TRUST AND VERIFY

TrustCB SESIP Scheme Interpretation 1: Re-use of CC certification results

Version 1.2

Contents

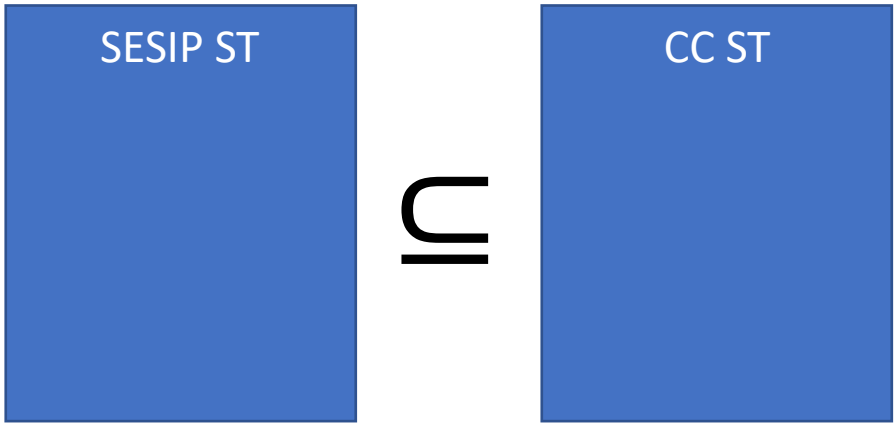
1 Introduction

TrustCB owns and operates the TrustCB SESIP (Security Evaluation Standard for IoT Platforms) scheme, and as such maintains the scheme documentation, including interpretations and procedures such as this document.

This document describes a process that can be applied to re-use CC certifications into a SESIP certification. It is intended mostly for re-using CC EAL4+ into SESIP4 and SESIP5 certifications, but can be used for all SESIP levels. If this process is applied, it is to be applied in full.

The input of this process is a CC certificate, a CC ST with CC SFRs and CC SARs, and a SESIP ST (with SESIP SFRs and the SESIP level defining the SARs).

The intent is to ensure that the SESIP ST's claims are fully covered by the CC ST and certificate. Therefore, the SESIP ST will be a reformulated subset of the CC ST.



The output of this process, besides the evaluator and positive decision by certifier's reporting, when successfully completed, is a SESIP certificate.

1.1 Intended audience

This document is publicly available and is aimed at the following involved parties engaging in a SESIP certification:

1. Scheme owner
2. Developer (Sponsor)
3. Evaluator (Lab)
4. Certifier (TrustCB)

The content of this document is informative, providing an option of how results of CC certifications may be used as input to a SESIP certification. If adopted, the entirety of this document must be applied.

1.2 Terminology

Although formally SESIP is an optimized version of CC, for clarity and brevity we'll refer to the 'traditional CC' input using terms with "CC", and the SESIP output with "SESIP". Standard CC terminology is used.

The following terminology of RFC 2119 is used in this document:

- "shall" or "must" indicates mandatory requirements

- "should" indicates a strong recommendation, deviation of which must be discussed with and approved by the scheme
- "can" or "may" denotes an option

1.3 Contact details

All requests or enquiries related to the security evaluation should be addressed by email to: SESIP@trustcb.com.

1.4 Changes

Changes in this interpretation since the previous version are indicated in Track Changes marks in the TC version.

The changes to this interpretation do not impact verdicts based on older versions of this interpretation. Additional possibilities made available by the changes in this interpretation:

- CCRA certificates can now also be re-used, up to and including AVA_VAN.2 level for 1 year. See Re-use requirements for re-use of CC SARs to fulfil the SESIP levels.
- SOGIS certificates can now be re-used for more than 1.5 years, "at the cost" of 1 AVA_VAN level per 0.5 year. See Re-use requirements for re-use of CC SARs to fulfil the SESIP levels.
- Certificates compliant with PP-117 can now also be used as with PP-0084. See Security IC Platform PP [PP-0084] and Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile [PP-117] re-use.

2 Certificate acceptance procedure

The CCRA/SOGIS CC certificate must be valid, and (re-)issued no longer than 1/1.5 year ago by the time the SESIP certificate is issued.

