



Guidance note 1/2016

FAQ on controls of 'Information Security' items and implementation of the Cryptography note exemption

The purpose of this Note is to provide guidance to the economic operators by setting out good practices for interpreting certain provisions of Council Regulation (EC) N° 428/2009 with a view of reducing occasional divergences in the application of EU law. This Note has been agreed upon with the competent authorities of the Member States and does not lay down additional obligations or pre-conditions to those of existing EU law. It is not legally binding. Only the Court of Justice of the European Union is competent to give a legally binding interpretation of EU law.

"Information security" items (e.g. equipment, software, systems, application specific electronic assemblies, modules, integrated circuits, components or functions) employing cryptography or performing cryptographic functions other than authentication, digital signature or the execution of copy-protected software, and meeting certain technical criteria, may be controlled under the terms of Category 5 Part 2 of Annex I to Regulation (EC) No 428/2009.

Recently, encryption has become a common functionality in many Information and Communication technology goods sold or distributed without restrictions by retail selling points. In recognition of the commercial availability of these items, Note 3 to Category 5 Part 2 - the "Cryptography note" - stipulates that controls do not apply to equipment and software (entries 5A2 & 5D2) that meet certain criteria and can be considered as generally available to the public.

The purpose of this note is to provide the exporters with further guidance on interpretation and implementation of the Cryptography note, including cases where various competent authorities are called upon to assess the applicability of the Cryptography note.

1. Do exporters have to apply to the Competent authority for an exemption from control pursuant to the Cryptography note or can exporters operate a system of self-assessment where they determine themselves if the items qualify for (de)control?

It is in the first place the responsibility of exporters to determine if the items are subject to control or qualify for decontrol under the Cryptography note. Nevertheless, exporters are advised to request guidance from the Competent authority or to notify it of the results of their assessment for further confirmation, according to national regulations or practices.

In circumstances where exporters have determined themselves that the cryptography note applies, licensing and/or customs officials in the Member State of export may suspend the process of export from the territory of that Member State, if they adopt an interpretation of the applicability of the

Cryptography note that is different from that of the exporter. Where the Member State of export is not the Member State where the exporter is established, the authorities of the Member State in question should immediately consult the competent authority and provide the relevant information to determine the applicability of the Cryptography note.

2. In situations where the competent authority is called upon to assess the applicability of the Cryptography note, and has confirmed that the item qualifies for an exemption from licensing requirements pursuant to the Cryptography note, should such exemption be applicable throughout the Union or should the case be re-examined by another authority?

Without prejudice to the exporter's responsibility to assess the applicability of the Cryptography note, situations may arise where various competent authorities are called upon to assess the application of the Cryptography note. For example, this could arise where:

- *the exporter had sought a determination on the eligibility of an export vis-à-vis the Cryptography note from the competent authority in the Member State where the exporter is established and the competent authority has determined that an authorisation is not required pursuant to the Cryptography note;*
- *a proposed export is suspended by licensing and/or customs officials in the Member State of export, based on a different interpretation of the Cryptography note, and that Member State is not the Member State where the exporter is established.*

Under the Regulation, the competent authority of the Member State where the exporter is established has the responsibility for deciding on the application of the Cryptography note and, therefore, the controllability of the items. In circumstances where an exporter has either submitted an application for export authorisation, or has requested a clarification from a competent authority on the applicability of the Cryptography note, the exporter should inform the competent authority where an export will be made from another Member State.

If the competent authority plans to confirm that the Cryptography note applies (i.e. no authorisation is required), a consultation process will, where appropriate, be immediately initiated between the authorities of the Member State(s) concerned. Such consultation might take maximum 30 working days.

A Member State may also suspend the process of export from its territory, or, if necessary, otherwise prevent the export of dual-use items which are covered by the Cryptography note from leaving the Union via its territory, where it has grounds for suspicion that:

- (a) *relevant information was not taken into account when assessing the applicability of the Note, or*
- (b) *circumstances have materially changed since the assessment of the applicability of the Note.*

In such a case, the Member State concerned immediately consults the competent authority. Such consultation will take maximum 30 working days.

3. Do decisions of competent authorities – including the award of an exemption under the Cryptography note – take into consideration and apply to the item or to the exporter?

The item characteristics are key elements in the assessment of competent authorities regarding the applicability of the Cryptography note and possible resulting exemption from control. Competent authorities may however also take into consideration other elements of the relevant export transaction.

Decisions of competent authorities – including the award of an exemption under the Cryptography note – made upon requests for an individual or global authorisation apply to a specific exporter for a specific item.

4. Which licensing procedures apply to exports of category 5A2 and 5D2 items that do not qualify for the Cryptography note exemption?

Competent authorities may grant individual or global authorisations for exports of category 5A2 and 5D2 items that do not qualify for the Cryptography note exemption.

As regards exports of category 5A2 and 5D2 items to Australia, Canada, Japan, New Zealand, Norway, Switzerland and Liechtenstein, exporters might consider registering for use of Union General Export Authorisation EU001. Exporters should register with the competent authorities in order to be able to use this general export authorisation.

Annex

Note 3: Cryptography Note

5A002 and 5D002 do not control items as follows:

a. Items that meet all of the following:

1. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:

- a. Over-the-counter transactions;
- b. Mail order transactions;
- c. Electronic transactions; or
- d. Telephone call transactions;

2. The cryptographic functionality cannot easily be changed by the user;

3. Designed for installation by the user without further substantial support by the supplier; and

4. When necessary, details of the goods are accessible and will be provided, upon request, to the competent authorities of the Member State in which the exporter is established in order to ascertain compliance with conditions described in paragraphs 1. to 3. above;

b. Hardware components or 'executable software', of existing items described in paragraph a. of this Note, that have been designed for these existing items, meeting all of the following:

1. "Information security" is not the primary function or set of functions of the component or 'executable software';

2. The component or 'executable software' does not change any cryptographic functionality of the existing items, or add new cryptographic functionality to the existing items;

3. The feature set of the component or 'executable software' is fixed and is not designed or modified to customer specification; and

4. When necessary as determined by the competent authorities of the Member State in which the exporter is established, details of the component or 'executable software' and details of relevant end-items are accessible and will be provided to the competent authority upon request, in order to ascertain compliance with conditions described above.