Netherlands Scheme for Certification in the Area of IT Security (NSCIB)

Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB)

NSCIB Scheme Procedure 6

Alternative Evaluator Reporting

Procedure	6
Report title	Alternative Evaluator Reporting
Date of issue	May 20, 2014
Version	1.2
Filename	NSP_6_Alternative_Evaluator_Reporting_v1.2_draft.doc

TÜVRheinland®
Precisely Right.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Document history

Version	Date	Comment
1.0	June 1, 2012	1st release for EAL3
1.1	July 1, 2013	Draft with EAL4 extensions
1.2	May 20, 2014	2nd Draft after internal comments (items marked yellow are still under discussion)

References

[CC] Common Criteria for IT Security Evaluation, Part 1,2 and 3, v3.1r4, September 2012
[CCRA] Arrangement on the Recognition of CC Certificates in the field of IT Security, May 2000
[CEM] Common Methodology for IT Security Evaluation, v3.1r4, September 2012
[CoDE] Collection of Developer Evidence, v1.5, JIL, January 2012 / CCDB-2012-04-005
[SOG3] SOGIS MRA of IT Security Evaluation Certificates, v3.0, January 2010

Glossary of terms and abbreviations

This list does not contain terms already defined by the [CC] or [CEM].

NSCIB	Netherlands Scheme for Certification in the Area of IT Security (Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging)
NSP	NSCIB Scheme Procedure

Table of contents

1 Introduction

The current procedures in the NSCIB are oriented towards:

1. "The developer shall provide developer documentation that completely and consistently complies with every aspect of every relevant work unit of the CEM, and does not contain any ambiguity whatsoever"
2. "The lab shall document for each work unit a complete rationale and a summary of the evidence so that the certifier can ascertain that each work unit has been completely and correctly performed and each piece of CEM guidance has completely and correctly been applied."

This is a significant amount of work for the developer who has to learn in depth about the CC (or pay for a consultant to completely rewrite all documentation), for the lab, which has to write very extensive reports, and for the CB who then has to check it all. Often there is more than one feedback cycle (caused either by lab or CB), causing more work and delay.

In the international area, point 1 has been acknowledged, and as a reaction, the document "Collection of Evidence" [CoDE] was developed to support the evaluator extracting information from developer documentation and interviews with the developer rather than having the developer/consultant rewrite the documentation.

This NSCIB Scheme Procedure (NSP) aims at improving point 2 and presents an alternate method of reporting from evaluator to CB. The goal is for the evaluator to:

- continue to perform all activities mandated by [CC], [CEM] and NSCIB Scheme Procedures;
- spend less time on reporting these results, by reporting in a different style;
- spend more time on testing and especially penetration testing.

The alternative and more efficient approach is generally described in Chapter 2 with references to the Chapters 4-14 which describe the more detailed procedures. This approach may in the future be the default method of reporting from evaluator to CB and replace the standard process with Intermediate Reports.

Appendix A analyses the actual reporting requirements of the [CCRA], SOGIS-MRA [SOG3] and CEM. From this Appendix follows that this NSP complies with all of these requirements.

In appendix B a cross-reference is given between the CC requirements and the corresponding sections of this procedure.

2 Process overview

The general process consists of the following 6 steps:

1. Application
2. Kick-off meeting (Preparation Phase: same as standard process)

---

3. ST Evaluation
4. First Evaluation Meeting
5. Second Evaluation Meeting (Monitoring Phase: new for this process)
6. Third Evaluation Meeting
7. Final Evaluation Reporting

---

8. Certification Phase (Certification Phase: same as standard process)

These steps are explained below.

2.1 Application

The developer submits an application form and draft ST to TÜV Rheinland Nederland and in copy to the scheme technical manager. After approval of the application, the lab provides a draft workplan to the assigned certifier. This step is identical to the standard scheme procedure.

2.2 Kick-off meeting (optional)

If the certifier deems this necessary, the certifier organizes a kickoff meeting between developer, laboratory and certifier. This step is identical to the standard scheme procedure.

