Council of the European Union

Brussels, 25 May 2022
(OR. en)

9558/22

LIMITE

CSC 217
ESPACE 60
CSCI 69

NOTE

From:	Council Security Committee
To:	Working Party on Space
Subject:	Opinion of the Council Security Committee on security of information aspects of the proposal for a Regulation establishing the Union Secure Connectivity Programme (2023-2027)

1. This opinion was requested by the Working Party on Space on 22 February 2022[1].

2. The Council Security Committee discussed the text of the Commission proposal for a Regulation establishing the Union Secure Connectivity Programme (2023-2027)[2] at its meetings on 10 March[3] and 26 April 2022[4].

3. After thorough examination of the proposal and in particular the parts relating to, or impacting on, information security and protection of EU classified information, the Council Security Committee (CSC) agreed on 25 May 2022 on the recommendations that form the content of its opinion requested by the Working Party on Space.

[1] WK 2612/22
[2] doc. 6318/22
[3] doc. 7152/22 (outcome of proceedings)
[4] WK 5635/22 (discussion paper)

4. The recommendations are structured around four main issues that the CSC has identified:
    a) Integration of the European Quantum Communication Infrastructure (EuroQCI), and in particular the quantum key distribution (QKD), in the Programme;
    b) Creation of EUCI by the European Space Agency;
    c) Accreditation aspects;
    d) Secure Connectivity Competent Authority.

5. The text of the opinion can be found in the Annex. For each issue, the opinion presents rationale and suggest modifications to be made. Changes are made to the Commission proposal (doc. 6318/22) unless otherwise indicated. They are indicated in **bold underlined** for new text and in ~~strikethrough~~ for deleted text.

ANNEX

Opinion of the Council Security Committee
on security of information aspects of the proposal for a Regulation establishing the Union Secure Connectivity Programme (2023-2027)

Issue 1: Integration of European Quantum Communication Infrastructure (EuroQCI)

1. Given the highly technical nature of this issue, the CSC decided to consult its technical sub-committee, the AQUA Reference group (ARG). In its opinion[5], the ARG stated that since many questions regarding the security of the quantum key distribution (QKD) technology still need to be solved, it did not believe that there will be technology and devices sufficiently mature to protect EU classified information (EUCI) within the timeframe of the programme, i.e. 2023-2027.

2. The ARG opinion was examined by the CSC. While some delegations shared the ARG views, several other were more nuanced. They expressed the preference to keep the QKD as part of a cryptographic product for the protection of classified information within the Programme in order to ensure that the work towards the technology's maturity will progress. They considered it to be a good signal to the industry to continue developments and investment in quantum computer resistant technology.

3. The CSC reached a compromise that QKD technology can be covered by the Programme, but must be accompanied by a reinforced governance that appropriately reflects the role and competences of Member States and of the Council concerning the approval of cryptographic products, as set out in the Council Security Rules[6]. The security accreditation authority must verify this within the accreditation process. At the same time, since the QKD is a technology that will probably not be mature for the protection of EUCI by the end of the Programme, the CSC proposes to modify the text so it is clarified that the QKD is one of other technologies that could provide for approved quantum secure cryptography. In this regard, there was a general support for the ARG opinion that post-quantum cryptography should be part of a solution to counter the threat to asymmetric cryptography posed by quantum computing.

[5] doc. 8162/1/22 REV 1
[6] Council Decision 2013/488/EU

4. Against this background, the CSC proposes the following modifications:

Recital 12

(12) Since June 2019, Member States have signed the European Quantum Communication Infrastructure (EuroQCI) Declaration, agreeing to work together, with the Commission and with the support of ESA, towards the development of a quantum communication infrastructure covering the whole EU. According to that Declaration, EuroQCI aims at deploying a certified secure end-to-end quantum communication infrastructure, enabling information and data to be transmitted and stored ~~ultra~~-securely and capable of linking critical public communication assets all over the Union. ~~To that purpose an interconnected space infrastructure and terrestrial infrastructure, should be built to enable the generation and distribution of cryptographic keys based on quantum information theory~~. The Programme will contribute to meet the objectives of the EuroQCI Declaration by developing a EuroQCI space infrastructure integrated into the space and ground infrastructure of the Programme. The EuroQCI space infrastructure should be developed in the Programme in two main phases, a preliminary validation phase and a full deployment phase, which should see full integration with the Programme, including appropriate solutions for inter-satellite connectivity and data relay between satellites and the ground. ~~The Programme should integrate the EuroQCI in its governmental infrastructure, as it will provide future-proof cryptographic systems that offer unprecedented levels of secure communications by resisting future quantum computing attacks.~~