- **In the case of a SOGIS CC certificate, the evaluator shall check that the SOGIS CC certificate issued under the technical domain for "smartcards and similar devices. The evaluator shall check the certificate is still valid and (re-)issued no longer than 1.5 year ago at the time the completed evaluation evidence is provided to the certifier. This can be extended by an additional 0.5 year per AVA_VAN level the CC certificate is higher than the SESIP level. This certificate can be re-used up to and including to an AVA_VAN.5 level.**
- **In the case of a CCRA CC certificate, the evaluator shall check that the CCRA CC certificate is still valid and (re-)issued no longer than 1 year ago at the time the completed evaluation evidence is provided to the certifier. A CCRA CC certificate can be re-used at AVA_VAN.2 level.**
    - The technical domain "smartcards and similar devices" has a traditional re-use procedure for composition of 1.5 years, hence the extension.
    - For each AVA_VAN.x level the CC certificate is higher than the SESIPy/AVA_VAN.y level, 0.5 years can be extended. For example, an AVA_VAN.5 SOGIS certificate can be used for 1.5y+0.5y+0.5y = 2.5y at a SESIP3 level.
    - A safety margin of 3 months is recommended to the developer, to ensure the CC certificate validity requirement is likely to be met at the time of certification, noting the time required for contractual tasks as well as the evaluation & certification tasks.
- **The evaluator shall examine the CC ST and CC certificate to ensure that all claims in the SESIP ST, including the SESIP SFRs and SARs, are fully covered by CC.**
    - The evaluator should fulfil the section "Re-use requirements for re-use of CC SARs to fulfil the SESIP levels".
    - The developer and evaluator may use the section "Guidance for re-use of CC SFRs in SESIP".
    - The developer may provide a mapping of the SESIP SFRs to the CC SFRs as part of their SESIP ST to fulfil the SESIP ASE_TSS requirements.
    - **The evaluator shall examine this mapping as part of the SESIP ASE_TSS evaluator activities to determine if it is correct and complete.**
    - **The evaluator shall report how all claims in the SESIP ST are fully covered by the CC certification.**
- **The evaluator shall provide the evaluation evidence (at least the evaluation technical report, the CC ST and the CC certificate, and the SESIP ST) to the certifier.**
- **The certifier shall check that the evaluator has fulfilled the requirements.**
- **The certifier shall check that the CC certificate was (re-)issued no longer than 1/1.5+x year ago before issuing the SESIP certificate.**

3 Re-use requirements for re-use of CC SARs to fulfil the SESIP levels

To show the SESIP assurance requirements of a given SESIP level are covered by the CC certification results, the SESIP evaluator should perform the indicated evaluator actions. In this way, the SESIP evaluator (and later in the process the SESIP certifier) can check that all conditions to re-use the CC certification are met.

As this activity happens to show compliance to a specific SESIP level, this chapter uses the SESIP levels as structure. Per SESIP level, a table with is provided. The "evaluator actions for re-use" show what needs to be done, to meet the SESIP assurance requirements for that SESIP level.

Like this:

Assurance Class	Assurance Families	Evaluator actions for re-use
<Lists the SESIP assurance class addressed>.	<Lists the SESIP assurance requirements that need to be fulfilled by the CC certification results.>	This lists the evaluator actions expected to show that the CC certification results are sufficient. Evaluator actions are marked thus for clarity: ○ **The evaluator shall check that the CC ST claims ….** ○ **The evaluator shall examine that the SESIP augmentations are met**. The conclusion that can be taken, is described as: If these requirements are met, SESIP ALC_FLR.2 is met by CC ALC_FLR.2.
		For ease of maintenance of this document and any documents that are deduced from it, re-use requirements already covered in an earlier SESIP level's description, are referred with: See SESIPx.

Note that there are subtle dependencies between the assurance activities, so mixing re-use of the CC results and additional evaluation activities under SESIP is non-trivial. You are advised to consult your certification body with an explanation why this will work before performing such actions.

3.1 ASE re-use requirements

For all SESIP levels, the SESIP ST is different from the CC ST, therefore the re-use requirements are described here once.

1. **The evaluator shall examine the SESIP ST to determine that it meets SESIP ASE_REQ.3.**
2. **The evaluator shall check that the CC Certificate to determine that the CC ST meets CC ASE_REQ.1 or ASE_REQ.2.**
3. **The evaluator shall examine the SESIP ST to determine that the SESIP platform is (a subset of) the TOE configuration(s) covered by the CC ST and CC certificate.**
4. **The evaluator shall check that the CC ST complies to Common Criteria version 3.1 (any revision).**
5. **The evaluator shall examine the SESIP ST to determine that all guidance needed to understand and implement the objectives for the environment described in the CC ST**

are included in the objectives for the environment and the references to the guidance of the SESIP ST.

a. The developer/evaluator may determine this by ensuring that all objectives for the environment described in the CC ST are included in the SESIP ST, and all guidance is identical between the CC ST and the SESIP ST.

i. If the SESIP ST describes a platform that is a strict subset of the CC TOE configurations, possibly only a subset of the CC ST objectives or guidance is needed.

b. **The evaluator shall examine any objectives for the environment or guidance listed in the CC ST that are not completely included in the SESIP ST to determine that these do not impact the CC evaluation activities for the CC TOE configurations specific to the SESIP platform.**

i. This is expected only for situations where the missing guidance is solely for an CC TOE configuration not used in SESIP.

6. **The evaluator shall examine the SESIP ST and the CC ST to determine that all SESIP SFRs are fully satisfied by the CC SFRs.**

a. See "Guidance for re-use of CC SFRs in SESIP" for additional guidance.

b. **The evaluator shall report how the SESIP SFRs are satisfied**.

c. The evaluator may refer to or create a table mapping the SESIP SFR details to the CC SFRs and their details.

d. The developer/evaluator may use the CC objectives for the TOE as an intermediate step in mapping the SESIP SFRs to the CC SFRs.

e. Prepared mappings already accepted by the scheme are listed in "Guidance for re-use of CC SFRs in SESIP".

