eUICC Security Assurance Methodology

Version 2.0

19 December 2023

Security Classification: Non-Confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSMA makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Contents

1 Introduction

1.1 Overview

The classical approach to security evaluation and assurance has a high documentation focus:

1. The Developer providing Developer documentation that completely and consistently complies with every aspect of every relevant work unit of the Common Criteria evaluation methodology,
2. The Licensed Laboratory documenting, for each work unit, a complete rationale and summary of the evidence so that the Certifier can ascertain that each work unit has been completely and correctly performed and each piece of methodology guidance has been completely and correctly applied.

An alternative approach to this classical approach has been developed by organisations working within the Dutch NSCIB organisation, as NSCIB document Scheme Procedure #6. This alternative approach introduces efficiencies whereby all Common Criteria activities are performed but with a lower dependency on documentation.

This methodology for eUICC security assurance has been developed, based on the NSCIB Scheme Procedure #6. Additional optimisations are described specific to embedded UICCs that have been designed to the GSMA remote provisioning PRDs, SGP.01 [9], SGP.21 [10] and SGP.31 [23]. Within this document, eUICC optimisations are included in specific subsections entitled “GSMA optimisation.”

Using this approach, the Licensed Laboratory performs all activities mandated by ISO15408 [1] but adopts the style of reporting described in this document. This results in less time reporting results and more time on testing, especially penetration testing.

This document describes the methodology for eUICC security evaluations under the GSMA eUICC Security Assurance scheme and SHOULD be read in conjunction with the GSMA eUICC Security Assurance Principles [17]. The methodology is intended to provide an eUICC focussed implementation of Common Criteria (CC), with Appendix A providing a template for mapping CC Evaluator actions to the resulting Evaluator reports that demonstrate compliance to the requirements.

1.2 Scope

This document covers the security assurance evaluation for the remote provisioning functionality of embedded UICCs that have been designed referencing GSMA PRDs SGP.01 [9], SGP.21 [10] or SGP.31 [23]. The associated Protection Profiles are described in GSMA PRDs SGP.05 [11] and SGP.25 [12].

Embedded UICCs assessed under these procedures are expected to be able to declare compliance to the eUICC security assurance requirements of the GSMA M2M, RSP and IoT compliance processes, SGP.16 [6] and SGP.24 [7].

This document assumes familiarity with the terminology of GSMA PRDs SGP.05 [11], SGP.25 [12] and Common Criteria CC:V3.1 Part 1 [2] or Common Criteria version CC:2022

Part 1 [26] and so abbreviations taken from those documents are used throughout the document'.

1.3 Definitions

Term	Description
Certifier	Person acting on behalf of the GSMA Certification Body
eUICC	A removable or non-removable UICC which enables the remote and/or local management of Profiles in a secure way. NOTE: The term originates from "embedded UICC".
Developer	Person acting on behalf of the EUM
Evaluator	Person acting on behalf of the Licensed Laboratories
PP	Protection Profiles
GSMA Certification Body	Certification Body role, appointed by GSMA
GSMA Protection Profiles	GSMA PRD SGP.05[11]and GSMA PRD SGP.25 [12]
NSCIB	Netherlands Scheme for Certification in the Area of IT
Licensed Laboratory	A security evaluation laboratory licensed by a GSMA CB to perform eUICC security evaluations for the GSMA eUICC Scheme

1.4 Abbreviations

Term	Description
CB	Certification Body
CEM	Common Methodology for Information Technology Security Evaluation
CC	Common Criteria
EWP	Evaluation Work Plan
EM1/2/3	First, Second, and Third Evaluation Meeting
ETR	Evaluation Technical Report
EUM	eUICC Manufacturer
GSMA CB	GSMA Certification Body
IR_ASE	Intermediate Report Security Target Evaluation
ST	Security Target
SAR	Shared Audit Report
STAR	Site Technical Audit Report
TOE	Target of Evaluation

1.5 References

Ref	Doc Number	Title
[1]	[ISO15408]	Information technology — Security techniques — Evaluation criteria for IT security

Ref	Doc Number	Title
[2]	[CC]	Common Criteria for IT Security Evaluation, Part 1,2 and 3, v3.1r5, April 2017
[3]	Void	Void
[4]	Void	Void
[5]	[CoDE]	Collection of Developer Evidence, v1.5, JIL, January 2012 / CCDB-2012-04 005
[6]	[SGP.16]	M2M Compliance Process
[7]	[SGP.24]	RSP Compliance Process
[8]	[SGP.02]	Remote Provisioning Architecture for Embedded UICC Technical Specification
[9]	[SGP.01]	Embedded SIM Remote Provisioning Architecture
[10]	[SGP.21]	Remote SIM Provisioning Architecture
[11]	[SGP.05]	Embedded UICC Protection Profile, version: • 1.0, GSM Association, September 2014 • 1.1, GSM Association, August 2015 also published by BSI as BSI-CC-PP-0089-2015 • 4.0, GSM Association, October 2022 • 4.1, GSM Association, March 2023
[12]	[SGP.25]	RSP eUICC for Consumer Device Protection Profile, version • 1.0, GSM Association, June 2018 also published by BSI as BSI-CC-PP-0100-2018 • 2.0 GSM Association, December 2023
[13]	[SGP.11]	Remote Provisioning architecture for Embedded UICC test specification
[14]	[SGP.23]	RSP test specification
[15]	[SGP.22]	RSP Technical Specification
[16]	[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels," S. Bradner http://www.ietf.org/rfc/rfc2119.txt
[17]	[SGP.06]	GSMA eUICC Security Assurance Principles
[18]	[CCDB]	CCDB-2007-11-001; Site Certification, Version 1.0, October 2007
[19]	[EMVCo]	EMVCo Security Guidelines – Development and Production Site Audit Guidelines; 1.1 – May 2015
[20]	[GSMA PRD AA.35]	Procedures for Industry Specifications
[21]	SGP.17-1	Security Target template for eUICC Consumer Devices
[22]	[COMP]	Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018.
[23]	[SGP.31]	eSIM IoT Architecture and Requirement Specification
[24]	[SGP.32]	eSIM IoT Techncial Specification
[25]	[SGP.33-1]	eSIM IoT Test Specification - eUICC

Ref	Doc Number	Title
[26]	[CC]	Common Criteria for Information Technology Security Evaluation, Part 1,2, 3 and 5 version CC:2022 Revision 1, November 2022.

1.6 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC2119 [16].

2 Process Overview

The eUICC security assurance evaluation and certification process consists of the following 8 steps:

1. Application
2. Kick-off meeting (OPTIONAL)

----

3. ST Evaluation
4. First Evaluation Meeting
5. Second Evaluation Meeting (Monitoring Phase: detailed in this scheme procedure)
6. Final Evaluation Meeting
7. Final Evaluation Reporting

----

8. Certification Phase

For some evaluations, the first and second evaluation meetings MAY be combined into one (1) meeting where all the required deliverables for EM1 and EM2 will be presented in one step. The combination of the first and second evaluation meetings is the default when the Alternative ADV method is used because for this method a separation of the design-level and the implementation-level assessment is counter-intuitive. Whether first and second evaluation meetingsare combined needs to be decided during the Application process because the reduction of the number of meetings MAY impact the certification cost. Factors which are relevant for the decision are for example the complexity of the product in combination with the required level of assurance. It SHOULD also be noted that the amount of material and discussion for complex products MAY mean that a combined meeting has to stretch over multiple days.

2.1 Security Target Evaluation

The Developer SHALL provide a draft Security Target (ST). For eUICC Consumer devices, the ST template defined in [21], based on SGP.25 [12], MAY be used. The Licensed Laboratory adds the accompanying evaluation report with the ASE evaluation results to the

Certifier. After one or more feedback loops based on official review reports, as detailed below, the ST is provisionally[1] approved by the Certifier.