2.3 ST Evaluation

The developer provides a more-or-less final ST. The lab adds the accompanying Intermediate Report (IR) with the ASE evaluation results to the certifier. After one or more feedback loops, the ST is provisionally[1] approved. Also this step is identical to the standard scheme procedure.

2.4 First Evaluation Meeting

2.4.1 First Evaluation Meeting Procedure

The laboratory organizes a meeting with the certifier at a mutually agreed location. The developer is encouraged, but not required, to attend the meeting. Other parties are only allowed to attend if developer, lab and certifier agree.
Five working days before the meeting the laboratory will send all First Evaluation Meeting Deliverables (see 2.4.2) to the certifiers.

In this meeting the First Evaluation Meeting Deliverables are presented by the evaluator, according to the following rules:

- Not all First Evaluation Meeting Deliverables actually 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 of 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] There is always room for later changes due to developer changes, new information coming to light or new insights at lab, developer or CB. Note that this term “provisionally approved” is used throughout this document.

1. All First Evaluation Meeting Deliverables were either correct or successfully amended/annotated during the meeting. In this case all of 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 laboratory will take notes of all issues raised by the certifier and the action that took place or was agreed (i.e. amended/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.

2.4.2 First Evaluation Meeting Deliverables

The First Evaluation Meeting Deliverables consist of the following:

- Updated ST and IR_ASE according to certifier comments;
- The ADV Presentation (see section 4);
- The Implementation Representation Sampling rationale (see section 5);
- The ADV/AGD Reference Document (see section 6) and all guidance documents that this document refers to;
- The Configuration Item Identification Presentation (see section 7);
- The Consultancy/Evaluation Improvement Presentation (see section 13);
- Any other observations that were found before this meeting and are deemed relevant.

2.5 Second Evaluation Meeting

2.5.1 Second Evaluation Meeting Procedure

The Second Evaluation Meeting Procedure is identical to the First Evaluation Meeting Procedure, with the exceptions that it concerns different deliverables (see 2.5.2).

For some evaluations, the First and Second Evaluation Meetings may be combined into one (1) meeting where all the required deliverables will be presented in one go. This will be decided at the kick-off meeting and depends on the complexity of the product in combination with the required level of assurance.

2.5.2 Second Evaluation Meeting Deliverables

The Second Evaluation Meeting Deliverables consist of the following:

- Any First Evaluation Meeting Deliverables that were rescheduled to this meeting;
- The Implementation Representation Presentation (see section 8);
- The ATE/AVA Testplan Presentation (see section 9);
- The ATE/AVA Test descriptions (see section 10);
- The ALC Presentation, including ALC verification plan (see section 11);
- Any other observations that were found before this meeting and are deemed relevant.

2.6 Third Evaluation Meeting

2.6.1 Third Evaluation Meeting Procedure

This procedure is identical to the First and Second Evaluation Meeting Procedure, with the following exceptions:

- It concerns different deliverables (see 2.6.2)
- It cannot end with outcome #3 (see 2.4.1) as there is no meeting to reschedule to.

2.6.2 Third Evaluation Meeting Deliverables

The Third Evaluation Meeting Deliverables consist of the following:

- Any Second Evaluation Meeting Deliverables that were rescheduled to this meeting;
- The final ST;
- The ATE/AVA test results (see section 12);
- The ALC Results Presentation (see section 13);
- Any further observations that were found before this meeting and are deemed relevant.

2.7 Final Evaluation Reporting

The laboratory delivers its Evaluation Technical Report (ETR) and, if this is found correct; the certifier formally approves the ETR and all provisionally approved items.

2.8 Certification Phase

The certifier generates the Certification Report and the Certificate. This step is identical to the standard scheme procedure.

3 Notation

In the following chapters, the following notation is used:

CC assurance requirement elements are always encased in a yellow box and are grouped for EAL2, EAL3 and EAL4. For higher or lower assurance levels or augmentations, the certification body will provide additional guidance.

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

These boxes always occur in pairs: the actions in the green box are those actions that this procedure defines[2] as sufficient reporting[3] to meet the requirement elements in the yellow box.