Notes:

i. There may be additional claims in the CC ST (for example more CC SFRs, more details in the CC SFRs, objectives for the TOE), but these are ignored for the SESIP ST and SESIP certificate.

ii. If a SESIP SFR is not fully satisfied by the CC SFRs, the certifier may allow the partial re-use to be combined with extension of the SESIP evaluation activities. Such re-use is however generally subtly very complex and not advised by TrustCB. The evaluators are advised to have discussions with the CB on this prior to starting the evaluation.

iii. The SESIP SFRs are required to be fully satisfied by the CC SFRs. Therefore, all the mappings of the CC SFRs to TSFI (ADV_FSP), to subsystems and modules (ADV_TDS), to the implementation representation (ADV_IMP), to the tests (ATE_COV and ATE_DPT) are also mappings of the SESIP SFR to these assurance requirements. From a methodology point of view, the extra steps of having the CC SFRs and CC ADV_TDS and ADV_IMP.1/2 mapping documents between the SESIP SFRs and the implementation representation (ADV_IMP.3) are considered only as informative information.

3.2 CC re-use requirements for SESIP1

Assurance Class	Assurance Families	Evaluator actions for re-use
ASE: Security Target evaluation	ASE_INT.1 – ST Introduction *ASE_OBJ.1 – Security requirements for the operational environment* **ASE_REQ.3 – Listed security requirements** *ASE_TSS.1 – TOE summary specification*	The SESIP ST and CC have significant differences. **See "ASE re-use" for the re-use requirements.**
AGD: Guidance documents	AGD_OPE.1 – Operational user guidance AGD_PRE.1 – Preparative procedures	The AGD requirements are identical, therefore they are directly re-usable in both directions. Therefore: **i. The evaluator shall check that the CC ST claims AGD_OPE.1 and AGD_PRE.1.** If these requirements are met, SESIP AGD_OPE.1 and AGD_PRE.1 are met. Note that the SESIP ST is required to list the mapping of the objectives for the environment to the guidance (as defined in SESIP), something that in CC is often done in the context of AGD. See "ASE re-use" for more details.
ALC: Life-cycle support	ALC_FLR.2 – Flaw reporting procedures	SESIP refines the ALC_FLR.2 requirements slightly. Therefore: **i. The evaluator shall check that the CC ST claims ALC_FLR.2.** **ii. The evaluator shall examine that the SESIP augmentations are met.** If these requirements are met, SESIP ALC_FLR.2 is met. Note that compared to classical CC's typical focus on the internal procedures, in SESIP there is an emphasis on the external facing part of the flaw remediation (how to submit a flaw report, and especially how the updates are communicated to all customers).

Assurance Class	Assurance Families	Evaluator actions for re-use
AVA: Vulnerability Assessment	AVA_VAN.1 – Vulnerability survey	SESIP refines the AVA_VAN.1 requirements slightly. Therefore: **i. The evaluator shall check that the CC ST claims at least AVA_VAN.1[1].** **ii. The evaluator shall examine that the SESIP augmentations are met, specifically that the developer, a test lab on behalf of the developer, or the evaluator has determined the platform is resistant against publicly known vulnerabilities.** If these requirements are met, SESIP AVA_VAN.1 is met.

3.3 CC re-use requirements for SESIP2

Assurance Class	Assurance Families	Evaluator actions for re-use
ASE: Security Target evaluation	ASE_INT.1 – ST Introduction *ASE_OBJ.1 – Security requirements for the operational environment* **ASE_REQ.3 – Listed security requirements** *ASE_TSS.1 – TOE summary specification*	The SESIP ST and CC have significant differences. **See "ASE re-use" for the re-use requirements.**
ADV: Development	ADV_FSP_4 – Complete functional specification	The ADV_FSP.4 requirements are identical, therefore they are directly re-usable in both directions. Therefore: **i. The evaluator shall check that the CC ST claims at least ADV_FSP.4.** If these requirements are met, SESIP ADV_FSP.4 is met.
AGD: Guidance documents	AGD_OPE.1 – Operational user guidance AGD_PRE.1 – Preparative procedures	AGD_OPE.1 and AGD_PRE.1: **See CC re-use requirements for SESIP1.**

[1] Technically the CC evaluation does not cover attacks of 14 or 15 points, as the rating of SESIP uses the [AAP] limit of 16 points, and general CC only 14 points. However, considering that the evaluator is not necessarily performing testing anyway, the developer declaration in the ST is considered sufficient to cover this gap.