The review SHALL check at least that:

1. The ST is compliant with the applicable GSMA Protection Profiles, SGP.05 [11] or SGP.25 [12].
2. The ST is clear and understandable, the TOE scope is defined.
3. The ST does not contradict the ST of the underlying platform as it is defined in [22].

2.1.1 GSMA Optimisation

The GSMA SGP.05 [11] and SGP.25 [12] are certified to fulfil the APE requirements. Provided the ST is compliant with the PP (as verified in ASE_CCL), the following Evaluator activities are considered completed by a simple verification check performed by the Licensed Laboratory: ASE_SPD, ASE_OBJ, and ASE_ECD. ASE_REQ is expected to be limited to the verification of the correct application of the operations.

For the [COMP] activities, in case the ST does not contain a statement of compatibility, these activities can be still completed by the evaluator by providing evidences that applying direct verification between both TOE ST and underlying platform ST can fulfil these requirements.

2.2 General Requirements for the Evaluator Presentations

Apart from the Security Target (ASE) evaluation results (as discussed above), the Evaluator reporting within GSMA evaluations is based on evaluation meetings and presentations. In the meeting deliverables the Evaluator SHALL show how all content and Evaluator action elements for the processing of the assurance components relevant to the evaluation are met. This MUST be done within the presentation and MAY additionally be supported by an annex or other Evaluator analysis documents. The Evaluator SHALL also provide a checklist where Evaluator action items are demonstrated in the meeting deliverables, to a level of content and presentation elements.

At EM1 the checklist for the entire assurance level SHALL be presented, populated as appropriate for EM1. This document is then further populated for subsequent evaluation meetings. This means that the checklist presented in EM3 will be completely populated.

When the methodology applied by the Evaluator describes explicit reporting to be provided, this explicit reporting SHALL be automatically provided as part of the evaluation documentation.

2.3 First Evaluation Meeting

2.3.1 First Evaluation Meeting Procedure

The Licensed Laboratory organises a remote or physical meeting with the Certifier at a mutually agreed location. The Developer is encouraged, but not required, to attend the

[1] There is always room for later changes due to Developer changes, new information coming to light or new insights at Licensed Laboratory, EUM, or GSMA CB. Note that this term “provisionally approved” is used throughout this document.

meeting. Other parties are only allowed to attend if the Developer, Licensed Laboratory and Certifier agree.

Five working days before the meeting the Licensed Laboratory will send all first evaluation meeting deliverables (see 2.3.2) to the Certifier.

In this meeting the First evaluation meeting deliverables are presented by the Evaluator, according to the following rules:

- Not all first evaluation meeting deliverables need to be presented. As the Certifier has had one week to study the deliverables, he/she MAY allow the Evaluator to skip certain sections that the Certifier deems to be self-explanatory.
- The Certifier is allowed to question the Evaluator on any or all the items to ascertain that the evaluation was performed correctly and completely.
- If there are any missing items in the First evaluation meeting deliverables, or items that are not clear, these will be corrected during the meeting, by amending the First evaluation meeting deliverables where possible and annotating them where amending would take too much time.

The meeting can have four possible outcomes:

1. All first evaluation meeting deliverables were either correct or successfully amended/annotated during the meeting. In this case all these deliverables are provisionally approved.
2. One or more deliverables could not be successfully amended/annotated, but the Certifier determines that this can be further handled by email. In this case, the other deliverables are provisionally approved, and after an email process, where the remaining deliverables are amended/annotated will also be provisionally approved.
3. One or more deliverables could not be successfully amended/annotated and cannot be handled by email, but the Certifier determines that this can be rescheduled to the Second Evaluation Meeting. In this case, the other deliverables are provisionally approved, and the remaining deliverables are rescheduled.
4. One or more deliverables could not be successfully amended/annotated, and the Certifier determines that this cannot be handled by email or rescheduling. In this case, the entire first evaluation meeting is nullified, and MUST be repeated once the Evaluator has remedied everything.

The Licensed Laboratory will take notes of all decisions made and issues raised by the Certifier where further action is required (i.e. deliverable annotated during meeting, further handling by email or renewed discussion of the issue at a rescheduled meeting). This list with issues and related actions will be emailed to the Certifier for confirmation within 2 working days after the meeting.

No full meeting minutes or detailed review reports are required, but the Certifier will endeavour to provide a written list of issues before, or at the meeting.

2.3.2 First Evaluation Meeting Deliverables

The First evaluation meeting deliverables consist of the following:

- Checklist of all Evaluator action items and content and presentation element relevant for the claimed assurance level (populated to show where the Evaluator actions relevant to EM1 are demonstrated).
- Updated ST and IR_ASE according to Certifier comments;
- The ADV Presentation (see Chapter 5);
- The Implementation Representation Sampling Rationale (see Chapter 6).
- The ADV/AGD Reference Document (see Chapter 7) and all guidance documents that this document refers to.
- The Configuration Item Identification Presentation (see Chapter 8).
- Any other observations that were found before this meeting and are deemed relevant.

2.4 Second Evaluation Meeting

2.4.1 Second Evaluation Meeting Procedure

The second evaluation meeting procedure is identical to the First evaluation meeting deliverable, with the exceptions that it concerns different deliverables (see 2.4.2).

2.4.2 Second Evaluation Meeting Deliverables

The second evaluation meeting deliverables consist of the following:

- Updated Checklist showing where the Evaluator actions relevant to EM1 and EM2 are demonstrated.
- Any First evaluation meeting deliverables that were rescheduled to this meeting;
- The Implementation Representation Presentation (see section 6);
- The ATE/AVA Test Plan Presentation (see section 10);
- The ATE/AVA Test Descriptions (see section 11).
- The ALC Presentation, including ALC verification plan (see section 12);
- Any other observations that were found before this meeting and are deemed relevant.

2.5 Final Evaluation Meeting

2.5.1 Final Evaluation Meeting Procedure

This procedure is identical to the first and second evaluation meeting procedure, with the following exceptions:

- It concerns different deliverables (see 2.5.2)
- It cannot end with outcome #3 (see 2.3.1) as there is no further meeting to reschedule to.

2.5.2 Final Evaluation Meeting Deliverables

The final evaluation meeting deliverables consist of the following:

- Updated Checklist showing where all Evaluator actions are demonstrated.
- Any second evaluation meeting deliverables that were rescheduled to this meeting;
- The final ST (and if applicable ST-Lite);
- The final guidance documentation for the TOE satisfying AGD_PRE and AGD_OPE.
- The ATE/AVA Test Results (see section 13);

- The ALC Results Presentation (see section 14);
- Draft ETR, draft ETRfc (if applicable)
- Any further observations that were found before this meeting and are deemed relevant.

2.6 Final Evaluation Reporting

The Licensed Laboratory delivers its revised Evaluation Technical Report (ETR) and the revised (final) versions of the evaluation deliverables of the final meeting and, if this is found correct; the Certifier formally approves the ETR and all provisionally approved items.

3 Handling of EUM Documentation

The GSMA CB will not get any product documentation except the Security Target. The evaluation is completely handled by the Evaluator. All EUM documentation SHALL be available for the GSMA CB to review during the evaluation meetings at either the Evaluator or the Developer site.

4 Notation

In the following chapters, the following notation is used:

Evaluator presentation actions (the actions an Evaluator has to do) are always encased in a green box.

