Council of the European Union

Brussels, 15 January 2021
(OR. en)

5154/21

CSC 3
RELEX 8

NOTE

From:	General Secretariat of the Council
To:	Coordination Committee for Communication and Information Systems (CCCIS)
Subject:	Business and security needs for a secure videoconferencing system (sVTC) for the European Council and the Council

I. INTRODUCTION

1. In doc. 10502/20 (R-UE/EU-R) the GSC proposed setting up a secure videoconferencing system for discussions on sensitive and classified topics in the Council and the European Council. The need for such a secure system has been identified *inter alia* for President of the European Council, who is currently able to hold SECRET level VCs (S-UE/EU-S RELEASABLE TO THE U.S.) with the US President, but not with his colleagues as members of the European Council.

2. At its meeting on 15 December, the Antici Group confirmed:

   (i) the need for a secure videoconferencing system capable of handling classified (up to SECRET UE/EU SECRET) or very sensitive discussions for heads of state or government, ministers and senior officials;

   (ii) that the system should be capable of handling classified discussions up to the level of SECRET UE/EU SECRET, given that certain discussions, in particular relating to certain activities of third countries, should normally be classified higher than RESTREINT UE/EU RESTRICTED.

   It invited the Coordination Committee for Communication and Information Systems and the Security Committee to examine the necessary high-level documentation, including a more detailed assessment of the budgetary impact, with a view to

reporting back to the Antici Group around the end of February with a detailed proposal on how to proceed. It also invited the Budget Committee to examine the budgetary aspects.

3. The Coordination Committee for CIS is invited to examine this requirements paper and two accompanying notes:

   (i) the business and security context for a secure videoconferencing system for the Council and the European Council (doc. 5156/21);

   (ii) budgetary planning for a secure videoconferencing system (sVTC) for the European Council and the Council (doc 5157/21);

   with a view to providing a recommendation to the Antici Group and COREPER around the end of February on the business functional requirements and the overall planning envisaged for the project. The Security Committee and the Budget Committee will both be consulted before the final report is submitted to the Antici Group and COREPER.

II. PURPOSE

4. This document describes the needs for the new system to hold secure video conferences (for very sensitive[1] and classified discussions up to SECRET UE/EU SECRET or their national equivalents) in support of the European Council and Council. It draws on document 5156/20 which sets out the business context in which the system is to be deployed and used; the secure videoconferencing context (i.e. what videoconferencing capabilities are in the scope); and the security context (i.e. the applicable rules and policies, and possible threats) representing the enterprise constraints driving the security of systems.

III. HIGH LEVEL BUSINESS REQUIREMENTS

5. Based on preliminary indications, the following is suggested at the high level business requirements for the new secure videoconferencing system:

   (i) the system must provide an end to end video conferencing platform for discussions that are very sensitive or classified up to the level of SECRET EU/EU SECRET or their national equivalents[2].

---

[1] Very sensitive, for the purpose of this document, is considered to be non-classified information with strict requirements on confidentiality and need-to-know.

[2] National classified information are to be treated and protected according to the EUCI equivalents in accordance with the Council Decision on the Security Rules for Protecting EU Classified Information (2013/488/EU - OJ L 274 of 15.10. 2013, p.1)

(ii) the system will always show the classification level of the conversation in progress, and inform the participants of any change in classification level of the conversation in progress.

(iii) the users of the systems are EU Member State Governments and EU institutions, bodies or agencies (EUIBA) which will use the system in the context of the EU decision-making process.

(iv) the system will allow videoconferences with the simultaneous participation of all participants normally present in a European Council or Council meeting, and their preparatory bodies, excluding guests other than participants from suitably equipped EU institutions and bodies.

(v) the system will allow for videoconferences of a subset of the above actors in the context of the European Council and the Council's mission or in the broader context of EU collaboration.

(vi) The system should be easy to use, be adaptive to allow for easy connectivity to the videoconference for authorised participants, and provide tools to test the quality of the connection before the actual videoconference is started.

(vii) the system should have easy optical indicators to draw attention to the activation of the video camera and microphone.

(viii) The system must provide an easy way to identify all participating parties in a videoconference.

(ix) The system should be available, upon request, for meetings outside normal business hours.

(x) The system will **not** provide facilities to hold public sessions as part of the meeting.

(xi) The system will **not** provide recording options, and its secure operating procedures will detail that it is strictly forbidden to record voice and/or video (including photos) of an ongoing meeting.

(xii) Remote technical assistance shall be provided before and during the meeting to all participants by the GSC services.

(xiii) Document sharing and collaboration features are not in the scope of the system, although there should be a possibility to share presentations and videos made available prior to the meeting.

(xiv) The system will **not** provide for simultaneous interpreting of any discussions. Users may use their own interpreter if needed.

IV. BUSINESS FUNCTIONAL NEEDS

Scenario 1: Informal European Council meeting

6. The members of the European Council, possibly assisted by other senior EU officials, meet to discuss a predefined agenda. Supporting services (e.g. Council Legal Service, note taker) may attend without normally intervening. If topics on this agenda require discussion of very sensitive or classified items, the choice can be made by the chair to hold this meeting on a properly secured virtual environment, if no physical meeting is possible.

7. In such cases, all participants would receive invitations indicating that the meeting will be held using the sVTC system. The solution will be made available to the participants, in a location easily accessible for the various Heads of State or Government. To offer a sufficient level of comfort to participants, the solution consists of a small group videoconferencing system managed and operated by the GSC. The participant is able to easily see the status of his input devices (camera and microphone(s)).

8. Preceding the meeting, a test session will be set-up with the participants authorised technical staff to verify their ability to participate in the conference. During the meeting, facilities should be present to conduct a videoconference, with participants being able to request the floor. When the meeting is finished, no content of the meeting will be retained.

