Council of the European Union

Brussels, 22 January 2021
(OR. en)

5156/1/21
REV 1

LIMITE

CIS 13
CSC 5
RELEX 9

NOTE

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

This document describes:

- the business context in which the secure videoconferencing system allowing discussions up to SECRET UE/EU SECRET in support of European Council and Council decision making is to be deployed and used;

- the secure videoconferencing context (i.e. what videoconferencing capabilities are in scope);

- the security context (i.e. applicable rules and policies, potential threats, …) representing the enterprise constraints driving the security of systems.

1 Business context

1. The 'business context' is a high level description of the activities of the European Council, the Council and the GSC which demarcates the business activities which are in the scope of the defined capabilities of the system.

1.1 Institutional set-up

2. The **European Council and the Council** are two of the most important decision-making institutions of the European Union. They are both assisted by the General Secretariat of the Council under the responsibility of the Secretary-General appointed by the Council[1].

3. The **European Council** shall provide the Union with necessary impetus for its development and shall define the general political directions and priorities thereof[2]. It does not exercise legislative functions. It shall identify the strategic interests and objectives of the Union relating to the Common Foreign and Security Policy (CFSP) and in other areas of the external action of the Union[3] and shall identify the Union's strategic interests, determine the objectives of and define general guidelines for the CFSP, including matters with defence implications, and shall adopt the necessary decisions[4].

4. It consists of Heads of State or Government of the Member States, its President and the President of the European Commission. The High Representative of the Union for Foreign Affairs and Security Policy takes part in its work. The full-time President of the European Council is elected for a period of two and a half years, renewable once.

5. It meets at least four times a year, with additional meetings as necessary. This has been especially the case in recent years when different external or internal crises affecting the European Union required the action at the level of Heads of State or Government. It is also pertinent in the current sanitary situation that impose travel restrictions.

6. The **Council**[5], jointly with the European Parliament, exercises legislative and budgetary functions. It consists of a representative of each Member State at ministerial level. It meets in ten different configurations depending on the subject matter. The **General Affairs Council (GAC)** prepares and ensures the follow-up

[1] TFEU, Article 240(1)
[2] Treaty on European Union (TEU), Article 15
[3] TEU, Article 22
[4] TEU, Article 26
[5] TEU, Article 15

to meetings of the European Council, in liaison with the President of the European Council and the Commission. The Council is chaired by a Member State holding the office of its Presidency for six month on a basis of equal rotation, with the exception of the Foreign Affairs Council.

7. The **Foreign Affairs Council (FAC)** elaborates the Union's external action on the basis of strategic guidelines laid down by the European Council and ensures that the Union's action is consistent. It is chaired by the High Representative of the Union for Foreign Affairs and Security Policy. The High Representative is assisted by a **European External Action Service (EEAS)**, which works in cooperation with the diplomatic services of the Member States[6].

8. The **Permanent Representative Committee (Coreper)**[7] is responsible for preparing the work of the Council. Coreper is chaired by rotating Presidency and meets at least once a week in two distinct formations - Coreper I and Coreper II. There are more than 100 Coreper meetings a year (Coreper I and Coreper II together) and, especially for Coreper II, may require quick reaction time for its preparation and document exchange (including HCI).

9. The **Political and Security Committee (PSC)**, provided for in Article 38 TEU, plays a central role in the CFSP and CSDP domains. It performs two main functions:

   (1) it monitors the international situation in areas falling within the CFSP and contributes to the definition of policies, delivering opinions within the Council, without prejudice to the work of Coreper;

   (2) under the responsibility of the Council and of the High Representative, it ensures the political control and strategic direction of civilian and military crisis management missions and operations and may, when appropriate and if so empowered by the Council, take decisions in this area.

   The PSC is chaired by a representative of the High Representative.

10. The work of above mentioned bodies is supported by large number (approximately 160) of **preparatory bodies (committees and working parties)** that bring together experts from the Member States, the Commission and, in the CFSP/CSDP area, the EEAS. Some 35 of these support the work of the Foreign Affairs Council and are organised thematically or geographically.