This reporting is not “complete” in the sense that it reports every CEM detail at the level of a work unit. However, for the GSMA this, together with the checklist mapping where the evaluation action items and content and presentation elements are reported, is sufficient to meet the reporting requirements indicated in the green box. Note that this does not allow the Evaluator to avoid using the CC or CEM: this is only intended for what needs to be reported. Any further recording of results is left to the Licensed Laboratory and to the ISO-17025 standard.

Often these boxes are then followed by an example, to illustrate some important concept.

Finally, a brief summary of the result is then given. This result is always encased in an orange box.

5 The ADV Presentation

The overall goal of the assurance class ADV is for the Evaluator to understand the TOE to the level that he can understand how it implements security, and to assist the Evaluator in determining his tests and penetration tests.

The role of the Certifier is to ascertain that the Evaluator understands the design (and has fulfilled the assurance requirements or work unit). To this end, while the presentation MAY contain useful examples from the Developer evidence, the presentation SHOULD NOT just be comprised of copied material from the Developer evidence. It SHOULD reflect the Evaluators’ summary of that material with appropriate references.

For the evaluation (and presentation) of ADV, two methods exist:

1. The regular ADV method,
2. The alternative ADV method

The regular ADV method is based on Evaluator analysis of a full set of Developer evidence to meet each Developer action item (down to the level of content and presentation elements)

The alternative method for ADV is an extension of the Collection of Developer evidence [5] process, using implementation representation as a basis. This approach can always be used for eUICC evaluation, in order to be licensed by the GSMA CB, the Licensed Laboratory has to show experience with the TOE type in question and is able to determine the full TSF security behaviour from the implementation representation. The regular ADV method is to be used in all other cases.

For a Licensed Laboratory to use the alternative ADV method, these conditions MUST be met:

- The entire implementation representation MUST be made available to the Evaluator and sufficiently annotated with informal text to enable the Evaluator to trace all SFRs to the modules, as defined in the implementation representation.
- The alternative method for ATE MUST be used (see section 10.2).

The alternative method exploits the fact that the Licensed Laboratory is familiar with the TOE type to the extent that the Licensed Laboratory can:

- Perform a vulnerability analysis directly on the implementation representation, without requiring detailed TDS Developer evidence.
- Determine whether the SFRs are met by the implementation representation, without requiring detailed ADV_TDS Developer evidence.
- Determine whether the constructs described in the Developer ARC document are correctly implemented, without requiring detailed TDS Developer evidence.

Under the three conditions above, the entire of ADV_TDS is defined by the implementation representation, that is:

- Modules are sets of implementation representation (e.g. source code), and the interfaces of those modules are the interfaces of that implementation representation. Since the modules are defined by the implementation representation, they automatically meet any semi-formal description requirements required for the evaluation assurance level.
- The Evaluator uses his experience with the TOE type in question to identify all SFR-enforcing and SFR-supporting modules as part of the ADV_IMP work. The entire implementation representation MUST be described at a level as if it is SFR-enforcing. A summary of this identification is provided by the Evaluator in the form of an overview of the TOE and how it implements the SFRs. While the full mapping needs to be completed in order to ensure the necessary modules are identified for ADV_TDS, there is no need to present the full mapping of the SFRs to the modules. The presentation MUST provide an example of how this mapping is generated and,

on demand, the Evaluator MUST be able to show how a specific SFR is implemented by the modules.

- Subsystems are sets of modules and the interfaces of those subsystems are the externally accessible interfaces of the modules. If the modules are sufficiently described, then also the subsystems are sufficiently described, and additional subsystem level descriptions are not required.

If all SFRs can be traced to the implementation representation, and the implementation representation meets the ADV_IMP.1 requirement (as considered in section 9.2 or 10 as applicable for the assurance level), all ADV_TDS requirements are met and need not be checked separately or described further by the Evaluator. The only Evaluator activity required is the presentation of the method used by the Evaluator to identify the modules from the sets of code. This description SHOULD be accompanied with examples of the identified modules and rationale of how they fit the method for identifying modules.

The ADV presentation will present the following elements:

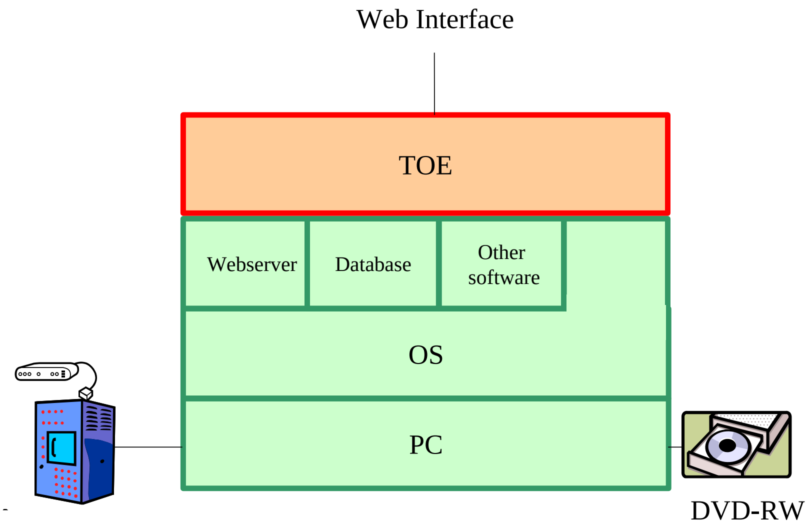
- The TOE and the TSFI
- Subsystems
- Modules
- Tracing SFRs to TSFI and Subsystems
- Security Architecture

5.1 The TOE and the TSFI

This section applies to both the regular and the alternative ADV method.

1. The Evaluator presents a model of the TOE in its environment:
   - where necessary, this model SHALL be supplemented with photos of the TOE or the actual TOE;
   - this model SHALL clearly show all interfaces of the TOE;
   - all interfaces SHALL be explained as TSFI or non-TSFI;
   - the purpose and method of use of all TSFI SHALL be presented;
   - this model SHALL show all user roles that interact with each TSFI, and where useful, all other interfaces.
2. The Evaluator explains how he determined completeness.

Example of a model:



The only TSFI is the Web Interface (defined in [FSP] section x.y). The interface with the DVD-RW, and other external boxes are not TSFI, as they are B1 interfaces. The interfaces to Webserver, Database, Other Software, OS, and PC are not TSFI, as they are B2 interfaces. See CC Part 3 Annex A.2.2.2.

Result: The Evaluator demonstrates that all interfaces and TSFI have been identified and described.

5.1.1 GSMA Optimisation

An eUICC that has been designed to the following GSMA specifications is considered to fulfil all requirements of ADV_FSP.4:

- eUICCs designed to meet the architecture requirements of GSMA PRD SGP.01 [9] and technical implementation of GSMA PRD SGP.02 [8].

Or

- eUICC designed to meet the architecture requirements of GSMA PRD SGP.21 [10] and technical implementation of GSMA PRD SGP.22 [15].

Or

- eUICC designed to meet the architecture requirements of GSMA PRD SGP.31 [23] and technical implementation of GSMA PRD SGP.32 [24].

5.2 Subsystems

5.2.1 The Regular ADV Method for Subsystems

1. The Evaluator presents a subsystem level model of the TOE (with some parts of the environment):

- this model SHALL be sensible and useful[3] [4];
- this model SHALL show all TSFI, and where useful, all other interfaces;
- this model SHALL clearly clarify whether subsystems are TOE, TSF or environment and whether they are SFR-enforcing, SFR-supporting, or SFR non-interfering.

2. The Evaluator explains the behaviour of each subsystem and its interaction with other subsystems. This explanation SHALL make use of examples from the Developer evidence (e.g. diagrams).