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

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

[2] This reporting is not "complete" in the sense that it reports every CEM detail at the level of a work unit. However, in the NSCIB, it is sufficient to meet the reporting requirements indicated in the green box (also see the next footnote).
[3] Note that this does *not* allow the evaluator not to use the CC or CEM: this is only intended for what needs to be reported. Any further recording of results is left to the lab and to the ISO-17025 standard.

4 The ADV Presentation

The overall goal of 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 done all the work). 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. Rather it should reflect the evaluators' summary of that material with appropriate references.

The ADV presentation will present the following elements:

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

4.1 The TOE and the TSFI

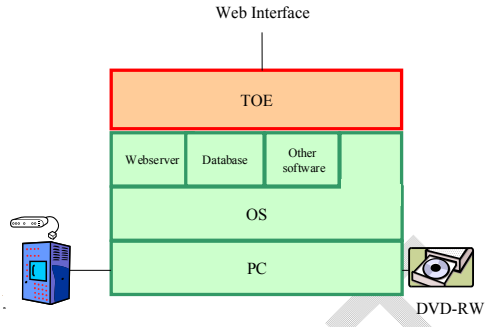
@EAL2:
ADV_FSP.2.1C The functional specification shall completely represent the TSF.
ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@EAL3:
ADV_FSP.3.1C The functional specification shall completely represent the TSF.
ADV_FSP.3.2C The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@EAL4:
ADV_FSP.4.1C The functional specification shall completely represent the TSF.
ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

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 (also note NSI#7 for a detailed definition of 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.[4]

Result: The evaluator has demonstrated to the certifier that all interfaces and TSFI have been identified.

[4] See also NSCIB Scheme Interpretation #6: 'TSFI definition'.

4.2 Subsystems

@EAL2:
ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.1.2C The design shall identify all subsystems of the TSF.
ADV_TDS.1.3C The design shall describe the behaviour of each SFR-supporting or SFR non-interfering TSF subsystem in sufficient detail to determine that it is not SFR enforcing.
ADV_TDS.1.4C The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems.
ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.
ADV_TDS.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.1.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

@EAL3:
ADV_TDS.2.1C The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.2.2C The design shall identify all subsystems of the TSF.
ADV_TDS.2.3C **The design shall describe the behaviour of each SFR non-interfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.**
ADV_TDS.2.4C The design shall **describe** the SFR-enforcing behaviour of the SFR-enforcing subsystems.
ADV_TDS.2.5C The design shall summarise the **SFR-supporting and SFR-non-interfering** behaviour of the SFR-enforcing subsystems.
ADV_TDS.2.6C The design shall summarise the behaviour of the **SFR-supporting** subsystems.
ADV_TDS.2.7C **The design shall provide a description of the interactions among all subsystems of the TSF.**
ADV_TDS.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.2.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

@EAL4:
ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.3.3C The design shall identify all subsystems of the TSF.
ADV_TDS.3.4C The design shall **provide a description** of **each subsystem of** the **TSF.**
ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.
ADV_TDS.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.3.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

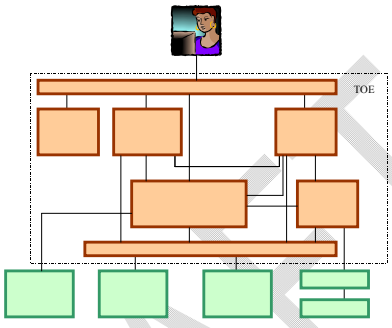
1. The evaluator presents a subsystem level model of the TOE (possibly with some parts of the environment):
   - this model shall be sensible and useful[5] [6];

[5] The current CC allows and some schemes advocate the use of "stupid" designs for EAL2, which have e.g. one TSFI per SFR and one subsystem per TSFI. These add nothing to understanding.

- 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).

Example of subsystems:



Result: The evaluator has demonstrated to the certifier that he has a basic understanding of the TDS.