1.2 Stakeholders and Actors

11. This section identifies stakeholders and key actors. The following stakeholders

[6] Treaty on European Union, Article 27
[7] TFEU, Article 240

have been identified, as consumers as well as contributors, in the context of secure videoconferencing:

- the European Council and the President of the European Council;
- the Council of the European Union and the Presidency of the Council;
- General Secretariat of the Council[8] and the Secretary General of the Council;
- Council preparatory bodies.

12. For identified stakeholders, the following actors may require communication needs of a very sensitive[9] or classified nature:

- European Council: elected full-time President, other members of the European Council (heads of state or government, the President of the European Commission), the High Representative of the Union for Foreign Affairs and Security Policy, the Secretary General of the Council and a very limited number of regular additional attendees or participants (e.g. President of the European Parliament and President of the European Central Bank);
- the Council of the European Union: Presidency of the Council (rotating Presidency and the High Representative for the Foreign Affairs Council), members of the Council (government ministers or state secretaries from each member state), European Commissioners. The High Representative supported by the EEAS plays a particular role in the CFSP/CSDP policies and coordination of the external action of the European Union;
- the General Secretariat of the Council: Secretary-General of the Council, Council Secretariat staff involved in preparation of meetings of the European Council, Council and its preparatory bodies (i.e. policy Directorates-Generals (RELEX, JAI, ECOMP, TREE, LIFE), Legal Service (JUR), General and Institutional Policy Directorate (GIP)); Interpretation Services managed by ORG/Conference Services, Digital Services (SMART) as a service provider and manager of the system, including Network Defence Capability; ORG/Safety and Security as responsible for assessing security threats, controlling accesses and defining information security rules, policies and guidelines in the GSC, including together with the Council's Security Committee.

---

[8] Article 235, paragraph 4 of the TFEU: *"The European Council shall be assisted by the General Secretariat of the Council"* in conjunction with Article 240, paragraph 2 of the TFEU: *"The Council shall be assisted by the General Secretariat, under the responsibility of the Secretary-General appointed by the Council"*.

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

- Council preparatory bodies:

  - Permanent Representatives Committee (COREPER): rotating Presidency (chair) and Member States' Permanent Representatives (COREPER II) or their deputies (COREPER I), Commission, which participates on permanent basis, and, when applicable EEAS;

  - Political and Security Committee (PSC): permanent chair from EEAS, Member States' representatives and Commission, which participates on permanent basis; PSC deals with the Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CDSP);

  - Committees and Working Parties: chair persons (rotating Presidency, elected chairs or GSC official for some committees, appointed EEAS representatives for defined working parties dealing with CFSP and CDSP), Member States' delegates, Commission experts and, when applicable, EEAS experts.

- Other actors

  - In addition to actors representing stakeholders regularly involved in the decision making processes of the European Council and the EU Council - EU Member States, the Commission and the EEAS - other actors representing EU bodies or agencies (e.g. EDA, Europol, Eurojust, Frontex …) could be involved in secure videoconferencing.

1.3 Business activities in scope

13. The decision making processes of the European Council and the Council involve information sharing and collaboration/communication, and convergence of positions and consensus-building through negotiation.

14. Information is a critical asset that enables the European Council and the Council to exercise their Treaty mandates and achieve their objectives. The General Secretariat of the Council has several platforms that allow for the exchange of information between stakeholders. depending on the nature of the information. These include in particular Delegates Portal for the exchange of unclassified information with the Member States and two wide area networks (WAN) - CORTESY and EXTRANET - for exchange of classified information (up to CONFIDENTIEL UE/EU CONFIDENTIAL) with the Member States, EEAS and the Commission. The GSC is currently deploying a new system for high classified information (HCI) for exchanging information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET.

15. The activities around the Council Decision Making Processes are mostly organised around physical meetings, where the GSC offers an environment, either in Brussels or Luxembourg, where collaboration and communication among actors involved (Council Presidency, the Member States, the Commission, EEAS, the GSC) can take place in an optimal manner on the basis of the information exchanged with the use of above mentioned systems. To complement the environments for physical meetings, the GSC has implemented on an experimental basis a complementary VTC system that has been first used in 2019 by few Council preparatory bodies. An initial proof of concept took place under the Finnish Presidency.