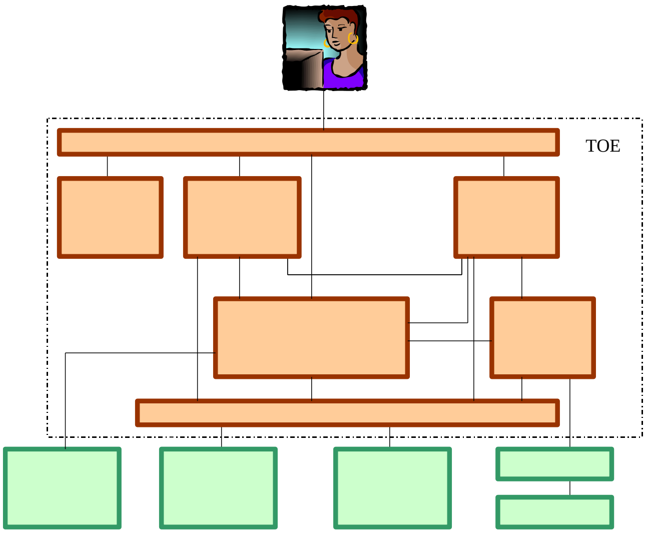


Figure 1 Example of the subsystem level model:

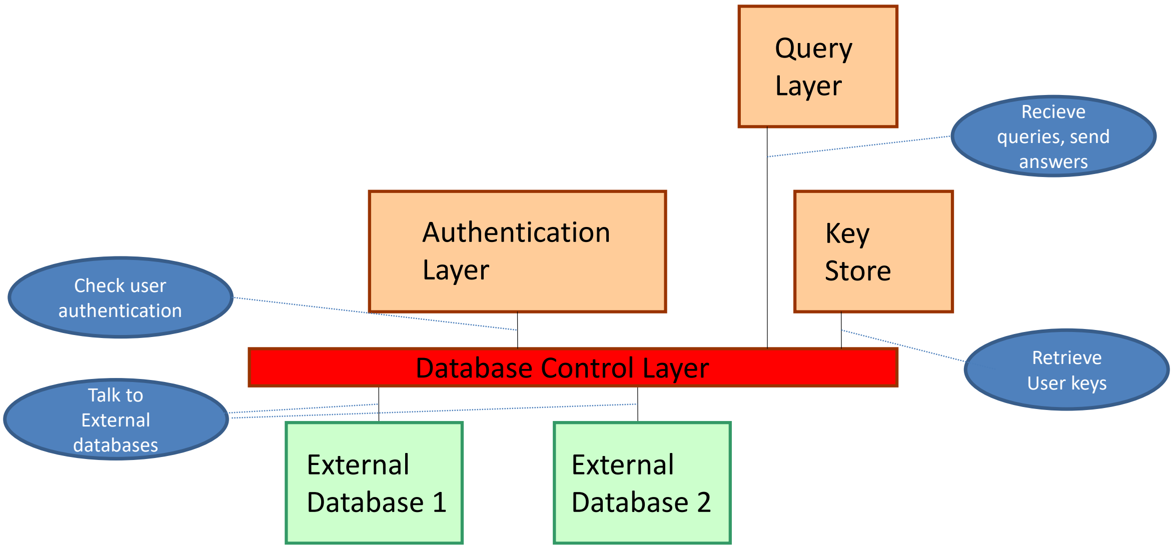


Figure 2 Example of the subsystem behavior and interaction (of the red subsystem)

Result: The Evaluator demonstrate that he understands the TOE design and that it identifies and describes all subsystems

[4] It is highly recommended that the Evaluator presents a model that is (closely related to the model) used by the EUM. The model presentation shall include references to the relevant sections of the Developer evidence.

5.2.2 The Alternative ADV Method for Subsystems

In the alternative ADV method for subsystems, all requirements for the subsystems are met by the implementation representation. As noted early in section 5 subsystems and their interfaces are sets of modules. Hence, if the modules are sufficiently described then by inference any subsystem from which they are derived are also sufficiently described. Therefore, no further Evaluator actions to those specified in section 5.3.2 are required at this point.

5.3 Modules

5.3.1 The Regular ADV Method for Modules

1. The Evaluator presents a module level model of the TOE (with some parts of the environment):
   - this model SHALL be sensible and useful[5] [6];
   - this model SHALL show how the subsystems are decomposed in modules;
   - this model SHALL clearly clarify whether modules are SFR-enforcing, SFR-supporting, or SFR-non-interfering.
2. The Evaluator takes a sample of modules and explains the purpose for each sampled module and its interaction with other modules. This explanation SHALL, where possible, make use of examples from the Developer evidence (e.g. diagrams).

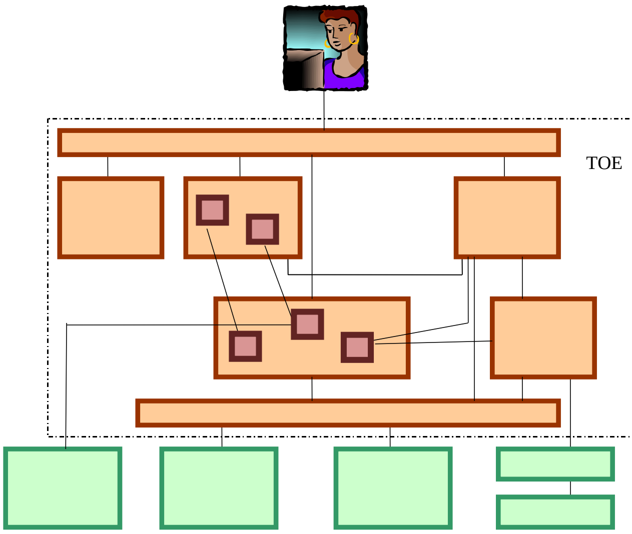


Figure 3 Example of the module level model

[5] That is, the modules SHOULD NOT correspond one-to-one with subsystems and they should provide a further level of detail than that provided for the subsystem; they SHOULD NOTjust be a division of the subsystem with no additional explanation of the design of the security functionality.

[6] It is highly recommended that the Evaluator presents a model that is (closely related to the model) used by the Developer. The model presentation shall include references to the relevant sections of the Developer evidence.

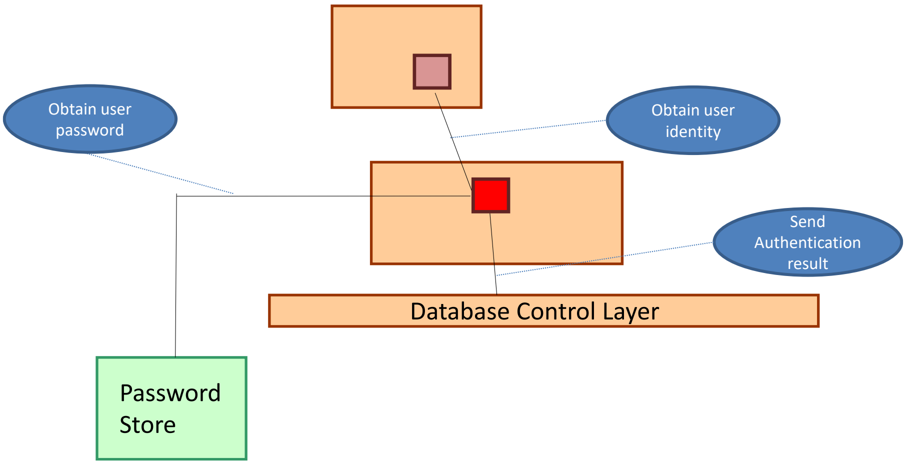


Figure 4 Example of the module behavior and interaction (of the red module)

Result: The Evaluator demonstrates that he understands the TOE design at module level and that all modules are identified and described

5.3.2 The Alternative ADV Method for Modules

In the alternative ADV method for modules, all requirements for the modules are met by the implementation representation.

