GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology
SESIP Profile for Secure External Memories Version 0.0.1.1

Public Review
July 2021
Document Reference: GPT_SPE_148

Contents

Figures

Tables

1 Introduction

This SESIP profile describes a secure external memory Platform (in this chapter) and the exact security properties of the Platform that are evaluated against [SESIP] (in chapter “Security requirements and implementation”) that a potential consumer can rely upon the product upholding if they fulfill the objectives for the environment (in chapter “Security Objectives for the Operational Environment”).

1.1 Audience

This document is intended primarily for the use of the Security Target (ST) writer.

1.2 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that have been brought to the attention of GlobalPlatform, please visit https://www.globalplatform.org/specificationsipdisclaimers.asp. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.3 References

Table 1-1: Normative References

Standard / Specification	Description	Ref
GlobalPlatform SESIP	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.0, March 2020	[SESIP]

Table 1-2: Informative References

Standard / Specification	Description	Ref
Secure Memory	GlobalPlatform Technology SESIP profile for Secure External Memories Version 0.0.1.0	[Profile]

1.4 Terminology and Definitions

The following meanings apply to SHALL, SHALL NOT, MUST, MUST NOT, SHOULD, SHOULD NOT, and MAY in this document (refer to **Error! Reference source not found.**):

- **SHALL** indicates an absolute requirement, as does **MUST**.
- **SHALL NOT** indicates an absolute prohibition, as does **MUST NOT**.
- **SHOULD** and **SHOULD NOT** indicate recommendations.
- **MAY** indicates an option.

Application Notes are marked throughout the text using SHADED GRAY. They must be addressed by the Security Target (ST) writer.

Informational paragraphs are marked throughout the text using SHADED CYAN.

Selected terms used in this document are included in Table 1-3. Additional terms are defined in [**#** an appropriate specification, such as [SESIP].

Table 1-3: Terminology and Definitions

SESIP Term	Definition
Platform	The discrete secure external memory device
User(s)	The logical entity(ies) accessing the content of the secure memory
Application	The host system that connects to the platform via a physical link

1.5 Abbreviations and Notations

Table 1-4: Abbreviations and Notations

Abbreviation / Notation	Meaning
0 - 9	Decimal digits are not enclosed in quotation marks.
'0' - '9' and 'A' - 'F'	Hexadecimal values are enclosed in straight single quotation marks.
*n*b, *nn*b, ...	The character “b” is appended to bit values (e.g. 1b and 0000b).

1.6 Revision History

GlobalPlatform technical documents numbered *n*.0 are major releases. Those numbered *n*.1, *n*.2, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered *n.n*.1, *n.n*.2, etc., are maintenance releases that incorporate errata and precisions; all non-trivial revisions are indicated, often with revision marks.

Table 1-5: Revision History

Date	Version	Description
December 2020	0.0.0.1	Draft
April 2021	0.0.0.2	Draft, following 1st discussion in TEE-MCU WG
May 2021	0.0.0.3	Draft, following 2nd and 3rd discussion in TEE-MCU WG
June 2021	0.0.1.1	Draft, release to members review

2 Platform definition and scope

The Platform consists of a secure external memory. A secure external memory is a discrete component that is part of the secure application (system) and performs the task of data and code storage in a secure manner. A secure external memory can be, e.g., a nonvolatile flash memory that is part of a secure sub system in a complex System on Chip (SoC), holding the secure function code and user data.

The Platform is intended to be used as a Platform Part in composition with a host Platform Part. The host Platform Part is named the Application in this document.

