



Dutch Authority for Digital
Infrastructure
*Ministry of Economic Affairs and
Climate Policy*

File number

NP002

Version

1.0

Date

1 February 2024

NCCA processes

Subject

NP002 - EUCC processes

Document history

Version	Date	Comment
1.0	2024-02-01	Final version for 1 st publication and use

References

- [CC] ISO/IEC 15408 and/or Common Criteria for IT Security Evaluation
- [CEM] ISO/IEC 18045 and/or Common Methodology for IT Security Evaluation
- [CSA] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
- [EUCC] EUCC Implementing Regulation, C(2024) 560, 31-01-2024
- [UITVW] Regels ter uitvoering van Verordening (EU) 2019/881 (Uitvoeringswet cyberbeveiligingsverordening) – Voorstel van Wet no. 35838

Glossary of terms and abbreviations

- CAB Conformity Assessment Body
- ENISA European Union Agency for Cybersecurity
- ERM Evaluation Review Meeting
- IT Information Technology
- ITSEF IT Security Evaluation Facility
- NCCA National Cybersecurity Certification Authority
- RDI Rijksinspectie Digitale Infrastructuur / Dutch Authority for Digital Infrastructure
- TOE Target of Evaluation

Table of contents

1. Introduction	4
1.1 Background and purpose	4
1.2 Information products	5
1.3 Roles	6
2. Forecast Process	8
2.1 Phase 0: Forecast Phase	8
2.1.1 Step 0.1: Prepare and submit monthly forecast	9
2.1.2 Step 0.2: Collect monthly forecasts and create forecast overview	10
3. Certification Process	13
3.1 Phase 1: Notification Phase	14
3.1.1 Step 1.1: Prepare for certification	14
3.1.2 Step 1.2: Prepare notification	16
3.1.3 Step 1.3: Assess notification	19
3.2 Phase 2: Evaluation and Review Phase	24
3.2.1 Step 2.1: Assess developer evidence and generate meeting deliverables	25
3.2.2 Step 2.2: Prepare developer evidence	27
3.2.3 Step 2.3: Conduct evaluation review meeting 1, 2 and 3	28
3.2.4 Step 2.4: Generate final evaluation & certification reports	32
3.2.5 Step 2.5: Project monitoring	35
3.3 Phase 3: Certification Approval Phase	38
3.3.1 Step 3.1: Assess request for approval	38
3.3.2 Step 3.2: Issue certificate	42
3.3.3 Step 3.3: Conclude approval process	43
4. Assurance continuity process	45
5. The vulnerability management and disclosure process	47
Annex A Content and presentation of Evaluation Review Meetings	48

1. Introduction

1.1 Background and purpose

The European Common Criteria scheme (EUCC) is the first cybersecurity certification scheme developed under the Cybersecurity Act (CSA). This scheme aims to serve as a successor to the current existing national schemes operating under the SOGIS MRA (Senior Officials Group on Information Systems Security Mutual Recognition Agreement) and covers the certification of ICT products, using the Common Criteria ISO/IEC 15408 standard.

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs and Climate Policy. The UITVW expresses the Dutch government choice to use the 'prior approval model' as mentioned in article 56(6)a of the CSA as the only option for issuing certificates at the assurance level 'high'.

This document provides details of the steps and activities that the parties involved shall take in the EUCC processes in which the RDI as NCCA has a role¹. The EUCC processes are:

1. The forecast process (further described in chapter 2);
2. The certification process (further described in chapter 3);
3. The assurance continuity process (further described in chapter 4);
4. The vulnerability management and disclosure process (further described in chapter 5).

The forecast, the certification and assurance continuity processes are applicable for products and protection profiles where assurance level 'High' is claimed. Approval is necessary from the NCCA before a CAB is allowed to issue a certificate at this assurance level 'High'. Note that a similar approach may also be applied to the certification of products and protection profiles where assurance level 'Substantial' is claimed. In this case the approval is not required, and the involvement of the NCCA in the certification process would be nil².

Depending on the nature of the certification, the actual activities may differ and need to be tailored as described in the following chapters.

The vulnerability management and disclosure process is applicable for products certified at either the 'Substantial' or 'High' assurance level.

This document is aligned with the accreditation norms ISO/IEC 17025 & ISO/IEC 17065 and the related EUCC State-of-the-Art documents while also providing detailed guidance to the formal approval steps as specified in the UITVW. The overall goal is to ensure that the formal approval can

¹ Note that this document does not cover the processes related to the NCCA activities specified in article 58 section 7 of the CSA.

² Current discussions in the CCRA might lead to NCCA involvement for all assurance levels if CCRA recognition is also requested. Note that this is not mandatory for EUCC, but is optional for those cases where CCRA recognition is required by the sponsor.

be given efficiently based on a process that reduces risks for all stakeholders by having the following characteristics:

- Quality: approval based on verification that certification is meeting scheme requirements
- Predictability: assurance that certification is on the right track
- Responsiveness: small work packages/intermediate results are faster to review
- Timeliness: fast final approval based on intermediate results

1.2 Information products

The following information products are identified in the EUCC processes:

Information product	From	To	Description
Monthly forecast	CAB	NCCA	A document containing the certification leads of a CAB. It is used by the NCCA operational manager for initial resource planning and allocation.
Forecast overview	NCCA	NCCA	NCCA internal document compiled by the operational manager from the individual monthly forecasts.
EUCC notification	CAB	NCCA	Official notification from a CAB to the NCCA that they wish to start the certification-process for a product or protection profile. It consists of a notification form, assessment plan and (draft) Security Target/ Protection Profile
Assessment plan	CAB	NCCA	A document describing how the CAB will conduct the product assessment.
Notification Review Report	NCCA	NCCA	NCCA internal report in which the NCCA keeps track of everything leading up to the rejection or acceptance of the assessment plan.
Acceptance of assessment plan	NCCA	CAB	Official notification of acceptance of the assessment plan, after which the certification process can proceed to the certification monitoring phase.
Rejection of assessment plan	NCCA	CAB	Official notification of rejection of the assessment plan.
Request for developer evidence	CAB	Sponsor	A request from the CAB to the sponsor to provide the developer evidence necessary for assessment.
Developer evidence	Sponsor	CAB	Evidence provided by the sponsor to the CAB for assessment.
Evaluator evidence	CAB	NCCA	Reports or other material describing how the evaluator actions have been performed. This evidence is presented in the ERM for internal review by the certifier and monitoring by the NCCA.
Evaluation Technical Report (ETR)	CAB	NCCA	Report that combines and compiles all evaluator evidence from the product evaluation.
Meeting minutes	CAB	NCCA	Report of an ERM that records all issues raised during the meeting, the decisions made and the conclusion.
Project actions list	CAB	CAB NCCA	A list in which the CAB keeps track of all actions including their status related to the assessment as discussed during the ERMs. The final version will be provided to the NCCA as part of the request for approval.
Certifier Review Report	CAB	CAB NCCA	Report in which the CAB keeps track of all its review activities leading up to its certification decision. Final version will be provided to the NCCA as part of the request for approval.

EUCC process descriptions – v1.0

Certification Report (CR)	CAB	NCCA	A document containing a high-level description of the product and the certification performed. This document will be published in conjunction with the certificate.
Draft certificate	CAB	NCCA	A draft of the certificate that the CAB makes before formal approval for certification is given by the NCCA.
Request for approval	CAB	NCCA	Request from the CAB to the NCCA to approve the issuance of an EUCC certificate.
Approval Review Report	NCCA	NCCA	NCCA internal document in which the NCCA keeps track of everything leading up to its decision regarding the final approval.
Approval to issue certificate	NCCA	CAB	Official notification sent by the NCCA to the CAB to approve the issuance of an EUCC certificate.
Rejection of approval	NCCA	CAB	Official notification sent by the NCCA to the CAB to reject the issuance of an EUCC certificate.
Certification notification	CAB	Sponsor NCCA ENISA	Notification to the sponsor, NCCA and ENISA that a product has been certified under EUCC.
Protection Profile (PP)	Sponsor	CAB NCCA	A document describing a set of security requirements for a class of products. I.e. it specifies the security needed in a IT product. This document can be the subject of a certification, or can be used by a product's Security Target to claim compliance with.
Security Target (ST)	Sponsor	CAB NCCA	A document describing a set of implementation-dependent security requirements for a product. I.e. it specifies the security provided in a specific IT product and forms the basis for a product assessment.
Security Target Lite (ST-Lite)	Sponsor	CAB NCCA	A Security Target sanitised by the removal or paraphrasing of proprietary technical information.
Evaluation Technical Report for composite evaluations (ETRFC)	CAB	NCCA CAB	A subset of an ETR that is intended for re-use in a composite certification process (by another CAB).
Site Technical Audit Report (STAR)	CAB	NCCA CAB	A report describing the audit results of the development and production environment of the product that is intended for re-use in another product certification process (by another CAB).
Impact Analysis Report (IAR)	Sponsor	CAB NCCA	A document describing changes to a certified product, used as input for assurance continuity.

All documents or other material (e.g., presentations) exchanged with the NCCA shall be in electronic form and in the English language. If the material contains proprietary or sensitive information, it should be submitted in encrypted form with PGP encryption using the public NCCA keys, which can be downloaded from the NCCA website.

Please refer to the NCCA instruction [NI001 - InformationExchange](#) for further guidelines on how documents or other material shall be exchanged with the NCCA. This applies to all instances in this document where the words “send to the NCCA” is used.

1.3 Roles

The following roles are identified in the EUCC processes:

Role	Responsible Entity	Description
Certificate issuer	CAB	Designated person within a CAB with the authority to issue certificates.
Certifications manager	CAB	Overall point-of-contact for the general operation of the CAB.

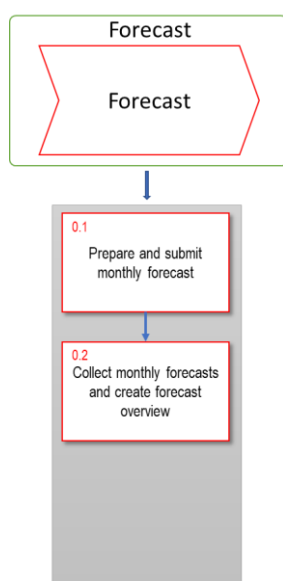
		Will submit the monthly forecasts and the certification notifications.
Certifier	CAB	Person from the CAB responsible for the review of the evaluation activities and generation of the certification report.
Evaluator	CAB	Person performing the evaluation activities and generation of the evaluator evidence and ETR.
Certification auditor	NCCA	Person responsible for the monitoring of the certification process comprising the activities of the certifier who has reviewed and assessed the activities of the evaluator.
Audit supervisor	NCCA	Person responsible for processing the monthly forecast and pre-allocating resources, preparing the official rejection or acceptance of the notification and providing the official rejection or acceptance of the certificate.
External expert	CAB	Person (internal to the RDI or from an external organisation) supporting the certification auditor providing technical expertise not possessed by the NCCA itself.
Sponsor role	Sponsor	The sponsor is the entity that wishes a product to be certified under EUCC and is responsible for providing all the necessary developer evidence. The sponsor will become the holder of the certificate. Usually the sponsor is the manufacturer or supplier of the product to be certified under EUCC.

2. Forecast Process

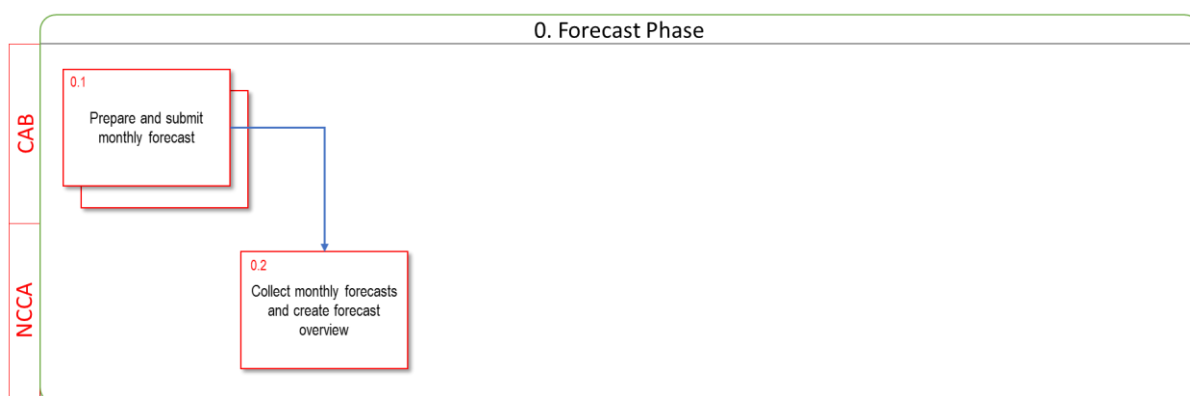
The Forecast Process is asynchronous to the Certification Process and is intended to allow the NCCA to take the necessary preparation steps for upcoming EUCC notifications. Knowing beforehand the amount and type of EUCC notifications enables the NCCA to perform adequate resource planning and allocation such that the lead time of the Certification Process can be optimised.

Every CAB is expected to report to the NCCA on a monthly basis all certification leads for assurance-level high of which it expects with more than 70% certainty that they will lead to a notification within the next three months.

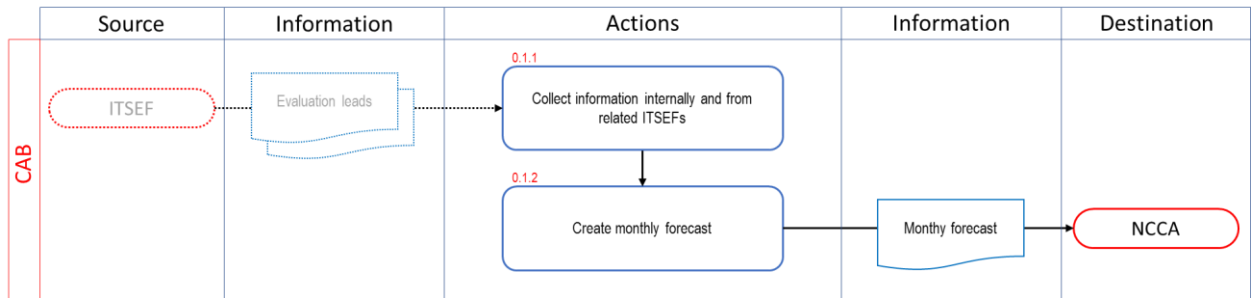
The Forecast Process only consists of one phase: the *Forecast Phase*.