Business functional needs

9. Needs identified for planning and set-up of the meeting include:

- FN1.1: System available on short notice (1 business day);
- FN1.2: Limited and identifiable number of meeting participants in Member States and EU institutions;
- FN1.3: Agenda of the meeting available made available to all participants;
- FN1.4: Documents relevant to the meeting to be distributed using GSC document distribution systems;
- FN1.5: Participants and technical teams having access cleared to the required level, as attested by their national NSA;

- FN1.6: Locations easily accessible by participants of the meeting;

- FN1.7: Locations compliant with the required security specifications in the Council security rules for protecting EU classified information;

- FN1.8: System test prior to the meeting with predefined time slot;

- FN1.9: Support from GSC technical staff (operators) during the set-up and testing;

10. Needs identified for the meeting conduct include:

- FN2.1: Sufficient level of comfort for meeting conduct:

  - FN2.1.1: Comfort of room (HVAC);

  - FN2.1.2: Comfort of furniture (Chair(s) / table)

  - FN2.1.3: Comfort of audio and video quality (minimal HD video)

- FN2.2: Visual indication of use of camera and microphone(s);

- FN2.3: Easy facility to request the floor;

- FN2.4: Remote support from GSC technical staff during the meeting.

11. Meeting closure needs:

FN3.1: No meeting content available after the meeting.

Scenario 2: Informal Meeting of the Council or Council preparatory bodies

12. The members of a specific Council configuration or a Council preparatory body, assisted by the Council Secretariat meet virtually to discuss a predefined agenda. If topics on this agenda could result in discussion items that are deemed very sensitive or classified, the choice can be made by the chair to hold this meeting a properly secured (virtual) environment, if no physical meeting is possible.

13. In such cases, participants will receive invitations indicating this mode via the usual channels (Delegates Portal). The meeting will be held using the sVTC equipment and solution made available to the participants. To offer a sufficient level of comfort to the participants, the solution consists of a small group videoconferencing system, managed and operated by the GSC. The participant is able to easily see the status of his input devices (camera and microphone(s)).

14. Preceding the meeting, a test session will be set-up with the participants and authorised technical staff to verify the equipment. During the meeting, participants should have the facility to request the floor. Presentations can be shared (displayed) in the system under the condition that they are delivered to the relevant GSC services in advance of the meeting, using the document sharing facilities provided by the GSC (outside this scope).

15. No joint drafting functionality is foreseen. The meeting will have no public sessions. When the meeting is finished, no content of the meeting will be retained.

Business functional needs

16. Planning and set-up of the meeting:

- FN1.1 to FN1.9 are applicable;
- FN1.10: Presentations to be visualised during the meeting will be inserted by GSC staff, and will need to be received in advance;
- FN1.11: The preferred location for the sVTC room is the Ministry of Foreign Affairs, as most of the possible contextual needs as described in the sVTC Applicable Context document will be in the domain of the CFSP.

17. Meeting conduct:

- FN2.1 to FN2.4 are applicable.

18. Meeting closure:

- FN3.1 is applicable.

Scenario 3: Meetings with two or more members of the European Council

19. In addition to the use cases described above, the system may serve two further use cases:

(i) the President of the European Council or the Council may hold consultations with one or more members of the European Council,

(ii) two or more members of the European Council or the Council or its preparatory bodies may hold a bi-or multi-lateral secure videoconference. In such cases, the meeting organiser would submit a request well in advance to the appropriate service in the General Secretariat of the Council to verify

availability of the system, with the same functional requirements identified above.

V BUSINESS SECURITY REQUIREMENTS

20. In all scenarios identified above the sVTC system will be considered 'secure enough' when It conforms to the Council Security Rules, underlying policies and guidelines and it is successfully security accredited to the level SECRET UE/EU SECRET;

21. Authenticity of the participants will be ensured by the means that resist a motivated state level attacker operating remotely (for more details concerning attack techniques assumed for such an attacker see GSC Threat Landscape [R-UE/EU-R]). Single mistake or failure of a participant must not allow the attacker operating from the Internet for successful impersonation. Users of the system are accountable for security credentials offered to them. To participate in a videoconference covering matters classified SECRET UE/EU SECRET or CONFIDENTIEL EU/EU CONFIDENTIAL, all participants require a security clearance up to the requisite level or be otherwise duly authorised by virtue of their functions, in accordance with Council security rules. In addition, participants will ensure before establishing the videoconference that all additional staff present have the same appropriate level of security clearance. The Security Operations Instructions will develop a procedure to establish compliance to this requirement prior to the videoconference taking place.

22. The system always shows the classification level of the conversation in progress, and informs the participants of any change in the classification level of the conversation in progress.

23. Integrity of the conversations and other information (e.g. presentations) exchanged via VTC will be protected by means that resist a motivated state level attacker operating remotely

24. The system (videoconferencing service) shall ensure proper functioning between 8:00 till 18:00 Brussels time, for 3 parallel sessions up to 32 users per session with the outage no longer than 5 minutes per session for all participants and no longer than 10 minutes for a single participant during technical problems.

25. The total time of planned unavailability of the system within the working hours (not including maintenance activities) should not exceed 24h per year (availability of 99.7%).

26. Users/participants will be responsible for ensuring two Internet connections with a sustained incoming and outgoing bandwidth of 4 Mbps and availability equal or above 99.7% as well as the availability of a local technical team (identified and known to the GSC operations team).

27. Information collected during the videoconference sessions must only be available on need-to-know basis and with appropriate security clearance when required. This includes also the IT staff operating the system (e.g. four-eyes access procedure)

28. These security requirements shall be demonstrated (tested) in the acceptance tests for the system.