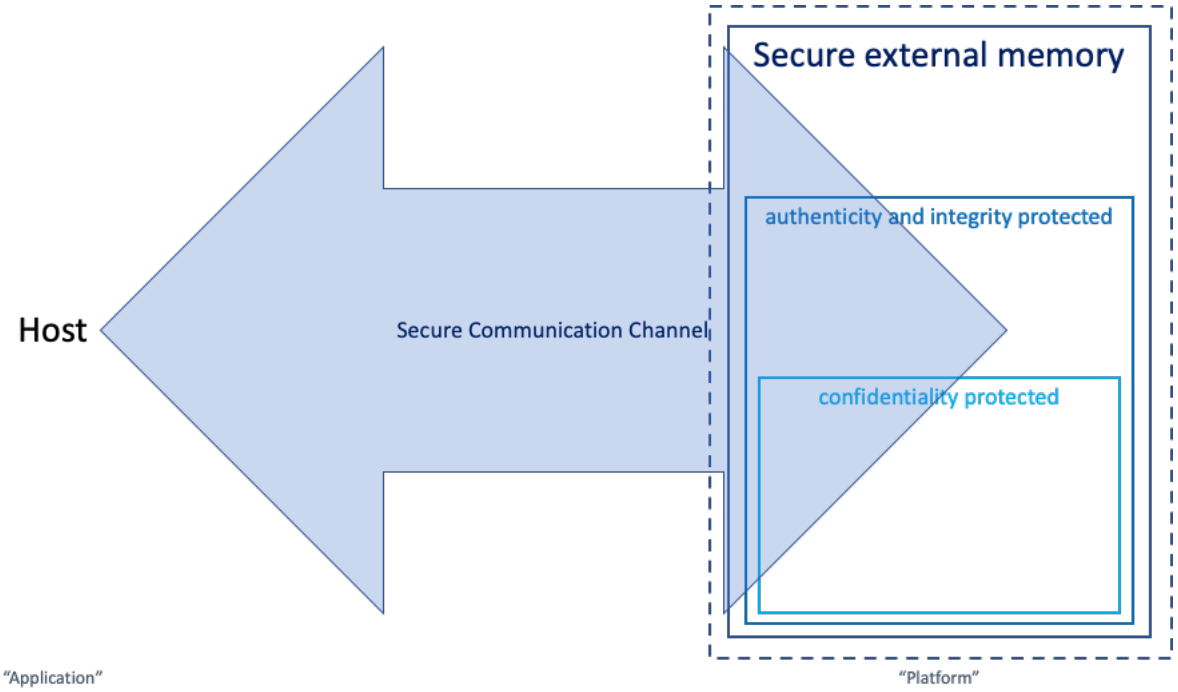

Figure 2-1: Platform scope: the secure external memory

There are three levels of compliance: Augmented/Protected/Secured Memory.Each level describes a different subset of requirements, per the requirements of the composition application. One use case may require authentication of the user before the memory component allows read access to the content. In such case, only protected of secured memory may be used. The Protected memory and Secure memory have similar Security Functional Requirements (SFRs) but are certified to different SESIP levels.

	Augmented Memory	Protected Memory	Secured Memory	Comment
Communicated data confidentiality protection	Mandatory	Mandatory	Mandatory	Data encryption for read and write commands issued for protected data
Authenticity and integrity protection	Mandatory	Mandatory	Mandatory	Replay-protected signature on write commands issued for protected data
Access control: authenticated User	Optional	Mandatory	Mandatory	User Authentication for allowing read access to protected data. E.g., by establishing a secure channel with mutual authentication
~~Access control: per user authentication read~~ INFO: This SFR is not yet supported by SESIP methodology. Left here for reference purpose only	~~Optional~~	~~Optional~~	~~Mandatory~~	~~Multi-user model with separate access policies for different address ranges of protected data~~
SESIP2	Minimum	NA	NA	Only Augmented memory can be evaluated per SESIP2
SESIP3	Augmented	Minimum	NA	Only Augmented or Protected memory can be evaluated per SESIP3
SESIP5	Augmented	Augmented	Minimum	

The ST writer shall select one of these levels and refer to it.

The main security feature of the Platform is to provide the needed secure external memory functionality to protect the confidentiality, integrity and authenticity of stored data assets:

- The host can request data communicated with the secure external memory to be protected for confidentiality as per "Secure Communication Enforcement" SFR.
- The host can request data stored in the secure external memory to be protected for authenticity and integrity uniquely for that memory as per "Secure Storage" SFR.

- Communication with the secure external memory for data requested to be confidentiality, or authenticity and integrity protected as above, is protected against disclosure, modification, replay, impersonation as per "Secure Communication Support" and "Secure Communication Enforcement " SFR, thus allowing for secure binding and anti-cloning properties.
- Freshness support for the application is provided by the "Reliable Index" (also commonly known as "monotonic counter").
- And all these security features are with "Physical Attacker Resistance", so protected to an attacker with physical access to the secure external memory, up to the SESIP level described.

