Council of the
European Union

Brussels, 17 November 2021
(OR. en)

12920/21

SAB 5
CSC 356
CSCI 131
CIS 114

REPORT

From:	General Secretariat of the Council
To:	Security Accreditation Board Security Committee
Subject:	Status report on SAB activities

Delegations will find in Annex an updated report on the status of the different systems and projects under accreditation.

The report is aimed to serve as basis for discussion at the SAB meeting on 25 November 2021.

Annex

Status Report on Security Accreditation Board activities

1. EDA S-UE/EU-S AND R-UE/EU-R CIS SECURITY ACCREDITATION

The EDA-S CIS Initial Operating Capability (IOC) implementation phase II is moving forward.

The first batch of the accreditation documentation on the S-UE/EU-S portion of the system was provided on 28 May 2021 and covers six documents, namely the SSRS, the Risk assessment, the SecOps, the traceability matrix, the resource plan, and the system disposal procedure.

With WK 7327/2/21 + ADD 1 - 9 the above six documents together with a copy of the CONOPS, a first security test plan and the Low level Design have been reviewed by the MS. Comments received from the MS have been redistributed with WK 9805/21 INIT. EDA has addressed the comments received by the MS and has updated the documentation accordingly.

The IOC implementation phase kicked off at end of October 2021. The audit team from Slovenia who confirmed their participation in the audit exercise on the S-UE/EU-S system will visit EDA premises in December this year.

On the R-UE/EU-R portion, both EDA and the contractor are finalising the batch of accreditation documentation that will be shared on 19 November 2021. This first batch contains a number of documents, namely the business needs, context document and CONOPS. Further batches of documentation will be share with the Council in due time and with sufficient notice, containing the SSRS, Risk Assessment, the SecOps, the Low-level design, the security test plan, the resource plan and the system disposal procedure.

2. SVTC

2.1 sVTC Project Status Summary

sVTC project has been initiated, the high level design is ready and the project enters now in the "proof of concept" and the construction phase (design phase, ref. doc. 5157/1/21 REV 1)

Major project milestones and deadlines – estimation:

- Initiation phase : due by Q3 2021 (status : completed in October 2021);
- Design & POC phase : due by Q1 2022 (status : started in October 2021 and ongoing);
- Procurement phase : due by end Q3 2022;
- Implementation at GSC : due by end Q4 2022;
- Security accreditation process : due by Q4 2022 for the GSC side, - to be continued depending on progress in MS
- End of deployment & activation phase : Q2 2023

Project initiation and planning - closed

- The budgetary planning presented to CCCIS (ref. doc. 5157/1/21 REV 1) has been reviewed and accepted by the GSC Project Evaluation Committee.
- The Project Charter and planning has been reviewed and validated by GSC IT Governance office.

Project construction – design phase - ongoing

- Design and POC phase : started in October 2021 and ongoing
  - First version of the High Level Design of the IT infrastructure completed, under revision of the GSC internal stakeholders;
  - Assessment of the capacity of the GSC data centres to host sVTC equipment is ongoing.

Next activities:

- Design and POC phase:
  - Building the infrastructure for a "Proof of Concept":
    - Building, in a smaller scale, a VTC system to perform functional tests.
    - Selection of the equipment type
    - Validation of the solution.
  - Low level Design
- Start the Accreditation process :
  - first iteration of the SRSS (conceptual design from HLD)

2.2. High Level Design – sVTC IT Architecture

The High Level Design document proposes a technical architecture to support the sVTC functionalities fulfilling the Business and Security needs (doc. 5154/1/21 REV 1, 5156/1/21 REV 1, 9457/21 + COR 1).

The High level Architecture presents a logical design and the technical requirements to deliver the following services:

- Video communication services using modern endpoints supporting H.323, SIP and WebRTC protocols from accredited meeting rooms.
- Allowing authorized users to join video conferences using endpoints remotely managed.
- Deploy, in the Central Hub, VTC components with High Availability configuration.
- Endpoints and crypto devices installed in meeting rooms will not be redundant.
- Deploy commercial, off-the-shelf (not Tempest), endpoints that support conference features without the installation of additional devices.

The High Level Design includes from the beginning elements that contribute to the functioning of the VTC infrastructure:

- Backup, monitoring and auditing requirements
- Roles required to support the conferences and to manage the VTC service.

3. EU RESTRICTED CLASSIFIED INFORMATION (RCI)

The GSC will provide an oral statement during the SAB.

4. HCI

Project status

HCI is in Phase 2 - Engineering as described in IASP-L.

Phase 1- Justification

HCI has already undergone the Phase 1 - justification activities as requested by IASP-L.

The applicable context, business functional needs and the risk assessment from the business owner's point of view[1] were reviewed both by the CCCIS and the SAB.

The conceptual security architecture and the first iteration of the system specific requirements statement[2] were reviewed and approved by the SAB.

[1] WK 23/19
[2] WK 4869/19

The security accreditation strategy[3] was reviewed and approved by the SAB.