16. In 2020, in response to the sanitary restrictions imposed due to the Corona-19 crisis, the GSC put in place a new videoconferencing platform allowing informal ministerial meetings and meetings of officials to continue. This platform can be used in the context of non-classified, non- sensitive collaboration.

17. The need has been confirmed to establish a videoconferencing platform allowing for discussions on very sensitive and classified information (up to SECRET UE/EU SECRET). It is to be noted that classified discussions currently take place only in specific meeting rooms in Council premises.

18. The following business processes of the (European) Council may require discussions on very sensitive and classified information throughout or at certain critical stage(s) of the process:

	Business process name
(European) Council decision making processes	European Council: Define the EU's overall political direction and priorities European Council: External representation of the EU European Council: Nominate and appoint for senior EU roles Council/European Council: Develop strategic planning and agendas Council: Negotiate and adopt EU laws Council: Coordinate policies of Member States Council: Develop EU's common foreign and security policy Council: Coordination in international organisations Council: Conclude international agreements Council: Crisis management

2 The context for secure videoconferencing (sVTC) capabilities

2.1 General considerations

19. In general, *collaboration* should be understood as virtual collaboration via technology-mediated communication through verbal, visual, written and digital means. Following collaboration capabilities can be distinguished:

- Asynchronous written collaboration capabilities: this occurs when community members communicate without the ability to instantly respond to messages or ideas. Examples include e-mail, discussion boards, application-specific groupware and shared information on central storages. Asynchronous written collaboration includes also support for non-routinely collaboration processes, often referred to as case management, including electronic signing as needed;

- Synchronous written collaboration capabilities: it occurs when community members are able to share information and ideas instantaneously. Examples include instant messaging and chat rooms;

- Audio-conferencing: it allows collaborators to communicate verbally in real-time without the use of continuously updated, shared imagery. Examples include phone calls and conference calls involving multiple participants;

- Video-conferencing: it allows communication with the use of real-time sharing of verbal and visual information. Video-conferencing includes continuously updated visuals of collaborators, diagrams, physical objects, or computer screens (e.g. for simultaneous drafting). Not all these features are available or enabled in all types of video conference systems, and the proposed service will detail what is required for the different scenarios. Examples of video-conferencing are group video- conferencing in dedicated rooms and desktop video-conferencing;

2.2 Capabilities in scope

20. The capability addressed in this document is the **video-conferencing component** of the overall collaboration set out above, more specifically the secure videoconferencing capability allowing for virtual meetings handling information up to and including level SECRET UE/EU-SECRET.

21. This sVTC capability will be complemented, when necessary, by information exchange ensured by classified CIS, namely Extranet, Cortesy and HCI in the near future.

2.3 Current technical solutions

22. The VTC capabilities currently available to the identified stakeholders are the following:

1. A videoconferencing platform operated and supported by the GSC used for informal virtual meetings of European Council members, Council members and members of its preparatory bodies. This platform has the following functionalities:

    - multipoint videoconferencing with a current capacity of around 1000 simultaneous connections, divided over multiple virtual meeting rooms;
    - simultaneous interpretation for all videoconferences for up to 24 languages, integrated with the on-site interpretation capabilities of the GSC;
    - management of videoconference sessions via tools embedded in the conference tool, or with additional applications, such as the 'request the floor' application;
    - continuous monitoring of the videoconference sessions by operators;
    - from a security point of view, the following measures are implemented:
        - each virtual meeting room is protected with a uniquely generated meeting room ID (5 figures) and associated PIN (6 figures), totalling 11 figures;
        - where required, participants are received in a lobby and transferred in a second stage, after visual identification, to the main virtual meeting room;
        - all channels are end-to-end encrypted using commercial encryption based on AES-256;
        - the software used is from a company located in the EEA;
        - the system software is hosted on a private instance of a hyper-scaler (IaaS: Infrastructure as a Service), located in an EU datacentre, and an additional on-premises instance is available. Both instances are operated by the GSC;
        - platform management is done through the on-site identity management service of the GSC;
        - the platform is monitored with real time alerts and logging by the GSC's Network Defence Capability.

2. A platform called Interactio, being a SaaS (Software as a Service) hosted on a hyper-scaler in an EU datacentre, which is operated by the European Parliament and used for some trilogue virtual meetings;

3. Videoconferencing platforms operated and selected by the Presidency used for some informal virtual meetings hosted by the Presidency.

