Council of the European Union

Brussels, 27 April 2026
(OR. en)

8600/26

CSCI 95
CSC 263
CIS 83

INFORMATION NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Information Assurance Security Policy on the Approval and Withdrawal process for Cryptographic Products for the Protection of EU Classified Information (IASP 2-5)

Delegations are informed that the attached Information Assurance Security Policy on the Approval and Withdrawal process for Cryptographic Products for the Protection of EU Classified Information was approved by the Council, at its 4169th meeting on 27 April 2026.

IA Security Policy on the Approval and Withdrawal process for Cryptographic Products for the Protection of EU Classified Information

IASP 2-5

This page intentionally left blank

I. PURPOSE AND SCOPE

1. This policy, approved by the Council in accordance with Article 6(1) of the Council Security Rules (hereinafter 'CSR'), lays down standards for protecting EU classified information (EUCI). It constitutes a commitment to help achieve an equivalent level of implementation of the CSR.

2. This policy describes the EU and interim approval and withdrawal processes for cryptographic products used to protect EUCI.

3. The Council and the General Secretariat of the Council (GSC) will apply this security policy with regard to protection of EUCI in their premises and communication and information systems (CIS).

4. Member States will act in accordance with national laws and regulations to the effect that the standards laid down in security policies are respected when EUCI is handled in national structures, including in national CIS.

5. This policy, as well as the List of EU Approved Cryptographic Products (LACP), do not cover any contractual relationship with a manufacturer concerning the procurement, warranty and maintenance of cryptographic products.

6. Users are required to comply with the conditions outlined in the Security Operating Procedures (SecOps) accompanying the product, which may include obligations for future upgrades or configuration modifications.

7. Before procuring cryptographic products for the protection of EUCI, it is recommended to contact the Crypto Approval Authority (CAA) of the Member State who approved the product nationally for up-to-date details on the approval status, before entering into contractual agreements with vendors.

II. DEFINITIONS

8. An **EU approval** is an approval of a cryptographic product for the protection of EUCI, based on the second-party evaluation in accordance with CSR Article 10(6) and Annex IV, paragraph 26.

9. An **interim approval** is a time-limited approval of a cryptographic product with a clearly defined expiration date, for the protection of EUCI warranted on specific operational grounds in accordance with CSR Annex IV, paragraph 27.

10. A **producing Member State,** in the context of this policy, is the EU Member State responsible for conducting the first evaluation of a cryptographic product.

11. A **cryptographic product type** is a categorisation by the CAA of the producing Member State, grouping cryptographic products with similar intended use and protection objectives.

12. The **cryptographic product version** is a specific instance of a cryptographic product at a defined stage in its lifecycle made commercially available to customers. Versions are typically identified using a manufacturer/defined scheme (e.g., <major version>.<minor version>.<patch>).
    The term **cryptographic product** should be understood as referring to one or more product versions.
    Where no formal versioning scheme is used, the unique product name will serve as the version identifier.

13. A **general-purpose cryptographic product** is a cryptographic product designed for use across a wide range of applications and operational contexts, capable of integration within diverse CIS. Such products are approved without restrictions, other than those specified in SecOps.

14. A **special-purpose cryptographic product** is a cryptographic product designed for a specific operational function or environment. It is approved solely for use within a defined context.

15. The **expiration date of an EU approval of a cryptographic product version** is an optional characteristic of the EU approved product version, specifying the point in time after which the approval for that specific version will no longer be valid.

16. A **product lifecycle indicator** is a three-level designation that reflects the current approval validity and projected lifecycle of an EU approved product:

- **Stable** - the product is approved and, to the best knowledge of the evaluating authority, there are no known issues that would jeopardize the approval of the product in the next review;
- **Under consideration** - the product remains approved, but its continued validity is subject to conditions, or there are identified issues that may affect the outcome of the next review;
- **To be retired** - the product has a formally established expiration date and its national approval will be withdrawn.

17. The product lifecycle indicator should be used as the primary means of predicting the future approval status of a cryptographic product on the LACP/LACPS. While each national review may lead to changes, producing Member States, by categorising a product as ‘stable’, communicate their expectation of continued successful evaluations. Where necessary, additional explanations will be provided in the comments on the national evaluation plan (see paragraph 18.d).

