وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS

# QCCS CB Scheme Certification Procedure

## [CB-4-PCD-QCCS]

## Procedure

**Compliance and Data Protection Department**

**27.08.2020**

**v1.0**

**Public**

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS

compliance.qcert.org

Q-CERT

# Document Authorization

*This page detail may intentionally be removed or hidden when publicly published or shared*

| | |
|---|---|
| ***DOCUMENT TITLE:*** | QCCS CB Scheme Certification Procedure |
| ***DOCUMENT REFERENCE:*** | [CB-4-PCD-QCCS] |
| ***ISSUE:*** | v1.0 |
| ***DATE:*** | 27.08.2020 |

# DISCLAIMER / LEGAL RIGHTS

Compliance and Data Protection (CDP) Department of Ministry of Transport and Communications (MOTC) has designed and created this publication, titled “QCCS CB Scheme Certification Procedure” - v1.0 - Public, is for any party interested in gaining a general understanding of the Qatar Common Criteria Scheme (QCCS) operation.

CDP is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge MOTC and CDP as the source and owner of the “QCCS CB Scheme Certification Procedure”.

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the CDP and MOTC. CDP and MOTC shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from CDP and MOTC shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

# LEGAL MANDATE(S)

Article 18 of the Emiri Decree no (4) for the Year 2016 setting the mandate of Ministry of Transport and Communications (hereinafter referred to as “MOTC”) provides that MOTC has the authority to regulate and develop the sector of Information and Communications Technology in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual’s life and community and build knowledge-based society and digital economy.

Based on Cabinet decision (26) for the year 2018, the Compliance & Data Protection Department (herein referred to as CPD) is entrusted by the Ministry of Transport and Communications (MOTC) as the competent authority, responsible for determining, in the public interest, the technical competence and integrity of organizations such as those offering assessments, testing and compliance services and the Issuance of Certifications those seeking certificates of compliance within the State of Qatar.

This Procedure has been prepared to take into consideration the current applicable laws of the State of Qatar. If a conflict arises between this document and the laws of Qatar, the latter shall take precedence. Any such term shall, to that extent be omitted from this Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments, in that case, shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

# REFERENCES

- All references are listed in [CB-2-LST-DocRefList] Documentation Control Reference List.

# Table of Contents

# 1 Introduction

This document defines the organizational basis for certification according to Qatar Common Criteria Scheme (QCCS) under the Certification Body (hereafter referred as 'CB') in the Compliance and Data Protection (CDP) Department, for IT Security within the Ministry of Transport and Communications (hereafter referred to 'MoTC').

CB is also hereafter referred as QCCS CB (Qatar Common Criteria Scheme Certification Body).

## 1.1 Purpose

The intended audience for this document is any party interested in gaining a general understanding of the Qatar Common Criteria Scheme (QCCS) operation under Certification Body in the CDP Department for IT Security within MoTC. Other detailed information on the operation of the scheme may be available through other publication. Any parties seeking access to documents that are not publicly available must submit a request in formal writing to the MoTC.  This document also provides guidance and workflow instructions for QCCS personnel for the delivery of certification services of the scheme.

The objective of this document is to achieve:

i. conformance to the requirement of Information Technology Security Evaluation of the ISO/IEC 15408 Part I, II, III and ISO/IEC 18045 version 3.1 Revision 5;

ii. compliance to the requirement of Bodies Certifying Products, Processes and Services ISO/IEC 17065:2012;

iii. the overall process has available the correct version of the evaluation evidence necessary for the evaluation and that it is adequately protected. Otherwise, the technical accuracy of the evaluation cannot be assured, nor can it be assured that the evaluation is being conducted in a way to provide repeatable and reproducible results;

iv. that an evaluation was done sufficiently – where every scheme has a means of verifying the technical competence, understanding of work and the work of its evaluators, whether by requiring the evaluators to present their findings to the oversight body, by requiring the oversight body to redo the evaluator's work, or by some other means that assures the scheme that all evaluation bodies are adequate and comparable;

v. presence of objectivity exists where impartiality ensure that conflicts of interest do not exist, so as not to adversely influence the activity of the bodies.

## 1.2 Scope

This certification scheme procedure applies to the operation of the Qatar Common Criteria Scheme (QCCS) Certification Body under CDP department within MoTC Qatar. Any customer can be Developer, Sponsor, Evaluation Body or interested parties that involved with the process of this Common Criteria Certification Scheme must also follow this document requirement.