Assurance Class	Assurance Families	Evaluator actions for re-use
ALC: Life-cycle support	ALC_FLR.2 – Flaw reporting procedures	ALC_FLR.2: **See CC re-use requirements for SESIP1.**
ATE: Tests	ATE_IND.1 – Independent testing: conformance	The ATE_IND requirements are identical, therefore they are directly re-usable in both directions. Therefore: **i. The evaluator shall check that the CC ST claims at least ATE_IND.1.** If these requirements are met, SESIP ATE_IND.1 is met. Note that re-use of standard test-suites by any party is encouraged in SESIP (which may not be the case in generic CC schemes).

Assurance Class	Assurance Families	Evaluator actions for re-use
AVA: Vulnerability Assessment	AVA_VAN.2 – Vulnerability analysis	SESIP refines the AVA_VAN.2 requirements slightly. Therefore: **i. The evaluator shall check that the CC ST claims AVA_VAN.2 (if the CC vulnerability analysis used the rating method of [AAP][2] or if the TrustCB-licensed lab performing the CC AVA confirms that it used a limit of least 16 points, not 14 points[3]), or AVA_VAN.4[4] (otherwise).** **ii. The evaluator shall report which rating method was used in the CC vulnerability analysis, including any declaration of using the 16 point limit.** iii. **The evaluator shall examine that the SESIP augmentations are met, specifically that the minimum test effort is met and that all guidance covering the objectives for the environment for composition is considered in the vulnerability analysis**. If these requirements are met, SESIP AVA_VAN.2 is met.

[2] This is the least likely situation.

[3] This applies mostly for the situation where the same lab is performing the CC and SESIP evaluations, although SESIP labs declaring the CC work was done with SESIP attack potential levels is also acceptable.

[4] [AAP] CC and SESIP AVA_VAN.2 require at least 16 points, default CC AVA_VAN.2 and AVA_VAN.3 only 14. Next bigger step that is visible in a CC ST is AVA_VAN.4 guaranteeing 20 points.

3.4 CC re-use requirements for SESIP3

Assurance Class	Assurance Families	Evaluator actions for re-use
ASE: Security Target evaluation	ASE_INT.1 – ST Introduction *ASE_OBJ.1 – Security requirements for the operational environment* **ASE_REQ.3 – Listed security requirements** *ASE_TSS.1 – TOE summary specification*	The SESIP ST and CC have significant differences. **See "ASE re-use" for the re-use requirements.**
ADV: Development	ADV_FSP_4 – Complete functional specification **ADV_IMP.3 – Complete mapping of the implementation representation of the TSF to the SFRs**	ADV_FSP.4: **See CC** re-use requirements for SESIP2**.** ADV_IMP.3: SESIP compresses ADV_TDS.4 and ADV_IMP with access to the full implementation representation[5] into ADV_IMP.3. Therefore: **i. The evaluator shall check that the CC ST claims ADV_TDS.4 or higher.** **ii. The evaluator shall check that the CC ST claims ADV_IMP.2, or that that the CC ST claims ADV_IMP.1 and the TrustCB-licensed CC lab declares that the full implementation representation was available and considered in the CC evaluation.** **iii. The evaluator shall report which re-use method was used, including any declaration of availability and consideration of the full implementation representation.** If these requirements are met, SESIP ADV_IMP.3 is met.

[5] Some traditional CC schemes like the SOGIS CC schemes encode full access to the implementation representation by stating ADV_IMP.2, even though that formally only means a full mapping to the implementation representation is checked, not that the full implementation representation was available. Other CC schemes, like NSCIB, require the full implementation representation to be available even at ADV_IMP.1.

Assurance Class	Assurance Families	Evaluator actions for re-use
AGD: Guidance documents	AGD_OPE.1 – Operational user guidance AGD_PRE.1 – Preparative procedures	AGD_OPE.1 and AGD_PRE.1: **See CC re-use requirements for SESIP1.**
ALC: Life-cycle support	ALC_CMC.1 – Labelling of the TOE ALC_CMS.1 – TOE CM coverage ALC_FLR.2 – Flaw reporting procedures	ALC_CMC.1 and ALC_CMS.1: The ALC_CMC.1 and ALC_CMS.1 requirements are identical, therefore they are directly re-usable in both directions. Therefore: i. **The evaluator shall check that the CC ST claims at least ALC_CMC.1.** ii. **The evaluator shall check that the CC ST claims at least ALC_CMS.1.** If these requirements are met, SESIP ALC_CMC.1 and ALC_CMS.1 are met. ALC_FLR.2: **See CC re-use requirements for SESIP1.**
ATE: Tests	ATE_IND.1 – Independent testing: conformance	**See CC re-use requirements for SESIP2.**

Assurance Class	Assurance Families	Evaluator actions for re-use
AVA: Vulnerability Assessment	AVA_VAN.3 – Focused vulnerability analysis	SESIP refines the AVA_VAN.3 requirements slightly. Therefore: **i. The evaluator shall check that the CC ST claims AVA_VAN.3 (if the CC vulnerability analysis used the rating method of [AAP][6]) or AVA_VAN.4 (if the TrustCB-licensed lab performing the CC AVA confirms that it used a limit of least 21 points, not 20 points[7]), or AVA_VAN.5[8] (otherwise).** **ii. The evaluator shall report which rating method was used in the CC vulnerability analysis, including any declaration of using the 21 point limit.** **iii. The evaluator shall examine that the SESIP augmentations are met, specifically that the minimum test effort is met and that all guidance covering the objectives for the environment for composition is considered in the vulnerability analysis.** If these requirements are met, SESIP AVA_VAN.3 is met.