18. **A National Review Plan** is a schedule established by the producing Member State's CAA, which sets out when a cryptographic product will be reviewed, potentially determining the approval status within the Producing Member State. The national review plan contains the following information:

a) Last national evaluation date - the date when the product was last evaluated nationally;

b) Next national evaluation timeframe - the period (e.g. quarter) during which the next evaluation is scheduled; defined as a minimum by a start date of that period. If no timeframe is provided, this should be understood as no evaluation currently planned;

c) National evaluation validity date - where applicable, the date until which the national certificate remains valid under the rules of the national scheme; if no date is provided, this should be understood as unlimited validity;

d) Optional comments on future re-evaluations.

III. ROLES AND RESPONSIBILITIES

19. The GSC Information Assurance Authority (IAA) is responsible for administering all processes and outputs related to the interim and EU approvals, as well as the-withdrawal of EU approvals for cryptographic products used for the protection of EUCI. The GSC IAA maintains a comprehensive database of all requests for EU and interim approvals of cryptographic products protecting EUCI and ensures on-going oversight of these requests. All documentation and correspondence related to an EU and interim approvals should be channelled through the GSC.

20. The Appropriately Qualified Authority (AQUA) that performs the second-party evaluation is responsible for submitting a recommendation for the EU approval of the cryptographic product to the GSC. The submission should include the mandatory information specified in paragraph 24 (with the exception of Council approval date), the product documentation (including SecOps), and second-party evaluation report.

21. The producing Member State's CAA is the sole authoritative source of information on products as recorded in the LACP/LACPS (List of EU Approved Products for Special Purpose). With the exception to the parameters described in paragraph 33, any other information on products may be updated at any time by the producing Member State's CAA through a request to the GSC.

IV. EU APPROVAL PROCESS

22. An EU approval of a cryptographic product is granted based on the approval by a CAA of the producing Member State in line with the IA Security Policy on Cryptography (IASP 2), and a successful second-party evaluation (SPE) conducted by an AQUA, in line with the Information Assurance Security Guidelines on Second Party Evaluation (IASG 2-02).

23. After completion of a successful SPE a recommendation and all required information for an EU approval will be submitted to the GSC by the AQUA that conducted the SPE.

IV.1 GENERAL-PURPOSE CRYPTOGRAPHIC PRODUCTS

24. For general-purpose cryptographic products the GSC will publish the following information in the LACP:

Mandatory information for general-purpose cryptographic products:

m.1) Name of the product enabling unique identification on the market;

m.2) Product strength level (in accordance with IASP 2);

m.3) Product type;

m.4) Name and legal address of the manufacturer;

m.5) Name of the producing Member State (first evaluator);

m.6) Name of the second evaluator (AQUA);

m.7) Date of Council approval;

m.8) Version(s) covered by the approval;

m.9) National review plan;

m.10) Product lifecycle indicator;

Optional information to be published when included in the evaluation report or provided later by the producing Member State:

o.1) Expiration date - the date after which the EU approval will no longer be valid. Where different versions covered by the evaluation have different expiration dates, the date should be specified for each version;

o.2) End-of-sale date - a date after which the manufacturer will no longer sell the product. Where different versions covered by the evaluation have different end-of-sale dates, the date should be specified for each version;

o.3) End-of-support date - a date after which the manufacturer will no longer provide support for the product. Where different versions covered by the evaluation have different end-of-support dates, the date should be specified for each version.

25. The administrative procedure for an EU approval and the supporting information requirements should ensure that the minimum lifecycle-related information (as defined in paragraph 24) are submitted in all cases. Incomplete submissions will not be considered for LACP publication unless accompanied by a formal justification approved by the GSC.

26. Producing Member States' CAAs should provide the GSC with information on the product's lifecycle indicator not less frequent than after each national review cycle. The GSC will ensure that this information is updated on LACP.

27. The detailed procedure for an EU approval of general-purpose products is set out in Annex I.

IV.2 SPECIAL-PURPOSE CRYPTOGRAPHIC PRODUCTS

28. The process to approve special-purpose cryptographic products is similar to the process for general-purpose cryptographic products. However, the documentation of the decision-making process will be classified, and the cryptographic products will not appear on the LACP.

