German Criminal Procedure Law does not provide for a specific obligation to disclose encryption keys or passwords for persons in possession of a device/e-data. In general, however, a password or encryption key may be obtained through the following measures:

- Persons other than the suspect or accused can be obliged to testify as witnesses (if no statutory exception, such as a right to refuse on personal/professional grounds, applies). According to Section 48 Subsection 1 Sentence 2 Code of Criminal Procedure, witnesses are obliged to disclose encryption keys/passwords as far as they have knowledge thereof and when questioned by a judge or prosecutor. For the wording of Sections 48 et seq. Code of Criminal Procedure, please see below:

  https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0176

- In case the key/password is not, as such, known to the witness, but stored on a physical device or printed on a document, such document or storage device can be requested or searched and seized according to Sections 94 et seq. upon an order issued by a judge, or, in exigent circumstances, the police. The wording of Sections 94 et seq. is shown here:

  https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0430

- other persons:

Yes, but only provider of telecom services concerning passwords and access keys they have stored:

According to Section 100j of the Code of Criminal Procedure, provider of telecommunication services may be ordered to disclose passwords or access codes to the authorities as far as they have stored such passwords or access codes (e.g. PIN or PUK code for mobile phones). Such an order is only admissible if the statutory requirements for the use of the password or access code have been met. In any case, the request for the password or access key needs to be issued by a judge, or, in exigent circumstances, the police. The wording of Section 100j Code of Criminal Procedure can be found here:

https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0672

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: Please see answer to question 3; in addition, please note that, even if the legal requirements for such an obligation are fulfilled service providers can only be obliged to provide law enforcement authorities with encryption keys/passwords (or, in case of surveillance measures, unencrypted data streams) if – and only if – the provider itself applies the encryption layer. Providers cannot be obliged to provide such data whenever the encryption is applied by the user or by third parties..

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:

National Law allows for interception and monitoring of both unencrypted and encrypted data flow.

It is possible to obtain encrypted content data the same way and under the same conditions as non-encrypted data. Stored computer data may be object of a search (Section 102 German Criminal Procedure Code) and be seized (Section 94 German Criminal Procedure Code), a court order is required (Sections 98, 105 German Criminal Procedure Code). Encrypted content data may also be obtained by an interception of telecommunications. The conditions are laid down in Sections 100a, 100b of the German Criminal Procedure Code. The measure is only admissible if the suspect has committed a serious crime listed in the catalogue in subsection (2), the offence is of particular gravity in the individual case and other means of establishing the facts would be much more difficult or offer no prospect of success.

A court order is required.

However, to intercept encrypted data is usually not helpful for the purposes of criminal proceedings, as decryption is very time consuming and expensive.

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 is that recorded data is encrypted, e.g. using end-to-end encryption, and can therefore not be analyzed in detail. In many cases, analysis of actual communication content is not feasible.

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:

For communication data:

One possibility would be to install a software specifically designed for and limited to lawful interception on a target system and extract communication data before it gets encrypted or after it has been decrypted ("lawful interception at the source"). A search of data at rest stored on the system is not possible with such software.

The use of surveillance software for the interception of telecommunications has been regarded admissible in a verdict of the Constitutional Court in 2008 (BVerfGE 120, 274 ff.), if the surveillance software can only be used to obtain the ongoing conversation, but not to search the whole system. The court has reaffirmed this position in a 2016 ruling (1 BvR 966/09, 1 BvR 1140/09). However, the Code of Criminal Procedure does not foresee explicitly the use of such surveillance software.

For data at rest:

As explained above, Code of Criminal Procedure does not foresee an authorization for collecting data at rest through remote surveillance software. Such measures are only possible in cases of preventive police measures related to combating international terrorism under the Act on the Federal Criminal Police Office.

Under the Code of Criminal Procedure, data at rest may be obtained for example by search and seizure of physical storage devices. Such storage devices may then be examined using forensic methods in order to extract and/or decrypt stored data.

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:

In general, national law allows sufficiently effective securing of e-evidence. However, potential changes to the legal framework are constantly being examined and discussed.

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: Main issues are encountered with regard to shortcomings in the areas "personal" and "technical". With sufficient resources, many new and innovative approaches can be leveraged to mitigate the detrimental effect of encrypted data on criminal investigations.

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:

Development of practical tools for LEAs should be supported. This seems possible and useful in many technical areas, whenever the development can be clearly separated from the application in the cases and from case data.

Second, information exchange between EU member states and LEAs is an important aspect, since technical issues and approaches are the same – worldwide. Third, technical expertise at an EU Level can support an improved information exchange and cooperation on international cases.

- ○

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.

Yes. A regulation to prohibit or to weaken encryption for telecommunication and digital services has to be ruled out, in order to protect privacy and business secrets.