2.1 Phase 0: Forecast Phase



2.1.1 Step 0.1: Prepare and submit monthly forecast



2.1.1.1 Action 0.1.1: Collect information internally and from related ITSEFs

Responsible: CAB
Executed by: Certifications manager
1. Collect information about possible evaluation/certification leads
<ul style="list-style-type: none"> Request information on possible evaluation/certification leads for assurance-level high from internal account management or sales department. Request information on possible evaluation/certification leads for assurance-level high from associated external ITSEFs (when applicable). <p><i>Note 1:</i> This information has to be collected on a monthly basis. If the CAB makes use of external ITSEFs, then it may request this information every month from the ITSEFs, or procedurally demand from the ITSEF that they send this information structurally every month to them.</p> <p><i>Note 2:</i> A CAB is expected to report to the NCCA on a monthly basis all evaluation/certification leads for assurance-level high of which it expects with more than 70% certainty that they will lead to a notification within the next three months.</p>

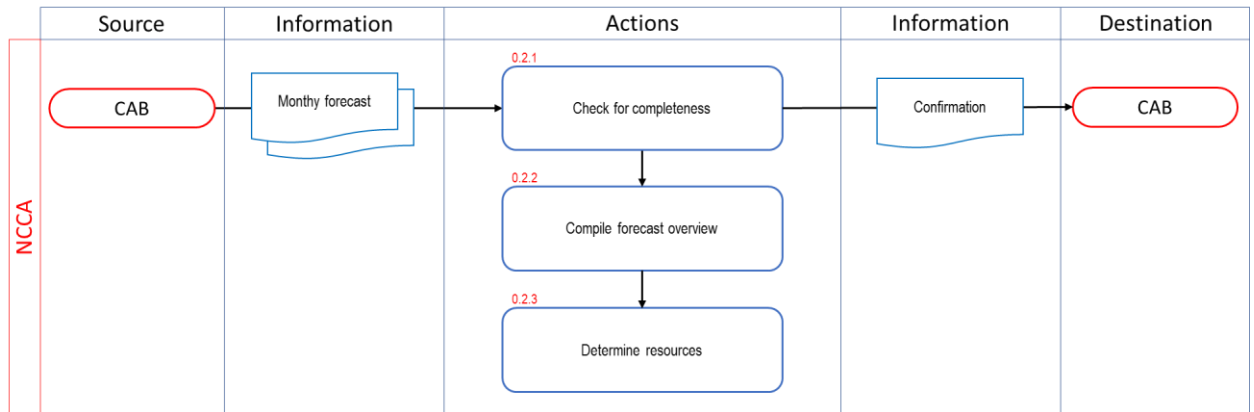
2.1.1.2 Action 0.1.2: Create monthly forecast

Responsible: CAB
Executed by: Certifications manager
1. Compile monthly forecast
<ul style="list-style-type: none"> Download the monthly forecasting template from NCCA website. Fill in the required fields using the collected information. <p><i>Note:</i> In the case a sponsor approached multiple CABs/ITSEFs to perform an evaluation on their product, add all these requests to the forecasting template.</p>
2. Submit monthly forecast to the NCCA
<ul style="list-style-type: none"> Send the monthly forecast to the NCCA on the first working day of the month.

Note 1: It is understood that the information is commercially sensitive. NCCA will only use this information for its resource planning.

Note 2: The monthly forecast may be submitted encrypted or unencrypted. If the CAB wishes to submit the monthly forecast encrypted it may do so with PGP encryption using the public NCCA keys, which can be downloaded from the NCCA website.

2.1.2 Step 0.2: Collect monthly forecasts and create forecast overview



2.1.2.1 Action 0.2.1: Check for completeness

Responsible: NCCA
Executed by: Audit supervisor
1. Receive the monthly forecast
<ul style="list-style-type: none"> Receive (and decrypt if required) the monthly forecast from every CAB. Archive and register the monthly forecasts in the NCCA document management system.
2. Check the monthly forecasts for completeness
<ul style="list-style-type: none"> Check that all necessary information is contained in the monthly forecasts. Notify a CAB in the case their monthly forecast is incomplete and request missing information.
3. Send confirmation
<ul style="list-style-type: none"> Send a message to the CABs that their monthly forecasts are well received.

2.1.2.2 Action 0.2.2: Compile forecast overview

Responsible: NCCA

Executed by: Audit supervisor
1. Combine monthly forecasts
<ul style="list-style-type: none"> • Transfer every entry from the monthly forecasts to the central NCCA forecast overview, while keeping the references to the CABs and ITSEFs. • Highlight the changes compared to the forecast from previous month.

2.1.2.3 Action 0.2.3: Determine resources

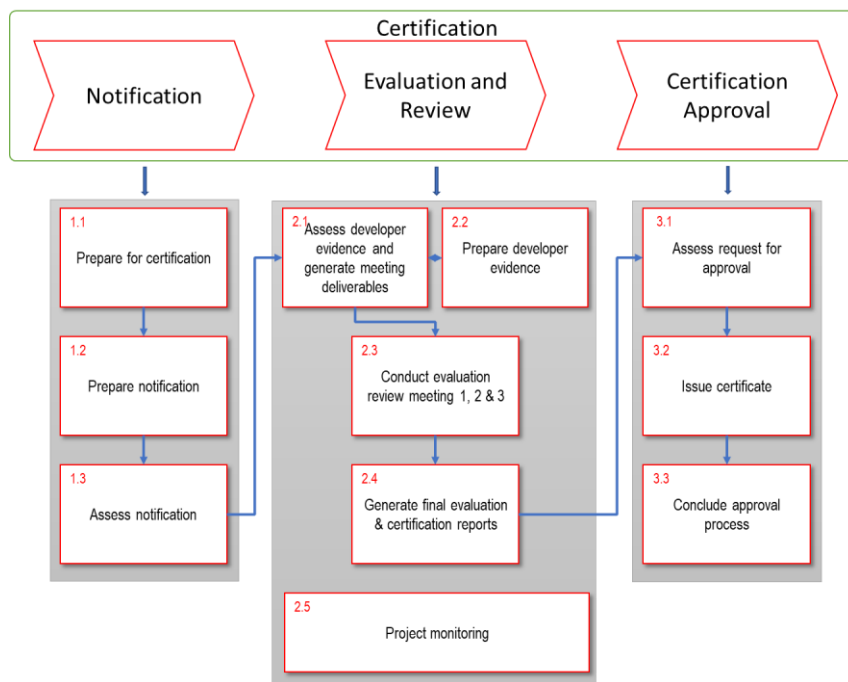
Responsible: NCCA
Executed by: Audit supervisor
1. Determine monitoring type
<ul style="list-style-type: none"> • Based on the following factors, determine whether there is a need for certification monitoring: <ul style="list-style-type: none"> ○ The importance-level of the product for the public or Dutch government (e.g. Netherlands passport). ○ If the product is of specific interest for RDI (Relations with areas of interest and research). ○ The level of experience of the CAB (including the ITSEF) with the type of product. ○ The level of experience of the sponsor/developer with the Common Criteria standard. ○ The past performance of the CAB (including the ITSEF). ○ The assessment type (new, re-certification, maintenance). ○ The expected duration of the evaluation/certification. • Include in the forecast overview if monitoring will be foreseen.
2. Pre-allocate resources
<ul style="list-style-type: none"> • For every potential project pre-allocate a certification auditor based on availability and specific knowledge related to the type of product or previous experience with the product that will be evaluated. • Include the name of the pre-allocated certification auditor in the forecast overview. <p><i>Note 1:</i> The pre-allocated certification auditor must be independent from, and not be involved in, the activities of the sponsor/developer and the CAB.</p> <p><i>Note 2:</i> There may be a need for additional expertise from outside the NCCA. This could be because the relevant expertise is not present within the NCCA, there are insufficient</p>

resources available or for other reasons. In such cases the certification auditor could be assisted by an external expert.

3. Certification Process

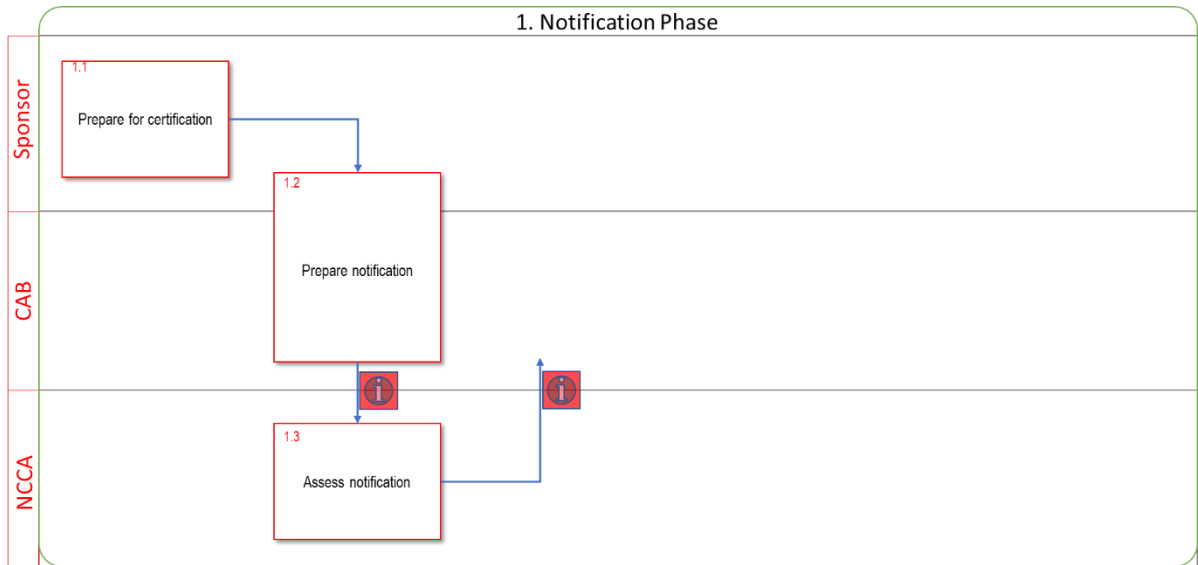
The certification process comprises of the following three phases:

1. The *Notification Phase*: in which the formal notification is submitted and processed, resulting in a formal approval or rejection by the NCCA;
2. The *Evaluation and Review Phase*: in which the actual assessment is performed by the CAB and its (subcontracted) ITSEF. The phase normally ends in a formal request for approval from the CAB to the NCCA for the issuance of a certificate;
3. The *Certification Approval Phase*: in which the concluding actions are performed, resulting in a formal approval or rejection by the NCCA and the actual issuance of an EUCC certificate.



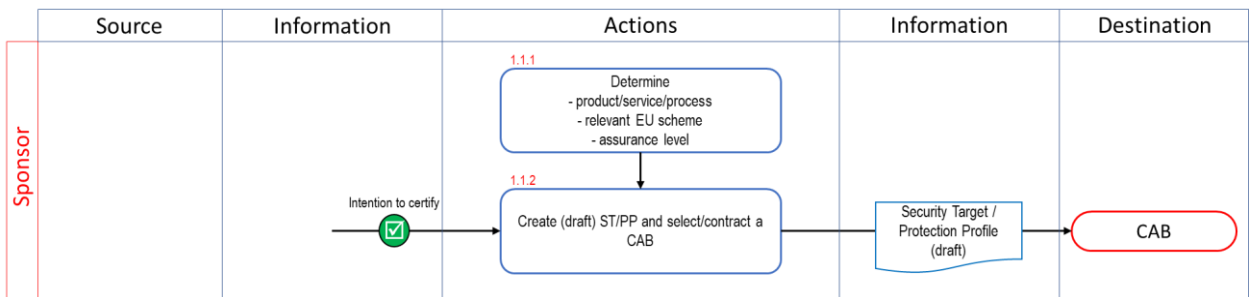
During the assessment of the notification, the NCCA will determine whether there will be NCCA monitoring throughout the evaluation and review phase or not. In the latter case it is expected by the NCCA that a timely approval to issue a certificate can be given without this monitoring.

3.1 Phase 1: Notification Phase



3.1.1 Step 1.1: Prepare for certification

This first step in the notification phase and the related actions are described for completeness and are solely intended as guidance to the sponsor.



3.1.1.1 Action 1.1.1: Determine certification object, scheme and assurance level

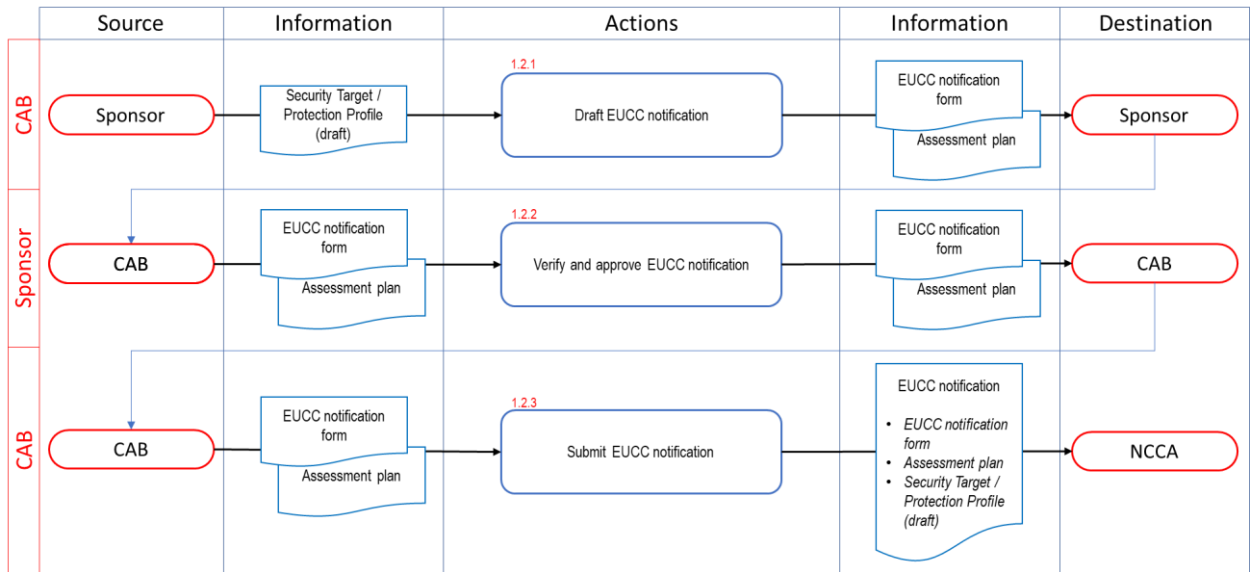
Responsible: Sponsor
Executed by: Sponsor role
1. Determine object to be certified
<ul style="list-style-type: none"> The EUCC can only be used to certify products or protection profiles. If a sponsor wants to certify a process or service under the Cyber Security Act, determine which other EU scheme is relevant.
2. Determine assurance level
<ul style="list-style-type: none"> Determine the assurance level that is required for the evaluation based on the threat-level that the product needs to counter, intended use, marketing needs, etc.