29. The GSC will establish a list of products approved for special purpose or for which the producing Member States required classification (LACPS). This list will be classified at the level RESTREINT UE/EU RESTRICTED.

30. All requests for approval of products using Type A algorithms intended for export outside the EU, should be accompanied by a description of the applicable cryptographic export legal framework in which the product will be used.

31. The information listed on the LACPS, when justified, can be tailored to a specific product and does not have to adhere to the requirements listed for general-purpose cryptographic products as defined in paragraph 24.

32. The detailed procedure for an EU approval of special-purpose products is set out in Annex II.

V. MODIFICATIONS OF AN EU APPROVAL

V.1 General rules

33. Only changes to the following parameters of the cryptographic product are considered as a modification to its EU approval:

a) Changing the versions covered by the approval that result in the withdrawal of at least one version of the product;

b) Establishing an expiration date where none was previously provided;

c) Changing an existing expiration date to an earlier date;

d) Downgrading the strength level for which the product is approved;

A modification of a product's EU approval will always result in the shortening or setting of an expiration date for at least one version of the product.

34. The GSC will change the product lifecycle indicator to 'to be retired' for the affected version(s) and set an expiration date to reflect the date after which the product is no longer approved nationally.

35. A request for a modification to an EU approval must include the following information:

a) Version(s) affected;

b) Date after which the product will no longer be approved nationally;

c) Lower strength level for downgraded products;

d) Mode of the change (either technical obsolescence or urgent security grounds see paragraphs 41 and 44);

e) Versions replacing the product, for upgradable products;

f) Optional explanations.

36. Without prejudice to the exceptional circumstances set out in paragraph 39, any request to modify the EU approval may only be submitted in writing by the CAA of the producing Member State to the GSC.

37. The producing Member State's CAA is responsible for promptly notifying the GSC and all known users of any modification to a product's EU approval. The GSC will notify the Member States, the European Commission, and the External Action Service. Such notifications should include the timeline and effective date. Where possible they should also include:

- The reason for withdrawal;
- The recommendation for replacement products;
- Any known upgrade paths.

38. The GSC will update the LACP or LACPS to reflect the changes to an EU approval.

39. The Council Security Committee may, in exceptional cases, after consulting the CAA of the producing Member State, recommend to the Council a modification of the EU approval status of any product listed in the LACP or LACPS. Such a recommendation must include the modification procedure to be followed by the GSC, following approval by the Council.

40. The detailed procedure for updating the LACP/LACPS when a product's EU approval is changed is set out in Annex III.

V.2 Request for Modification to an EU Approval on Urgent Security Grounds

41. A request to modify an EU approval on urgent security grounds refers to a change in a product's EU approval status due to security risks associated with the continued use of the product under the current approval. The CAA of the producing Member State is the sole entity responsible for assessing the risk. Such requests must be accompanied by information on any available short-term workarounds or risk-mitigation measures.

42. In cases of urgent requests, the CAA of the producing Member State should notify users and provide information on workarounds and any additional explanations.

43. The GSC will process requests to modify the EU approval on urgent security grounds as soon as practically possible.

V.3 Request for Modification to an EU Approval on Technical Obsolescence Grounds

44. A request to modify an EU approval on the grounds of technical obsolescence refers to a modification of a product's EU approval status which, to the best knowledge of the producing Member State, does not compromise the product's security strength.

45. The CAA of the producing Member States must signal issues potentially affecting the product's EU approval by requesting an update of the product lifecycle indicator to 'under consideration'. This request should be submitted sufficiently in advance of any potential modification of the EU approval status, in order to allow product purchasers to accommodate it.

46. Following the signalling referred to in paragraph 45, the CAA should submit an EU approval modification request immediately after a national decision has been made in order to allow the users of the product to prepare for the change.

47. For products with no lifecycle indicator or with a lifecycle indicator of ‘stable’, the expiration dates introduced by the modification must not be earlier than the date of the next evaluation, as indicated in the product’s national review cycle.
Exceptionally, where no next evaluation date is provided for a product, the following dates will apply:
    a) three years from the date of the request for products with strength levels HIGH or ENHANCED;
    b) one year from the date of the request for products with strength levels STANDARD or lower.