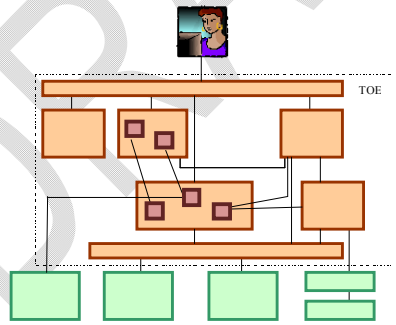
[6] It is highly recommended that the evaluator presents a model that is (closely related to the model) used by the developer. The model presentation shall include references to the relevant sections of the developer evidence.

4.3 Modules

@EAL4:
ADV_TDS.3.2C The design shall describe the TSF in terms of modules.
ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.
ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.
ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.
ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.
ADV_TDS.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.3.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

1. The evaluator presents a module level model of the TOE (possibly with some parts of the environment):
   - this model shall be sensible and useful[7] [8];
   - 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 explains the purpose of each module and its interaction with other modules. This explanation shall make use of examples from the developer evidence (e.g. diagrams).

Example of modules:



Result: The evaluator has demonstrated to the certifier that he has a detailed understanding of the TDS.

[7] 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 not just be a division of the subsystem with no additional explanation of the design of the security functionality.
[8] 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.

4.4 Tracing SFRs to TSFI, Subsystems and Modules

@EAL2:
ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.2.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

@EAL3:
ADV_FSP.3.7C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.3.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

@EAL4:
ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.4.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

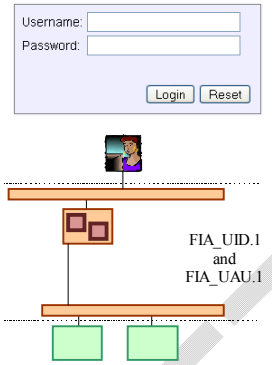
@EAL2:
ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.
ADV_TDS.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.1.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

@EAL3:
ADV_TDS.2.8C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.
ADV_TDS.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.2.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

@EAL4:
ADV_TDS.3.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.
ADV_TDS.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.3.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

1. The evaluator presents, for each SFR, how the TSFIs, subsystems (and modules) provide this SFR, using the TOE, diagrams, screenshots, submodels 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.

Example of relation between SFRs, TSFI, subsystems and modules



Result: The evaluator has demonstrated to the CB that he has an in-depth understanding of the TDS and FSP, and their completeness wrt the SFRs

4.5 Security Architecture

@EAL2-7:
ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.
ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.
ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.
ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.
ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.
ADV_ARC.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

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.

No example as this is similar to "normal" ARC.

Result: The evaluator demonstrates to the CB that he understands how the TOE achieves the ARC properties.

5 Implementation Representation Sampling Rationale

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 entire set. The actual evaluator work of ADV_IMP is handled in the TOE Implementation Representation presentation (see section 8).

@EAL4:
ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.
ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.
ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.
ADV_IMP.1.1E The evaluator *shall confirm* that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

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 to the CB that he has chosen a proper set of Implementation Representation.

6 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.

6.1 The ADV-part

@EAL2:
ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.
ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.
ADV_FSP.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@EAL3:
ADV_FSP.3.3C The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.3.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.
ADV_FSP.3.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from **SFR-enforcing actions and exceptions** associated with **invocation of** the **TSFI.**
ADV_FSP.3.6C **The functional specification shall summarise the SFR-supporting and SFR-non-interfering actions associated with each TSFI.**
ADV_FSP.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@EAL4:
ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.4.4C The functional specification shall **describe all** actions associated with each TSFI.
ADV_FSP.4.5C **The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.**
ADV_FSP.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

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.
2. The evaluator shall make available the relevant ADV documentation for spot checks during the meeting.

No example, as it is self-explanatory

Result: The evaluator gives evidence to the CB with the supplemental report that all TSFI are fully described.

6.2 The AGD part

@All EAL:
AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.
AGD_OPE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@All EAL:
AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
AGD_PRE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

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.

No example, as it is self-explanatory

Result: The evaluator gives evidence to the CB with the supplemental report that all AGD requirements are met.

7 The Configuration Item Identification Presentation

This is a relatively small presentation of a single ALC item: the identification of configuration items. This is presented to allow the certifier to track how configurations items change when the TOE is patched as a result of testing. The remainder of ALC is handled in the ALC presentation (see section 11).