## 1.3 Target Audience and Publication

This document should be made available to the following target audience:

- employees of the QCCS CB for their daily work
- auditors in the context of an accreditation or an international mutual recognition
- evaluators of EBs (Evaluation Bodies) recognized by the CB
- customers in the context of a certification process

## 1.4 Related Standards

The document is written with the aim to comply to various international standards, either completely or partially as a component. The considered standards are primarily the following:

- ISO/IEC 17065:2012 [17065]
- Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology [CCRA]

# 2 Scheme

**ISO/IEC 17065 clause 7.1 General**

**CCRA Annex C C.9a**

The current document describes the procedural requirements for an evaluation of IT product security according to Common Criteria (hereafter known as CC). The technical requirements for products are given by the documents described in the next sections.

## 2.1 Requirements documentation

The QCCS CB performs certifications according to the current official versions of the following standards:

- CC and CEM
- Supporting Documents authorized through CCRA

- This scheme document

Evaluation Requirements described in section 4 onwards are the requirements to be fulfilled by the customers (between sponsors, developer, or any interested parties)

### 2.1.1 CC and CEM

- CC: Common Criteria for Information Technology Security Evaluation
    - Part 1: Introduction and general model
    - Part 2: Security functional components
    - Part 3: Security assurance components
- CEM: Common Evaluation Methodology for Information Technology Security Evaluation

Note: CC and CEM are also established as international ISO/IEC standards:

- CC: ISO/IEC 15408 [CCPart1],[CCPart2],[CCPart3]
- CEM: ISO/IEC 18045 [CEM]

The current versions of the standards above are provided on the Common Criteria Portal: https://www.commoncriteriaportal.org/

The version applied for a product is initially defined in the application form and finally stated in the certificate issued by the certification body.

Unless otherwise agreed with the sponsor the versions used should be the versions valid at the time of the final evaluation report.

If the valid versions have been updated during the evaluation and certification an impact analysis may have to be performed and some part of the evaluation may have to be updated. (See also section 4.2.5 Maintenance section below)

Should the impact be too extensive, the certification may also be based on older versions of the standards, as long as this is consistent with the recommendations made by the CCRA.

### 2.1.2 Supporting Documents authorized through CCRA

According to the CCRA regulations, the QCCS CB has to check whether supporting documents as published on https://www.commoncriteriaportal.org have to be considered for an evaluation.

Requirements from applicable documents have to be included in a CC evaluation. When the QCCS CB or the EB refers to these documents in an evaluation, they have to be cited with version and date.

### 2.1.3 The current scheme document

This document.

### 2.2 Official language of the scheme

Documents delivered in the framework of a certification (i.e. security targets, protection profiles, evaluation reports, observation reports, product manuals, developer documents) shall be written in English.

The QCCS CB will provide certification reports and certificates in English as outcome of the certification procedure.

Other languages may be used in the certification procedure but must be agreed by the QCCS CB beforehand.

## 3 Roles and Responsibilities

### 3.1 Sponsor

The sponsor is the organization that applies and pays for the certification. The sponsor may establish a separate contract with the EB on its own to perform the evaluation, later with the QCCS CB to perform certification. However, the QCCS CB reserve the definitive right to assign the suitable EB to perform the evaluation. The project shall commence when all parties agreed on all the arrangements (between EB, QCCS CB and sponsor).

The sponsor shall ensure that the EB and the QCCS CB are granted access to all information that is relevant for the certification. This includes the support by other involved third parties, e.g. the design information provided by the developer or access to production premises and documentation. It may also be necessary to provide product related trainings.

The sponsor may receive consultancy from an external organization that is proficient in IT security and CC. If the external organization is identical with the EB that evaluates the product, the EB has to ensure impartiality according to scheme requirements.

### 3.2 Developer

The developer is the organization that produces the product to be certified and is responsible to provide the evaluation evidence, e.g. training, design information or testing instructions.

Note: Sponsor and developer can be the same organization.

### 3.3 Evaluation Body

**ISO/IEC 17065 clause 7.4 Evaluation**

The QCCS CB itself does not conduct evaluations but relies on an EB for this work. The EB is an evaluation lab that performs evaluation according the CC scheme, i.e. according to CC (see [CCPart1], [CCPart2], [CCPart3]) and CEM (see [CEM]) and additional requirements from the current document. The EB must be recognized first by the QCCS CB in order to perform evaluation within the QCCS CB (see Evaluation Body Recognition procedure [CB-4-PCD-EBRecog]).

To start an evaluation the sponsor may choose an EB from the list of EBs recognized by the CB, which will be listed in as public information. When contracting an EB from the list, the sponsor can be sure that the EB fulfils the requirements of the current CC scheme and the CB concerning management, organization, procedures and technical expertise. Besides evaluation, the EB may also provide consultancy to the sponsor, as long as impartiality requirements of the scheme are fulfilled.