VI. INTERIM APPROVAL PROCESS

48. All information associated with an interim request will be classified RESTREINT UE/EU RESTRICTED, and products with an interim approval will not be publicly disclosed and will not be listed on the LACP or the LACPS.

49. A request for an interim approval may be submitted by EU Institution or body, or the CAA of a Member State.

50. The GSC will oversee the administrative procedure for interim approvals to ensure that the process continues until a compliant solution is agreed by the CSC.

51. The requesting entity should provide the following information:

a) Name of the product enabling unique identification on the market;
b) Product strength level (in accordance with IASP 2);
c) Product type;
d) The requested validity period of the interim approval (start and end dates);
e) Reference to any relevant documentation, including SecOps;
f) Name and legal address of the manufacturer;
g) Name of the state where the product is manufactured;
h) Justification and plans for migration to EU-approved cryptographic product if applicable (see Annex IV step 1 for further details on the justification);
i) An undertaking by the Member State to inform the GSC when the migration has been implemented and tested;
j) Information on key management - at least, who generates the keys and how.
k) A copy of national approval, if it exists.

52. The GSC will provide an annual report to the CSC on the status of interim approvals.

53. The interim approval procedure and supporting information requirements for an interim approval are described at Annex IV.

VII. TRANSITIONAL PROVISION

54. The producing Member States will provide all missing mandatory information, as defined in paragraph 24, for the products listed on LACP and LACPS within six months after the approval of this policy.

Annex I. Detailed procedure for a request for EU approval for general-purpose crypto products

Step	Activity	Actor	Default marking or classification	Remarks
0	Cryptographic product has successfully completed an SPE by an AQUA	CAA of the producing Member State and AQUA	The GSC will apply the marking listed below to all communications related to this procedure, unless instructed otherwise by the originators.	In accordance with IASG 2-02 Products submitted for a SPE can be at all strength (classification) levels
1	Notification of a successful SPE Required: AQUA sends letter of recommendation for approval and the SPE report to the GSC	AQUA	LIMITE	By email to: cscia@consilium.europa.eu
2	Checks GSC checks letter and SPE report for completeness and consistency. GSC may also request additional information	GSC	-	-

Step	Activity	Actor	Default marking or classification	Remarks
3	Distribution to CSC(IA) GSC sends a ST doc. with the letter of recommendation to the CSC(IA)	GSC	LIMITE	Only the letter of recommendation is sent to the CSC(IA). The evaluation report and the SecOps are available on request. The document will include the draft cover note for COREPER/Council.
4	CSC(IA) endorses the recommendation for approval of the cryptographic product 2 weeks' written consultation at CSC(IA)	CSC(IA)	LIMITE	A Member State may register an objection to the process in writing by either: <u>Prolongation of a written consultation</u> A letter (or e-mail) requesting a prolongation of the written consultation should detail a reasonable length of time for the prolongation and the reasons for the request. The letter should be sent to the GSC before the end of the written consultation. <u>Written comments by a delegation:</u> A letter (or e-mail) with specific reasons for written comments and a description of the elements that could resolve the issue should be sent to the GSC before the end of the written consultation. The GSC will make an effort to mediate.

Step	Activity	Actor	Default marking or classification	Remarks
5	If either a request for prolongation of a written consultation or written comments are received by the GSC, they will be circulated to the CSC(IA)	GSC	LIMITE	If the written comments cannot be resolved in a reasonable timeframe, it will be discussed at the next meeting of the CSC(IA)
6	Distribution to CSC The GSC sends an ST document about the CSC(IA)'s endorsement of the recommendation to the CSC	GSC	LIMITE	Only the letter of recommendation is sent to the CSC. The document will include the draft cover note for COREPER/Council.