3.1.1.2 Action 1.1.2: Create (draft) ST/PP and select/contract a CAB

<p>Responsible: Sponsor</p> <p>Executed by: Sponsor role</p> <p>In co-operation with: Optionally with a CC consultant or the envisaged CAB</p>
<p>1. Determine which CAB's are accredited to perform the EUCC certification activities³</p>
<ul style="list-style-type: none"> • Determine which CAB's are accredited to perform certification activities at the required assurance-level, and where relevant the technical domain. A list of CAB's is available on the NCCA website.
<ul style="list-style-type: none"> • Determine, based on own needs, requirements and preferences, which of the CAB's is preferred to perform the EUCC certification activities.
<p>2. Create a (draft) Security Target (ST) / Protection Profile (PP)</p>
<ul style="list-style-type: none"> • Create an initial version of the ST or PP that describes the TOE in sufficient details such that the logical and physical boundary is clearly defined. Also the Security Problem Definition and Objectives must be complete. <p><i>Note:</i> drafting a ST or PP is a specialised task for which the sponsor may want to contract/hire a CC consultant or expert. This may be an independent consultant, but the envisaged CAB could also provide this consultancy service. However the CSA and EUCC impose restrictions on consulting services.</p>
<p>3. Consult envisaged CAB and reach an certification agreement</p>
<ul style="list-style-type: none"> • (Optionally) Submit the (draft) ST/PP to the envisaged CAB. • Consult the envisaged CAB to determine to what extend the CAB is able and willing to perform the certification activities based on the (draft) ST/PP and under which conditions. • Come to a contractual agreement with the CAB for performing the certification activities. <p><i>Note:</i> If the CAB makes use of external ITSEFs, then the sponsor may also need to come to a contractual agreement with the ITSEF for performing the evaluation part of the certification activities.</p>

³ The term 'certification activities' is used in accordance with ISO/IEC 17065 chapter 7 and includes evaluation activities.

3.1.2 Step 1.2: Prepare notification



3.1.2.1 Action 1.2.1: Draft EUCC notification

<p>Responsible: CAB</p> <p>Executed by: Certifications manager</p>
<p>1. Draft an EUCC notification form</p> <ul style="list-style-type: none"> • Receive the (draft) ST/PP (if not already in possession). • Check that the (draft) ST/PP describes the TOE in sufficient details so that the logical and physical boundary is clearly defined. Also check the completeness of the Security Problem Definition and Objectives. • Download the <i>EUCC notification form</i> from the NCCA website. • Fill in the required fields.
<p>2. Draft assessment plan</p> <ul style="list-style-type: none"> • Draft an assessment plan describing the evaluation and certification activities based on the draft ST/PP and NCCA procedures. The assessment plan must address the following five items in clearly separated sections: <ol style="list-style-type: none"> 1. <u>Appropriateness</u>: Is the chosen assurance level appropriate and is the chosen level commensurate with the level of risk associated with the intended use of the ICT product? 2. <u>Evaluation and certification approach</u>: the CAB shall describe which entity will perform the evaluation activities in case of outsourcing. Also some background information regarding the product to be evaluated shall be provided. The evaluation and certification approach shall be based on the default set of ERMs (see introduction of chapter 3.2 and Annex A Content and

<p>presentation of Evaluation Review Meetings) where the content is tailored in accordance with the EAL. If the CAB wants to deviate from this default set or content, the deviation must be described and motivated. This also applies in case the CAB wants to use the alternative approach for ADV and ATE. When previous evaluation results (e.g. ETR for composite evaluations, STAR reports or otherwise) will be re-used this must be indicated and described how;</p> <p>3. <u>Applicable standard and additional evaluation methodology</u>: The CAB shall identify the version and revision of the ISO/IEC 15408 or the CC and which additional evaluation methodology, besides ISO/IEC 18045 or the CEM, will be used. This additional evaluation methodology shall be in accordance with the EUCC scheme requirements, the product type, technical domain and State-of-the-Art documents;</p> <p>4. <u>Staff involved in consultancy, evaluation and certification</u>: in this section, the CAB must identify the key-staff involved in the evaluation and certification activities, especially the persons that authorise the deliverables. The CAB must also identify and describe any consultancy services that have been provided to the sponsor and list the staff involved. This is of particular importance when the consultancy has involved writing documentation on behalf of the sponsor or in any (pre-) evaluation activities. Staff involved in consultancy may not perform evaluation or certification activities or mentor other employees during these activities;</p> <p>5. <u>Evaluation and certification schedule</u>: this is the schedule for the delivery of all required evaluator evidence and the Evaluation Technical Report by the evaluators and the review thereof by the certifiers, including the ERMs. Also the planned date for the delivery of the Certification Report and the (draft) Certificate to the NCCA for approval must be indicated.</p> <p><i>Note 1:</i> The EUCC (in recital 3 and 5) requires the sponsor to provide a rationale for selecting the correct assurance level which the CAB shall review. This review must be included under the ‘appropriateness’ section in the assessment plan.</p> <p><i>Note 2:</i> While scheduling the ERMs, consideration must be given that the ERMs cannot be held without the NCCA approval for the suggested ERM dates in the assessment plan. In practice the first ERM should not be planned soon after the notification has been submitted as this increases the risk that the ERM will have to be rescheduled due to NCCA resource management and preparation. In general a 15 working days delay is needed after the formal approval has been issued by the NCCA (see Action 1.3.4: Issue formal decision on assessment plan).</p>
<p>3. Submit EUCC notification to sponsor</p>
<ul style="list-style-type: none"> Send the EUCC notification form and assessment plan to the sponsor for verification and approval.

3.1.2.2 Action 1.2.2: Verify and approve EUCC notification

Responsible: Sponsor
Executed by: Sponsor role
1. Receive the EUCC notification
<ul style="list-style-type: none"> • Receive the EUCC notification form and assessment plan. • Check the EUCC notification form for correctness, and fill in the remaining open fields.
2. Approve EUCC notification form
<ul style="list-style-type: none"> • Return the completed EUCC notification form and assessment plan to the CAB with a statement of approval.

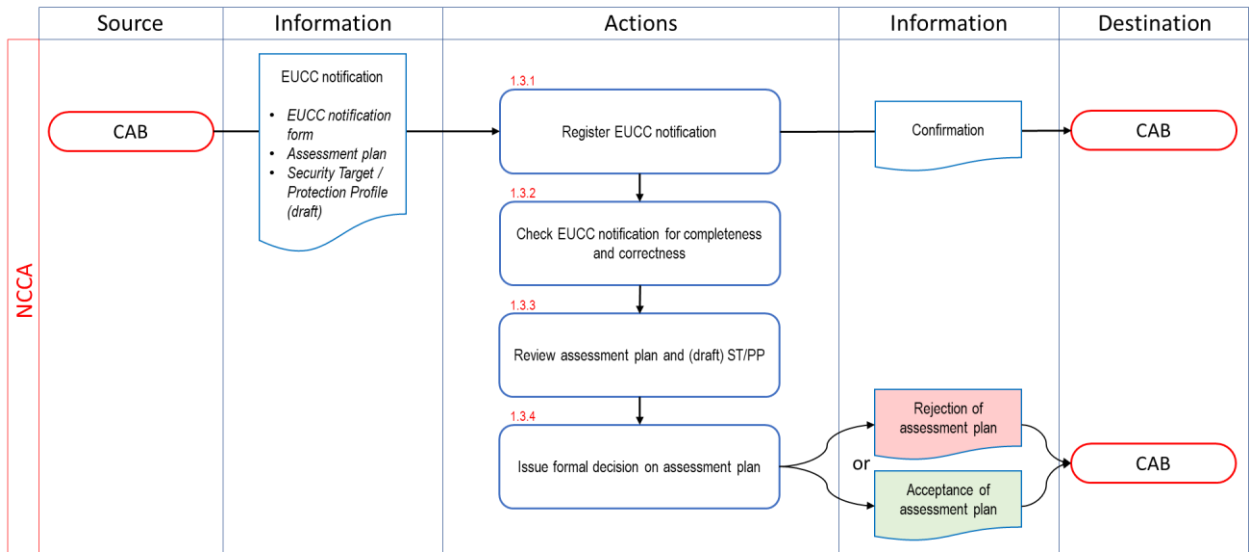
3.1.2.3 Action 1.2.3: Submit EUCC notification

Responsible: CAB
Executed by: Certifications manager
1. Receive the EUCC notification
<ul style="list-style-type: none"> • Receive the EUCC notification form and assessment plan.
2. Submit the EUCC notification
<ul style="list-style-type: none"> • Gather the (draft) ST/PP (already in possession of the CAB). • Sign the EUCC notification form, if not already done. • Compose the EUCC notification: <ul style="list-style-type: none"> ○ EUCC notification form; ○ Assessment plan; ○ (draft) ST/PP. • Send the notification to the NCCA. <p><i>Note 1:</i> The EUCC notification form and related documents may be submitted encrypted or unencrypted. If the CAB wishes to submit the documents encrypted it may do so with PGP encryption using the public NCCA keys, which can be downloaded from the NCCA website.</p>



The reception of the notification is a milestone for the NCCA after which the notification has to be processed within the legally defined terms.

3.1.3 Step 1.3: Assess notification



3.1.3.1 Action 1.3.1: Register EUCC notification

Responsible: NCCA
Executed by: Audit supervisor
1. Receive the notification
<ul style="list-style-type: none"> Receive (and decrypt if required) the EUCC notification form, the assessment plan and the (draft) ST/PP. Confirm the reception of the notification to the CAB. Archive and register the notification in the NCCA document management system and create an audit file. Check if the notification is on the forecast overview. If present, copy the certification information from the forecast overview to the audit file and update the forecast overview.
2. Determine monitoring type
<ul style="list-style-type: none"> Based on the following factors, verify if the envisioned monitoring decision from the forecast overview is still appropriate, or determine whether certification monitoring is needed: <ul style="list-style-type: none"> The importance-level of the product for the public or the Dutch government (e.g. Netherlands passport). If the product is of specific interest for RDI (Relations with areas of interest and research). The level of experience of staff involved from the CAB (including the ITSEF) with the type of product.

<ul style="list-style-type: none"> ○ The level of experience of the sponsor/developer with the Common Criteria standard. ○ The past performance of the CAB (including the ITSEF). ○ The assessment type (new, re-certification, maintenance). ○ The expected duration of the evaluation/certification. ● Include or update if monitoring is foreseen in the audit file.
<p>3. Appoint Certification Auditor</p>
<ul style="list-style-type: none"> ● Verify if the envisioned certification auditor is still available. If not, select a certification auditor based on availability and specific knowledge related to the type of product or previous experience with the product that will be evaluated. ● Inform the certification auditor that he/she is appointed to the certification process and if monitoring is foreseen. ● Include or update the name of the certification auditor in the audit file. <p><i>Note 1:</i> The appointed certification auditor must be independent from, and not be involved in, the activities of the sponsor/developer and the CAB.</p> <p><i>Note 2:</i> There may be a need for additional expertise from outside the NCCA. This could be because the relevant expertise is not present within the NCCA, there are insufficient resources available or for other reasons. In such cases the certification auditor could be assisted by external expert(s).</p>

3.1.3.2 Action 1.3.2: Check EUCC notification for completeness and correctness

<p>Responsible: NCCA</p> <p>Executed by: Certification auditor</p>
<p>1. Create Notification Review Report</p> <ul style="list-style-type: none"> ● Create an Notification Review Report to document any discussions and comments related to the notification. <p><i>Note:</i> The Notification Review Report is intended to collect findings on the notification documents, and forms the basis for the formal decision on the assessment plan.</p>
<p>2. Check the EUCC notification for completeness</p> <ul style="list-style-type: none"> ● Perform a high level check on the following items as a minimum: <ul style="list-style-type: none"> ○ Does the notification include a complete assessment plan and (draft) ST/PP? ○ Are all required fields in the notification form filled in? ○ Is the notification form signed by the CAB?

<ul style="list-style-type: none"> • Notify CAB in case the application is incomplete and request missing information. • Update the Notification Review Report with findings.
<p>3. Check the EUCC notification for correctness</p>
<ul style="list-style-type: none"> • Perform a high level check on the following items: <ul style="list-style-type: none"> ○ <u>Scope of the CAB:</u> Does the TOE fall within the accreditation scope of the CAB? ○ <u>Authorisation of the CAB:</u> Is the CAB authorised by the NCCA? ○ <u>Authorisation of the ITSEF:</u> Is the evaluation task performed by an authorised ITSEF? • Update the Notification Review Report with findings. • Continue with Action 1.3.4: Issue formal decision on assessment plan in case the application is incorrect or remains incomplete. This will lead to a rejection of the application and the termination of the certification process. Otherwise continue with Action 1.3.3: Review assessment plan and (draft) ST/PP. <p><i>Note:</i> The checks on scope and authorisation will not take part in case the EUCC notification is part of an initial assessment that the CAB needs to perform as part of its initial accreditation and licensing process.</p>

3.1.3.3 Action 1.3.3: Review assessment plan and (draft) ST/PP

<p>Responsible: NCCA</p> <p>Executed by: Certification auditor</p> <p>In co-operation with: Optionally with an external expert</p>
<p>1. Review assessment plan</p>
<ul style="list-style-type: none"> • Perform a detailed review of the assessment plan based on the Notification review guidance. Focus areas are: <ul style="list-style-type: none"> ○ <u>Appropriateness:</u> Is the chosen assurance level appropriate and is the chosen level commensurate with the level of risk associated with the intended use of the ICT product and does the CAB review confirms this? ○ <u>Evaluation & certification approach:</u> Does it describe which entity will perform the evaluation activities in case of outsourcing and does it provide sufficient background information regarding the product to be evaluated? Is the approach correctly based on the default set of ERMs (see introduction of chapter 3.2 and Annex A Content and presentation of Evaluation Review Meetings) and are deviations and choices well motivated? Check if re-use of previous results is possible as described, i.e.