2.4 Target solution

23. The implementation of the secure videoconferencing platform aims to offer the following benefits compared to the current platforms described above:

- ensure that the (European) Council has a secure capability to allow virtual meetings and discussion on classified information or information deemed very sensitive;

- offer an alternative for onsite meetings dealing with classified or very sensitive information;

24. It is envisaged to implement a solution that meets all the requirements of stakeholders related to the required level of collaboration, building on its functional characteristics identified above and allowing discussion up to and including the level SECRET UE/EU SECRET.

25. The sVTC should have following functionalities:

- multipoint videoconferencing with a capacity to hold multiple simultaneous conferences taking into account the physical limitation of the end points in the member states and institutions;

- management of the videoconference sessions via tools embedded in the conference tool, or with additional applications, like the 'request the floor' application;

- continuous monitoring of the videoconference sessions by operators;

- Security features compliant to the Council Security Rules and their implementing policies and guidelines, enabling the security accreditation to the level SECRET UE/EU SECRET (to be detailed and documented in the security accreditation process that will accompany the development).

26. Management of EUCI classified information and collaboration at the levels of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET require specific measures in accordance with Council Security Rules in terms of personal security (such as 'personal security clearance'), physical security and industrial security, in particular:

(a) special protective measures applied to the CIS, namely:

- TEMPEST security measures;
- use of approved cryptographic products.

(b) application of physical security measures (currently already applied for physical SECRET UE/EU SECRET meetings) meaning that the sVTC capability will allow for videoconferencing from a fixed location endpoint using technical equipment provided by the GSC and using the GSC services as a central hub;

2.5 System ownership and management

27. System Owner: the system will be owned by the Council and operated by the GSC as the service provider.

28. Internal GSC business owner: Digital Platforms Directorate within Digital Services (SMART) and DG RELEX are the GSC business owners for classified platforms and systems linking GSC with delegations.

29. Risk owner: COREPER is the risk owner for all systems handling EU classified information operated by the GSC and linking the GSC with delegations.

3 Security context

3.1 Threat landscape

30. The European Union and its Member States are global players, especially in economic, foreign policy and also in military terms. Under its common foreign and security policy, the EU plays a role at the global scale and is an important player in international organisations. It is present in its immediate neighbourhood (e.g. Western Balkans) and in other regions of the world (Africa, the Middle East and Asia) not only politically, but also with concrete civilian and military missions (over 30) in support the EU foreign and security policy objectives.

31. The EU's global role is underpinned in the EU Global Strategy (EUGS) on Foreign and Security Policy adopted 28 June 2016. This is an updated doctrine of the European Union to improve the effectiveness of the defence and security of the Union and its Member States against evolving security threats and challenges, the protection of civilians, cooperation between the Member States' armed forces, management of immigration, crises etc. The EUGS focuses on Europe's own security and on the neighbourhood. Following the terrorist attacks in Paris and Brussels and the refugee crisis, the counter- terrorism and control of Union's external borders became much more important than before and led to increased cooperation between the Member States, EU institutions and EU agencies.

32. EUGS also recognises that European Union and its Member States should work together to counter threats and challenges created by economic volatility, climate change, energy insecurity and illegal migration.

33. The increased activity of the EU and the growth of the EU's global role attracts increased interest in general, but especially from those who can be influenced by EU external action, in particular actors that may be directly affected by EU action or the third states whose policies (commercial, military, human rights, etc.) are in conflict with EU policies. In some cases, this leads to increased intelligence gathering or even influence operations against EU decision-making processes. Intelligence activities against institutions in Brussels (Council, EEAS, Commission, Parliament and EU-agencies) and EU Delegations worldwide, as well as against EU Member States are a constant threat. This issue was recently addressed by the June 2018 Foreign Affairs Council and European Council[10].

[10] On 29.06.2018 the European Council in its Conclusions called *"for further coordination between Member States and, as appropriate, at EU level and in consultation with NATO, to reduce the threat from hostile intelligence activities"* while the 25.06.2018 Foreign Affairs Council Conclusions took "*note of the proposals to strengthen resilience /.../ and help the EU and its Member States to bolster their capabilities to address hybrid threats, including in the areas of cyber, strategic communication and counter-intelligence."*

34. The EU is often involved in international trade negotiations, where the disclosure of negotiating positions can be damaging to the EU interests. The disclosure of EU negotiating positions has been a concern during the negotiation of TTIP agreement.