@EAL2:
ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

@EAL3:
ALC_CMC.3.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

@EAL4:
ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

The evaluator shall present the method used to uniquely identify the configuration items.

No example, as it is self-explanatory

Result: The certifier understands how configuration items are uniquely identified.

8 TOE Implementation Representation Presentation

@EAL4:
ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.
ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.
ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.
ADV_IMP.1.1E The evaluator *shall confirm* that for the selected sample of the implementation representation the information provided meets all requirements for content and presentation of evidence.

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 to the certifier he has confirmed the selected portions of the implementation representation are consistent with the design.

9 The ATE/AVA Testplan Presentation

9.1 Approach (overview)

The approach will consist of the following phases:

1. The evaluator will analyse the developer testing and creates an overview testplan.
2. The evaluator will present the developer testing and the overview testplan 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 of the above
3. The evaluator will analyse all the other evidence and come up with a vulnerability analysis and pentest plan based on this evidence.

9.2 Coverage

@EAL2:
ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@EAL3-5:
ATE_COV.2.1C The **analysis** of the test coverage shall **demonstrate** the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.2.2C **The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.**
ATE_COV.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

The evaluator shall present[9]:
- a systematic overview of which tests have been done by the developer;
- how these tests cover the various TSFIs.

Example of coverage

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

Result: The evaluator demonstrates to the CB that all TSFI have been tested by the developer.

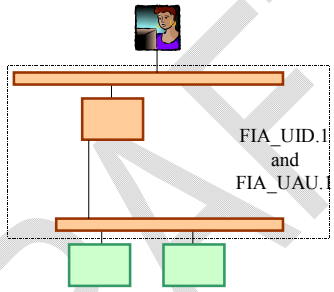
[9] This presentation may be integrated with the "Tracing SFRs to TSFI and Subsystems" presentation (Section 4.4).

9.3 Depth

@EAL3-4:
ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.
ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.
ATE_DPT.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

The evaluator shall present[10]:
- a systematic overview of which tests have been done by the developer;
- how these tests cover the various subsystems.

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 to the CB that all TSF subsystems have been tested by the developer.

[10] This presentation may be integrated with the "Tracing SFRs to TSFI and Subsystems" presentation (Section 4.4).

9.4 Developer Testplan

@EAL2-5:
ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

The evaluator shall present:
- a sample of the testplan to show general style.

Result: The evaluator demonstrates to the CB 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.

9.5 Evaluator ATE Test Plan

The planning part of:
@EAL2-6:
ATE_IND.2.2E The evaluator *shall execute* a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3E The evaluator *shall test* a subset of the TSF to confirm that the TSF operates as specified.

The evaluator shall present[11]:
- the selection of tests that will be repeated;
- the additional tests.

Result: The evaluator demonstrates to the CB 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 testplan.
If so desired, the certifier can indicate which tests he intends to witness.

[11] This presentation may be integrated with the "Tracing SFRs to TSFI and Subsystems" presentation (Section 4.4).

9.6 Evaluator AVA Test Plan

@EAL2-3:
AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.
The planning part of:
AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

@EAL4:
AVA_VAN.3.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.3.3E The evaluator shall perform an independent, **focused** vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description **and implementation representation** to identify potential vulnerabilities in the TOE.
The planning part of:
AVA_VAN.3.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing **Enhanced-Basic** attack potential.

The evaluator shall present[12]:
- the results of the public domain vulnerability search;
- the focus of the independent vulnerability analysis (if applicable);
- the results of the independent vulnerability analysis (possibly supported by an additional Implementation Representation review report, see also section 8);
- 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:

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 to the CB that he has chosen a proper set of AVA tests

The certifier is expected to comment on the search, analysis and AVA testplan during the second evaluation meeting, and the evaluator and certifier will come to an agreed AVA testplan.
If so desired, the certifier can indicate which tests he intends to witness.

[12] This presentation may be integrated with the "Tracing SFRs to TSFI and Subsystems" presentation (Section 4.4).

10 The ATE/AVA Test descriptions

As the presentations for the ATE and AVA testplan will only present a very general test goal, the evaluator shall also deliver an ATE/AVA Test descriptions (this is a document).