The SAB concluded that the Phase 1 was completed and that the procurement and "Phase 2 - Engineering" for the HCI system could start[4].

As a consequence of the decision of the Commission to use the same provider and technology (based on SECUNET Solutions) for handling of high-classified information to meet requirements of several Commission's Directorate Generals ('SUE project'), the new business need has been identified[5]: the possible use of the same hardware (SINA workstations) for connection to HCI (GSC) and SUE (Commission). Therefore an addendum to the already approved WK 23/2019 outlining the applicable context, business functional needs and the risk assessment has been submitted to CCCIS the 21 April 2021, and approved[6] by CCCIS in June 2021. A questionnaire[7] was prepared and send to delegations to assess their opinion on the 'dual usage configuration' of HCI and/or SUE workstations. The outcome of this questionnaire might have an impact on the SAS, Risk Analysis, SecOPS and SSRS. The GSC is still awaiting the replies from some Member States on the questionnaire.

Phase 2 – Engineering

The SAB has received the SSRS Phase 2[8]. Comments from France were received.

The SecOPS[9] were submitted to the SAB the 28 May 2021. Comments from Portugal and France were received.

A new version of the SSRS Phase 2[10] and the SecOPS[11] were submitted to the delegations by the CIS Provider. Answers[12] from the CIS Provider to the FR and PT comments were also provided.

A Security Tests, Evaluations and Inspections Plan[13] has been developed and send to delegations the 24 October 2021. Comments were received from NL, LU and PT. The inspection has started.

---

[3] 7968/3/21
[4] 11676/19
[5] WK 2518/21
[6] ST 10697/21
[7] WK 8443/1/21
[8] WK 3931/1/21 (R-UE/EU-R) and WK 5435/21
[9] WK 7019/21 (R-UE/EU-R)
[10] WK 3931/2/21 (R-UE/EU-R)
[11] WK 7019/2/21 (R-UE/EU-R)
[12] WK 9214/1/21 and WK 13649/21

Proposed next steps

Calendar

The project calendar has been updated:

Phase	Activities		Document	SAB action
Phase 1 (System security justification) documentation (Ref: IASP-L: Phase 2, doc. 16268/12, point 17)	Elicitation of business needs • Business functional needs • Applicable context • Risk assessment (Business viewpoint)		WK 23/19 05/02/2019	Endorsed by SAB Note to COREPER 11676/19 20/08/2019
	System specific security requirements statement (SSRS) - 1st iteration		WK 4731/19 (R-UE/EU-R) 04/04/2019	
	System conceptual architecture		WK 4869/19 09/04/2019	
	Security accreditation strategy		7968/3/21	Approved by SAB 21/06/2021
	Update of 'Elicitation of business needs' 'Dual use' of HCI workstations		WK 23/2019 ADD1 Decision by CCCIS deferred	
Phase 2 (System security engineering) documentation (Ref: IASP-L: Phase 2, doc.	SSRS 2nd iteration	October 2021	WK 3931/2/21 (R-UE/EU-R)	CIS comments review
	Security Operational Procedures (SecOPs)	November 2021	WK 7019/2/21 (R-UE/EU-R)	Review 26/11/2021
	Security Test Plans template for validation	October 2021	WK 12396/21	Breach of silence

[13] WK 12396/21 (R-UE/EU-R)

	of the security posture and contingency activities		(R-UE/EU-R)	procedure
	Security Resources Plans (budget, contracts…)	March 2021	GSC internal doc 22/01/2021	Validated by SAG 30/03/2021
	Proposal to SAB for the residual risks acceptance	December 2021		
	Approval of residual risks by COREPER (risk owner)	January 2022		
Acceptance and deployment in the GSC	Solution high level design (HLD)	June 2020	WK 3916/21 18/03/21	
	Solution low level design (LLD)	January 2021		N.A.
	Secure workflows adaptation	February -June 2021		N.A.
	Final production, staging and training environments implementation in the GSC	July 2021		N.A.
	Security tests	October- December 2021		N.A.
	Adaptations of security settings in view of security test	July 2021		N.A.
	The initial accreditation of the central and crypto management infrastructures at the GSC premises (PROD environment only)	January 2022		

Deployment in the Member States (MFA and PermReps)	Progressive deployment in the Member States. Each time a Statement of Compliance (SoC) is received from a MS and approved by the SAB, the scope of the HCI accreditation statement will be updated (as long as the accepted residual risks remain equivalent).	January 2022 onwards (subject to successful completion of proceeding activities)		

5. CORTESY

The IATO of Cortesy has been extended[14] until 31 December 2021. Member States will find in doc. 13731/21 R-UE/EU-R the last updated status on CORTESY SoC's.

Outstanding issues

IATO expiration

The SAB has endorsed the Member States Network Risk Statement[15].