In CC, the evaluation plan is fully determined by the CC method (see [CCPart1]). The EB conducts the project planning for the evaluation and all the evaluation activity required in CC. The QCCS CB supervises these activities.

In order to conduct the evaluation, the EB will request evaluation evidence from the sponsor or directly from the developer of the product.

According to the recognition agreement concluded with the EB (see [CB-2-AGR-EBRecog], the QCCS CB is entitled to supervise the EB’s work, to schedule audits and to decide on evaluation technical or procedural details if required.

The EB may have access to confidential information or nationally sensitive information during the evaluation. This information shall be kept confidential. Sharing information with the QCCS CB, if the information is necessary for the certification decision, is however required.

## 3.4 Customer

The organization (sponsors, developers or consumers) that make use of services provided by the Qatar Common Criteria Scheme and from the Evaluation Bodies.

## 3.5 Consumer

The organization (end-users) that uses the certified product within their infrastructure.

## 3.6 Certification Body

The CB manages the scheme, monitors the evaluation process and may provide input and advice to the sponsor, developer and EB regarding the application of the scheme.

The CB evaluates the final evaluation report and decides on the certification of the product. It issues the certificate and lists the product on its certified products list.

### 3.6.1 Roles within the Scheme under Certification Body

The following roles exist are integral to the operation of QCCS CB:

a) **Scheme Director** – The Scheme Director is responsible for making a decision to grant certification if there is sufficient evidence of conformity, or not to grant certification if there is not sufficient evidence of conformity, based on evaluation conclusions.

Further, the decision to certify will be based upon the certification report produced by the certifiers and the following:

i. certification processes have been completed in accordance with respective scheme requirements; and
ii. Certifiers have no conflict of interest in the outcome.

b) **Quality Manager**. This role is responsible for the maintenance of quality and conducts reviews of the application of the management system within the scheme. To ensure impartiality of certification services, the Quality Manager provides outcomes of management system reviews to the Management Review members.

c) **Scheme Manager**. This role is responsible on day-to-day management and administration of the QCCS CB including providing strategic planning for the scheme, implementing the quality and certification management system, management of personnel, financial, and over-sighting any potential or real conflict of interest. The Scheme Manager reports administratively to the Scheme Director. This role is also responsible for:

i. General management of QCCS scheme services;
ii. The relationship and interface with recognized (licensed) evaluation bodies (EBs) and;
iii. Continuous application and implementation of the policy and procedures;
iv. Ensuring minimum staffing levels are maintained to sustain scheme operations and within recognized EBs;
v. Ensuring that new and existing staffs within the scheme are free from any actual or potential conflict of interest in the performance of their duties; and
vi. Recommending certification report as the senior approver.

d) **Certifier**. This role is responsible for:

i. Ensuring the effective application of IT security evaluation criteria amongst certifiers;
ii. Ensuring that the highest standards of competence and impartiality are maintained, and that consistency is achieved across all evaluation and certification activities;
iii. The relationship and interface with the Evaluator(s);
iv. The technical development of other new Certifiers;
v. The continuous application of QCCS CB scheme documentations to the conduct of all certification activities; and
vi. Signing QCCS scheme certification reports as the technical certification expert and providing such reports to the Scheme Manager for recommendation and Scheme Director for approval.

vii. conduct of day-to-day certification, certificate maintenance and mutual recognition projects and in compliance with scheme documentations. The Certifier signs certification reports for only those evaluations that they perform the certification role.

Further information of each roles are also stated in QCCS CB Organization Chart [CB-4-QCCSOrgChart].

# 4 Evaluation requirements

## 4.1 Scope of the CB

The QCCS CB offers the following types of certification:

- Generic CC certification of products
- CC certification based on cPPs (Collaborative Protection Profiles)
- CC certification of PPs (Protection Profiles)
- CC site certification

The types of certification will be referenced in the next sections of this document.