The ATE/AVA Test descriptions shall contain:
- all tests of the ATE and AVA Testplan Presentation
- for each tests, 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:
  1. record an NTP timestamp from the server
  2. Replay the ntp reply one hour later
  3. 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 to the certifier 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.

11 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.

@EAL3-6:
ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.
ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.
ALC_LCD.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@EAL3-5:
ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
The planning part of:
ALC_DVS.1.2E The evaluator *shall confirm* that the security measures are being applied.

@EAL2-7:
ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
ALC_DEL.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
The planning part of:
(implied) ALC_DEL.1-2 The evaluator *shall examine* aspects of the delivery process to determine that the delivery procedures are used.

@EAL2:
ALC_CMC.2.1C The TOE shall be labelled with its unique reference.
ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.
ALC_CMC.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@EAL3:
ALC_CMC.3.1C The TOE shall be labelled with its unique reference.
ALC_CMC.3.3C The CM system shall uniquely identify all configuration items.
ALC_CMC.3.4C **The CM system shall provide measures such that only authorised changes are made to the configuration items.**
ALC_CMC.3.5C **The CM documentation shall include a CM plan.**
ALC_CMC.3.6C **The CM plan shall describe how the CM system is used for the development of the TOE.**
ALC_CMC.3.7C **The evidence shall demonstrate that all configuration items are being maintained under the CM system.**
ALC_CMC.3.8C **The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.**
ALC_CMC.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@EAL4:

ALC_CMC.4.1C The TOE shall be labelled with its unique reference.
ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.
ALC_CMC.4.4C The CM system shall provide **automated** measures such that only authorised changes are made to the configuration items.
ALC_CMC.4.5C **The CM system shall support the production of the TOE by automated means.**
ALC_CMC.4.6C The CM documentation shall include a CM plan.
ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.4.8C **The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.**
ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.
ALC_CMC.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@EAL2:
ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs and the parts that comprise the TOE.
ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.
ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@EAL3:
ALC_CMS.3.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; **and the implementation representation.**
ALC_CMS.3.2C The configuration list shall uniquely identify the configuration items.
ALC_CMS.3.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@EAL4:
ALC_CMS.3.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; **and security flaw reports and resolution status.**
ALC_CMS.3.2C The configuration list shall uniquely identify the configuration items.
ALC_CMS.3.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

@EAL4:
ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.
ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.
ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.
ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

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 has demonstrated that he has checked whether the developer meets the ALC Criteria and has presented a plan of how to verify the application of these measures.

11.1 Site Visits under this NSP

It is the intention that under this NSP the use of site visits will be limited as far as possible with NO site visits done by default for evaluations at EAL3 or below. However, this does not mean that no evidence of compliance with ALC should be gathered by the evaluator: the evaluator should obtain evidence from the developer that he indeed follows the described procedure: screenshots of CM systems, photographs of physical security measures etc. Should the developer provide insufficient or confusing evidence, the evaluator and/or certifier may judge that a site visit is needed after all.

12 The ATE/AVA Test Results

@All EAL:
AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

@EAL2-6:
ATE_IND.2.1C The TOE shall be suitable for testing.
ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
The execution part of:
ATE_IND.2.2E The evaluator *shall execute* a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3E The evaluator *shall test* a subset of the TSF to confirm that the TSF operates as specified.

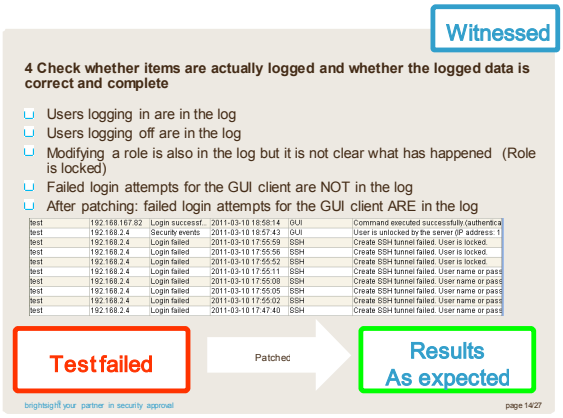
@EAL2-3:
AVA_VAN.2.1C The TOE shall be suitable for testing.
AVA_VAN.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
The execution part of:
AVA_VAN.2.4E The evaluator *shall conduct* penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

@EAL4:
AVA_VAN.3.1C The TOE shall be suitable for testing.
AVA_VAN.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
The execution part of:
AVA_VAN.3.4E The evaluator *shall conduct* penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing **Enhanced-Basic** attack potential.