The GSC's objective is to decommission CORTESY in a mid-term. This depends on the advancement of both HCI project (CORTESY/CDM segment) and the RCI project (CORTESY/COREU segment). The new HCI system shall replace CORTESY/CDM and CORTESY/COREU-C segments. It is expected this will be done by mid-2023 after HCI workstations have been deployed in all Member States' locations in 2022, system has been technically tested and pilot phase has been completed (tentatively Q1-Q2/2023).

The RCI system shall replace the CORTESY/COREU-R+L[16]. The 'Phase 1' security accreditation documentation should be submitted to the SAB towards end of Q1/2022 (see point 3 above). It is considered ineffective to start the accreditation of CORTESY that should be decommissioned. Instead, resources (both at the GSC and Member States sides) should focus on the accreditation of the new RCI system.

[14] WK 8339/21 and doc.10658/21
[15] WK 7611/1/21
[16] 14408/19, p. 6

The SAB is invited to review and approve the list of SOCs received between June 2021 and November 2021 (list provided on DVD). Delegations concerned are invited to update their expired SOCs whereas those, whose SOCs are expiring soon, are invited to plan on time their renewal.

The SAB is invited to extend the IATO for CORTESY until **December 2022**.

6. EXTRANET-R/DELEGATES' PORTAL-R

The IATO of Extranet -R/DP-R has been extended[17] until 31 December 2021. Member States will find in Doc. 13731/21 R-UE/EU-R the last updated status on Extranet-R/Delegates' Portal-R SoC's.

Outstanding issues

Extranet-R/DP-R IATO expiration

The extension of the Extranet-R/DP-R IATO come with two clauses required by the delegations. The first one was the enforcement of a stricter approach for the outdated SoCs. The GSC is working on a procedure for improving their management and way of communication with delegations (see the point on SoC Management below).

The second clause was the production of the result of the impact analysis of the situation as described in WK 2560/21 (R-UE/EU-R). The SAB has approved the impact assessment as stated in WK 7836/1/21. The GSC will put in place the following remediation plan:

a. the GSC will perform an independent static code analysis in order to identify vulnerabilities and potential malicious modifications;

b. the analysis will be limited only to the components considered critical from security point of view;

c. the GSC will perform an external penetration test of Delegates Portal / Delegates Portal R focusing on existing vulnerabilities or vulnerabilities introduced in the software production process;

d. the analysis will be presented to the Member States together with risk and mitigation plan should test discover any new severe vulnerabilities;

[17] WK 8336/21 and doc. 10653/21

e. the analysis will be finalised before the end of 2021 and shared with the delegates.

The Delegates Portal security code review has already been contracted and is planned for week 46 (15-19 Nov). The Delegates Portal external penetration test is foreseen for week 49 (6-10 Dec). The reports for both activities should be available by end December 2021.

The SAB is invited to review and approve the list of SOCs received between June 2021 and November 2021 (list provided on DVD). Delegations concerned are invited to update their expired SOCs whereas those, whose SOCs are expiring soon, are invited to plan on time their renewal.

The SAB is invited to extend the IATO for EXTRANET-R/DELEGATES' PORTAL-R until **December 2022**.

7. FADO

The IATO of FADO has been extended[18] until 31 December 2021. Member States will find in doc. 13731/21 R-UE/EU-R the last updated status on FADO SoC's.

Preparations for the connection of Frontex to the existing Expert FADO system are ongoing; the crypto devices have not yet been shipped to Poland.

Outstanding issues

New Expert FADO PoP for Frontex

The GSC expects to receive the SoC for the planned new Expert FADO PoP for Frontex later this year. The SAB will be invited to review and approve the SoC by using a silent procedure.

IATO expiration

The SAB has approved the impact assessment as stated in WK 7836/1/21. The GSC will assess the risk generated by the potential FADO source-code leak and seek SAB's directions for the treatment.

In order to assess the risk on FADO, the GSC proposes the following action plan:

a. The GSC will analyse the isolation of Expert-FADO in order to ensure that this isolation provides sufficient protection against exploitation of internal vulnerabilities of the system.

[18] WK 8334/21 and doc.10655/21

b. A report on this analysis will be provided to the SAB later this year to support the residual risk acceptance process.

The expert-FADO isolation analysis has already started. The report with the conclusions of the analysis should be sent out by the end of 2021.

The SAB is invited to review and approve the list of SoCs received between March 2021 and June 2021 (list provided on DVD). Delegations concerned are invited to update expired SoCs whereas those, whose SoCs are expiring soon, are invited to plan on time their renewal.

Proposed next steps

As soon as the risk assessment described above is available, the GSC will send it to SAB for comments.

The SAB is invited to extend the IATO for FADO until **December 2022**.

8. INFORMATION ON SoCs MANAGEMENT

As requested by delegations, the GSC SAA is developing a stricter approach to deal with outdated SoCs.

With doc. 11120/1/21 REV 1 the GSC launched a consultation on how to address SoC management issues. Replies provided by the MS have been consolidated in doc. 12182/21.

With doc. 13274/21 the GSC will propose a way-forward on this issue.