35. In internal security terms, terrorism, hybrid threats and organised crime are a significant concern. The EUGS calls for tighter institutional links between EU external and the internal area of freedom, security and justice. Closer ties shall be fostered through joint Council meetings and joint task forces between the EEAS and the Commission. More information sharing and intelligence cooperation is encouraged between Member States and EU agencies to prevent acts of violent extremism, terrorist networks and foreign terrorist fighters, as well as monitoring and removing unlawful content from the media.

36. The ENISA[11] Threat Landscape Report 2020 points out the following main trends relevant to our service, among others, that:

- Attack surface in cybersecurity continues to expand as we are entering a new phase of the digital transformation;

- There will be a new social and economic norm after the COVID-19 pandemic even more dependent on a secure and reliable cyberspace;

- Finely targeted and persistent attacks on high-value data (e.g. intellectual property and state secrets) are being meticulously planned and executed by state-sponsored actors.

37. The GSC Threat Landscape confirms that the compromise of the information can have a negative consequences for the Council, GSC or EU Member States, for example disruption of the work of the Council working party, the possibility to influence EU policies and negotiations or the cancellation of the European Summit. The threat sources may pursue different objectives by compromising the information, such as:

(a) **Espionage/Intelligence** - the Council deal with sensitive topics and the information handled by the GSC may be exploited for intelligence gain purposes. Unauthorised disclosure of classified information supporting Council activities may lead to high degree of prejudice to the interest of the EU and/or its Member States.

(b) **Terrorism** - terrorist attack on the Council may be a compelling option for terrorist organisations.

(c) **Public Order** - the EU is seen as one of the main antagonists for some

[11] European Union Agency for Network and Information Security (www.enisa.europe.eu)

extreme right activists and anarchists groups. There are also state actors that may have an interest to undermine the reputation and thrust in the EU by increasing the likelihood of internal conflicts within the EU. 'Fake' news or other means of propaganda are key mechanisms used to influence the way in which institutions are perceived by society and can damage the EU reputation. As the GSC serves as a 'hub' for distributing information to the Member States, attacking its distribution systems allows for creating a havoc in the whole EU.

(d) **Crime/cybercrime** - while the Council and/or GSC information related to the Council decision making process may not directly be an attractive target for criminal purposes, non-targeted attacks and scenarios by organised crime for asking ransom or on behalf of other groups should not be neglected.

38. The EU needs to protect the autonomy of its decision-making processes and information sharing between EU institutions and agencies[12], which are vital for the EU to be able to conduct its foreign and security policy, to pursue EU economic interests and ensure its internal security. Therefore any system handling classified information in support of decision-making and/or information sharing shall be reliable and trustworthy and its security objectives in a broad sense shall be:

- to safeguard EUCI against threats to confidentiality (espionage, compromise or unauthorised disclosure;
- to safeguard EUCI information handled in communications and information systems and networks, against threats to integrity and availability;
- to ensure availability of EUCI information in communications and information systems;
- to safeguard installations housing EUCI information from sabotage and malicious wilful damage;

39. As VTC system the list of adversaries against which the system will be protected include:

- motivated state level actors operating remotely;
- insiders, including IT staff, acting individually;
- cyber-crime and lower skilled attackers.

[12] European Council meeting (20 June 2019) - Conclusions (par. 6/7)

3.2 Information security rules, policies and guidelines applicable for handling of EU classified information

40. Classifying information as EUCI guarantees the continuity of its protection under existing legal framework when exchanged. The legal framework for EUCI handling and exchange applicable to the Council, European Council, GSC and EU Member States is defined by the EU Member States. It consists of the following rules, policies and guidelines:

