Council of the
European Union

Brussels, 18 January 2024
(OR. en)

5568/24

CSCI 7
CSC 15
CIS 7

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Information Assurance Security Policy on Selection and Procurement of Cryptographic Products

Delegations are informed that the attached Security Policy on Selection and Procurement of Cryptographic Products was approved by the Council, at its 4000th meeting on 16 January 2024.

ANNEX

Information Assurance Security Policy on Selection and Procurement of Cryptographic Products

IASP 2-2

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[1] (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 security policy sets out the process the General Secretariat of the Council (GSC) will apply for the acquisition[2] of cryptographic products and related services to be used for the protection of EUCI in any Communication and Information System (CIS) operated by the GSC.
3. The Council and the GSC will apply this security policy with regard to protection of EUCI in their premises and communication and information systems.
4. EU Agencies and bodies established under Title V, Chapter 2 of the TEU, Europol and Eurojust should use this security policy as a reference for implementing security rules in their own structures.
5. This security policy establishes the administrative provision for contracts declared to be 'secret' or for contracts whose performance must be accompanied by special security measures as referred to in point 11.1(i) of Annex I to the Financial Regulation[3].
6. For the purpose of this policy, a cryptographic product is a product whose primary and main functionality is the provision of security services (confidentiality, integrity, availability, authenticity, non-repudiation) through one or more cryptographic mechanisms.
7. The GSC may only participate in or use procurement procedures launched by other EU institutions, bodies, or agencies, if the provisions of this policy have been respected.

1 Council Decision 2013/488/EU, OJ L 274, 15.10.2013, p.1.
2 Whatever the value of the contract, including e.g. products offered at zero cost.
3 Regulation (EU, EURATOM) 2018/1046 of the European Parliament and the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, OJ L 193, 30.07.2018, p.1 (hereinafter the 'Financial Regulation').

II Procurement, Preparation and Requirement Specification

8. The acquisition of a new cryptographic product must be considered in the context of the whole life cycle[4] of the CIS handling EUCI, in which the product will be used. The same security engineering[5] considerations expressed in the relevant policies and guidelines must be applied.
9. The GSC will define the Minimum Technical Characteristics (MTC) for the required cryptographic product in terms of functional and non-functional requirements and, in particular, strength level of the cryptographic mechanism(s) implemented, as defined in the Information Assurance security policy on Cryptography and related guidelines[6]. The minimum requirements to be included in the MTC are listed in Annex I.
10. In the case the acquisition of cryptographic products is necessary to add, change or upgrade products in an existing CIS, the MTC must clearly detail the interoperability constraints to ensure the cryptographic product will be fully operational in the existing CIS with the current applications. Procurement documents must clearly specify that the tenderer to whom the contract is awarded will be responsible for ensuring the interoperability and compatibility of the supplied cryptographic products in the existing CIS.
11. The Council Security Committee (CSC) will examine the MTC document against the cryptographic needs and the context in which the product will be used to protect EUCI, including any special condition to be taken into account, and will approve it if deemed accurate and complete. Once approved, the MTC will be part of the tender specifications.

4 IASP L - IA Security Policy on Security throughout the Communication and Information System Life Cycle (16268/12)

5 IASP 5 - IA Security Policy on Communication and Information System Security Engineering (10416/15)

6 IASP 2 - IA Security Policy on Cryptography (10745/11) and IASG 2-01 - IA Guidelines on the Application of the Policy on Cryptography (12022/13)

III Procurement Process and Selection of Candidates

12. The GSC must comply with this security policy, the CSR and the Financial Regulation for all procurement and tendering processes involving the procurement of cryptographic products. Only cryptographic products approved in accordance with Article 10(6) of the CSR may be considered.
13. In accordance with a corresponding decision of the Secretary General, the GSC will use the negotiated procurement procedure without prior publication of a contract notice for contracts declared to be secret or for contracts whose performance must be accompanied by special security measures[7].
14. Whenever the GSC prepares a procurement or tendering processes based on a MTC agreed by the CSC, the Member States must be invited to nominate appropriate qualified companies for that tender. Only companies nominated by their Member States through notification to the CSC will be added to the list of candidates for the individual procurement or tendering processes.
15. Only the candidates on the list established under paragraph 14 of the present policy may be invited to tender and receive the tender documents including the MTC. In the context of framework contracts only the candidates on that list may be providers of the cryptographic products.
16. Where the procurement process involves a Classified Contract[8], the provisions specified in Art. 11 of the CSR must be complied with and the GSC must impose requirements aimed at protecting EUCI, which must be communicated to potential tenderers throughout the tendering and contracting procedure.

[7] Point 11.1 (i) of Annex I to the Financial Regulation.

[8] 'Classified contract' means a contract entered into by the GSC with a contractor for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or the creation of EUCI (Appendix A to the CSR).

IV Award of the Contract

17. The GSC must base the award of contracts on the most economically advantageous tender. The award method[9] 'lowest cost' must be applied for contracts within the scope of this security policy.
18. In the definition phase, for the detailed award criteria, the GSC Information Assurance Authority (IAA), Information Assurance Operational Authority (IAOA) and the Crypto Distribution Authority (CDA) of the GSC will be consulted to determine the quality of the proposed cryptographic products and related services.
19. The GSC will set up a Tender Evaluation Committee (TEC) for the evaluation of tenders. The TEC must include at least one member designated by the GSC IAA and one member designated by the IAOA of the GSC to perform the technical evaluation.
20. The GSC may consider admissible only tenders concerning cryptographic products approved by the relevant Crypto Approval Authority (CAA) in accordance with paragraph 12 of the present policy at the relevant strength/classification level by the deadline for the submission of tenders.
21. The GSC will perform an evaluation of the initial admissible tenders and will start the negotiation phase, providing feedback to each tenderer on the evaluation of its initial tender and indicating elements not compliant with the minimum requirements expressed in the MTC and other aspects which should or could be improved. The feedback must not contain elements of comparison with the other tenders.
22. In all procedures involving negotiation, the MTC and security related criteria specified in the procurement documents will not be subject to negotiation.

[9] Article 167(4) of the Financial Regulation.

Minimum requirements to be included in the Minimum Technical Characteristics (MTC) for Cryptographic Products and related services

The MTC are a specification in a document defining the required characteristics of a cryptographic product and related service, such as strength level of the cryptographic mechanism(s) implemented (or, in case of confidentiality services, highest classification level of EUCI that can be handled or transmitted), cryptographic resistance (for Public Key Infrastructure - PKI), performance, use of the product, safety or dimensions, testing and test methods, user instructions.
The MTC must be comprehensive, clear and precise. They must define the characteristics actually required of the cryptographic product and must not have the effect of creating unjustified obstacles to competitive tendering.
The following list contains the criteria for each type of cryptographic products:

1. GENERAL REQUIREMENTS

    1.1. Operational model

    1.2. Level of protection

    1.3. Cryptographic resistance (for PKI)

    1.4. Classification and administrative markings of equipment and components

    1.5. Operational Continuity

    1.6. Availability

    1.7. Minimum speed (where applicable)

    1.8. Security Management

    1.9. Timetable

2. SECURITY REQUIREMENTS

2.1. Security services

2.2. Key management

2.3. Security operational requirements

2.4. Emergency disabling

2.5. Fail-safe alarms

2.6. Anti-tampering

2.7. TEMPEST requirements

3. PHYSICAL, MECHANICAL AND ELECTRICAL CHARACTERISTICS

3.1. Human Safety

3.2. Support and Maintenance

4. ENVIRONMENTAL TEST CONDITIONS

4.1. Temperature Limits

4.2. Humidity

4.3. Altitude