[6] This is the least likely situation.

[7] This applies mostly for the situation where the same lab is performing the CC and SESIP evaluations, although SESIP labs declaring the CC work was done with SESIP attack potential levels is also acceptable.

[8] [AAP] CC and SESIP AVA_VAN.3 require at least 21 points, default CC AVA_VAN.3 only 14 and AVA_VAN.4 only 20. Next bigger step that is visible in a CC ST is AVA_VAN.5 with 25 points guaranteed.

3.5 CC re-use requirements for SESIP4

Assurance Class	Assurance Families	Evaluator actions for re-use
ASE: Security Target evaluation	ASE_INT.1 – ST Introduction *ASE_OBJ.1 – Security requirements for the operational environment* **ASE_REQ.3 – Listed security requirements** *ASE_TSS.1 – TOE summary specification*	The SESIP ST and CC have significant differences. **See "ASE re-use" for the re-use requirements.**
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP_4 – Complete functional specification **ADV_IMP.3 – Complete mapping of the implementation representation of the TSF to the SFRs**	ADV_ARC.1: The ADV_ARC.1 requirements are identical, therefore they are directly re-usable in both directions. Therefore: **i. The evaluator shall check that the CC ST claims at least ADV_ARC.1.** If these requirements are met, SESIP ADV_ARC.1 are met. ADV_FSP.4: **See CC re-use requirements for SESIP2.** ADV_IMP.3: **See CC re-use requirements for SESIP3.**
AGD: Guidance documents	AGD_OPE.1 – Operational user guidance AGD_PRE.1 – Preparative procedures	AGD_OPE.1 and AGD_PRE.1**: See CC re-use requirements for SESIP1.**

Assurance Class	Assurance Families	Evaluator actions for re-use
ALC: Life-cycle support	ALC_CMC.1 – Labelling of the TOE ALC_CMS.1 – TOE CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_FLR.2 – Flaw reporting procedures ALC_TAT.1 Well-defined development tools	ALC_CMC.1 and ALC_CMS.1: **See CC re-use requirements for SESIP3.** ALC_DEL.1 and ALC_DVS.1: The ALC_DEL.1 and ALC_DVS.1 requirements are identical, therefore they are directly re-usable in both directions. Therefore: **i. The evaluator shall check that the CC ST claims ALC_DEL.1.** **ii. The evaluator shall check that the CC ST claims at least ALC_DVS.1.** If these requirements are met, SESIP ALC_DEL.1 and ALC_DVS.1 are met. ALC_FLR.2: **See CC re-use requirements for SESIP1.** ALC_TAT.1: The ALC_TAT.1 requirements are identical, therefore they are directly re-usable in both directions. Therefore: **i. The evaluator shall check that the CC ST claims at least ALC_TAT.1.** If these requirements are met, SESIP ALC_TAT.1 are met.

Assurance Class	Assurance Families	Evaluator actions for re-use
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing ATE_IND.1 – Independent testing: conformance	ATE_COV.1 and ATE_FUN.1: The ATE_COV.1 and ATE_FUN.1 requirements are identical, therefore they are directly re-usable in both directions. Therefore: i. **The evaluator shall check that the CC ST claims at least ATE_COV.1.** ii. **The evaluator shall check that the CC ST claims at least ATE_FUN.1.** If these requirements are met, SESIP ATE_COV.1 and ATE_FUN.1 are met. ATE_IND.1: **See CC re-use requirements for SESIP2.**
AVA: Vulnerability Assessment	AVA_VAN.4 – Methodical vulnerability analysis	SESIP refines the AVA_VAN.4 requirements slightly. Therefore: i. **The evaluator shall check that the CC ST claims AVA_VAN.4 (if the CC vulnerability analysis used the rating method of [AAP][9]) or AVA_VAN.5[10] (otherwise).** ii. **The evaluator shall report which rating method was used in the CC vulnerability analysis.** iii. **The evaluator shall check that the lab performing the CC evaluation is a SOG-IS accredited laboratory.** If these requirements are met, SESIP AVA_VAN.4 is met.

[9] This is the more likely situation.

[10] [AAP] CC and SESIP AVA_VAN.4 require at least 25 points, default CC AVA_VAN.4 only 20. Next bigger step that is visible in a CC ST is AVA_VAN.5 with exactly the required 25 points guaranteed.