<p>check the validity of evaluation results in case of re-use for composite evaluations, site audit results and maintenance activities.</p> <ul style="list-style-type: none">○ <u>Applicable standard and additional evaluation methods</u>: Are the standard and additional evaluation methods correctly identified and do they include all applicable methodology as required by the EUCC scheme?○ <u>Staff involved</u>: Is key-staff identified? Are there any issues related to independence and competence expected?○ <u>Project planning</u>: Do the dates of planned ERMs and the delivery of the final evaluation & certification reports (i.e. the request for approval) allow for reasonable time to address open issues. <ul style="list-style-type: none">● Discuss any items that are unclear with the CAB to gain necessary clarification in order to finalise the review.● Update the Notification Review Report with findings. <p><i>Note</i>: The EUCC (in recital 5) requires the sponsor to provide a rationale for selecting the correct assurance level which the CAB shall review. This review must be included under the ‘appropriateness’ section in the assessment plan.</p>
<p>2. Review (draft) ST/PP</p>
<ul style="list-style-type: none">● Perform a detailed review of the (draft) ST/PP based on the Notification review guidance:<ul style="list-style-type: none">○ <u>Clarity</u>: Is the ST or PP clear and understandable, is the TOE scope with its logical and physical boundaries well defined?○ <u>Meaningfulness</u>: Does the ST or PP comprise sufficient functionality to come to a meaningful certificate and does the security problem definition not contain any assumptions that unreasonably limit the usability expected by the end-user?○ <u>Assurance requirements</u>: Check the assurance requirements contain the appropriate AVA_VAN and ADV_IND components and its dependencies. Also check if the appropriate ALC_FLR component is included to address the sponsor requirements described in EUCC Chapter V and VI.● Discuss any items that are unclear with the CAB to gain necessary clarification in order to finalise the review.● Update and finalise the Notification Review Report with findings. <p><i>Note</i>: The EUCC (in article 7) requires security assurance requirements classes for vulnerability assessment and independent functional testing to be included in the evaluation. The EUCC in Chapter V and VI also has requirements related to vulnerability monitoring, management and disclosure for which the sponsor shall establish and maintain the necessary procedures. In the Netherlands these procedures need to be included in the evaluation.</p>

3.1.3.4 Action 1.3.4: Issue formal decision on assessment plan

Responsible: NCCA	
Executed by: Audit supervisor	
1. Validation of the Notification Review Report	<ul style="list-style-type: none"> • Check if the Notification Review Report is complete, correct and consistent. • Sign off the Notification Review Report.
2. Draft a formal acceptance or rejection letter	<ul style="list-style-type: none"> • Fill-in the applicable <i>NCCA letter template</i>. • Have the letter signed. <p><i>Note:</i> The letter of acceptance will include the name of the certification auditor and where applicable the name of the external expert(s). Also if monitoring will be performed is indicated.</p>
3. Submit the formal decision letter (acceptance or rejection) to the CAB	<ul style="list-style-type: none"> • Send the letter to the CAB. <p><i>Note:</i> The formal acceptance is based on the content of the provided assessment plan. This plan may need to change at a later stage and then requires a renewed acceptance by the NCCA. Changes of the assessment plan or deviations thereof may have consequences for the NCCA approval to issue a certificate. See also Step 2.5: Project monitoring.</p>



The acceptance of the assessment plan is a milestone for the CAB after which the assessment can formally commence.

In case of rejection the certification process stops and a new submission of an EUCC notification is required.

3.2 Phase 2: Evaluation and Review Phase

The evaluation and review phase consists of an iteration of 3 activities, one for each of the Evaluation Review Meetings (ERMs) followed by a final reporting activity. By default there will be 3 ERMs in this phase, but this will be dependent on the evaluation approach as defined in the assessment plan during the notification phase.

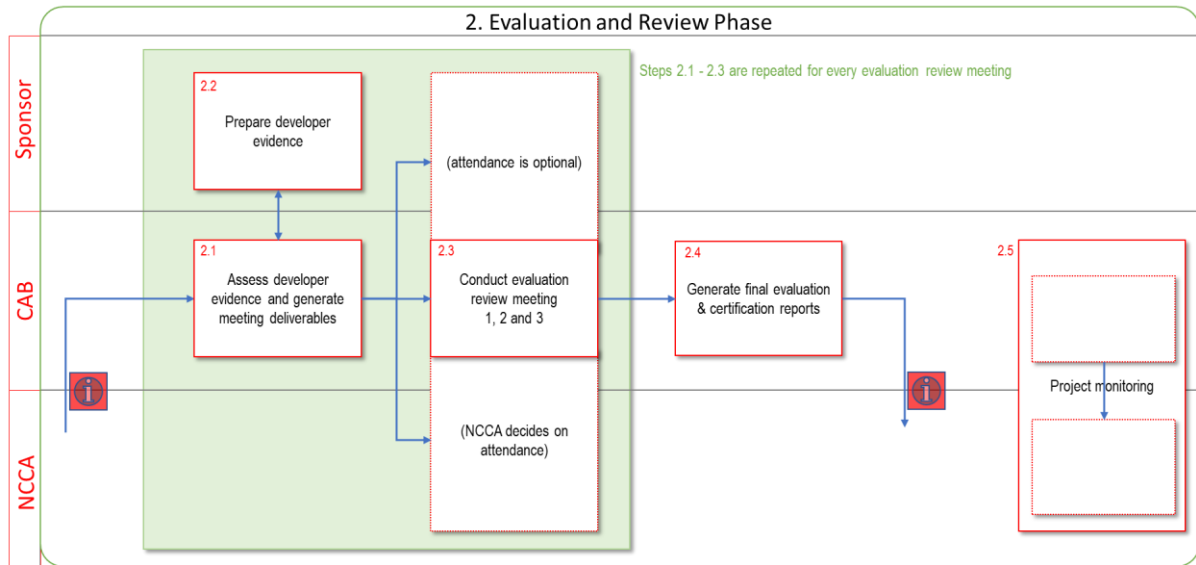
The evaluator is responsible for delivering the evaluator evidence which records the results of the evaluation activities (ref. ISO/IEC 17065 section 7.4 / ISO/IEC 17025 chapter 7). These reports are reviewed by the CABs certifier (ref. ISO/IEC 17065 section 7.5) and the review comments are communicated to the evaluator in Certifier Review Reports (and discussed in an ERM). The CAB is responsible for recording minutes of the ERMs and tracking of the action items.

After the final ERM, when all Certifier Review Report comments have been addressed and any action items closed, the evaluation is concluded with the generation of the final Evaluation Technical Report (ETR) by the evaluator. The certifier shall use the final ETR to create a Certification Report (CR) and draft Certificate. At the conclusion of the evaluation and review phase these documents will then be submitted to the NCCA for approval.

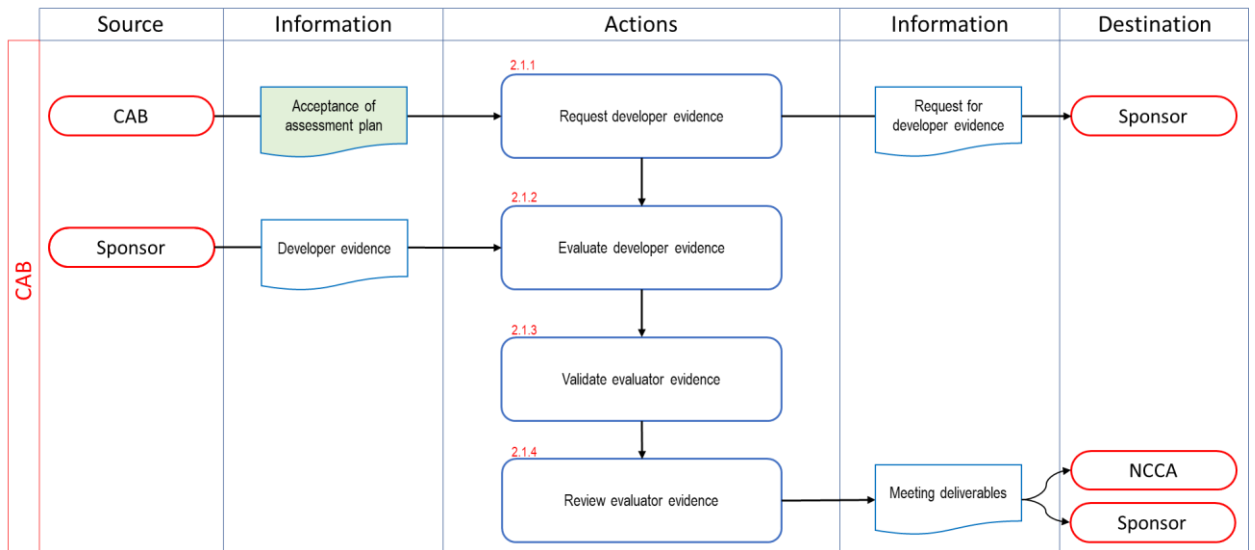
There are usually multiple iterations of the steps 2.1 – 2.3 according to the number of ERMs specified in the assessment plan. There are three ERMs defined for a typical EAL4 and higher evaluation (see Annex A Content and presentation of Evaluation Review Meetings), but some of these meetings can be combined for evaluations claiming lower assurance level packages (outside the scope of this document) and for maintenance and re-certification tasks. The content to be discussed in each ERM is also specified in Annex A Content and presentation of Evaluation Review Meetings and refined in the assessment plan. This will dictate what evaluator evidence is to be provided and what evaluation activities are to be performed by the evaluator in preparation for the ERM. Similarly, the agenda for each meeting is taken from the definition of the ERMs specified in the assessment plan.

In the case where there is NCCA monitoring foreseen throughout the evaluation and review phase, the certification auditor (NCCA) will be in copy of all meeting deliverables, but he may choose not to attend the ERMs. Being in copy shall not be the case when there is no NCCA monitoring, and only the request for approval including all associated documents will be delivered to the NCCA for approval (see output from Action 2.4.5: Submit request for approval). This means that when there is no NCCA monitoring, there will be no NCCA involvement during the evaluation and review phase other than Step 2.5: Project monitoring.

See also Annex A for an overview of the ERMs and the associated meeting deliverables.



3.2.1 Step 2.1: Assess developer evidence and generate meeting deliverables



3.2.1.1 Action 2.1.1: Request developer evidence

Responsible: CAB
Executed by: Evaluator
1. Define necessary developer evidence
<ul style="list-style-type: none"> The content to be discussed in each ERM is specified in the assessment plan and will dictate what developer evidence is to be provided by the sponsor. This developer evidence is related to the relevant developer action elements from the chosen assurance package and associated security assurance requirements from the Common Criteria standard (ISO/IEC 15408) and all other necessary information

that is required by the EUCC scheme. These will form the input for the evaluation activities that are to be performed by the evaluator in preparation for the ERM.
2. Submit request for the needed developer evidence
<ul style="list-style-type: none"> Send the request to the sponsor to provide the necessary developer evidence.

3.2.1.2 Action 2.1.2: Evaluate developer evidence

Responsible: CAB
Executed by: Evaluator
1. Receive evidence from sponsor
<ul style="list-style-type: none"> Record evidence received in accordance with the applicable evaluation procedures.
2. Evaluate evidence
<ul style="list-style-type: none"> Perform evaluation activities for the applicable ERM (as defined in the assessment plan) in accordance with the evaluation methodology specified in the CEM and any associated methodology specified in the assessment plan. Record findings and verdicts in the evaluator evidence as defined for the relevant ERM. Address actions from the project actions list (e.g. items raised in previous ERMs), providing a disposition of how the action has been addressed.

3.2.1.3 Action 2.1.3: Validate evaluator evidence

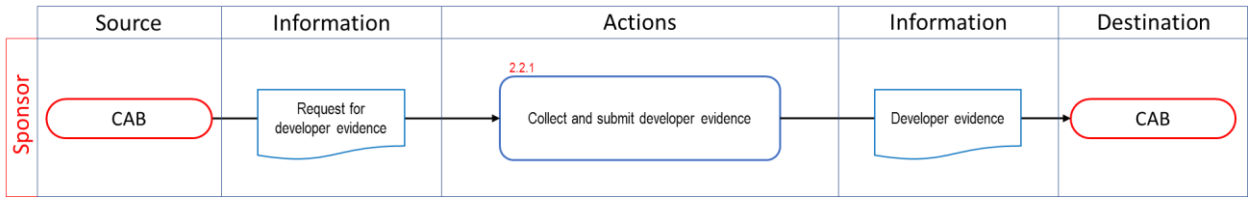
Responsible: CAB
Executed by: Evaluator
1. Finalise the evaluator evidence
<ul style="list-style-type: none"> Check that the evaluator evidence contain the necessary information.
2. Verify all evaluator evidence
<ul style="list-style-type: none"> Approve and authorize all evaluator evidence before submitting for formal CAB review.
3. Submit all evaluator evidence
<ul style="list-style-type: none"> Send the evaluator evidence and updated project action list to the CAB/certifier for formal review.

3.2.1.4 Action 2.1.4: Review evaluator evidence

<p>Responsible: CAB</p> <p>Executed by: Certifier</p>
<p>1. Receive completed package of evaluator evidence from the CAB/evaluator.</p>
<ul style="list-style-type: none"> • Check the package is complete in accordance with the list of deliverables specified in the assessment plan.
<p>2. Review evaluator evidence.</p>
<ul style="list-style-type: none"> • Review the evaluator findings and conclusions reported in the evaluator evidence and record any comments/notes for discussion in a Certifier Review Report. • Review disposition of action items and updates made to evaluator evidence to address actions (if any) from the project actions list.
<p>3. Preparation of Evaluation Review Meeting</p>
<ul style="list-style-type: none"> • Once the certifier is confident that the evaluation activities relevant for the ERM have been completed successfully, the ERM data/time/location can be confirmed by the certifier. • The CAB organises a meeting at a mutually agreed location. The sponsor/developer is encouraged, but not required, to attend the meeting. The NCCA endeavours to attend most meetings. Other parties are only allowed to attend if sponsor and CAB agree. • Send the complete package of evaluator evidence including the project actions list and Certifier Review Report to the NCCA & optionally to the sponsor. • Confirm and invite the NCCA and optionally the sponsor to the ERM. <p><i>Note 1:</i> The meeting deliverables are to be sent to the NCCA/certification auditor at least 5 working days before the meeting is scheduled to be held.</p> <p><i>Note 2:</i> The meeting deliverables and invitation are optionally sent to the sponsor depending on the agreement between the CAB and sponsor.</p> <p><i>Note 3:</i> The ERMs shall be held as a physical only meeting on a location in the Netherlands.</p>

3.2.2 Step 2.2: Prepare developer evidence

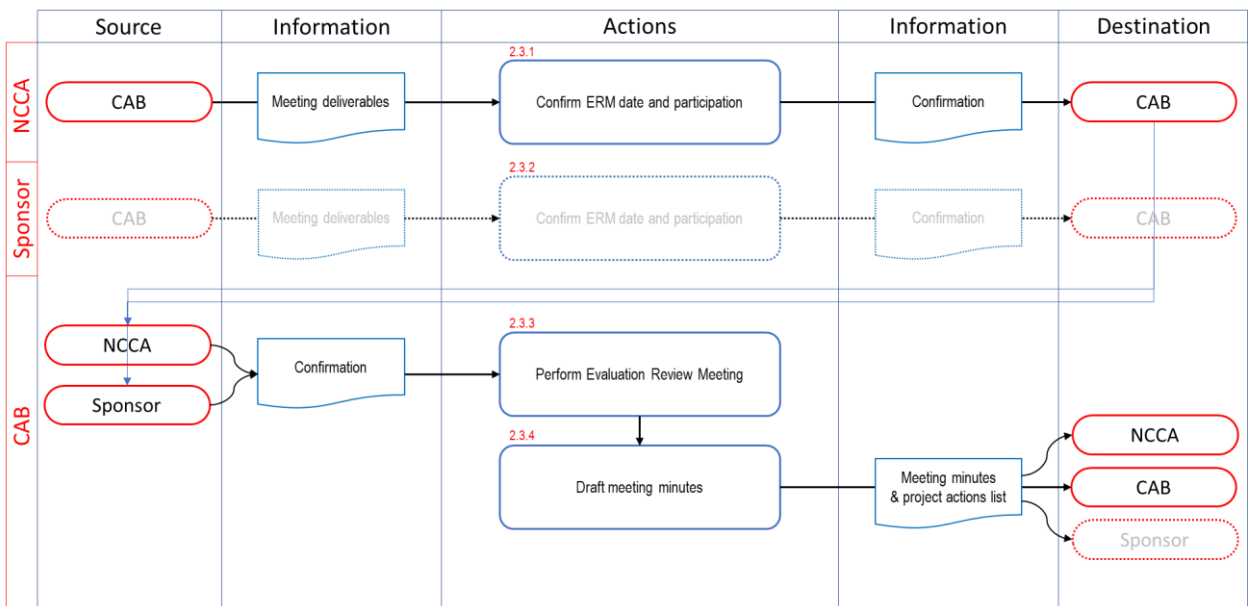
The developer evidence necessary for the appropriate iteration of the ERM must be delivered to the CAB in accordance with the assessment plan.