NEW recital 12a

(12a - NEW) One of the main functions of the Quantum Communication Infrastructure will be to allow for quantum distribution of cryptographic keys. To date, the QKD technology and products are not sufficiently mature to be used for the protection of EUCI. The main questions about QKD security still need to be solved such as standardisation of QKD protocols, side channel analysis and evaluation methodology. The Programme should therefore support the EuroQCI and allow for the inclusion of approved cryptographic products in the infrastructure when available.

NEW recital 12b

(12b - NEW) In order to protect EUCI in a satisfactory secured manner, primary solutions to counter threats posed by quantum computing should be the combination of conventional solutions, post-quantum cryptography and possibly QKD in hybrid approaches. The Programme should therefore use such approaches with the aim to have both state of the art cryptography and key distribution.

Recital 51

(51) Without prejudice to the sole responsibility of the Member States in the area of national security, as provided for in Article 4(2) TEU, and to the right of the Member States to protect their essential security interests in accordance with Article 346 TFEU, a specific governance of security should be established to ensure a smooth implementation of the Programme. That governance should be based on three key principles. Firstly, it is imperative that Member States' extensive, unique experience in security matters be taken into consideration to the greatest possible extent. Secondly, in order to prevent conflicts of interest and any shortcomings in applying security rules, operational functions should be segregated from security accreditation functions. Thirdly, the entity in charge of managing all or part of the Programme's infrastructure is also the best placed to manage the security of the tasks entrusted to it. The security of the Programme would build upon the experience gained in the implementation of the Union Space Programme over the past years. Sound security governance also requires that roles be appropriately distributed among the various players. As it is responsible for the Programme, the Commission, without prejudice to Member States prerogatives in the area of national security, should determine **together with the Member States** the general security requirements applicable to the Programme. **In particular in the area of classified information, the security governance of the Programme should reflect the role and competences that the Council and Member States have in the evaluation and approval of cryptographic products for protecting EUCI.**

In Article 7, in the version contained in doc. 8934/22 (Presidency compromise text proposal), the following modification in point c) of paragraph 1-a is proposed:

Article 7

Service portfolio

"1-a. The service portfolio for the governmental services shall be established. It shall consist of the following categories of services, which complements the portfolio of GOVSATCOM services referred to in Article 63(3) of the Space Regulation:

(…)

c) **quantum communications services, such as** quantum key distribution service.

(…)"

In Article 27, a new paragraph 1a is proposed to be added:

Article 27

Governance of security

"(…)

1a (NEW).

The Council and the Member States shall be consulted regarding the specification and design of any aspect of the EuroQCI infrastructure, in particular the QKD that relates to the protection of EUCI.

Evaluation and approval of cryptographic products for protecting EUCI shall be carried out while respecting the role and competences of the Council and the Member States.

The Security Accreditation Authority shall verify within the security accreditation process that only approved cryptographic products are used.

(…)"

Issue 2: Creation of EUCI by ESA

5. Delegations reiterated their long-standing views that the only appropriate legal framework under which ESA can create EUCI is the EU-ESA agreement on the security and exchange of classified information (security of information agreement). Since the current security of information agreement from 2008 does not contain provisions on the creation of EUCI, it has to be re-negotiated and modified with the aim, amongst other things, to clarify the scope and content of the possibility for ESA to create EUCI and the obligations attached. In this regard it should be noted that in February 2022, the Council sent a letter to the High Representative in which the High Representative was invited to submit to the Council a recommendation to re-open the 2008 security of information agreement[7].

6. The CSC therefore suggests to clarify in the text proposed in paragraph 2 of Article 35 that ESA can create EUCI only after the EU-ESA security of information agreement will have been revised. Member States confirmed their readiness to treat the re-negotiation of the security of information agreement with utmost urgency, once the High Representative submits a recommendation in this regard to the Council[8], in order to ensure its timely adoption before the conclusion of the contribution agreement that the Commission intends to sign with ESA to implement the Programme.