As the implementation representation itself is considered to act as the documentation of the modules in the alternative ADV approach, all modules are implicitly categorised as SFR-enforcing. It is at the time of tracing SFRs to the implementation representation[7] (and hence also to modules and subsystems) that the Evaluator makes a distinction between that which is SFR-enforcing and SFR-supporting and that which is SFR-non-interfering. If the Evaluator traces an aspect of the implementation representation to SFRs, then it is considered to be SFR-enforcing or SFR-supporting, depending on the role the Evaluator determines it plays in achieving the SFR. The Evaluator can use their experience to quickly determine whether an aspect of the implementation representation does not play a role in achieving the SFR and hence is SFR-non-interfering.

Subsystems are sets of modules and the interfaces of those subsystems are the externally accessible interfaces of the modules. If the modules are sufficiently described, then also the subsystems are sufficiently described, and additional subsystem level descriptions are not required.

While the full mapping needs to be completed in order to ensure the necessary modules are identified for ADV_TDS, there is no need to present the full mapping of the SFRs to the modules. The presentation MUST provide an example of how this mapping is generated and, on demand, the Evaluator MUST be able to show how a specific SFR is implemented by the modules. There is no need to provide the full mapping.

Therefore, only limited Evaluator actions are required at this point.

The Evaluator presents the method used to identify the modules from the sets of implementation representation (e.g. source code or VHDL), providing examples of

[7] See section 5.4.2

the identified modules and rationale of how they fit the method for identifying modules (e.g. modules could be represented by source code classes, each source code function could represent a module).

Result: The Evaluator demonstrates that he understands the TOE design at module level and that all modules are identified and described.

5.4 Tracing SFRs to TSFI, Subsystems and Modules

5.4.1 The Regular ADV Method for Tracing

1. The Evaluator presents, for each SFR, how the TSFIs, subsystems (and modules) provide this SFR, using the TOE, diagrams, screenshots, submodules etc.
2. Where SFRs/TSFI interactions are complex (e.g. FMT_SMF applying to multiple administrator interfaces) this SHALL be split and clarified.
3. The Evaluator describes what the role is of the TSFIs, subsystems (and modules) in meeting these SFRs.

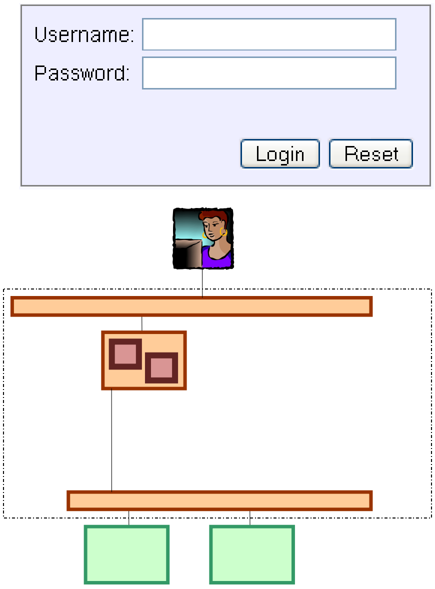


Figure 5 Example of relation between SFRs, TSFI, subsystems and modules

Result: The Evaluator demonstrates that he understands the TOE Design and FSP, and their completeness with regards to the SFRs

5.4.2 The Alternative ADV Method for Tracing

A mapping from SFRs to modules/subsystems is generated as a result of completing the ADV_TDS activities, as discussed in Section 5.3.2 above. Therefore, no addition mapping of SFRs to modules/subsystem is required here. However, the alternative ADV method still requires a mapping from the SFRs to the TSFI with references to the main points in the implementation representation as input.

It is important to observe that this information is extremely well suited for techniques such as pre-compiled evidence (i.e. cases where SFRs in Protection Profiles mandate compliance to an implementation standard so that SFR ~ TSFIs mappings are product independent). The reason is that product interfaces (TSFIs) are comparatively stable.

The Evaluator uses his experience with the TOE type to identify all security relevant part of the implementation representation from these high-level starting points using classical implementation review techniques like data flow analysis, tracing of call chains etc.

This way, the Evaluator ensures that all tracing requirements for the modules (and hence by inference, the subsystems) are met by the implementation representation without the need of explicit SFR-tracing information provided by the Developer.

1. The Evaluator maps each SFR to the relevant implementation representation items.
2. The Evaluator presents a few examples of this mapping
3. The Evaluator MUST be able to describe for each SFR how it is realised in the implementation representation.

Result: The Evaluator demonstrates that he understands the TOE design, and its completeness with regards to the SFRs

5.5 Security Architecture

This section applies to both the regular and the alternative ADV method.

The Evaluator presents the security architecture and explains:

- how the TOE maintains security domains;
- how the TOE initialises;
- how the TOE protects itself from tampering;
- how the TOE prevents bypass.

This presentation will be targeted towards the model developed in the previous sections (i.e. consider subsystems and modules if applicable) and explains how the implemented security mechanisms contribute to the security properties.

When applying the alternative ADV method, reference to standard architecture for that TOE type (e.g. within the GSMA Protection Profiles SGP.05 [11] or SGP.25 [12]) SHOULD be made and used as a basis of the explanation of the main security features implemented in the implementation representation to meet the ADV_ARC requirements.

Again, this is well suited to pre-compile evidence techniques as the high-level security architecture concepts (as considered in ADV_ARC) are comparatively stable and change only gradually over time.

Result: The Evaluator demonstrates that the security properties are described and that he understands how they are achieved by the TOE

6 Implementation Representation Sampling Rationale

This section consists of two cases:

1. ADV_IMP.1 is used in conjunction with the regular ADV method
2. ADV_IMP.1 is used in conjunction with the alternative ADV method

This is a small presentation that describes the subset of the TOE Implementation Representation that will be examined and why this is assumed to be representative for the complete set. The actual Evaluator work of ADV_IMP is handled in the TOE Implementation Representation presentation (see Chapter 9).

The Evaluator SHALL present:

- the selected sample of implementation representation;
- a justification for the selected sample of implementation representation including the considerations that were given in this selection process.

Result: The Evaluator demonstrates that he has chosen a proper set of Implementation Representation.

6.1 The Sampling Rationale for ADV_IMP.1 and The Alternative ADV Method

In case the alternative approach is used, the whole implementation representation is made available to the Evaluator because it is required to gain the required information about the modular (and hence subsystem) design of the TOE. Therefore, no sampling rationale is necessary in the alternative ADV method for the EM1 deliverables.

The Evaluator uses the implementation representation also to acquire the information about the modular design of the system. Consequently, the correspondence between the modular design inferred by the Evaluator and the implementation representation is implicit and no sampling rationale is needed.

There is nothing for the Evaluator to present in relation to EM1 deliverables.

Result: The GSMA CB implicitly approves the sampling strategy as the whole source code is used by the Evaluator in the ADV_TDS and ADV_IMP activities for the alternative ADV approach.

7 The ADV/AGD Reference Document

This document (not a presentation) is a list of references to the evidence, showing that certain ADV requirements are met that are hard to capture in a presentation. It consists of an ADV part and an AGD part.

The goal of the document is to show to the Certifier *that* the work was done, but not give much detail on *how* it was done.

The Certifier can perform spot checks if so desired. It is not intended that the Certifier repeat part of the ADV or AGD evaluation by completely checking everything.