3.2.2.1 Action 2.2.1: Collect and submit developer evidence

Responsible: Sponsor
Executed by: Sponsor role
1. Create developer evidence
<ul style="list-style-type: none"> Collect all necessary information that is relevant for the chosen assurance level and associated security assurance requirements as defined by the Common Criteria standard (ISO/IEC 15408) and requested by the CAB. Collect all other necessary information that is required by the EUCC scheme.
2. Compile and provide developer evidence to the CAB
<ul style="list-style-type: none"> Supply the developer evidence to the CAB for evaluation. <p><i>Note:</i> Developer evidence can take many forms, including documents, e-mails or physical access to the development site. The form in which the developer evidence is supplied to the CAB needs to be mutually agreed. The CAB may for example agree to get access to the information on the premises of the manufacturer or provider.</p>

3.2.3 Step 2.3: Conduct evaluation review meeting 1, 2 and 3



3.2.3.1 Action 2.3.1: Confirm ERM date and participation

Responsible: NCCA
Executed by: Certification auditor
1. Receive meeting deliverables
<ul style="list-style-type: none"> • Receive (and decrypt if required) the meeting deliverables from the CAB. • Archive and store the meeting deliverables in the NCCA document management system.
2. Check for completeness
<ul style="list-style-type: none"> • Check meeting deliverables for completeness.
3. Confirm participation
<ul style="list-style-type: none"> • Determine if the ERM needs to be attended based on the content of the meeting deliverables. • Send a message to the CAB indicating the participation and where appropriate request any missing information in the meeting deliverables.

3.2.3.2 Action 2.3.2: Confirm ERM date and participation

This action is optional based on agreements made between CAB and sponsor.

Responsible: Sponsor
Executed by: Sponsor role
1. Receive meeting deliverables
<ul style="list-style-type: none"> • Receive (and decrypt if required) the meeting deliverables from the CAB.
2. Confirm participation
<ul style="list-style-type: none"> • Determine if the ERM needs to be attended. • Send a message to the CAB indicating the participation.

3.2.3.3 Action 2.3.3: Perform Evaluation Review Meeting

Responsible: CAB
Executed by: Certifier
In co-operation with: Evaluator (Note: both NCCA and sponsor may attend)
1. ERM will be held
<ul style="list-style-type: none"> • The certifier chairs the meeting using the agenda defined by the assessment plan.

- The ERM deliverables are presented by the evaluator, according to the following guidance:
 - The certifier may 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 ERM deliverables, or items that are not clear, these will be corrected during the meeting, by amending the ERM deliverables where possible and annotating them where amending would take too much time.
 - In exceptional cases the certifier may, in agreement with the certification auditor (if present), decide that presentation of (parts of) ERM deliverables is skipped as they are deemed to be self-explanatory.
- The meeting can have four possible outcomes:
 - 1) All ERM 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 next ERM. In this case, the other deliverables are provisionally approved, and the remaining deliverables are rescheduled (for the final ERM this outcome is not possible and will lead to outcome 4).
 - 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 ERM is nullified, and must be repeated once the evaluator has remedied the not-approved deliverables.

Note: ERM deliverable can only be *provisionally* approved as subsequent ERMs may invalidate the verdicts due to new information found. The final formal approval takes place in Step 2.4: Generate final evaluation & certification reports.

3.2.3.4 Action 2.3.4: Draft meeting minutes

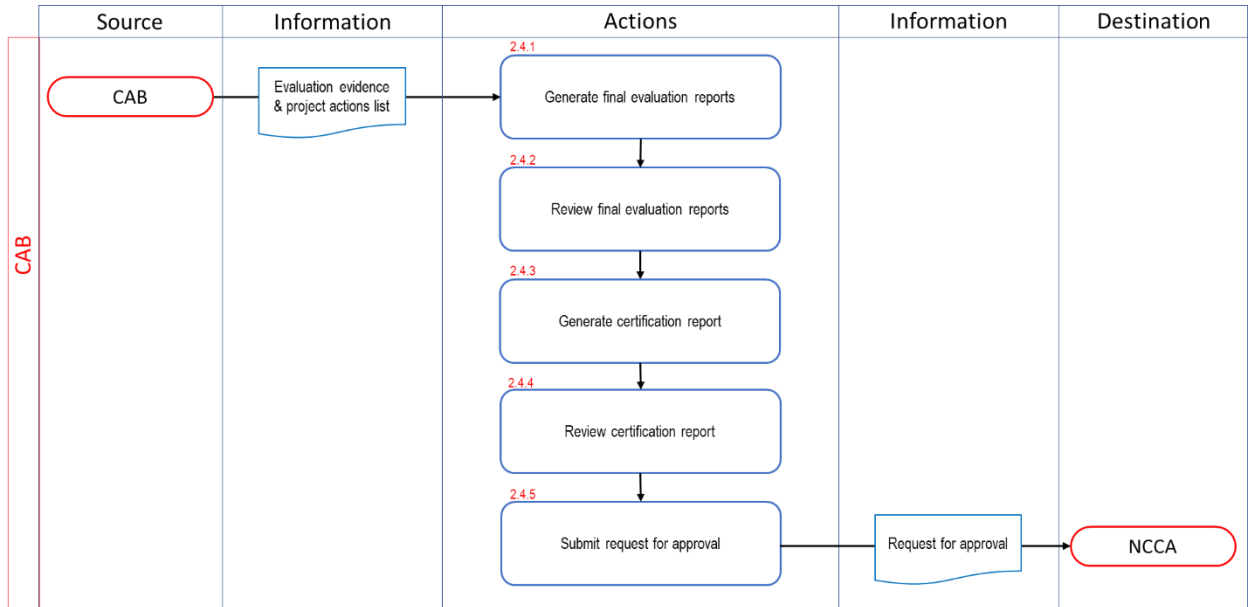
Responsible: CAB
Executed by: Certifier or evaluator
1. Create meeting minutes

- Either the certifier or the evaluator will draft meeting minutes to record all issues raised during the meeting, the decisions made and the conclusion. The meeting minutes shall contain the following topics:
 - The date, duration, location and attendees of the meeting;
 - All evaluator evidence including the Certifier Review Report that has been delivered for discussion at the ERM shall be listed by name and version;
 - Intermediate conclusions or verdicts and decisions made in regard to a specific deliverable shall be recorded (i.e. amended/annotated during meeting, further handling by email or renewed discussion of the issue at a rescheduled meeting);
 - All revised evaluator evidence including the Certifier Review Report coming out of the ERM shall be listed by name and version. Ideally, outputs of a meeting, should be attachments to the meeting minutes;
 - The final conclusion of the meeting (see the 4 possible outcomes of a meeting as described in previous step);
 - A reference to the (updated) project action list arising from the meeting.
- Either the certifier or the evaluator will create (or update) the project actions list based on the actions that were agreed upon during the ERM. This project actions list shall meet the following requirements:
 - Every action is uniquely identified in order to trace the action;
 - When an action relates to a evaluator evidence, the action should refer to the specific deliverable, including its version and location within that deliverable (e.g. section number, slide number);
 - Every action should be self-explanatory, not relying on (undocumented) discussion in the meeting for clarity;
 - When an action is closed, the action item should clearly state how the actions was closed, e.g. by reference to the specific deliverable from the evaluator evidence in where the action was closed;
 - Per action item it shall be noted whether and when the certifier has approved its closure.
- Send the meeting minutes and the updated project actions list to the meeting participants for confirmation (and in case of no NCCA participation: to the NCCA for information).
- Revise the meeting minutes and project actions list based on comments received.

Note 1: No full meeting minutes are required to record every aspect of discussion, but rather these minutes serve as a record summary of issues discussed, the verdicts and conclusions made during the meeting.

Note 2: The meeting minutes and updated project actions list needs to be provided within 3 working days after the meeting.

3.2.4 Step 2.4: Generate final evaluation & certification reports



3.2.4.1 Action 2.4.1: Create final evaluator evidence

Responsible: CAB
Executed by: Evaluator
1. Finalise all evaluator evidence
<ul style="list-style-type: none"> If not already done so for the final ERM, generate the Evaluation Technical Report (ETR) to collate all evaluator evidence and provide a conclusion of the overall verdict of the evaluation findings. Also generate a ETRfC, STAR and analysis of the ST-Lite, as applicable in accordance with the assessment plan. Revise any evaluator evidence necessary to close action items from the project action list, documenting a disposition of how they have been addressed.
2. Verify all final evaluator evidence
<ul style="list-style-type: none"> Once all verdicts are Pass and the evaluator considers all action items addressed, the final package of evaluator evidence (including ETR and other documents) needs approval and authorization before submitting for formal CAB review.
3. Submit all final evaluator evidence
<ul style="list-style-type: none"> Send the final package of evaluator evidence, along with the project actions list, and a copy of the final ST (and ST-Lite, if applicable) to the certifier for formal review.

3.2.4.2 Action 2.4.2: Review final evaluator evidence

Responsible: CAB	
Executed by: Certifier	
1.	Receive final package of evaluator evidence, the project actions list, and final ST (and ST-Lite if applicable) from the evaluator
	<ul style="list-style-type: none"> Ensure documents received are recorded in accordance with the ISO/IEC 17065.
2.	Review final package of evaluator evidence
	<ul style="list-style-type: none"> Determine whether all open action items from the project actions list have been addressed, and confirm closure or record items still not satisfactorily addressed in a Certifier Review Report. Review all finalised evaluator evidence, ETR and other documents, and record any comment in a Certifier Review Report. The review must ensure that the evaluator conclusions are consistent with the evidence adduced and that the accepted evaluation criteria and evaluation methods have been correctly applied. Check the final ST (and ST-Lite if applicable) for consistency with the final package of evaluator evidence and ensure that all ASE related comments are addressed.
3.	Deliver Certifier Review Report to the evaluator and the certification auditor along with the associated package of evaluator evidence
	<ul style="list-style-type: none"> If there are comments that require an update of the evaluator evidence, the Certifier Review Report is sent directly to the evaluator for the comments to be addressed and in copy to the certification auditor. This would require an iteration of Action 2.4.1: Create final evaluator evidence and Action 2.4.2: Review final evaluator evidence.
4.	Close Review Reports
	<ul style="list-style-type: none"> Once the certifier has confirmed all comments recorded in the Certifier Review Report have been closed, it can be closed with a formal acceptance of the evaluation work.

3.2.4.3 Action 2.4.3: Generate certification report

Responsible: CAB	
Executed by: Certifier	
1.	Generate certification report
	<ul style="list-style-type: none"> Create a draft version of the Certification Report.

<ul style="list-style-type: none"> • Check consistency with the mandatory EUCC content and format requirements of certification reports (ref. EUCC Annex V).
2. Create certificate
<ul style="list-style-type: none"> • Create draft version of the Certificate. • Check consistency with the mandatory EUCC content and format requirements of certificates (ref. EUCC Annex VII and VIII). • Check EUCC validity requirements (ref. EUCC article 12), and update the certificate validity as appropriate.
3. Send draft certification report and certificate for review
<ul style="list-style-type: none"> • Submit the draft Certification Report and draft certificate for review and acceptance to the evaluator (and in copy to the sponsor).

3.2.4.4 Action 2.4.4: Review certification report

<p>Responsible: CAB</p> <p>Executed by: Evaluator</p> <p>In co-operation with: Sponsor</p>
1. Receive draft certification report and draft certificate
<ul style="list-style-type: none"> • Receive the draft Certification Report and draft certificate from the certifier.
2. Assess draft certification report and draft certificate
<ul style="list-style-type: none"> • Check the draft certification report for: <ul style="list-style-type: none"> ○ Correctness with the ST/PP and ETR, and any other inconsistencies ○ Proprietary information that is unsuitable for publication • Check the draft certificate for: <ul style="list-style-type: none"> ○ Correctness with the ST/PP and ETR, and any other inconsistencies • Consult with the sponsor and accept the draft certification report and draft certificate.
3. Send review comments and/or acceptance to the certifier
<ul style="list-style-type: none"> • The evaluator sends the review comments and/or acceptance to the certifier after consulting the sponsor.

3.2.4.5 Action 2.4.5: Submit request for approval

Responsible: CAB

Executed by: Certifier	
1. Finalise certification report	<ul style="list-style-type: none"> • Receive comments and/or acceptance from the evaluator (and sponsor). • Update certification report and certificate based on received comments.
2. Decide on certification	<ul style="list-style-type: none"> • In accordance with ISO/IEC 17065 the CAB needs to take a formal decision on certification based on the evaluation results and the review thereof.
3. Draft request for approval	<ul style="list-style-type: none"> • Once the certification decision is positive, download the Request for approval form from the NCCA website. • Fill in the required fields. • Sign the request for approval.
4. Submit request	<ul style="list-style-type: none"> • Gather the following documents: <ul style="list-style-type: none"> ○ The final ETR, including the underlying evaluator evidence (and the ETRfC and STAR if applicable) ○ The final ST (and ST-Lite if applicable) ○ The link to the sponsor’s website containing the supplementary cybersecurity information referred to in article 55 of the CSA ○ The Certifier Review Report(s) including the project actions list with the agreed dispositions ○ The certification report ○ The draft certificate • Send the request for approval form and the documents mentioned above to the NCCA.



The reception of the request for approval is a milestone for the NCCA after which the request has to be processed with the legally defined terms.

3.2.5 Step 2.5: Project monitoring

Certification is in general a process that continues for some weeks, if not months. The assessment plan on which the NCCA based its initial approval may therefore be subject to changes and these changes may require a renewed approval.

Also the certification process may be terminated prematurely on request of either the sponsor or the CAB. The NCCA may also terminate the certification process under certain conditions in which case the approval of the assessment plan is withdrawn by a revocation decision.

The above two activities are combined into an asynchronous step that can be executed independent of the other steps and are further described below.