## 4.2 Certification procedure

In order to assure the quality of IT security evaluation by the EB and the maintenance of certificates, the QCCS CB requires the following phases in the certification procedure:

- Preparation
- Application
- Evaluation
- Certification
- Maintenance

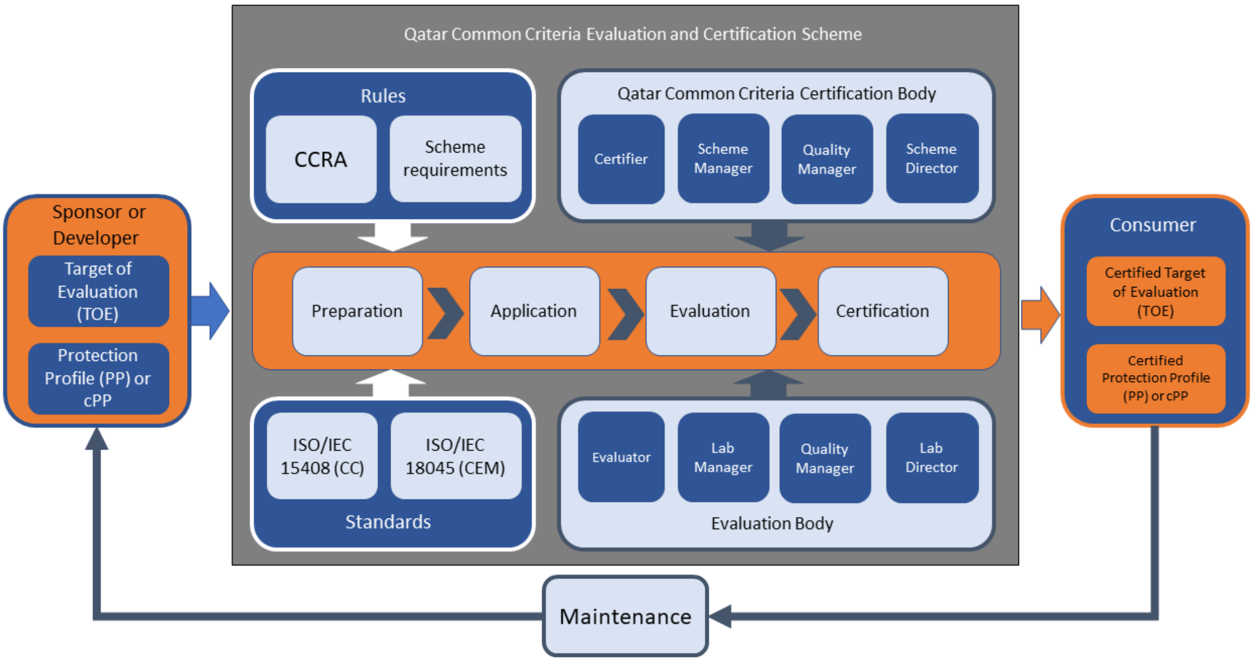

**Figure 1: Overall process of Qatar Common Criteria Scheme**

Note: As detailed in section 4.2.3, the types of certification require different activities within the evaluation phase.

Each flowchart steps are numbered, followed by a workflow describing each numbered step.

### 4.2.1 Preparation phase

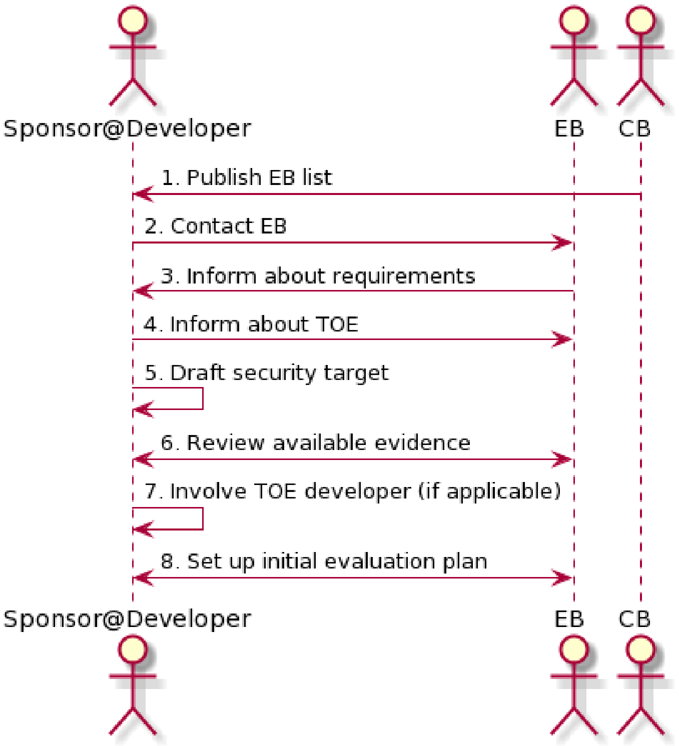
Sponsor@Developer
EB
CB
1. Publish EB list
2. Contact EB
3. Inform about requirements
4. Inform about TOE
5. Draft security target
6. Review available evidence
7. Involve TOE developer (if applicable)
8. Set up initial evaluation plan
Sponsor@Developer
EB
CB

**Figure 2: Preparation phase**

The preparation phase starts with an initial contact between the sponsor and the EB. This may be a separate arrangement between EB and the sponsor, which do not require QCCS CB involvement at the beginning. The sponsor may contact any of the EBs listed in the list of recognized EBs.