3.6 CC re-use requirements for SESIP5

Assurance Class	Assurance Families	Evaluator actions for re-use
ASE: Security Target evaluation	ASE_INT.1 – ST Introduction ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition *ASE_OBJ.1 – Security requirements for the operational environment* **ASE_REQ.3 – Listed security requirements** ASE_SPD.1 Security problem definition *ASE_TSS.1 – TOE summary specification*	The SESIP ST and CC have significant differences. **See "ASE re-use" for the re-use requirements.**
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP_4 – Complete functional specification ADV_TDS.3 Basic modular design ADV_IMP.2 Complete mapping of the implementation representation of the TSF	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.2: The ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, and ADV_IMP.2 requirements are identical, therefore they are directly re-usable in both directions. Therefore: **i. The evaluator shall check that the CC ST claims ADV_ARC.1.** **ii. The evaluator shall check that the CC ST claims at least ADV_FSP.4.** **iii. The evaluator shall check that the CC ST claims at least ADV_TDS.3.** **iv. The evaluator shall check that the CC ST claims ADV_IMP.2[11].** If these requirements are met, SESIP ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, and ADV_IMP.2 are met.

[11] Note that ADV_IMP.**2** is not part of EAL4, so check this carefully. ADV_IMP.2 is however typically part of the assurance package claimed by PPs that apply the [AAP] rating methods.

Assurance Class	Assurance Families	Evaluator actions for re-use
AGD: Guidance documents	AGD_OPE.1 – Operational user guidance AGD_PRE.1 – Preparative procedures	AGD_OPE.1 and AGD_PRE.1: **See CC re-use requirements for SESIP1.**
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.2 Sufficiency of security measures ALC_FLR.2 – Flaw reporting procedures ALC_TAT.1 Well-defined development tools	ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_TAT.1: The ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, and ALC_TAT.1 requirements are identical, therefore they are directly re-usable in both directions. Therefore: **i. The evaluator shall check that the CC ST claims at least ALC_CMC.4.** **ii. The evaluator shall check that the CC ST claims at least ALC_CMS.4.** **iii. The evaluator shall check that the CC ST claims ALC_DEL.1.** **iv. The evaluator shall check that the CC ST claims ALC_DVS.2[12].** **v. The evaluator shall check that the CC ST claims at least ALC_TAT.1.** If these requirements are met, SESIP ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, and ALC_TAT.1 are met. ALC_FLR.2: **See CC re-use requirements for SESIP1.**

[12] Note that ALC_DVS.**2** is not part of EAL4, so check this carefully. ALC_DVS.2 is however typically part of the assurance package claimed by PPs that apply the [AAP] rating methods.

Assurance Class	Assurance Families	Evaluator actions for re-use
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional testing ATE_IND.1 – Independent testing: conformance	ATE_COV.1, ATE_DPT.1 and ATE_FUN.1: The ATE_COV.1, ATE_DPT.1 and ATE_FUN.1 requirements are identical, therefore they are directly re-usable in both directions. Therefore: **i. The evaluator shall check that the CC ST claims at least ATE_COV.1.** **ii. The evaluator shall check that the CC ST claims at least ATE_DPT.1.** **iii. The evaluator shall check that the CC ST claims at least ATE_FUN.1.** If these requirements are met, SESIP ATE_COV.1, ATE_DPT.1 and ATE_FUN.1 are met. ATE_IND.1: **See CC re-use requirements for SESIP2.**
AVA: Vulnerability Assessment	AVA_VAN.5 – Advanced methodical vulnerability analysis	SESIP refines the AVA_VAN.5 requirements slightly. Therefore: **i. The evaluator shall check that the CC ST claims AVA_VAN.5 and used the rating method of [AAP])[13].** **ii. The evaluator shall check that the lab performing the CC evaluation is a SOG-IS accredited laboratory.** If these requirements are met, SESIP AVA_VAN.5 is met.

[13] Note that there is no method to upgrade CC AVA_VAN.5 evaluations that are not using [AAP] as the 'normal' CC rating ends at 25 points, far short of the 31 points SESIP and [AAP] require.

4 Guidance for re-use of CC SFRs in SESIP

This chapter suggests SESIP SFRs that can be claimed, coming from common CC protection profiles, with the suggested re-use acceptance steps.

Not all possible SESIP SFRs supported by the CC ST need to be claimed, this is only to support re-use. Note that the check is that the SESIP SFR is covered by the CC SFR, so all the SESIP details must be in the CC SFR but not all CC SFR details need to be in the SESIP SFR.

4.1 Security IC Platform PP [PP-0084] and Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile [PP-117] re-use

The below SESIP SFRs are considered met for CC TOEs SOGIS-CC certified against the Security IC Platform PP [PP-0084] or Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile [PP-117]. Re-use is accepted provided:

1. The stated requirement for re-use is met.
2. There are no changes to the CC SFRs beyond those allowed within strict conformance to the [PP-0084] / [PP-117].

4.1.1 Physical attacker resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other functional requirements, ensuring that the other functional requirements are not compromised.

Requirement for re-use:

The evaluator shall examine the CC ST is strictly compliant to [PP-0084]/[PP-117]. If so, this SESIP SFR is met.