Changes in the approved assessment plan

An assessment plan forms the baseline for the evaluation and certification work and the approval by the NCCA. As it is agreed upon by all involved parties it cannot be changed or executed in a different way by a single party. Possible changes that might have an impact can be categorised as follows:

- Re-scheduling of milestones; these include both deliverables and review meetings: The assigned certification auditor (and if applicable external experts) expects to review meeting deliverables and attend ERMs based on the agreed planning. Time is reserved in their agenda which is difficult to re-allocate if deliverables are not submitted at the agreed date. The same is also true for the delivery date of the request for approval with its associated documents and any re-scheduling of meetings;
- TOE scope changes: the (draft) ST/PP is reviewed during the notification phase, and is accepted as having a valid TOE scope by the approval of the assessment plan by the NCCA. Changes to the TOE scope mostly have an impact on the certification and evaluation work already performed and could in extreme cases even result in inappropriate removal of security features or inappropriate additions of assumptions;
- Evaluation scope/approach changes: changes to the evaluation scope (e.g. more or less development sites to be audited), additional/different deliverables, or when additional review meetings are needed, will always have an impact on the evaluation and certification work and the approval of the assessment plan by the NCCA;
- Certification project staffing assignment changes: the certification auditor only accepts deliverables that are authorized by the persons listed in the assessment plan.

All type of changes, including the rationale for the change, must be reported without undue delay so that their impact against the formal approval of assessment plan can be determined. Changes need to be communicated initially via e-mail. The impact is assessed by the NCCA as the assessment plan is used to verify that the evaluation and certification work has been conducted according to the assessment plan. This verification is part of the assessment of the CABs request to issue a certificate (see Action 3.1.3: Review ETR, CR and certificate). Based on its assessment, the NCCA may require the CAB to make an update of assessment plan so that an formal approval of it can be re-issued.

Changes in certification staffing (resulting in a change of point of contact at the CAB) and rescheduling of a ERM and meeting deliverables have to be communicated at the latest 5 working days before it was planned for the meeting deliverables to be sent to the NCCA/certification auditor. Preferably this change is communicated in combination with a proposal for a new delivery and meeting date. The NCCA/certification auditor will assess the change and where necessary seek agreement on a new delivery and meeting date. These type of changes generally do not require an update of the assessment plan.

An update to the assessment plan will generally be required when there is a change to the TOE scope or evaluation scope/approach. However it is not always the case that all certification scope/approach changes require an update to the assessment plan. For example, a change to discuss the ALC site audit checklist in ERM1 rather than ERM2 is a change in certification approach, but this change is considered minor and could be agreed by the NCCA through an e-mail.

Termination of the certification process

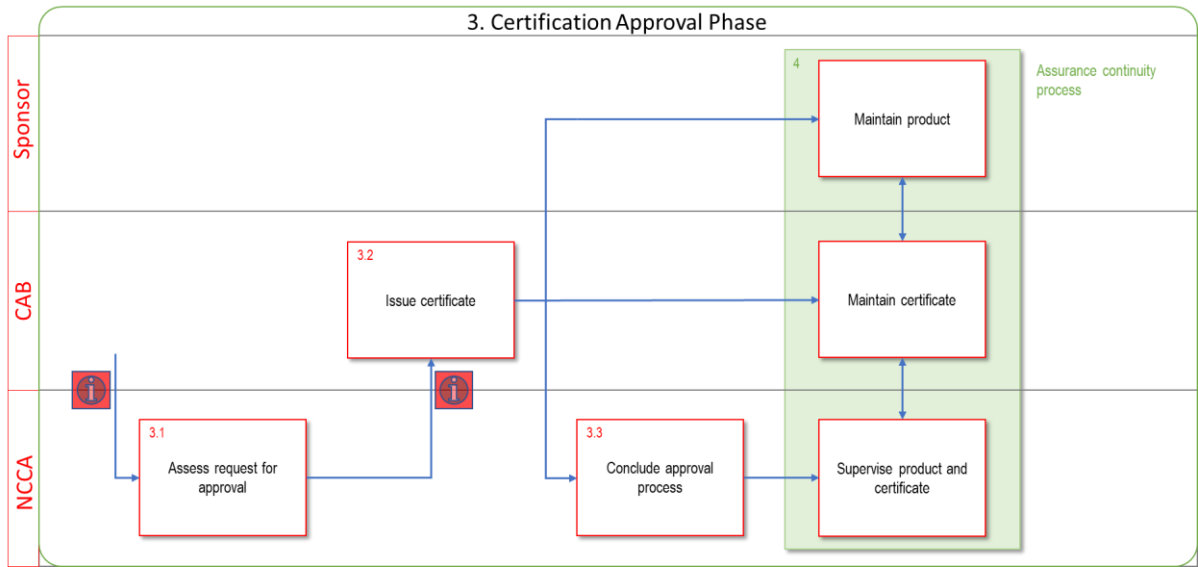
In most cases a certification is executed in accordance with the assessment plan and the delivery schedule mentioned, even though slight changes in the planned dates might occur.

However, if during a certification process there are no evaluation and certification activities for more than 6 months, the NCCA may decide to terminate the process so that resources are no longer allocated. In case of a monitored certification, the 6 months period will be calculated from the agreed date of the first upcoming ERM. When the certification is not monitored, the 6 Months will be calculated from the agreed delivery date of the request for approval.

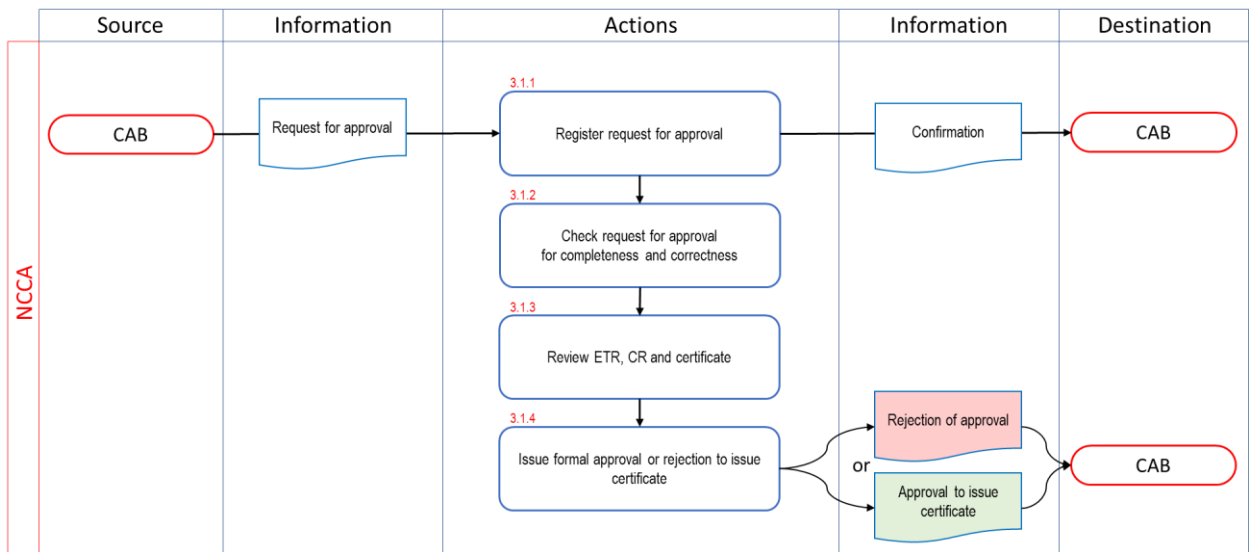
In exceptional cases also the CAB may decide that they do not want to continue the certification. In this situation the NCCA must officially be informed of such request to terminate the certification process and the rationale for it.

In either case the NCCA will document its decision in a [Termination Justification Report](#). Based on this a formal termination decision will be send after which the NCCA will close the project in the NCCA document management system.

3.3 Phase 3: Certification Approval Phase



3.3.1 Step 3.1: Assess request for approval



3.3.1.1 Action 3.1.1: Register request for approval

Responsible: NCCA
Executed by: Certification auditor
1. Receive the request for approval
<ul style="list-style-type: none"> • Receive (and decrypt if required) the request for approval form, and: <ul style="list-style-type: none"> ○ The final ETR, including the underlying evaluator evidence (and the ETRfC and STAR if applicable)

- The final ST (and ST-Lite if applicable)
- The link to the sponsor’s website containing the supplementary cybersecurity information referred to in article 55 of the CSA
- The Certifier Review Report(s) including an overview of the disposition of action items
- The certification report
- The draft certificate
- Archive and register the request for approval and associated documents in the NCCA document management system.
- Confirm the reception of the request for approval to the CAB.

3.3.1.2 Action 3.1.2: Check request for approval for completeness and correctness

Responsible: NCCA
Executed by: Certification auditor
1. Create Approval Review Report
<ul style="list-style-type: none"> ● Create an Approval Review Report to document any discussions and comments related to the notification. <p><i>Note:</i> The Approval Review Report is intended to collect findings on the request for approval document, and forms the basis for the formal approval or rejection to issue a certificate.</p>
2. Check the request for approval for completeness
<ul style="list-style-type: none"> ● Perform a high level check on the following items as a minimum: <ul style="list-style-type: none"> ○ Does the request for approval include all required documents? ○ Are all required fields in the request for approval form filled in? ○ Is the request for approval form signed by the CAB? ○ Is the accreditation of the CAB still valid (i.e. not suspended or revoked)? ○ Is the CAB still authorised? ● Notify CAB in case the request for approval is incomplete and request missing information. ● Update the Approval Review Report with findings. ● Continue with Action 3.1.4: Issue formal approval or rejection to issue certificate in case the request for approval remains incomplete. This will lead to a rejection to

issue a certificate. Otherwise continue with Action 3.1.3: Review ETR, CR and certificate.

3.3.1.3 Action 3.1.3: Review ETR, CR and certificate

Responsible: NCCA Executed by: Certification auditor In co-operation with: Optionally with an external expert
1. Inform external expert
<ul style="list-style-type: none"> • If an external expert is involved, provide the external expert with the request for approval and associated documents.
2. Review the Certifier Review Report(s) and overview of the disposition of action items
<ul style="list-style-type: none"> • Perform a detailed review of the Certifier Review Report(s) and overview of the disposition of action items based on the Approval review checklist and the knowledge gained while attending the ERM(s) (if applicable). Focus areas are: <ul style="list-style-type: none"> ○ Determination that the certifier did a thorough review of the final ETR, including the underlying evaluator evidence and the ETRfC and STAR if applicable. Check that the certifier has verified the: <ul style="list-style-type: none"> ▪ Correct application of the evaluation methodology; ▪ Correctness of the completed evaluator checklist; ▪ Consistency in version numbers of the final ETR, including the underlying evaluator evidence and the ETRfC and STAR if applicable, the product evaluated, including the ST (and ST-Lite if applicable) and its guidance documentation. ○ Closure and correct disposition of the action items. • Discuss any items that are unclear with the CAB to gain necessary clarification in order to finalise the review. • Update the Approval Review Report with findings.
3. Review the certification report and draft certificate
<ul style="list-style-type: none"> • Perform a detailed review of the certification report and draft certificate based on the Approval review checklist. Focus areas are: <ul style="list-style-type: none"> ○ Consistency with the ETR, including version numbers. ○ Consistency with the mandatory content and format requirements of EUCC scheme certificates and certification reports. • Discuss any items that are unclear with the CAB to gain necessary clarification in order to finalise the review.

<ul style="list-style-type: none"> • Update the Approval Review Report with findings.
4. Review the executed evaluation and certification process
<ul style="list-style-type: none"> • Check that the evaluation and certification process was executed in conformance with the approved assessment plan. • Update and finalise the Approval Review Report with findings.

3.3.1.4 Action 3.1.4: Issue formal approval or rejection to issue certificate

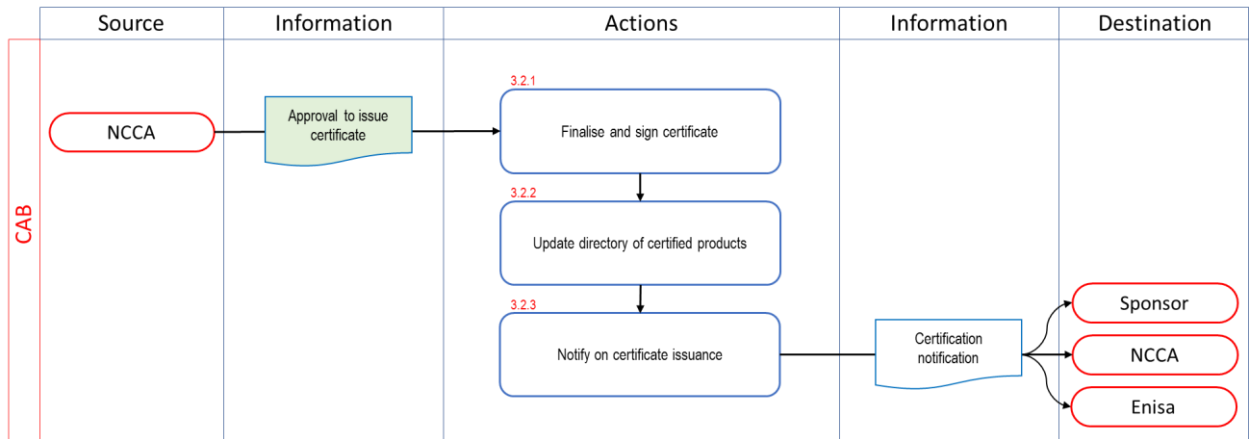
Responsible: NCCA
Executed by: Audit supervisor
1. Validation of the Approval Review Report
<ul style="list-style-type: none"> • Check if the Approval Review Report is complete, correct and consistent. • Sign off the Approval Review Report.
2. Draft a formal approval or rejection letter
<ul style="list-style-type: none"> • Fill-in the applicable NCCA letter template. • Have the applicable letter signed.
3. Submit the formal approval or rejection letter to the CAB
<ul style="list-style-type: none"> • Send the letter to the CAB.



The approval to issue a certificate is a milestone for the CAB after which the certificate can be formally issued.

In case of rejection the certification process stops and the CAB is not allowed to issue an EUCC certificate. A new submission of a corrected Request for Approval is required to restart the process.

3.3.2 Step 3.2: Issue certificate



3.3.2.1 Action 3.2.1: Finalise and sign certificate

Responsible: CAB	
Executed by: Certifier/Certifications manager	
1. Receive approval to issue certificate	
	<ul style="list-style-type: none"> Record approval in accordance with the applicable certification procedure.
2. Pre-notify ENISA	
	<ul style="list-style-type: none"> Request ENISA for a specific EUCC mark and label, including a QR-code to be placed on the certificate. <p><i>Note:</i> ENISA will develop a procedure for the release of the EUCC mark and label, including the QR code. This most likely will involve the CAB to provide a XML file containing information derived from the Certification Report.</p>
3. Update certificate	
	<ul style="list-style-type: none"> Update the certificate with the EUCC mark and label.
4. Sign certificate	
	<ul style="list-style-type: none"> Have the certificate signed by an authorised person.