The Evaluator shall present[13]:
- the test results of all tests in the ATE/AVA Testplan;
- if any tests failed, how these failures were handled by the developer and the test results of the subsequent evaluator retest.

Example of Test:

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



Result: The evaluator demonstrates to the certifier that the TOE has passed ATE and AVA tests.

13 The ALC Results

@EAL3-5:
The results of:
ALC_DVS.1.2E The evaluator *shall confirm* that the security measures are being applied.

@EAL2-7:
The results of:
ALC_DEL.1-2 The evaluator *shall examine* aspects of the delivery process to determine that the delivery procedures are used.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.4.10C The evidence *shall demonstrate* that the CM system is being operated in accordance with the CM plan.

The evaluator shall present the results of the verification that the lifecycle processes and procedures are applied.

Result: The evaluator has demonstrated that he has checked whether the developer applies the documented procedures.

14 Consultancy/Evaluation Improvement Presentation

Often, during the consultancy of an evaluation (or during the early stages of an evaluation) the developer makes significant security improvements to the TOE as the result of this consultancy/early evaluation. This process is often invisible to the certifier.

In some evaluations, when many or all of the problems have already been eliminated, the evaluation itself is a relatively sterile affair: the design is solid and all tests pass and it seems that both evaluator and certifier have contributed nothing to the security of the TOE.

To prevent this, this NSP mandates a Consultancy/Evaluation Improvement presentation.

None. This is not derived from CC requirements.

The evaluator shall present:

1. The security improvements made to the TOE during the consultancy phase. Note that this is only possible if the same lab also performed the consultancy. If this is not the case, this part of the presentation is skipped.
2. The security improvements made to the TOE before the Evaluation Meeting, as a result of evaluation activities.

Example of improvements:
During the consultancy, it was noticed that:

- The TOE always used the same communication key
- The TOE was not resistant against SQL-injection

All of this was repaired before the evaluation started.

During the evaluation, it was noticed that:

- There was an “anonymous/guest” account
- The TOE did not log start and stop of the audit functionality

All of this was repaired before the First Evaluation Meeting.

Result: The certifier obtains insight in the security improvements of the TOE.

A. What do the CCRA, SOGIS-MRA, CEM and JIL mandate for evaluator reporting?

Below, the relevant sections of [CCRA], SOGIS-MRA [SOG3] and [CEM] have been reproduced:

CCRA: B.2 The Role and Principal Characteristics of the CB

[…] The principal functions to be performed by the Certification/Validation Body are:

b) to monitor the performance of participating ITSEFs and, in particular, their adherence to, and application and interpretation of, the accepted evaluation criteria and evaluation methods;

e) to monitor all evaluations in progress within the Scheme at an appropriate level;

f) to review all evaluation reports (including especially Evaluation Technical Reports) to ensure that the conclusions are consistent with the evidence adduced and that the accepted evaluation criteria and evaluation methods have been correctly applied;

SOGIS: B.2 The Role and Principal Characteristics of the CB

[…] The principal functions to be performed by the Certification Body are:

b) to monitor the performance of participating ITSEFs and, in particular, their adherence to, and application and interpretation of, the accepted evaluation criteria and evaluation methods;

f) to monitor all evaluations in progress within the Scheme at an appropriate level;

g) to review all evaluation reports (including especially Evaluation Technical Reports) to ensure that the conclusions are consistent with the evidence adduced and that the accepted evaluation criteria and evaluation methods have been correctly applied;

CEM: 8.5.5.3.4 Results of the evaluation

133 For each activity on which the TOE is evaluated, the evaluator ***shall report***:
- the title of the activity considered;
- a verdict and a supporting rationale for each assurance component[14] that constitutes this activity, as a result of performing the corresponding CEM action and its constituent work units.