7.1 The ADV-Part

1. The Evaluator SHALL ensure that the ADV/AGD Reference Document contains detailed references (for each TSFI):
   - to the evidence where the parameters for that TSFI are described;
   - to the evidence where the actions are described;
   - to the evidence where the error messages and exceptions are described.
   - (for the discussion of non-TSFI error messages as required in higher ADV_FSP component-levels the Evaluator can decide whether to present the results in the ADV/AGD Reference Document or in the TOE Implementation Representation Presentation)
2. The Evaluator SHALL make available the relevant ADV documentation for spot checks during the meeting.

NOTE: No example, as it is self-explanatory

Result: The Evaluator demonstrates that all TSFI are fully described.

7.2 The AGD Part

1. The Evaluator SHALL ensure that the ADV/AGD Reference Document contains detailed references:
   - to the list of user roles;
   - to the list of user-accessible functions and privileges to be controlled in a secure processing environment (OPE.1.1C);

- for each user role, how that user role is meant to use the available interfaces in a secure manner (OPE.1.2C);
- for each role, the functions, and interfaces available to that user role, plus parameters and values (OPE.1.3C);
- for each role, the security relevant events (OPE.1.4C);
- to the general description of modes of operation for the TOE, and how to maintain secure operation for each mode (OPE.1.5C);
- to the security measures needed to fulfil each SO for the environment (OPE.1.6C);
- to the acceptance steps (PRE.1.1C);
- to the installation and preparation steps (PRE.1.2C).

2. The Evaluator SHALL make available the relevant AGD documentation before the meeting.

NOTE: No example, as it is self-explanatory

Result: The Evaluator demonstrates that all AGD requirements are met.

7.2.1 GSMA Optimisation

The GSMA PRDs for technical implementation of remote provisioning, SGP.02 [8] and SGP.22 [15], describe the expected implementation of the remote provisioning feature and are considered to meet the AGD_PRE.1 and AGD_OPE.1 requirements.

8 The Configuration Item Identification Presentation

This is a small presentation of a single ALC item: the identification of configuration items (as required by ALC_CMC.2/3/4. The “Configuration Items” of interest are the identification means for all relevant parts / components of the TOE including their configuration like versioning information for all hardware and software components that constitute the TOE, and additional information like patch-levels, versions of configuration tables etc.

This is presented to allow the Certifier to track how configurations items change when the TOE is patched as a result of testing.

In the first evaluation meeting, the Evaluator MUST present for all Configuration Items listed in the ST (including the TOE and its guidance):

- What the identification (including version) of those Configuration Items is in the ST, and
- how would those identifications change if the Configuration Item changes (e.g. version number is increased, hash value changes, patch level is increased), and
- what method will the user and the Evaluator use to verify these identifications (e.g. commands to send to the TOE and responses, comparison of hash values, comparing document identifiers, and names). If these methods are different, both need to be clear and linked.

Even if no change to the Configuration Items is expected, it still MUST be clear how any changes would be visible from the identification.

The rest of ALC is handled in the ALC presentation (see section 12).

The Evaluator SHALL present the method used to uniquely identify the configuration items.

NOTE: No example, as it is self-explanatory

Result: The Evaluator demonstrates how configuration items are uniquely identified.

9 TOE Implementation Representation Presentation

This section consists of two cases:

3. ADV_IMP.1 is used in conjunction with the regular ADV method
4. ADV_IMP.1 is used in conjunction with the alternative ADV method

9.1 ADV_IMP.1 Is Used in Conjunction with the Regular ADV Method

The Evaluator SHALL present:

- Findings of implementation representation inspection, including the form of the implementation representation inspected.
- Any changes/additions to the (agreed) selected sample made as a result of the analysis. For example, where analysis of a selected portion of the implementation representation led to the inclusion of an additional area to clarify an ambiguity.

Result: The Evaluator demonstrates that the selected portions of the implementation representation are consistent with the design.

9.2 ADV_IMP.1 Used in Conjunction with The Alternative ADV Method

The Evaluator SHALL present:

- Findings of implementation representation inspection, including the form of the implementation representation inspected.
- How the sample selection of SFRs is implemented in the implementation representation

Result: The Evaluator demonstrates that the implementation representation meets all SFRs, and, that as the implementation representation equals the design:

- the implementation representation is consistent with the design
- the subsystems implement all SFRs
- the modules implement all SFRs

10 The ATE/AVA Test Plan Presentation

10.1 Approach (overview)

The approach will consist of the following phases:

1. The Evaluator will analyse the Developer testing and creates an overview test plan.

2. The Evaluator will present the Developer testing and the overview test plan to the Certifier. This will be done at the second evaluation meeting. The Evaluator will distinguish between:

   a) Tests done by the Developer which will be repeated by or witnessed by the Evaluator
   b) Tests done by the Developer which will not be repeated or witnessed
   c) Additional tests done by the Evaluator
   d) The rationale for choosing all the above

3. The Evaluator will analyse all the other evidence and produce a vulnerability analysis and penetration test plan based on this evidence.

10.2 Two Methods for Developer ATE

For the evaluation (and presentation) of Developer ATE, two methods exist:

1. The regular ATE method,
2. The alternative ATE method.

The alternative method for ATE is to be used in cases where the Developer has a mature test system that can be used to show (near-) completeness of Developer ATE testing. The regular ATE method is to be used in all other cases.

For a Licensed Laboratory to use the alternative ATE method, the GSMA CB MUST give permission. Therefore, the use of this method MUST be documented in the EWP.

With the alternative ATE method, the Developer is able to provide a Developer Testing Rationale: a demonstration of the (near) - completeness of testing by other means than explicit enumeration and mapping of tests to TSFI, subsystems and modules. This can include, but is not limited to:

- Tests suites that test against a given interface standard (e.g. the JavaCard standard)
- Tools that measure code coverage
- Tools that systematically generate tests from code or interface specifications

In this case, the Evaluator can analyse the Developer Testing Rationale to establish that ATE_COV and ATE_DPT have been met, supported by sampling to determine that the Developer Testing Rationale is correct.

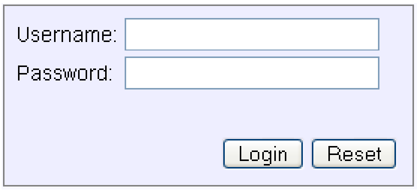
10.3 Coverage

10.3.1 Coverage Under the Regular ATE Method

The Evaluator SHALL present[8]:

- a systematic overview of which tests have been done by the Developer;
- how these tests cover the various TSFIs.

[8] This presentation may be integrated with the “Tracing SFRs to TSFI and Subsystems” presentation (Section 5.4).



TEST 1: Non-existent username
TEST 2: Incorrect password
TEST 3: Empty password
TEST 4: Correct password

Figure 6 Example of coverage

Result: The Evaluator demonstrates that all TSFI have been tested by the Developer.

10.3.2 Coverage Under the Alternative ATE Method

The Evaluator SHALL present:

- The Developer Testing Rationale on why all TSFIs are tested;
- How he sampled the Developer tests to determine that the Developer Testing Rationale was correct

Example of coverage:

"*The Developer uses the CodeComplete v4.18 tool to show that his tests have code coverage of 98.2%. The Developer explained that the remaining 1.8% of the code, either:*

- *does not exhibit behaviour visible at an external interface, or*
- *represents errors that do not normally occur*
- *The Evaluator sampled several functions from different places in the code and determined that these were tested by the test set of the Developer. The Evaluator also sampled:*
- *some code to verify that it was not visible at the external interfaces*
- *represented errors that do not normally occur*

and found this to be the case."

Result: The Evaluator demonstrates that all TSFI have been tested by the Developer.