3.3.2.2 Action 3.2.2: Update directory of certified products

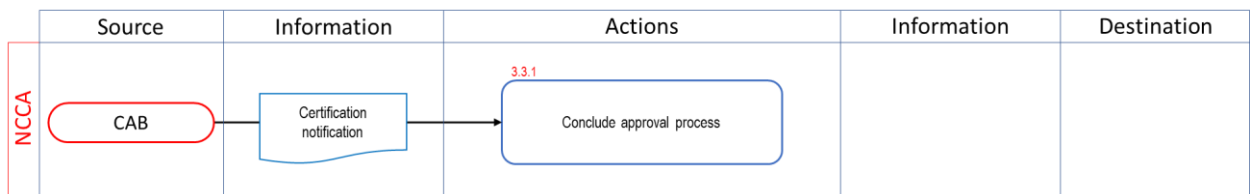
Responsible: CAB	
Executed by: Certifier/Certifications manager	
1. Register certification	
	<ul style="list-style-type: none"> Add the certification to the directory of certified products.

<ul style="list-style-type: none"> • Publish the certification on the CAB’s website (when appropriate).
2. Close certification files
<ul style="list-style-type: none"> • Finish certification project and archive all files in accordance with applicable certification procedures. <p><i>Note:</i> In accordance with EUCC (article 40), all records shall be securely and accessibly stored for a period of at least five (5) years after the withdrawal of the certificate.</p>

3.3.2.3 Action 3.2.3: Notify on certificate issuance

Responsible: CAB	
Executed by: Certifier/Certifications manager	
1. Notify Sponsor	<ul style="list-style-type: none"> • Inform sponsor that the certificate has been issued. • Send certificate in electronic form to the sponsor. A paper version may additionally be provided.
2. Notify NCCA	<ul style="list-style-type: none"> • Inform NCCA that the certificate has been issued. • Send certificate, certification report and final ST(ST-Lite)/PP in PDF-form to the NCCA.
3. Notify ENISA	<ul style="list-style-type: none"> • Inform ENISA that the certificate has been issued. • Send certificate, certification report and final ST(ST-Lite)/PP in PDF-form to ENISA in accordance to their prescribes procedures.

3.3.3 Step 3.3: Conclude approval process



3.3.3.1 Action 3.3.1: Conclude approval process

Responsible: NCCA
Executed by: Certification Auditor

1. Receive certificate and related documents
<ul style="list-style-type: none">• Receive the certificate, certification report and final ST(ST-Lite)/PP.• Archive and register the documents in the NCCA document management system.
2. Publish certification on CCRA website ⁴
<ul style="list-style-type: none">• Publish the certificate, certification report and final ST(ST-Lite)/PP on the commoncriteriaportal.org website.<ul style="list-style-type: none">○ Login to the member section of the CCRA website○ Go to CCRA area○ Add certification record and complete web entry.• Notify sponsor and CAB that the certification has been published on the CCRA website.
3. Close audit file
<ul style="list-style-type: none">• Close the project in the NCCA document management system.

⁴ This step will only be performed when the CCRA discussions have been concluded successfully.

4. Assurance continuity process

This chapter is work in progress and will be updated in the near future. The text below may serve as a guideline on how the maintenance process will be implemented. In any case the requirements from both EUCC Annex IV “Assurance Continuity and certificate review” and the CCRA supporting document “Assurance Continuity: CCRA Requirements” apply whereby the EUCC requirements take precedence.

In accordance with EUCC Annex IV “Assurance Continuity and certificate review” the sponsor can apply for a review of the certificate in the following cases:

- the EUCC certificate is due to expire within nine months;
- there has been a change either in the certified TOE or in another factor which could impact its security functionality;
- the sponsor demands that the vulnerability assessment is carried out again in order to reconfirm the EUCC certificate’s assurance associated with the TOE’s resistance against present cyberattacks.

The CAB that issued the certificate will then perform maintenance activities related to the following:

- a re-assessment if an unchanged certified ICT product still meets its security requirements;
- an evaluation of the impacts of changes to a certified ICT product on its certification;
- if included in the certification, the application of patches in accordance with an assessed patch management process;
- if included, the review of the certificate holder’s lifecycle management or production processes.

The following procedure applies:

- The sponsor submits an application form to the CAB with the request to perform the necessary activities to update the certificate. This step is similar to Step 1.1: Prepare for certification as described in section 3.1.1;
- In case the sponsor applies for an evaluation of the impacts of changes to a certified ICT product on its certification, the CAB assesses the IAR in consultation with the original ITSEF and decides whether a maintenance process can be followed or that re-certification is necessary;
- The *EUCC notification form* shall refer to an Impact Analysis Report (IAR) as defined in the CCRA supporting document “Assurance Continuity: CCRA Requirements”;

Remarks:

- In case of re-certification the standard procedure defined in section 3.2 Phase 2: Evaluation and Review Phase is applied. Depending on the nature of the alterations, it is possible that items from the earlier certification (of the 'same' TOE) are re-used. The details of the certification process and the options for re-use shall be described in the assessment plan.

5. The vulnerability management and disclosure process

This chapter is work in progress and will be updated in the near future. In any case the requirements from EUCC Chapter VI “Vulnerability management and disclosure” apply.

Annex A Content and presentation of Evaluation Review Meetings

1. General Requirements for the evaluator presentations

The review of the evaluation activities shall be based on evaluation evidence that is presented during Evaluation Review Meetings. In the meeting deliverables the evaluator shows *how* all content and evaluator action elements for the processing of the assurance components that are relevant for the evaluation are met. This must be done within a presentation, and may additionally be supported by an annex or other evaluator analysis documents. The evaluator shall also provide a checklist indicating where evaluator action items are demonstrated in the meeting deliverables, to a level of content and presentation elements.

At the first Evaluation Review Meeting (ERM1) the checklist for the entire assurance level shall be presented, populated as appropriate for ERM1. This document is then further populated for subsequent evaluation meetings. This means that the checklist presented in the final Evaluation Review Meeting (ERM3) will be completely populated and should contain only 'pass' verdicts.

Where the additional requirements and methodology defined by the EUCC scheme describes explicit reporting to be provided, this explicit reporting needs to be automatically provided as part of the evaluation documentation. For example, the EUCC State-of-the-Art document 'Security Architecture requirements (ADV_ARC) for smart cards and similar devices' explicitly describes content requirements, and this needs to be reported on a work unit level, either in a separate document or alternatively in the evaluation meeting presentation. The reporting should be added into the appropriate meetings.

2. First Evaluation Review Meeting

2.1 Goal of the First Evaluation Review Meeting

The intent of the first ERM is for the evaluator to demonstrate to the certifier its understanding of the product/TOE. The focus lies on the evaluation activities related to the security requirements and the operation and design of the product. With this understanding the evaluator should have a good starting point to perform a vulnerability analysis and develop a functional and penetration test plan.

The certifier who has performed a review on the meeting deliverables shall challenge the evaluator on its understanding of the product/TOE.

2.2 First Evaluation Review Meeting Deliverables

The deliverables for the first ERM consist of the following:

- Updated ST and the ASE evaluation results;
- The ADV Presentation (see Chapter 6);
- The Implementation Representation Sampling Rationale (see Chapter7);
- The ADV/AGD Reference Document (see Chapter 8) and all guidance documents that this document refers to;
- The Configuration Item Identification Presentation (see Chapter 9);
- The Consultancy/Evaluation Improvement Presentation (see Chapter 16);
- Checklist of all evaluator action items and content and presentation elements relevant for the claimed assurance level (populated to show where the evaluator actions and c&p elements relevant to ERM1 are demonstrated, see Chapter 17).
- Any other observations that were found before this meeting and are deemed relevant.

3. Second Evaluation Review Meeting

3.1 Goal of the Second Evaluation Review Meeting

The intent of the second ERM is for the evaluator to present to the certifier its vulnerability analysis and the developed functional and penetration test plans.

The certifier who has performed a review on the meeting deliverables shall challenge the evaluator on the soundness of vulnerability analysis and the tests proposed in the test plans.

3.2 Second Evaluation Review Meeting Deliverables

The deliverables for the second ERM consist of the following:

- Any First Evaluation Meeting Deliverables that were rescheduled to this meeting;
- The Implementation Representation Presentation (see section 10);
- The ATE/AVA Test plan Presentation (see section 11);
- The ATE/AVA test descriptions (see section 12);
- The ALC Presentation, including ALC verification plan (see section 13);
- Updated Checklist showing where the evaluator actions and c&p elements relevant to ERM1 and ERM2 are demonstrated (see Chapter 17);
- Any other observations that were found before this meeting and are deemed relevant.

4. Final Evaluation Review Meeting

4.1 Goal of the Final Evaluation Review Meeting

The intent of the final ERM is for the evaluator to present to the certifier the results of the functional and penetration tests, and also the results of the ALC activities.

The certifier who has performed a review on the meeting deliverables shall question the evaluator on the analysis of the results.

4.2 Final Evaluation Review Meeting Deliverables

The deliverables for the final ERM consist of the following:

- Any Second Evaluation Meeting Deliverables that were rescheduled to this meeting;
- The final ST (and ST-Lite if applicable);
- The final guidance documentation for the TOE satisfying AGD_PRE and AGD_OPE.
- The ATE/AVA test results (see section 14);
- The ALC Results Presentation and draft STAR (if applicable) (see section 15);
- Completed Checklist showing where all evaluator actions items and content and presentation elements relevant for the claimed assurance level are demonstrated (see Chapter 17);
- Draft ETR, draft ETRfc (if applicable);
- Any further observations that were found before this meeting and are deemed relevant.

5. 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 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 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 CAB and to the ISO/IEC 17065 and the ISO/IEC 17025 standard.

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.

6. 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 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
- Other items based on applicable mandatory methodology (e.g. EUCC Annex 'Composite product evaluation for smartcards and similar devices')

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

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 and every developer action item (down to the level of content and presentation elements).

The alternative method for ADV is using the implementation representation as a basis for the higher levels of design representation (i.e. the CCRA/SOG-IS collection of developer evidence process). This approach can only be used in cases where the laboratory has a vast 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.

In order for a CAB to use the alternative ADV method, three conditions must be met:

- The NCCA must be informed. Therefore the use of this method must be documented in the assessment plan.
- Even if ADV_IMP.1 is claimed, 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 11.2).

The alternative method exploits the fact that the laboratory is so familiar with the TOE type that the laboratory can:

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

Under those three conditions, the whole of ADV_TDS is considered to be defined by the implementation representation, that is:

- Modules are sets of implementation representation (e.g. source code, VHDL), 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 vast 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/ADV_IMP.2 requirements (as considered in section 10.2 or 10.3 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.

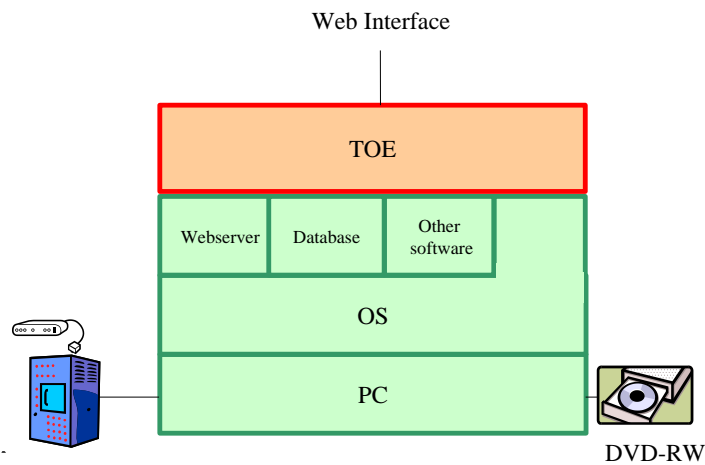
6.1 The TOE and the TSFI

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

Observe that the developer has to present for ADV_FSP.6 a formal model for the TSFI which has to be addressed in addition. Refer to Section 6.6 for further details. In this case the alternative ADV method cannot be applied.

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.

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

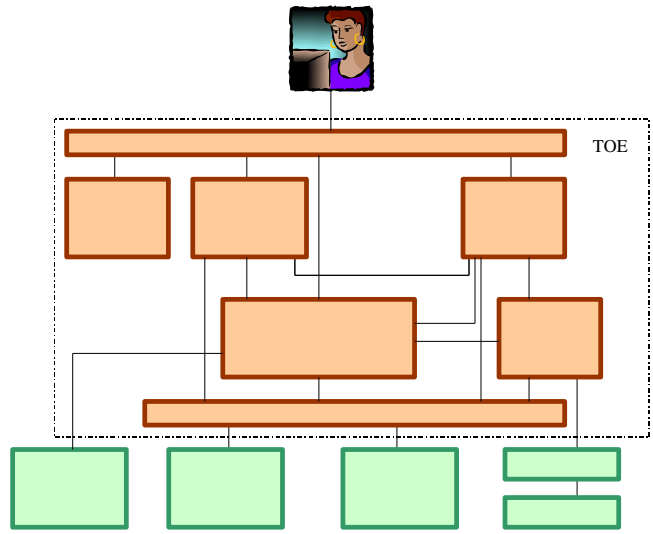
6.2 Subsystems

6.2.1 The regular ADV method for subsystems

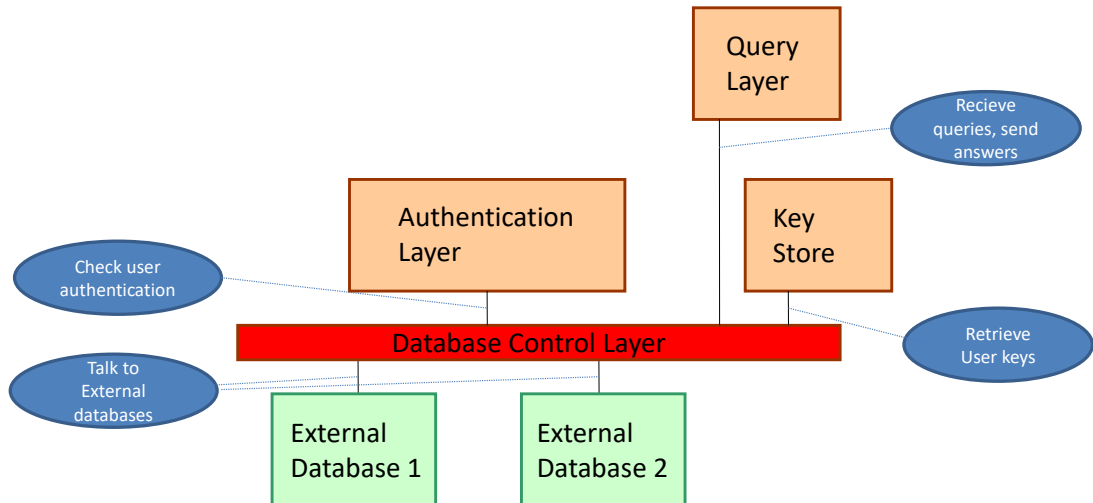
1. The evaluator presents a subsystem level model of the TOE (possibly with some parts of the environment):

- this model shall be sensible and useful⁵;
 - 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 the subsystem level model:



Example of the subsystem behaviour and interaction (of the red subsystem)



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.