134 The rationale justifies the verdict using the CC, the CEM, any interpretations and the evaluation evidence examined and shows how the evaluation evidence does or does not meet each aspect of the criteria. It contains a description of the work performed, the method used, and any derivation of results. The rationale **may**[15] provide detail to the level of a CEM work unit.

135 The evaluator ***shall report*** all information specifically required by a work unit.

136 For the AVA and ATE activities, work units that identify information to be reported in the ETR have been defined.

JIL documents

No current JIL documents address evaluator reporting.

Note that none of these do mandate the detailed work unit level of documentation that is currently mandated by the NSCIB. The “may” in CEM para 134 allows the evaluator to report on a higher than

[14] It does not say work unit: rationales can be given on groups of work units at the same time.
[15] This is not a shall or should: it is a possible option with no specific preference for that option.

work unit level (with the exception of certain specific “The evaluator shall report” ATE and AVA work units).

Summarised:

- The CCRA requires that the CB reviews all evaluation reports, but does not mandate the nature of these reports[16] or the nature of the review
- The CEM discusses the reporting in more detail, but only requires “a rationale” to be reported[17]

This gives flexibility in how the lab reports to the CB. This NSP uses this flexibility to provide a better balance of the reporting duty of the lab and the overseeing duties of the Certification Body, while still retaining full conformance to the CCRA, SOGIS-MRA and CEM requirements.

[16] With the exception of the ETR, which has specific reporting requirements listed in [CEMe].
[17] With the exception of a specific set of work units also listed in [CEMe].

B. Cross-reference

In the table below, the CC elements for an EAL3 evaluation are cross-referenced with the relevant sections of this procedure:

CC Family	Element	Section
ADV_ARC	1.1C	4.4
	1.2C	4.4
	1.3C	4.4
	1.4C	4.4
	1.5C	4.4
	1.1E	4.4
ADV_FSP	3.1C	4.1
	3.2C	4.1
	3.3C	5.1
	3.4C	5.1
	3.5C	5.1
	3.6C	5.1
	3.7C	4.3
	3.1E	4.1 / 4.3 / 5.1
	3.2E	4.3
ADV_TDS	2.1C	4.2
	2.2C	4.2
	2.3C	4.2
	2.4C	4.3
	2.5C	4.2
	2.6C	4.3
	2.7C	4.3
	2.8C	4.3
	2.1E	4.2 / 4.3
	2.2E	4.3
AGD_OPE	1.1C	5.2
	1.2C	5.2
	1.3C	5.2
	1.4C	5.2
	1.5C	5.2
	1.6C	5.2
	1.7C	5.2
	1.1E	5.2
AGD_PRE	1.1C	5.2
	1.2C	5.2
	1.1E	5.2
	1.2E	10
ALC_CMC	3.1C	11
	3.2C	6
	3.3C	11
	3.4C	11
	3.5C	11
	3.6C	11
	3.7C	11
	3.8C	11
	3.1E	11

CC Family	Element	Section
ALC_CMS	3.1C	11
	3.2C	11
	3.3C	11
	3.1E	11
ALC_DEL	1.1C	11
	1.1E	11
ALC_DVS	1.1C	11
	1.1E	11
	1.2E	11
ALC_LCD	1.1C	11
	1.2C	11
	1.1E	11
ATE_COV	2.1C	7.2
	2.2C	7.2
	2.1E	7.2
ATE_DPT	1.1C	7.3
	1.2C	7.3
	1.1E	7.3
ATE_FUN	1.1C	7.4
	1.2C	7.4
	1.3C	7.4
	1.4C	7.4
	1.1E	7.4
ATE_IND	2.1C	10
	2.2C	10
	2.1E	10
	2.2E	7.5/10
	2.3E	7.5/10
AVA_VAN	2.1C	10
	2.1E	10
	2.2E	7.6
	2.3E	7.6
	2.4E	7.6 / 10