10.3.2.1 GSMA Optimisation

The GSMA remote provisioning test suites SGP.11 [13], SGP.23 [14] and SGP.33-1 [25] are considered to meet the ATE_COV. 2, ATE_DPT.1, ATE_FUN.1, and ATE_IND.2 requirements for the remote provisioning functionality as defined in SGP.05 [11] and SGP.25 [12]. Any areas considered not to be covered by these test suites SHOULD be reported to the GSMA CB for it to report to the eSIM Group.

10.4 Depth

10.4.1 Depth Under the Regular ATE Method

The Evaluator SHALL present[9]:

- a systematic overview of which tests have been done by the Developer;
- how these tests cover the various subsystems, modules, or the implementation representation of the TSF (details depend on the ATE_DPT component level relevant of the evaluation)

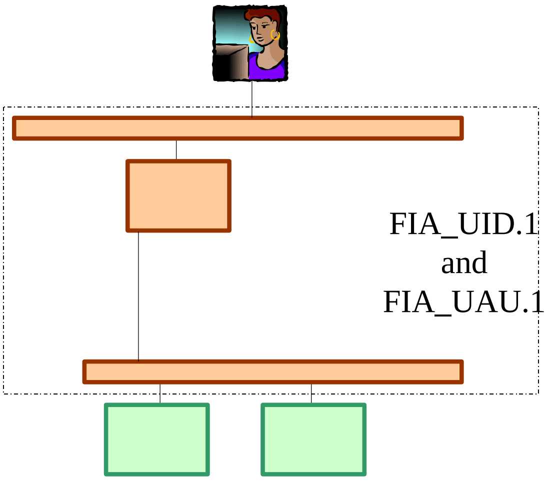


Figure 7 Example of depth

TEST A: Performing login retrieves correct password from password file

TEST B: Performing login correctly compares entered password with stored password

Result: The Evaluator demonstrates that all TSF subsystems have been tested by the Developer.

10.4.2 Depth Under the Alternative ATE Method

The Evaluator SHALL present:

- The Developer Testing Rationale on why all subsystems (and modules / the TSF implementation depending on the chosen ATE_DPT level) are tested;
- How he sampled the Developer tests to determine that the Developer Testing Rationale was correct

In many cases, the Developer Testing Rationale for subsystems (and for modules / for the implementation of the TSF) will be identical to or largely overlap the Developer Testing Rationale for TSFI. In that case, the presentation SHOULD be combined.

Result: The Evaluator demonstrates that all subsystems (and modules / the TSF implementation) have been tested by the Developer.

[9] This presentation may be integrated with the “Tracing SFRs to TSFI and Subsystems” presentation (Section 5.4).

10.5 Developer Test Plan

The Evaluator SHALL present:

- a sample of the test plan to show general style and how it meets the required criteria.

Result: The Evaluator demonstrates that the test documentation contains all necessary information. This is also demonstrated through the ability of the Evaluator to repeat the selected sample of Developer test cases.

10.6 Evaluator ATE Test Plan

The Evaluator SHALL present[10]:

- the selection of Developer tests that will be repeated;
- the additional Evaluator tests.

Result: The Evaluator demonstrates that he has chosen a proper set of ATE tests

The Certifier is expected to comment on the two sets of tests during the second evaluation meeting, and the Evaluator and Certifier will come to an agreed ATE test plan.

If so desired, the Certifier can indicate which tests he intends to witness.

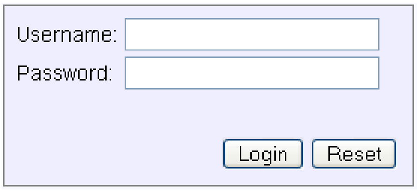
10.7 Evaluator AVA Test Plan

The Evaluator SHALL present[11]:

- the results of the public domain vulnerability search;
- the focus of the independent vulnerability analysis (if applicable);
- the results of the independent vulnerability analysis (supported by an additional Implementation Representation review report, see also Section 9);
- the resulting AVA tests.

Note that the Evaluator SHOULD include argumentation in his presentation allowing the Certifier to judge the completeness as required by the assurance requirements. Overview tables and consistent naming can support this significantly.

Example:



[10] This presentation may be integrated with the “Tracing SFRs to TSFI and Subsystems” presentation (Section 5.4).

[11] This presentation may be integrated with the “Tracing SFRs to TSFI and Subsystems” presentation (Section 5.4).

PENTEST 1: Standard accounts root/root, root/toor, anonymous/guest, guest/guest

PENTEST-2: Extremely long password

PENTEST-3: Password containing ^C, ^H and/or ^Z

Result: The Evaluator demonstrates that he has chosen a proper set of AVA tests

The Certifier is expected to comment on the search, analysis, and AVA test plan during the second evaluation meeting, and the Evaluator and Certifier will come to an agreed AVA test plan.

If so desired, the Certifier can indicate which tests he intends to witness.

11 The ATE/AVA Test Descriptions

As the presentations for the ATE and AVA test plan will only present a very general test goal, the Evaluator SHALL also deliver an ATE/AVA Test description (this is a document).

- The ATE/AVA Test descriptions SHALL contain:
- all tests of the ATE and AVA Test Plan Presentation
- for each test, the objective, test method and expected result

Example:

Test 10: MD5 Signatures

The actual use of the md5 signature will be tested: tap NTP traffic and determine it uses the MD5 authentication properly.

- Objective: Establish that the NTP service is using password authentication so that an attacker cannot inject a false time into the TOE.
- Method:

  i. record an NTP timestamp from the server
  ii. Replay the NTP reply one hour later
  iii. Check the time on the EMS server

- ExpRes: The time on the EMS server is not affected by the false reply

Result: The Evaluator demonstrates that he knows how to execute the AVA and ATE tests

The Certifier can sample this Test description for sufficiency. It is not intended that he completely verifies this document.

12 The ALC Presentation

The overall goal of ALC is for the Evaluator to understand the processes and procedures applied in the TOE development and manufacturing lifecycle and to then gain confidence that the processes and procedures are applied as documented. This is a two-stage process:

1. Review the documentation provided by the Developer to understand the processes/procedures and to develop a plan of what is to be verified and how to verify the application.
2. Gain confidence of the application of the processes and procedures. Confidence MAY be obtained through site audit(s) or through evidence of their application (e.g. completed review documents, logs of access control mechanisms) provided by the Developer.

The Evaluator SHALL present:

- An overview of each ALC assurance family:
    - A summary of how the Developer meets this family;
    - A summary of the evidence that the Developer has provided.
- A checklist/plan of how to verify application of the processes and procedures.

The following items SHALL specifically be addressed:

- The life-cycle model, including the site(s) where development and production takes place
- Physical, procedural, personnel and other security measures and why these measures are appropriate and sufficient for the TOE

Result: The Evaluator demonstrates that the Developer meets the ALC Criteria and that the Evaluator has plan of how to verify the application of these measures.

12.1 Site Visits Under This Procedure

For ALC_DVS.2, only integrity is mandatory. The Developer has the possibility to not claim the confidentiality. This MUST be documented, and the Evaluator will address the consequence of no confidentiality in the vulnerability assessment.