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.

Result: The evaluator demonstrates that he understands the TOE design and that it identifies and describes all subsystems

6.2.2 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 earlier in this section, 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 6.3.2 are required at this point.

Observe that the developer has to present for ADV_TDS.6 a formal model for the TSF subsystems which cannot be addressed under the alternative ADV method. Refer to Section 6.6 for further details.

6.3 Modules

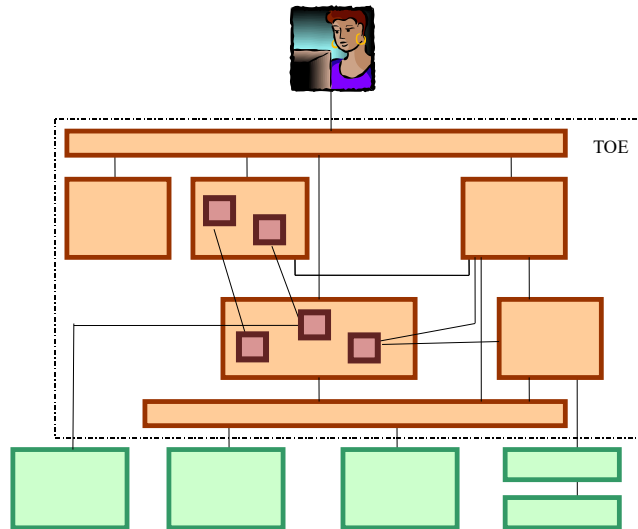
6.3.1 The regular ADV method for modules

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 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).

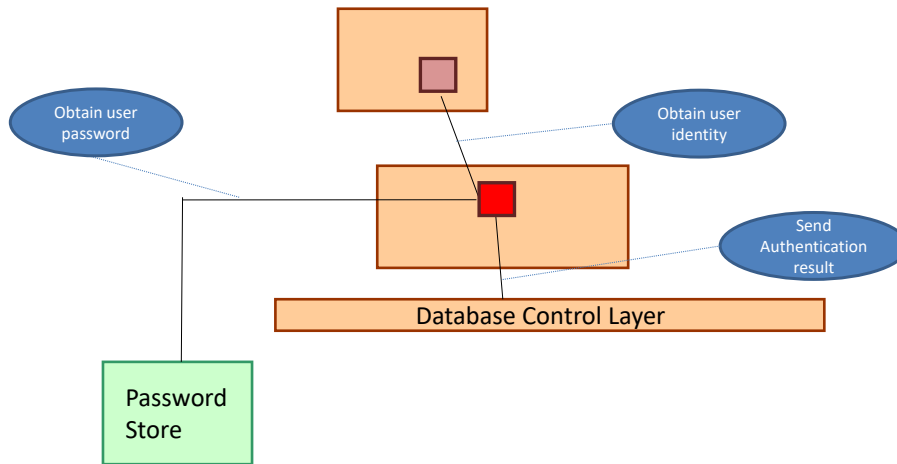
Example of the module level model:

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.



Example of the module behaviour 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.

6.3.2 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 modes are implicitly categorized as SFR-enforcing. It is at the time of tracing SFRs to the implementation representation⁹ (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-

⁹ See section 6.4.2

supporting, depending on the role the evaluator determines it plays in achieving the SFR. The evaluator can use their vast 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 provide or present the full mapping of the SFRs to the modules. The presentation must only provide evidence by showing 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.

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 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).

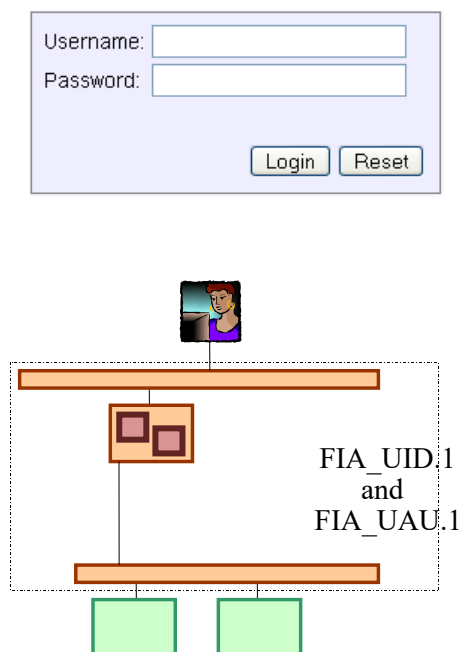
Result: The evaluator demonstrates that he understands the TOE design at module level and that modules are identified and described.

6.4 Tracing SFRs to TSFI, Subsystems and Modules

6.4.1 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.

Example of relation between SFRs, TSFI, subsystems and modules



Result: The evaluator demonstrates that he understands the TOE Design and FSP, and their completeness w.r.t. the SFRs.

6.4.2 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 6.3.2 above. Therefore, no additional 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 vast 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 FSP, and their completeness w.r.t. the SFRs.

6.5 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 a Protection Profile) 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-compiled 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,

6.6 Formal Security Modelling and other Formal Aspects of ADV (Optional)

In case the evaluation of the assurance component ADV_SPM.1 is in the scope of the evaluation, the evaluator adds the evaluation results to the ADV Presentation.

The evaluator includes the assessment for formal modelling aspects in other assurance classes (if claimed) in this part of the presentation as well.

Observe, that in the case that any formal modelling is claimed, the Alternative ADV Approach **cannot** be applied. This includes requirements such as ADV_TDS.6 as discussed above because the developer has to formally model their behaviour and therefore also define the TSF subsystems in the developer evidence.

For ADV_SPM.1 “Security policy modelling” the evaluator presents that:

- the security policy is modelled in a formal style;
- all policies modelled define the security of the TOE and that the formal proof shows that TOE cannot reach an insecure state;
- the correspondence between the model and the functional specification is at the right level of formality;
- the functional specification is consistent and complete with respect to the model.

For ADV_FSP.6 “Complete semi-formal specification with additional formal specification” the evaluator presents the results of the assessment:

- of the formal specification of the TSFI supported by informal explanatory text where appropriate.

For ADV_TDS.6 “Complete semiformal modular design with formal high-level design presentation” the evaluation presents the results of the assessment of

- the formal specification of the TSF subsystems supported by informal explanatory text where appropriate
- the proof of correspondence between the formal specifications of the TSF subsystems and the functional specification.

Result: The evaluator demonstrates that the formal modelling, any associated proofs and explanatory text meet all the requirements, and that the formal specification is consistent with all other ADV evidence.

7. Implementation Representation Sampling Rationale

This section consists of three 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
3. ADV_IMP.2 is used in conjunction with either method.

7.1 The Sampling Rationale for ADV_IMP.1 with the Regular 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 entire set. The actual evaluator work of ADV_IMP is handled in the TOE Implementation Representation presentation (see Chapter 10).

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.

7.2 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 ERM1 deliverables.

The evaluator uses the implementation representation also to acquire the information about the modular design of the system. As a consequence, 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 ERM1 deliverables.

Result: The 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.

7.3 The Sampling Rationale for ADV_IMP.2

Since ADV_IMP.2 is used, the entire implementation representation is considered, and there is no sampling for the correspondence between the implementation representation and the design.

8. 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.

8.1 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.

No example, as it is self-explanatory

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

8.2 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.

No example, as it is self-explanatory

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

9. The Configuration Item Identification Presentation

This is a relatively small presentation of a single ALC item: the identification of configuration items (as required by ALC_CMC.2/3/4/5.2C. 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 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). The method of identification used by the user should be covered under section “8.2 The AGD part”. 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 remainder of ALC is handled in the ALC presentation (see section 13).

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

No example, as it is self-explanatory

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

10. TOE Implementation Representation Presentation

This section consists of three 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
3. ADV_IMP.2 is used in conjunction with either method

10.1 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.

10.2 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.
- A mapping (in the form of a table) of all SFRs to the implementation representation.
- How the SFRs are 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.

10.3 ADV_IMP.2 used in conjunction with either method

The evaluator shall present:

- Findings of implementation representation inspection, including the form of the implementation representation inspected.
- A mapping (in the form of a table) of all SFRs to the implementation representation.
- How the SFRs are 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.

10.4 Presentation of TSF Internals (ADV_INT) (optional)

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

If one of the ADV_INT assurance components are claimed for the evaluation the evaluator presents the evaluation result as part of the TOE implementation representation in the second evaluation meeting.

The evaluator shall present:

- The criteria the developer used for well-structuredness and complexity of the TSF internals
- The results of the assessment of the well-structuredness and complexity of the TSF internals on the level required for the relevant assurance component. Under the regular ADV method this assessment is based on the developer internal analysis, which is then confirmed during the analysis of the implementation representation. Under the alternative ADV approach, this is based entirely on the evaluator findings during analysis of the implementation representation, which may be backed up by reports from static analysis tools.

Result: The evaluator shall report the criteria used by the developer and demonstrate that the well-structuredness and complexity requirements of the TSF internals are met.

11. The ATE/AVA Test Plan Presentation

11.1 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 of the above.
3. The evaluator will analyse all the other evidence and come up with a vulnerability analysis and penetration test plan based on this evidence.

11.2 Two methods for Developer ATE

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

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.

In order for a laboratory to use the alternative ATE method, the CB must give permission and the NCCA must be informed. Therefore, the use of this method must be documented in the assessment plan.

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.

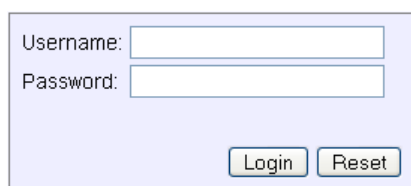
11.3 Coverage

11.3.1 Coverage under the regular ATE method

The evaluator shall present¹⁰:

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

Example of coverage



A screenshot of a login form. It features two input fields: 'Username:' and 'Password:'. Below the fields are two buttons: 'Login' and 'Reset'.

TEST 1: Non-existent username

TEST 2: Incorrect password

TEST 3: Empty password

TEST 4: Correct password

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

11.3.2 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*

¹⁰ This presentation may be integrated with the “Tracing SFRs to TSFI and Subsystems” presentation (Section 6.4).

- *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.

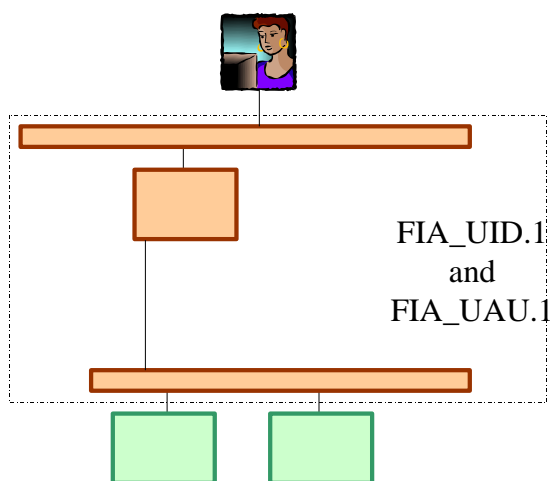
11.4 Depth

11.4.1 Depth under the regular ATE method

The evaluator shall present¹¹:

- 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)

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 subsystems, modules or the implementation representation of the TSF (details depend on the ATE_DPT component level relevant of the evaluation) have been tested by the developer.

11.4.2 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;

¹¹ This presentation may be integrated with the "Tracing SFRs to TSFI and Subsystems" presentation (Section 6.4).

- 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.

11.5 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.

11.6 Evaluator ATE Test Plan

The evaluator shall present¹²:

- 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.

¹² This presentation may be integrated with the "Tracing SFRs to TSFI and Subsystems" presentation (Section 6.4).

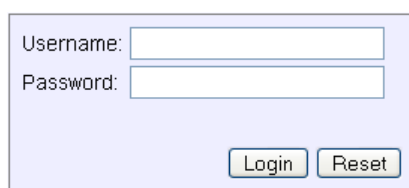
11.7 Evaluator AVA Test Plan

The evaluator shall present¹³:

- 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 TOE Implementation Representation Presentation, see also Section 10);
- 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:



A screenshot of a login form. It features two input fields: 'Username:' and 'Password:'. Below the fields are two buttons: 'Login' and 'Reset'.

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.

¹³ This presentation may be integrated with the "Tracing SFRs to TSFI and Subsystems" presentation (Section 6.4).

12. 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 descriptions (this is a document).

The ATE/AVA Test descriptions shall contain:

- all tests of the ATE and AVA Test Plan 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 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.

13. 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.

The evaluator shall make available the relevant STAR reports (if applicable) for spot checks during the meeting.

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

13.1 Site Visits under this NSP

By default, NO site visits have to be done for evaluations at EAL3 or below. However, this does not mean that no evidence of compliance with ALC should be gathered by the evaluator where ALC_DVS.1 is claimed but no site visit is performed: the evaluator should still obtain evidence from the developer that he indeed follows the described procedures: 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.

14. The ATE/AVA Test Results

The Evaluator shall present¹⁴:

- 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.(authenticat
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

➔

Results
As expected

brightsign your partner in security approval page 14/27

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

¹⁴ It is not intended that this consists of a set of "Pass". Detailed descriptions and screendumps are to be provided where appropriate

15. The ALC Results

1. The evaluator shall present the results of the verification that the lifecycle processes and procedures are applied.
2. The evaluator shall provide a STAR report in accordance with the relevant requirements, if applicable and requested in the application form.

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

16. Consultancy/Evaluation Improvement Presentation

Often, during the consultancy before 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, a Consultancy/Evaluation Improvement presentation is required.

The evaluator shall present:

- 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.
- 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.

It should be noted that such information is only reported in the reports discussed in the evaluation meetings, and not in the final reporting (i.e. this information is not included in the ETR document (including any ETRfc) or in the Certification Report.

17. 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 evaluation to the evaluator evidence. 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.

Note that this table may need to be expanded with additional elements in case of composite evaluations.

CC Family	Element	Report reference, including slide# or section #	Verdict (P/F/I)
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		

CC Family	Element	Report reference, including slide# or section #	Verdict (P/F/I)
	3.7C		
	3.8C		
	3.9C		
	3.10C		
ADV_TDS.3.2E			
AGD_OPE.1.1E	1.1C		
	1.2C		
	1.3C		
	1.4C		
	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		

CC Family	Element	Report reference, including slide# or section #	Verdict (P/F/I)
ALC_DEL.1.1E	1.1C		
ALC_DEL.1.2D (implied evaluator action)			
ALC_DVS.1.1E	1.1C		
ALC_DVS.1.2E			
ALC_LCD.1.1E	1.1C		
	1.2C		
ALC_TAT.1.1E	1.1C		
	1.2C		
	1.3C		
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		
ATE_IND.2.1E	2.1C		
	2.2C		
ATE_IND.2.2E			
ATE_IND.2.3E			
AVA_VAN.3.1E	3.1C		
AVA_VAN.3.2E			
AVA_VAN.3.3E			
AVA_VAN.3.4E			