Guidance:

The [PP-0084]/[PP117] in total describes physical secure hardware, especially with the CC SFRs FPT_PHP.3, FDP_SDI.2, FDP_SDC.1, FRU_FLT.2, FPT_FLS.1, FDP_ITT.1, FDP_ITT.1, FDP_IFC.1, FMT_LIM.1, FMT_LIM.2.

4.1.2 Secure initialization of platform

The platform ensures its authenticity and integrity during the platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to a secure state.

Guidance for re-use:

The evaluator shall examine the CC ST is strictly compliant to [PP-0084] / [PP-117]. If so, this SESIP SFR is met.

Guidance:

[PP-0084] / [PP-117] in total describes physical secure hardware and in practice secure initialization, especially with the CC SFRs FPT_PHP.3, FDP_SDI.2, FDP_SDC.1, FRU_FLT.2, FPT_FLS.1, FMT_LIM.1, FMT_LIM.2.

4.1.3 Verification of Platform Identity

The platform provides a unique identification of the platform type, including all its parts and their versions.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the details in the SESIP SFR are fully met in the FAU_SAS.1 and FDP_SDC.1 SFRs. If so, this SESIP SFR is met.

Guidance:

The CC SFR FAU_SAS.1 has open operations that can, but not necessarily do, contain sufficient information to identify the platform type, all its parts and their version.

1. Check the SFR operations and potentially the guidance for interpretation of the stored information.
2. The CC SFR FDP_SDC.1 is there to protect the stored information and only needs verification.

4.1.4 Verification of Platform Instance Identity

The platform provides a unique identification of that specific instantiation of the platform, including all its parts and their versions.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the details in the SESIP SFR are fully met in the FAU_SAS.1 and FDP_SDC.1 SFRs. If so, this SESIP SFR is met.

Guidance:

The CC SFR FAU_SAS.1 has open operations that can, but not necessarily do, contain sufficient information to provide a unique identification of a specific instantiation (i.e. a per-TOE-instance-unique identifier).

1. Check the SFR operations and potentially the guidance for interpretation of the stored information.
2. The CC SFR FDP_SDC.1 is there to protect the stored information and only needs verification.

4.1.5 Cryptographic Random Number Generation

The platform provides the application with a way based on <*physical, hybrid physical, hybrid deterministic*> *noise source* to generate random numbers to as specified in <*specification*>.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the details in the SESIP SFR are fully met in the FCS_RNG SFR. If so, this SESIP SFR is met.

4.2 Security IC Platform PP [PP-0084] augmentation packages re-use

The augmentation packages aren't necessarily claimed in the underlying CC evaluation.

4.2.1 Secure Install of Application

The application can be installed in the field such that the integrity, authenticity and confidentiality of the application is maintained.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the "Package 2: Loader dedicated for usage by authorized users only" SFRs from [PP-0084] are met. If so, this SESIP SFR is met for integrity and authenticity.

The evaluator shall examine that the confidentiality is also covered.

Guidance:

The [PP-0084] "Package 2: Loader dedicated for usage by authorized users only" describes the integrity with the CC SFRs FDP_UIT.1, FDP_ACC.1/Loader, FDP_ACF.1/Loader, , the authentication with the CC SFR FTP_ITC.1, and the confidentiality with the CC SFR FDP_UCT.1.

In the scope of [PP-0084] the platform is the IC. For a CC ST claiming consistency to [PP-0084] and [PP-0099], verify the scope.

4.2.2 Cryptographic Operation/TDES

The platform provides the application with encryption and decryption functionality with TDES as specified in NIST SP 800-67, NIST SP 800-38A for key lengths 112 bit, 168 bit and modes <*select: ECB mode, CBC mode*>.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the "TDES" SFRs from [PP-0084] are met and the mode selection is fully covered in the FCS_COP.1/TDES SFR. If so, this SESIP SFR is met.

Guidance:

The [PP-0084] "TDES" describes the cryptographic operation with the CC SFR FCS_COP.1/TDES and the associated destruction of the temporary key in the CC SFR FCS_CKM.4/TDES.

4.2.3 Cryptographic Operation/AES

The platform provides the application with encryption and decryption functionality with TDES as specified in FIPS 197, NIST SP 800-38A for key lengths 128 bit, 192 bit, 256 bit and modes <*select: ECB mode, CBC mode*>.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the "AES" SFRs from [PP-0084] are met and the mode selection is fully covered in the FCS_COP.1/AES SFR. If so, this SESIP SFR is met.

Guidance:

The [PP-0084] "AES" describes the cryptographic operation with the CC SFR FCS_COP.1/AES and the associated destruction of the temporary key in the CC SFR FCS_CKM.4/AES.

4.2.4 Cryptographic Operation/SHA

The platform provides the application with hashing functionality with <*selection: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*> as specified in FIPS 180-4 for key lengths none and modes none.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the "Hash functions" SFRs from [PP-0084] are met and the algorithm selection is fully covered in the FCS_COP.1/SHA SFR. If so, this SESIP SFR is met.

Guidance:

The [PP-0084] "Hash functions" describes the cryptographic operation with the CC SFR FCS_COP.1/SHA.