Step	Activity	Actor	Default marking or classification	Remarks
7	CSC endorses the recommendation for approval of the cryptographic product 2 weeks' written consultation at CSC	CSC	LIMITE	A Member State may register an objection to the process in writing by either: <u>Prolongation of a written consultation</u> A letter (or e-mail) requesting a prolongation of the written consultation should detail a reasonable length of time for the prolongation and the reasons for the request. The letter should be sent to the GSC before the end of the written consultation. <u>Written comments</u> A letter (or e-mail) with specific reasons for the written comments and a description of the elements that could resolve the issue should be sent to the GSC before the end of the written consultation. The GSC will seek to resolve the issue.
8	If either a request for the prolongation of the written consultation or written comments are received by the GSC, this will be circulated to the CSC	GSC	-	If the written comments cannot be resolved in a reasonable timeframe, then it will be discussed at the next meeting of the CSC

Step	Activity	Actor	Default marking or classification	Remarks
9	Formal approval The GSC sends a ST that invites COREPER to recommend that the Council approve the cryptographic product for the protection of EUCI to the next available COREPER/Council (I/A note) meeting	GSC	LIMITE	-
10	Notification GSC sends a ST informing MS about the l formal approval by Council	GSC	PUBLIC	-
11	Publication Details of the formally approved cryptographic product entered on the ST doc, List of Approved Crypto products (LACP), and the Council website	GSC	PUBLIC	Any additional information about the crypto product to be included on the Council's website to be supplied by the crypto producing Member State's CAA

Annex II. Detailed EU approval procedure for special-purpose products

Step	Activity	Actor	Default marking or classification	Remarks
0	Cryptographic product must have successfully completed an SPE by an AQUA	CAA of the producing Member State and AQUA	The GSC will apply the marking listed below to all communications related to this procedure, unless instructed otherwise by the originators.	In accordance with IASG 2-02 Products submitted for a SPE can be at all strength (classification) levels
1	Notification of a successful SPE Required: AQUA sends letter of recommendation for approval and the SPE report to the GSC	AQUA	R-UE/EU-R	By email to: cscia@consilium.europa.eu

Step	Activity	Actor	Default marking or classification	Remarks
2	Checks GSC checks letter and SPE report for completeness and consistency. GSC may also request additional information. The GSC checks the whether the request contains the target legal regime (context) into which the product is going to be used.	GSC	-	-
3	Distribution to CSC(IA) GSC the letter of recommendation to the CSC(IA)	GSC	R-UE/EU-R	Only the letter of recommendation is sent to the CSC(IA). The evaluation report is available on request. The document will include the draft cover note for Coreper/Council.

Step	Activity	Actor	Default marking or classification	Remarks
4	CSC(IA) endorses the recommendation for approval of the cryptographic product 2 weeks' written consultation at CSC(IA)	CSC(IA)	R-UE/EU-R	A Member State may register an objection to the process in writing by either: Prolongation of the written consultation A Member State can request a prolongation of the written consultation in writing, request should detail a reasonable length of time for the prolongation and the reasons for the request. The letter should be sent to the GSC before the end of the written consultation. Written comments by a delegation Written comments to include a description of the elements that could resolve the issue should be sent to the GSC before the end of written consultation. The GSC will make an effort to mediate.
5	If either a request for prolongation of written consultation or written comment is received by the GSC, it will be distributed to the CSC(IA)	GSC	R-UE/EU-R	If the written comment cannot be resolved in a reasonable timeframe, it will be discussed at the next meeting of the CSC(IA)

Step	Activity	Actor	Default marking or classification	Remarks
6	Distribution to CSC The GSC sends a ST doc about the CSC(IA)´s endorsement of the recommendation to the CSC	GSC	R-UE/EU-R	Only the letter of recommendation is sent to the CSC. The document will include the draft cover note for COREPER/Council.
7	CSC endorses the recommendation for approval of the cryptographic product 2 weeks' written consultation at CSC	CSC	R-UE/EU-R	A Member State may register an objection to the process in writing by either: <u>Prolongation of the written consultation</u> A Member State can request a prolongation of the written consultation in writing, request should detail a reasonable length of time for the prolongation and the reasons for the request. The letter should be sent to the GSC before the end of the written consultation. <u>Written comments by a delegation</u> Written comments to include a description of the elements that could resolve the issue should be sent to the GSC before the end of written consultation. The GSC will make an effort to mediate.