Ref.	Name	Reference
[1]	The Council Decision on the Security Rules for Protecting EU Classified Information	2013/488/EU - OJ L 274 of 15.10. 2013, p.1
[2]	Decision 33/2028 of the Secretary-General of the Council implementing in the GSC the Security Rules for Protecting EUCI (Council Decision 2013/488/EU)	DE 33/18 of 28 August 2018
[3]	Business ownership and security risk acceptance for IT platforms or systems and platforms processing documents and files for Council decision-making	ST 6888/16 LIMITE of 9 March 2016 and ST 7386/16 of 2 May 2018 (approved by Coreper)
[4]	Information Assurance Security Policy on Security throughout the Communication and Information System Life Cycle	ST 16268/12 of 16 November 2012
[5]	Information Assurance Security Guidelines on CIS Security Accreditation	ST 10346/14 LIMITE of 28 May 2014
[6]	Information Assurance Security Guidelines on System-specific Security Requirement Statement (SSRS)	ST 16085/13 of 14 November 2013
[7]	Information Assurance Security Guidelines on Security Operating Procedures (SecOPs)	ST 16086/13 of 14 November 2013
[8]	Policy on creating EU Classified Information	ST 10872/11 LIMITE of 30 May 2011
[9]	Policy on registration for security purposes	ST 16751/11 of 11 November 2011
[10]	Guidelines on marking EU classified information	ST 10873/11 of 23 August 2011
[11]	Guidelines on downgrading and declassifying Council documents	ST 14845/11 of 28 September 2011
[12]	Policy on security awareness and training	5998/15
[13]	Guidelines on procedures in case of EUCI compromise	12207/17
[14]	Guidelines on industrial security	15643/16

[15]	IA Security Policy on Cryptography IASP 2	ST 10745/11
[16]	IA Security Policy on Public Key Infrastructure	ST 11660/13
[17]	IA Security Guidelines on the Application of the Policy on Cryptography IASG 2-01	ST 12022/13
[18]	IA Security Guidelines on Second Party Evaluation IASG 2-02	ST 13910/12
[19]	IA Security Guidelines on Approval of Cryptographic Products IASG 2-04	ST 10199/19
[20]	IA Security Policy on Interconnection IASP 3	ST 6488/15
[21]	IA Security Guidelines on Boundary Protection Services IASG 3-02	ST 139909/12
[22]	IA Security Policy on Network Defence IASP 4	ST 8408/12
[23]	IA Security Guidelines on Network Defence IASG 4-01	ST 9650/15
[24]	IA Security Guidelines on Intrusion Detection and Prevention in CIS IASG 4-02	ST 7867/15
[25]	IA Security Guidelines on CIS Security Incident Handling IASG 4-03	ST 7049/16
[26]	IA Security Policy on CIS Security Engineering IASP 5	ST 10416/15
[27]	IA Security Guidelines on Access Control IASG 5-04	ST 17547/13
[28]	IA Security Guidelines on Web Applications IASG 5-06	ST 7124/13
[29]	IA Security Guidelines on Data Separation IASG 5-07	ST 12131/14
[30]	IA Security Policy on TEMPEST IASP 7	ST 16311/12
[31]	IA Security Guidelines on Selection and Installation of TEMPEST Equipment IASG 7-01	ST 14006/13
[32]	IA Security Guidelines on TEMPEST Zoning Procedures IASG 7-02	ST 9507/16
[33]	IA Security Guidelines on User generated Passwords and Password Management IASG BP-08	ST 17745/11

41. The Council Decision on the Security Rules for Protecting EU Classified Information (‘Council Security Rules') is the legal basis for protecting the EU classified information. It applies to the Council and the General Secretariat of the Council and the Member States. It applies to handling of EUCI by all Council preparatory bodies (i.e. Council working parties, Coreper, PSC, Committees established by Treaties, etc.). The rules are also supplemented by an intergovernmental agreement among the Member States.

42. The Council Security Rules are also applied by:

- EU agencies and bodies established under Titles V or VI of the Treaty on European Union;

- crisis management operations established under Titles V, Chapter 2, of the Treaty on European Union;
- EU Special Representatives and the members of their teams.

43. The Council, the Commission and the EEAS have committed to apply equivalent security standards for the protection of the EUCI.

3.3 Responsibilities

3.3.1 General Secretariat of the Council

44. The Secretary-General has responsibility to take all appropriate measures to ensure that, when handling EUCI, the Council Security Rules and any policy guidelines deriving from it are respected within the premises of the GSC by all staff employed by the GSC (EU official, contract agents, temporary agents), by personnel seconded to the GSC (e.g. seconded national experts) and by GSC external contractors.