3 Security Objectives for the Operational Environment

For a composite product to fulfill its security requirements, the operational environment (technical or procedural) shall fulfill the following objectives:

- The application shall verify the correct version of all platform components it depends on
- The application shall support the invocation of an update mechanism, if such mechanism, exists in the platform.
- The application shall implement the secure channel defined in “Secure Communication Enforcement ” by implementing the protocol mentioned, including detection of failed authenticity and integrity check. This implementation can be claimed as “Secure External Storage” if the additive composition is certified, before claims on the composition can be made.
- The application shall store data to be protected for authenticity, integrity, or confidentiality in the area that is indeed protected for authenticity/integrity/confidentiality.
- The application can where relevant implement a freshness/anti-rollback protection using a “Reliable Index” provided by the platform.

Application Note: Author should list all additional mandatory objectives for the environment with reference to where in the guidance documents these objectives are described.

4 Security requirements and implementation

4.1 Security Assurance Requirements

The claimed assurance requirements package is: <***SESIP2/SESIP3/SESIP5>*** as defined in [SESIP].

Application Note: Author should declare the SESIP level for the platform assurance

4.1.1 Flaw Reporting Procedure (ALC_FLR.2)

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to generate any needed software update and distribute it to the platform, the developer has defined the following procedure:

Application Note: Author should reuse the guidance from the SESIP methodology

4.2 Security Functional Requirements (mandatory for SESIP)

The platform fulfills the following security functional requirements:

4.2.1 Verification of Platform Identity

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

~~4.2.2 Secure Update of Platform~~

~~The platform can be updated to a newer version in the field such that the integrity, authenticity and confidentiality of the platform is maintained.~~

Info: Only this SFR from the [Profile] may be removed (use strike-through) and only when in ALC_FLR.2 a strong argumentation is provided why updates are not necessary for this kind of device. We expect that removing this SFR is the most likely situation (as most external memories don't have updatable functionality), so it is struck-through.

4.3 Security Functional Requirements (mandatory from [Profile])

4.3.1 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.

4.3.2 Attestation of Platform Genuineness

The platform provides an attestation of the "Verification of Platform Identity" and "Verification of Platform Instance Identity", in a way that cannot be cloned or changed without detection.

4.3.3 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.

Informational:

Note that this means that in all cases the attacker can physically access to the secure external memory, also during the exploitation phase, i.e. when the memory is deployed. Due to how SESIP's attack model works, as the attacker becomes more powerful from SESIP2 to SESIP5, so does this "Physical Attacker Resistance" scales.

Highly simplified this means that:

At Augmented Memory (SESIP2) level, the attacker has a low 15 attack points (AVA_VAN.2) budget. With this, the attacker can try to break the promised protection by accessing otherwise unconnected interfaces of the secure external memory. This means that for example unblocked test or debug interfaces allowing the bypassing of the security of the platform, will likely fail the evaluation.

At Protected Memory (SESIP3) level, the attacker has a modest 20 attack points (AVA_VAN.3), and with this budget can attempt for example simple glitching and side-channel analysis attacks. Only simple attacks on the physical memory array are likely to be in scope.

At Secured Memory (SESIP5) level, the attacker has a state-of-the-art 30 attack points (AVA_VAN.5) budget. This allows the attacker to attempt state-of-the-art smartcard attacks on the secure external memory, even including advanced attacks on the physical memory array.

4.3.4 Secure Storage

The platform ensures that all data stored by the application, except for *<list of data stored in plaintext, i.e. outside the authenticity and integrity protected area>*, is protected to ensure its

authenticity and integrity as specified in *<specification>* with a platform instance unique key of key length *<key length>.*

Application note:

At Augmented Memory (SESIP2) level or higher, the platform must implement at least read-only or authenticated-write memory.

At Secured Memory (SESIP5) level, the platform must implement authenticated-write memory, read-only is not sufficient.

4.3.5 Secure Communication Support

The platform provides the application with one or more secure communication channel(s).

The secure communication channel authenticates **the application and platform** and protects against **disclosure, modification, replay, and impersonation** of messages between the endpoints, using *<list of protocols and measures>.*

Application Note:

The protocols and measures must ensure that data requested with confidentiality protection is protected against disclosure, that data requested with authenticity and integrity protection are protected against modification, replay and impersonation in such a way that the platform instance cannot be impersonated, thus allowing for secure binding and anti-cloning properties.

Compromising the confidentiality of the keys used in the platform for these protocols and measures, constitutes a break of this SFR.

At Protected Memory (SESIP3) level, the platform must implement a protocol that provides access to parts of the memory only when authentication performed by the application is successful.

At Secured Memory (SESIP5) level, the platform must implement a protocol that allows different application identities to access different areas (allowing for user authentication).