Step	Activity	Actor	Default marking or classification	Remarks
8	If either a request for prolongation of written consultation or a written comment is received by the GSC, it will be distributed to the CSC	GSC	-	If the written comment cannot be resolved in a reasonable timeframe, it will be discussed at the next meeting of the CSC
9	Formal approval The GSC sends a ST that invites COREPER to recommend that the Council approves the cryptographic product for the protection of EUCI to the next available COREPER/Council (I/A note) meeting	GSC	R-UE/EU-R	-
10	Notification GSC informs Member States in written about the successful formal approval by Council	GSC	R-UE/EU-R	-
11	Publication Details of the formally approved cryptographic product entered on the ST document, List of Approved Crypto products for special purpose (LACPS). The list is maintained by the GSC and classified R-UE/EU-R	GSC	R-UE/EU-R	Any additional information about the crypto product to be included on LACPS should be supplied by the crypto producing Member State's CAA

Annex III. Procedure of updating LACP/LACPS for requests modifying EU approval status of the product.

Step	**Activity**	**Actor**	**Default marking or classification**	**Remarks**
0	This procedure concerns crypto products that are EU approved and which are already published on LACP or stored by the GSC on LACPS	-	The GSC will apply the marking listed below to all communications related to this procedure, unless instructed otherwise by the originators.	This procedure applies to cases in which the producing Member State's CAA requests modification of EU approval status on LACP/LACPS. In the exceptional situations, as defined in paragraph 39, the GSC will follow the procedure decided by the Council.

Step	Activity	Actor	Default marking or classification	Remarks
1	Request for status modification Requester sends a letter to GSC	Producing Member State	R-UE/EU-R	The request should include the following details: -The mode of the change request (urgent security grounds or technical obsolescence); -The proposed new expiration date (the date after which the product loses its national approval); -If the new expiration date applies to a specific version only, the affected product version; -For strength level downgrade requests, the new strength level effective after the expiration date; -For upgradable products, list of the versions that should be considered as valid upgrades, recommended upgrades; -If submitted under the urgency mode, a description of any available workarounds; - Optionally the reason for withdrawal; - Optional explanations; -Any additional information that the requester deems relevant By email to: cscia@consilium.europa.eu

Step	Activity	Actor	Default marking or classification	Remarks
2	Checks GSC checks request for completeness and consistency. GSC may also request additional information. GSC notifies the requester in writing upon completion of the checks.	GSC	R-UE/EU-R (notification of the successful checks)	The notification is sent to the requesting entity.
3	Formal approval of the modification The GSC launches the procedure for the modification of the EU approval status and invites the approving authority to decide on the proposed modification. The CSC(IA) and the CSC will be informed.	GSC	R-UE/EU-R	
4	Update of the LACP/LACPS Following the decision to approve the modification, the GSC will update the appropriate list.	GSC	PUBLIC (LACP)/ R-UE/EU-R (LACPS)	The list is updated based on the details provided in the request. Once the expiration date is reached, the GSC removes the product from the respective list (LACP or LACPS).

Annex IV. Detailed procedures to request an interim approval for general-purpose or special-purpose cryptographic products

Step	**Activity**	**Actor**	**Default marking or classification**	**Remarks**
0	This procedure concerns crypto products that do not have a valid EU approval, for example because they: - have no national approval - have no SPE - are a non-EU produced crypto product - are not approved by the Council - do not fulfil the conditions of the IASP 2	-	The GSC will apply the marking listed below to all communications related to this procedure, unless instructed otherwise by the originators.	Only CAAs of Member States and EU Institution or body may address a request to the GSC By default, an interim approval will be granted for a period no longer than 12 months