4.3 Java Card PP [PP-0099] re-use

The below SESIP SFRs are considered met for CC TOEs SOGIS-CC certified against the Java Card Open Configuration PP [PP-0099]. Re-use is accepted provided the requirement for re-use is met.

Note that the below CC SFRs have been taken literally from [PP-0099], as if strict conformance was claimed. However, the [PP-0099] requires only demonstrable conformance, therefore the evaluators must review the SFRs in the CC ST carefully.

4.3.1 Secure initialization of platform

The platform ensures its authenticity and integrity during the platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to a secure state.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the CoreG_LC SFRs from [PP-0099] are met. If so, this SESIP SFR is met.

Guidance:

The [PP-0099] does not itself require physical protection and secure initialization of the hardware, however usually compliance to [PP-0084] is also claimed and therefore "Security IC Platform PP [PP-0084] and Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile [PP-117] re-use" then also applies and covers the full platform initialization.

4.3.2 Secure Install of Application

The application can be installed in the field such that the integrity, authenticity ~~*<and confidentiality>*~~ of the application is maintained.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the CarG and InstG SFRs from [PP-0099] are met. If so, this SESIP SFR is met for integrity and authenticity.

The evaluator shall examine that the confidentiality is also covered.

Guidance:

If SCP02 and/or SCP03 is used for applet installation, *confidentiality* might also be claimed. Examine the CC ST for any claims.

4.3.3 Software Attacker Resistance: Isolation of Platform

The platform provides isolation between the application and itself, such that an attacker able to run code as an application on the platform cannot compromise the other functional requirements.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the CoreG_LC SFRs from [PP-0099] are met. If so, this SESIP SFR is met.

4.3.4 Software Attacker Resistance: Isolation of Application Parts

The platform provides isolation between parts of the application, such that an attacker able to run code as one of the *applets* cannot compromise the integrity and confidentiality of the other application parts.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the CoreG_LC SFRs from [PP-0099] are met. If so, this SESIP SFR is met.

4.3.5 Cryptographic Operation

The platform provides the application with <*list of cryptographic operations*> functionality with <*list of algorithms*> as specified in <*specification*> for key lengths <*list of key lengths*> and modes <*list of modes*>.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the details in the SESIP SFR are fully met in the FCS_COP SFR. If so, this SESIP SFR is met.

4.3.6 Cryptographic key generation

The platform provides the application with a way to generate cryptographic keys for use in <*list of cryptographic algorithms*> as specified in <*specification*> for key lengths <*list of key lengths*>.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the details in the SESIP SFR are fully met in the FCS_COP SFR(s). If so, this SESIP SFR is met.

4.3.7 Cryptographic random number generation

The platform provides the application with a way based on < *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*> *noise sources* to generate random numbers to as specified in <*specification*>.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the details in the SESIP SFR are fully met in the FCS_RNG.1 SFR(s). If so, this SESIP SFR is met.

4.3.8 Residual information purging

The platform ensures that *Class instances (objects), transient arrays, global arrays, APDU buffer*, *and temporarily used cryptographic keys* with the exception of *none,* is erased using the method specified in *[JCRE]* before the memory is (re)used by the platform or application again and before an attacker can access it.

Requirement for re-use:

The evaluator shall examine the CC ST to determine that the CoreG_LC SFRs from [PP-0099] are met. If so, this SESIP SFR is met.

Guidance:

The "class instances (objects)" are covered by the FDP_RIP.1/ABORT. "global arrays" by FDP_RIP/GlobalArray, "transient array" in FDP_RIP.1/TRANSIENT, "APDU buffer" is covered by FDP_RIP.1/APDU, "temporarily used cryptographic keys" is covered by FCS_CKM.4 and FDP_RIP.1/KEYS, as we currently don't see a use case for this.

5 Reference Materials

The documents listed in Table 1 may have been cited in this document or used to obtain background information.

Table 5-1: Reference documents

Title	Source	Reference
ISO Standard 15408 Common Criteria for Information Security Evaluation	2	[CC]
Common Criteria and CEM version 3.1	2	[CEM]
Security Evaluation Standard for IoT Platforms	1	[SESIP]
SESIP Scheme Documentation	1	[SESIP_Docn]
TrustCB SESIP Application Form (SESIP)	1	[SESIP_AF]
TrustCB Scheme Procedures	1	[TrustCB_Procs]
Security IC Platform Protection Profile BSI-PP-0084-2014	3	[HW-PP]
JIL Application of Attack Potential	4	[AAP]
Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014	2	[PP-0084]
Java Card System – Open Configuration Protection Profile, Reference PP-0099	2	[PP-0099]
Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile	2	[PP-117]

Key:

1 = Available online from TrustCB SESIP scheme website (TrustCB SESIP)

2 = Available online from ISO standards website (www.iso.org) or Common Criteria Portal (commoncriteriaportal.org)

3 = Available online from BSI website (www.bsi.bund.de)

4 = Available online from SOGIS website (www.sogis.eu)