4.3.6 Secure Communication Enforcement

The platform ensures the application can only communicate with **the platform** over the secure communication channel(s) supported by the platform using **the protocols described in the SFR "Secure Communication Support" for data requested to be protected for confidentiality, integrity or authenticity**.

4.3.7 Reliable Index

The platform implements a strictly increasing function.

Informational:

This index can be used by the application to ensure freshness when required. Note that this is commonly called “Monotonic Counter”.

5 Sufficiency rationales

5.1 Sufficiency rationale SESIP 2 (Augmented Memory)

Assurance Class	Assurance Family	Covered by	Rationale
ASE: Security Target Evaluation	ASE_INT.1 ST introduction	Section "Platform definition and scope" and title page. <Update as relevant>	The ST reference is in the title, the reference of the TOE is in the TBD, and the description is in "Platform definition and scope". <Update as relevant>
	ASE_OBJ.1 Security requirements for the operational environment	Section "Security Objectives for the ".	The objectives for the operational environment in "Security Objectives for the " refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	All SFRs are taken from [SESIP] Section "Security Functional Requirements (mandatory for SESIP)" list the "Verification of Platform Identity"" is included. "~~Secure Update of Platform~~" is **not** included as per refinement. <should be included for platform that support updates> Section "Security Functional Requirements (mandatory from [Profile])" lists the profile SFRs.	

		All SFRs have been mapped from the CC SFRs to the SESIP SFRs in TBD. < writer will need to make this mapping based on the CC ST. Note that the mapping is **from** CC SFR **to** SESIP SFR, showing that all SESIP SFRs are fully covered by the CC SFRs. This may mean some CC SFRs are not 'used' by the SESIP ST.>	
	ASE_TSS.1 TOE Summary specification	Section "Security Functional Requirements (mandatory for SESIP)" and "Security Functional Requirements (mandatory from [Profile])".	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in "Security Functional Requirements (mandatory for SESIP)" and "Security Functional Requirements (mandatory from [Profile])".
ADV: Development	ADV_FSP.4 Complete functional specification	TBD describe where the functional specs are, suggested this is done per SFR. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	TBD. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	AGD_PRE.1 Preparative procedures	TBD. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.

ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section “Flaw Reporting Procedure (ALC_FLR.2)”.	The flaw reporting and remediation procedure is described. < if you refer to the ALC_FLR of the underlying CC certification, be sure to check it is ALC_FLR.**2**. The evaluation lab must verify that the procedure fulfills the SESIP requirements on it, specifically the emphasis on the way how the outside interfaces with the vulnerability disclosure and gets informed of vulnerabilities.>
ATE: Tests	ATE_IND.1 Independent testing: conformance	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
AVA: Vulnerability Analysis	AVA_VAN.2 Vulnerability analysis	N.A. A vulnerability analysis is performed by the platform evaluator to ascertain the presence of potential vulnerabilities. Penetration testing is performed by the platform evaluator assuming an appropriate attack potential.	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.

5.2 Sufficiency rationale SESIP3 (Protected Memory)

Assurance Class	Assurance Family	Covered by	Rationale

ASE: Security Target Evaluation	ASE_INT.1 ST introduction	Section "Platform definition and scope" and title page. <Update as relevant>	The ST reference is in the title, the reference of the TOE is in the TBD, and the description is in "Platform definition and scope". <Update as relevant>
	ASE_OBJ.1 Security requirements for the operational environment	Section "Security Objectives for the ".	The objectives for the operational environment in "Security Objectives for the " refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	All SFRs are taken from [SESIP] Section "Security Functional Requirements (mandatory for SESIP)" list the "Verification of Platform Identity"" is included. "~~Secure Update of Platform~~" is **not** included as per refinement. <should be included for platform that support updates> Section "Security Functional Requirements (mandatory from [Profile])" lists the profile SFRs. All SFRs have been mapped from the CC SFRs to the SESIP SFRs in TBD.	

		< writer will need to make this mapping based on the CC ST. Note that the mapping is **from** CC SFR **to** SESIP SFR, showing that all SESIP SFRs are fully covered by the CC SFRs. This may mean some CC SFRs are not 'used' by the SESIP ST.>	
	ASE_TSS.1 TOE Summary specification	Section "Security Functional Requirements (mandatory for SESIP)" and "Security Functional Requirements (mandatory from [Profile])".	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in "Security Functional Requirements (mandatory for SESIP)" and "Security Functional Requirements (mandatory from [Profile])".
ADV: Development	ADV_FSP.4 Complete functional specification	TBD describe where the functional specs are, suggested this is done per SFR. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	TBD describe where the SFRs are implemented, suggested this is done per SFR. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	TBD. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.