Article 35

Protection of classified information

"(…)

2. **Subject to the provisions of the Agreement on the security and exchange of classified information between the EU and ESA, ESA may generate EUCI** ~~classified information generated by ESA~~ in relation with the tasks entrusted under Article 25(1) and (2) ~~shall be considered as EU Classified Information in accordance with Commission Decision (EU, Euratom) 2015/444 and Council Decision 2013/488/EU~~ ~~, created under the authority of the Commission.~~"

[7] doc. 6703/22
[8] doc. 7539/22

Issue 3: Accreditation aspects

7. The CSC proposes the following modifications in the provisions concerning accreditation:

8. In Article 29 on the Security Accreditation Authority, it is proposed to add the reference to "governmental services" to make it consistent with Article 24 of the Regulation:

Article 29

Security Accreditation Authority

"The Security Accreditation Board established within the Agency under Article 72(1) of Regulation (EU) 2021/696 shall be the security accreditation authority for the governmental infrastructure **and governmental services** of the Programme."

9. In Article 31 on the tasks and composition of the Security Accreditation Board (SAB), it is proposed to add some other tasks of the SAB in order to ensure consistency with Article 38 of the Regulation (EU) 2021/696 (Union Space Programme Regulation). It is also suggested to clarify that only representatives of the contractor involved in the governmental infrastructure and services can attend the SAB meetings and that the modalities for their participation will be defined in the SAB's rules of procedure:

Article 31

Tasks and composition of the Security Accreditation Board

"1. Article 38, with the exception of points (c) to (f) of paragraph 2 and point (b) of paragraph 3, and Article 39 of Regulation (EU) 2021/696 shall apply to this Programme.

1a. In addition to paragraph 1, the Security Accreditation Board shall also have the following tasks:

a) examining and, except as regards documents which the Commission is to adopt under Article 27(2) of this Regulation, approving all documentation relating to security accreditation;

b) **advising, within its field of competence, the Commission on the production of draft texts for acts referred to in Article 27(2) of this Regulation, including for the establishment of security operating procedures, and providing a statement with its concluding position;**

c) **examining and approving the security risk assessment drawn up in accordance with the monitoring process referred to in point (h) of Article 37 of Regulation (EU) 2021/696 and those drawn up in accordance with Article 27(2) of this Regulation, and cooperating with the Commission to define risk mitigation measures.**

2. In addition to paragraph 1 and on an exceptional basis, ~~representatives of the contractor referred to in Article 15(2) of this Regulation~~ **only representatives of the contractor involved in governmental infrastructure and services** may be invited to attend the meetings of the Security Accreditation Board as observers for matters directly relating to that contractor. **Modalities and conditions for such participation of a contractor shall be laid down in the rules of procedure of the Security Accreditation Board**."

10. In order to fulfill these additional tasks, the EU Agency for Space Programme (EUSPA) should be equipped with necessary resources for security accreditation.

Issue 4 - Secure Connectivity Competent Authority

11. The CSC suggests to clarify that the Programme participants do not need to establish a new competent authority for the purpose of the Programme but can attribute the function of Secure Connectivity Competent Authority to an already existing authority. The CSC also underlines that the designation of such an authority is a Member State's prerogative.

12. Recital 24 is proposed to be modified as follows:
"(24) Each Programme participant should designate a Secure Connectivity Competent Authority to monitor whether users, and other national entities that play a role in the Programme, comply with the applicable rules and security procedures as laid down in the security requirements. **Programme participants may assign the function of such an authority to an existing authority."**

Other issues

13. The CSC proposes to insert in Article 2 the definition of "EU classified information" and "sensitive non-classified information" in the wording used in Regulation (EU) 2021/696 (Space Programme Regulation).

Article 2

Definitions

"(…)

9a (NEW). 'EU classified information' or 'EUCI' as defined in Article 2(25) of Regulation (EU) 2021/696.

9b (NEW). 'sensitive non-classified information' as defined in Article 2(26) of Regulation (EU) 2021/696."