3.3.2 EU Member States

45. EU Member States (EU MSs) have the responsibility to take all appropriate measures, in accordance with their respective national laws and regulations, to ensure that when EUCI is handled, the provisions of the Council Security Rules are respected by their competent authorities, personnel or contractors.

3.3.3 Council (with regard to third states or international organisations)

46. As part of its responsibility for ensuring overall coherence in the application of the CSR, the Council shall approve:

- security cooperation levels with third States and international organisations;
- security agreements with third States or international organisations on the protection and exchange of EUCI to be sign by the Secretary-General;
- the release of EUCI to third States and international organisations (delegated to the Secretary General of the Council).

3.4 Security of the system (Risk owner requirements)

47. The following Information Assurance (IA) properties and concepts are essential

for the security and correct functioning of operations on CIS:

Authenticity	:	the guarantee that information is genuine and from bona fide sources;
Availability	:	the property of being accessible and usable upon request by an authorised entity;
Confidentiality	:	the property that information is not disclosed to unauthorised individuals, entities or processes;
Integrity	:	the property of safeguarding the accuracy and completeness of information and assets;
Non-repudiation	:	the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied

3.4.1 Authenticity

48. The system shall ensure the authenticity of the participants, i.e. that participants are unequivocally identified for every access and operation they perform within the system.

3.4.2 Availability

49. The sVTC system should ensure the availability of its service in accordance with following criteria:

    - service operations window: the service is made available on a request basis, where normal operations are foreseen during standard working days from 08:00 to 18:00. Operations of the service includes support.
    - crisis operations: on-site operations will be available 24/7 during crisis situations;
    - total unavailability (downtime) of sVTC system must not exceed a 24 hour period;
    - periods of unavailability will be tolerated for scheduled and announced maintenance.

50. The above rule of thumb doesn't apply to partial downtimes with a limited operational impact (e.g. failing terminal equipment in some end-points of the system). In this case partial downtimes must not exceed 1 week (the risk is ranked: Low).

3.4.3 Confidentiality

51. The system will handle information classified R-EU/EU-R, C-EU/EU-C and S-EU/EU-S, as well as very sensitive information. It shall ensure complete

confidentiality vis-à-vis the external world, i.e. any third state, organisation or persons not participating in the Council decision making process. The originator cannot assign need-to-know to any external actors (access to EUCI to third states and international organisations can only be decided by the Council in accordance with CRS). The confidentiality vis-à-vis the users using the system will be addressed in the Secure Operation Procedures to be developed during the implementation phase.

3.4.4 Integrity

52. A loss of integrity of the system is damageable inter alia to all dimensions of the security of information. The integrity of the system requires that only justified and approved items (e.g. hardware, software, settings) are present. This implies a rigorous inventory and management process. It also implies that only cryptographic products approved by the Council for the level up to and including S-UE/EU-S shall be used and TEMPEST measures must be implemented in accordance with the relevant Council Information Assurance policy.

3.4.5 Non-Repudiation

53. The system shall record all activities in auditable way to ensure the full control of EUCI.

3.5 Security of information (Risk owner requirements)

3.5.1 Authenticity

54. Authenticity of the collaboration is implicit in the system due to its limited access.

3.5.2 Availability

55. The availability of the information of the collaboration platform is only guaranteed during the actual collaboration window (during the videoconference). No information will be recorded, stored or otherwise processed about the collaboration activity. Metadata (logs) will be kept in accordance to applicable best practices which will be detailed in the system documentation.

3.5.3 Confidentiality

56. Confidentiality requirements consist of defining a set of strict rules to limit access

to the system. It is therefore essential that all participants to the collaboration activity are identified uniquely.

57. The 'need-to-know' can only be exercised by a named entities in an authenticated context ('deny by default' principle applies).

3.5.4 Integrity

58. Integrity of the information is ensured by the closed nature of the platform, and the visual verification of the author of the information in the secure videoconferencing platform.

3.5.5 Non-Repudiation

59. As no recording of collaboration will take place, non-repudiation of the information is out-of-scope.