1	Request for an interim approval Requester sends a letter to GSC	CAA Member States EU entity	R-UE/EU-R	This request should describe all the extenuating circumstances for the request for an interim approval including, where relevant: -Name of the product enabling unique identification on the market -Product strength level (in accordance with IASP 2); -Product type; -Reference to any relevant documentation, including SecOps; -The requested validity period of the interim approval (start and end dates); -Name and legal address of the manufacturer; -Name of the state where the product is manufactured; -The operational reasons for the request including how and under what conditions will the crypto product be used; - Why is it not possible to use an EU-approved product; - Why there is no national approval, or SPE or why a non-EU crypto is to be used. If there is a national approval, a copy of this should accompany the request; - What kind of EUCI and what level of EUCI will be protected by the crypto product; - How the risk related to lack of a second party evaluation be mitigated? - Who is the Security Accreditation Authority for the CIS where the crypto product will be used? - What measures are planned to replace the use of this cryptographic product with that of an EU cryptographic product;

Step	Activity	Actor	Default marking or classification	Remarks
				- an explanation of the reasons for the requested validity period for the interim approval; - The supporting documents: • SecOps, • Security Target and product description. - Information on the origin of key material and key management - Any other information that the requester may consider relevant By email to: cscia@consilium.europa.eu
2	Checks GSC checks request for completeness and consistency. GSC may also request additional information	GSC	-	-
3	Distribution to ARG GSC sends the substantiated request to the ARG	GSC	R-UE/EU-R	The document is sent to ARG for an initial opinion.

Step	Activity	Actor	Default marking or classification	Remarks
4	ARG issues an opinion on the request for an interim approval to the GSC .	ARG	R-UE/EU-R	An ARG Member State may ask in writing for more time to consider the request or indicate an issue that requires additional information or clarification from the requesting party. The GSC will send the response and justified request for further information to the requesting party.
5	Distribution to CSC(IA) GSC sends the substantiated request to the CSC(IA) for a written consultation	GSC	R-UE/EU-R	The original substantiated request and any supporting information received is sent to the CSC(IA). The document will include the draft cover note for COREPER/Council.

Step	Activity	Actor	Default marking or classification	Remarks
6	CSC(IA) endorses the recommendation for an interim approval of the cryptographic product 3 weeks' written consultation at CSC (IA)	CSC(IA)	R-UE/EU-R	A Member State may register an objection to the process in writing by either: Prolongation of the written consultation A Member State can request a prolongation of the written consultation in writing. Request should detail a reasonable length of time for the prolongation and the reasons for the request. The letter should be sent to the GSC before the end of the written consultation. Written comments by a delegation Written comments to include a description of the elements that could resolve the issue should be sent to the GSC before the end of written consultation. The GSC will make an effort to mediate.
7	Any request for a prolongation of the written consultation or written comments will be circulated to the CSC(IA)	GSC	R-UE/EU-R	If the written comments cannot be resolved in a reasonable timeframe, then it will be discussed at the next meeting of the CSC(IA)

Step	Activity	Actor	Default marking or classification	Remarks
8	Distribution to CSC The GSC informs the CSC in writing about the endorsement of the request by the CSC(IA)	GSC	R-UE/EU-R	Only the original substantiated request is sent to the CSC. The document will include the draft cover note for COREPER/Council.
9	CSC endorses the recommendation for an interim approval of the cryptographic product 2 weeks' written consultation at CSC	CSC	R-UE/EU-R	A Member State may register an objection to the process in writing by either: <u>Prolongation of the written consultation</u> A Member State can request a prolongation of the written consultation in writing. Request should detail a reasonable length of time for the prolongation and the reasons for the request. The letter should be sent to the GSC before the end of the written consultation. <u>Written comments by a delegation</u> Written comments to include a description of the elements that could resolve the issue should be sent to the GSC before the end of written consultation. The GSC will make an effort to mediate.

Step	Activity	Actor	Default marking or classification	Remarks
10	If either a request for prolongation of written consultation or written comments are received by the GSC, they will be distributed to the CSC	GSC	R-UE/EU-R	If the written comment cannot be resolved in a reasonable timeframe, it will be discussed at the next meeting of the CSC
11	Formal interim approval GSC sends an ST document about the endorsement of the request for interim approval to the next available COREPER/Council (I/A note) meeting	GSC	R-UE/EU-R	-
12	Notification GSC sends ST informing MS about the successful formal interim approval by the Council	GSC	R-UE/EU-R	-
13	Publication	N/A	N/A	There is no publication of information relating to an interim approval. An updated list of interim approved products will be sent to CSC(IA), SAB, requesting party