



Council of the
European Union

Brussels, 26 October 2023
(OR. en)

10745/1/11
REV 1 EXT 1

CSC 27

PARTIAL DECLASSIFICATION

of document:	10745/1/11 REV 1
new status:	Public
Subject:	Information Assurance Policy on Cryptography

Delegations will find attached the partially declassified version of the above-mentioned document.



**Brussels, 9 June 2023
(OR. en)**

**10745/1/11
REV 1**

RESTREINT UE/EU RESTRICTED

CSC 27

'I/A' ITEM NOTE

From:	Council Security Committee
To:	Corper/Council
Subject:	Information Assurance Policy on Cryptography

1. The Council Decision on the security rules for protecting EU classified information¹ require that “when necessary, the Council, on recommendation by the Security Committee, shall approve security policies setting out measures for implementing the provisions of this Decision” (cf. Article 6(1)).
2. The Council Security Committee has agreed to recommend a policy laying down standards for the use of cryptographic mechanisms, products and systems intended for the cryptographic protection of EU classified information (EUCI) on communication systems (CIS) in terms of confidentiality, integrity, availability and, where appropriate, authenticity and non-repudiation.

¹ Council Decision 2011/292/EU, OJ L 141 of 27.5.2011, p.17

3. The Council's Security Rules for protecting EUCI (Article 10(6)) require that where the protection of EUCI is provided by cryptographic products, such products must be approved by the appropriate Crypto Approval Authority (CAA). The attached policy sets out requirements defining the relationship between:
- the level of classification of the information to be protected, and
 - the strength level of the cryptographic product used to protect that information.
- The policy does not constrain the possibility laid down in Article 10(6) that within Member States' national systems, the confidentiality of EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or RESTREINT UE/EU RESTRICTED may be protected by cryptographic products approved by a Member State's CAA.
4. The cryptographic products subject to these requirements are components that perform a direct protection of the classified information itself. Implementing details will be the subject of specific Information Assurance (IA) security guidelines, which will specify the application of this policy for non-confidentiality services, protection such as access control, non-repudiation, etc.
5. The Council Security Committee (IA experts) examined this draft at its meeting on 22 March 2011 and subsequently endorsed it by silent procedure. Agreement on this draft was confirmed by the Council Security Committee on 23 May 2011. In the course of its examination, the Council Security Committee noted the need for Information Assurance security guidelines (see paragraph 4 above) on the application and implementation of the standards defined in the Policy on Cryptography.
6. Subject to confirmation by COREPER, the Council is invited to
- approve the attached security policy;
 - take note of the application of this policy as set out in paragraph 4 above.
-