In addition, the following security site certifications SHOULD be recognised:

1. Site certification according to CCDB-2007-11-001; Site Certification, Version 1.0, October 2007 [18] issued by SOG-IS Certification Bodies under the technical domain smart card and similar devices www.sogis.eu
2. EMVCo Security Guidelines – Development and Production Site Audit Guidelines; 1.1 – May 2015 [19]

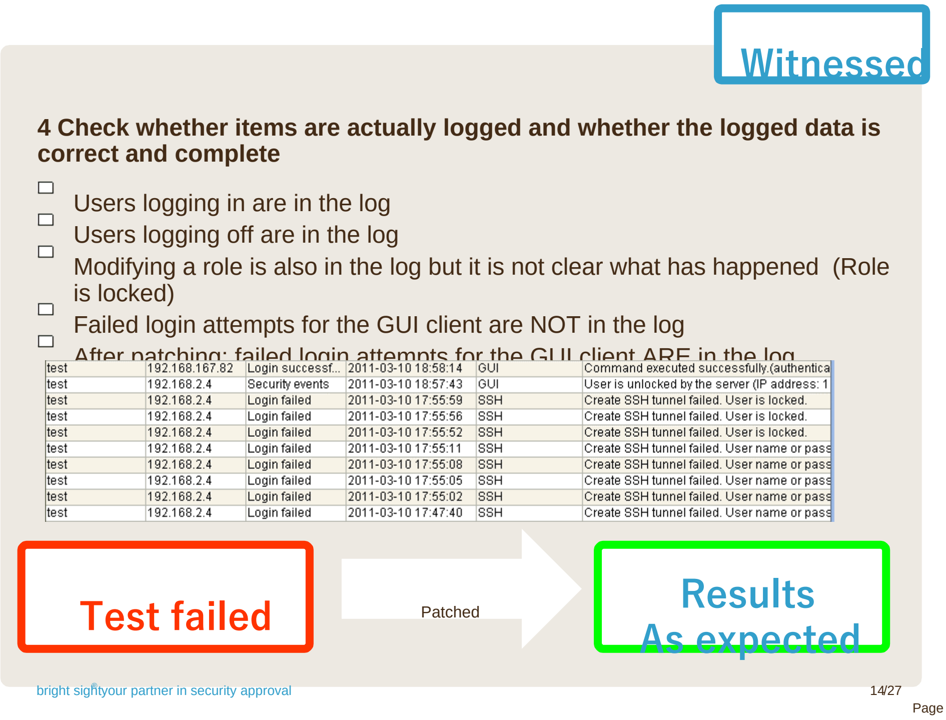
Evidence of site certification can be done by the Developer to the Evaluator and the GSMA CB by providing respectively for 1) the STAR (Site Technical Audit Report) or for 2) the SAR (Shared Audit Report) of the site audited.

13 The ATE/AVA Test Results

The Evaluator SHALL present[12]:

- the test results of all tests in the ATE/AVA Test plan;
- if any tests failed, how these failures were handled by the Developer and the test results of the subsequent Evaluator retest.

Example of Test:



Witnessed

4 Check whether items are actually logged and whether the logged data is correct and complete

□ Users logging in are in the log

□ Users logging off are in the log

□ Modifying a role is also in the log but it is not clear what has happened (Role is locked)

□ Failed login attempts for the GUI client are NOT in the log

□ After patching: failed login attempts for the GUI client ARE in the log

test	192.168.167.82	Login successf...	2011-03-10 18:58:14	GUI	Command executed successfully.(authentica
test	192.168.2.4	Security events	2011-03-10 18:57:43	GUI	User is unlocked by the server (IP address: 1
test	192.168.2.4	Login failed	2011-03-10 17:55:59	SSH	Create SSH tunnel failed. User is locked.
test	192.168.2.4	Login failed	2011-03-10 17:55:56	SSH	Create SSH tunnel failed. User is locked.
test	192.168.2.4	Login failed	2011-03-10 17:55:52	SSH	Create SSH tunnel failed. User is locked.
test	192.168.2.4	Login failed	2011-03-10 17:55:11	SSH	Create SSH tunnel failed. User name or pass
test	192.168.2.4	Login failed	2011-03-10 17:55:08	SSH	Create SSH tunnel failed. User name or pass
test	192.168.2.4	Login failed	2011-03-10 17:55:05	SSH	Create SSH tunnel failed. User name or pass
test	192.168.2.4	Login failed	2011-03-10 17:55:02	SSH	Create SSH tunnel failed. User name or pass
test	192.168.2.4	Login failed	2011-03-10 17:47:40	SSH	Create SSH tunnel failed. User name or pass

Test failed

Patched

Results As expected

bright sightyour partner in security approval

14/27

Page

Result: The Evaluator demonstrates that the TOE has passed ATE and AVA tests.

14 The ALC Results

The Evaluator SHALL present the results of the verification that the lifecycle processes and procedures are applied.

Result: The Evaluator demonstrates that he has checked whether the Developer applies the documented procedures.

[12] It is not intended that this consists of a set of “Pass.” Detailed descriptions and screendumps are to be provided where appropriate

Annex A Example Mapping of Evaluator Actions

The table below provides an example of how the Evaluator might report the mapping of CC Evaluator actions (to a level of content and presentation elements) for an EAL4+ ALC_DVS.2 + AVA_VAN.5 evaluation to the evaluation reports. The Evaluator will populate such a table with the reference to the report(s), including details of the slide (in the case of a presentation report) or section number (in the case of a document) in which the action is reported.

CC Family	Element	*Report reference, Slide# or section #*
ADV_ARC1.1E	1.1C	
	1.2C	
	1.3C	
	1.4C	
	1.5C	
ADV_FSP.4.1E	4.1C	
	4.2C	
	4.3C	
	4.4C	
	4.5C	
	4.6C	
ADV_FSP.4.2E		
ADV_IMP.1.1E	1.1C	
	1.2C	
	1.3C	
ADV_TDS.3.1E	3.1C	
	3.2C	
	3.3C	
	3.4C	
	3.5C	
	3.6C	
	3.7C	
	3.8C	
	3.9C	
	3.10C	
ADV_TDS.3.2E		
ADV_COMP1.1E	1.1C	
AGD_OPE.1.1E	1.1C	
	1.2C	
	1.3C	
	1.4C	

CC Family	Element	*Report reference, Slide# or section #*
	1.5C	
	1.6C	
	1.7C	
AGD_PRE.1.1E	1.1C	
	1.2C	
AGD_PRE.1.2E		
ALC_CMC.4.1E	4.1C	
	4.2C	
	4.3C	
	4.4C	
	4.5C	
	4.6C	
	4.7C	
	4.8C	
	4.9C	
	4.10C	
ALC_CMS.4.1E	4.1C	
	4.2C	
	4.3C	
ALC_DEL.1.1E	1.1C	
ALC_DEL.1.2D (implied Evaluator action)		
ALC_DVS.2.1E	2.1C	
	2.2C	
ALC_LCD.1.1E	1.1C	
	1.2C	
ALC_TAT.1.1E	1.1C	
	1.2C	
	1.3C	
ALC_COMP1.1E	1.1C	
ALC_COMP1.2E		
ATE_COV.2.1E	2.1C	
	2.2C	
ATE_DPT.1.1E	1.1C	
	1.2C	
ATE_FUN.1.1E	1.1C	
	1.2C	
	1.3C	
	1.4C	

CC Family	Element	*Report reference, Slide# or section #*
ATE_IND.2.1E	2.1C	
	2.2C	
ATE_IND.2.2E		
ATE_IND.2.3E		
ATE_COMP1.1E	1.1C	
AVA_VAN.5.1E	5.1C	
AVA_VAN.5.2E		
AVA_VAN.5.3E		
AVA_VAN.5.4E		
AVA_COMP1.1E	1.1C	

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0		Initial Document	ISAG	Gloria Trujillo, GSMA
V1.1	05 July 2023	CR0034R01 – Introduce ST Template for Consumer eUICC CR0037R01 - Fix reference to the ST template for Consumer eUICC CR0038R01 - Clarification about composite activities	ISAG	Gloria Trujillo, GSMA
2.0	19 December 2023	CR0039R02 - Add latest versions of SGP.05 and SGP.25 to the scope	ISAG	Gloria Trujillo, GSMA

B.2 Other Information

Type	Description
Document Owner	eSIM
Editor / Company	GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You MAY notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.