	AGD_PRE.1 Preparative procedures	TBD. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	TBD. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ALC_CMS.1 TOE CM Coverage	TBD. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ALC_FLR.2 Flaw reporting procedures	Section “Flaw Reporting Procedure (ALC_FLR.2)”.	The flaw reporting and remediation procedure is described. < if you refer to the ALC_FLR of the underlying CC certification, be sure to check it is ALC_FLR.**2**. The evaluation lab must verify that the procedure fulfills the SESIP requirements on it, specifically the emphasis on the way how the outside interfaces with the vulnerability disclosure and gets informed of vulnerabilities.>
	ATE_IND.1 Independent testing: conformance	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.

AVA: Vulnerability Analysis	AVA_VAN.3 Focused Vulnerability analysis	N.A. A vulnerability analysis is performed by the platform evaluator to ascertain the presence of potential vulnerabilities. Penetration testing is performed by the platform evaluator assuming an appropriate attack potential.	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.

5.3 Sufficiency rationale SESIP5 (Secured Memory)

INFO adapt this to your situation. The mapping below suggests the rationale based on the SESIP profile, but you are responsible for adjusting this.

Assurance Class	Assurance Family	Covered by	Rationale
ASE: Security Target Evaluation	ASE_INT.1 ST introduction	Section "Platform definition and scope" and title page. <Update as relevant>	The ST reference is in the title, the reference of the TOE is in the TBD, and the description is in "Platform definition and scope".
	ASE_CCL.1 Conformance claims	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ASE_OBJ.1 Security requirements for the operational environment	Section "Security Objectives for the ".	The objectives for the operational environment in "Security Objectives for the " refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	All SFRs are taken from [SESIP]	

		Section "Security Functional Requirements (mandatory for SESIP)" list the "Verification of Platform Identity"" is included. "~~Secure Update of Platform~~" is **not** included as per refinement. <should be included for platform that support updates> Section "Security Functional Requirements (mandatory from [Profile])" lists the profile SFRs. All SFRs have been mapped from the CC SFRs to the SESIP SFRs in TBD. < writer will need to make this mapping based on the CC ST. Note that the mapping is **from** CC SFR **to** SESIP SFR, showing that all SESIP SFRs are fully covered by the CC SFRs. This may mean some CC SFRs are not 'used' by the SESIP ST.>	
	ASE_SPD.1 Security problem definition	TBD refer to the associated CC ST. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.

	ASE_TSS.1 TOE Summary specification	Section "Security Functional Requirements (mandatory for SESIP)" and "Security Functional Requirements (mandatory from [Profile])".	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in "Security Functional Requirements (mandatory for SESIP)" and "Security Functional Requirements (mandatory from [Profile])".
ADV: Development	ADV_ARC.1 Security architecture description	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ADV_FSP.4 Complete functional specification	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ADV_TDS.3 Basic modular design	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ADV_IMP.2 Complete mapping of the implementation representation of the TSF	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.

	AGD_PRE.1 Preparative procedures	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ALC_CMS.4 Problem tracking CM Coverage	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ALC_DEL.1 Delivery procedures	TBD refer to the associated CC certificate.	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ALC_DVS.1 Identification of security measures	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ALC_FLR.2 Flaw reporting procedures	Section “Flaw Reporting Procedure (ALC_FLR.2)”.	The flaw reporting and remediation procedure is described.

			< if you refer to the ALC_FLR of the underlying CC certification, be sure to check it is ALC_FLR.**2**. The evaluation lab must verify that the procedure fulfills the SESIP requirements on it, specifically the emphasis on the way how the outside interfaces with the vulnerability disclosure and gets informed of vulnerabilities.>
	ALC_TAT.1 Well-defined development tools	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
ATE: Tests	ATE_COV.1 Evidence of coverage	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ATE_DPT.1 Testing: basic design	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
	ATE_FUN.1 Functional testing	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.

	ATE_IND.1 Independent testing: conformance	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.
AVA: Vulnerability Analysis	AVA_VAN.5: Advanced methodical vulnerability analysis	TBD refer to the associated CC certificate. <Update as relevant>	The platform evaluator has determined that the provided evidence is suitable to meet the requirement in the associated CC evaluation.