#### 1. Publish EB list

QCCS CB is responsible to make available to the public the list of recognized (licensed) EB in Qatar Common Criteria Scheme. This is to make sure the sponsors are aware of the recognized EB in the QCCS CB.

#### 2. Contact EB

The sponsor has the freedom to contact any of the EB in the list. The consideration factors could be because of price, expertise, experience and time of completion offered by the EBs.

#### 3. Inform about requirements

Each EB may have different requirements for a CC evaluation in which sponsor shall fulfill. This is separate arrangement between EB and sponsor.

### 4. Inform about TOE

The sponsor also needs to provide information about the Target of Evaluation (TOE), whether it is ready or not for evaluation.

### 5. Draft security target

Process **3.** and **4.** above may continuously repeat until both agreed on the requirements and readiness. The sponsor usually drafts the security target (ST). The ST is a precise description of the TOE security functionality under evaluation. There may be cases where the sponsor hired an independent consultant, or a consultant team separated from the EB evaluation team to prepare the ST.

Note: There are CC requirements for the correct authoring of an ST, see [CCPart1], [CCPart3] and [CEM].

### 6. Review available evidence

The sponsor and the EB check whether evidence about the TOE required by the CC is already available or has to be prepared for the evaluation. The list of available evidence will be needed for evaluation phase later. (see the list of evidence in evaluation phase section 4.2.3 of this document)

### 7. Involve TOE developer (if applicable)

When sponsor and developer are independent organizations, a declaration by the product developer may be required that he will support the ongoing evaluation.

### 8. Set up initial evaluation plan

Finally, the sponsor and the EB set up a time schedule for all evaluation activities planned.

In order to fill possible information gaps about the certification procedure or the certifiability of the TOE, the QCCS CB offers complementary information meetings with the sponsor and the EB, if needed.

### 4.2.2 Application phase

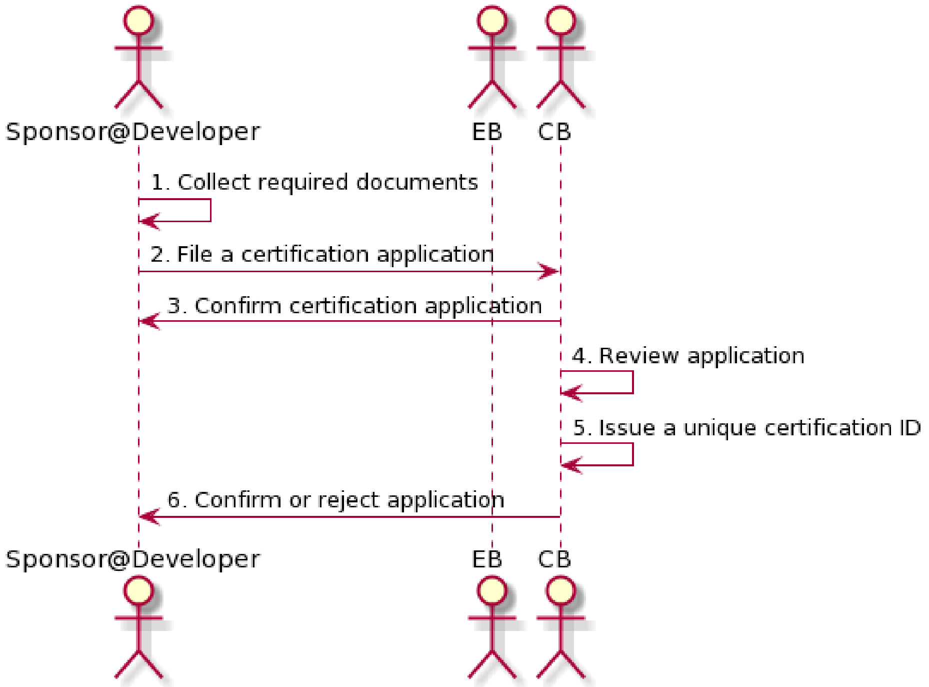
Sponsor@Developer
EB
CB
1. Collect required documents
2. File a certification application
3. Confirm certification application
4. Review application
5. Issue a unique certification ID
6. Confirm or reject application
Sponsor@Developer
EB
CB

**Figure 3: Application phase**

**ISO/IEC 17065 clause 7.2 Application**

Based on the evidence collected in the preparation phase, the sponsor applies with the QCCS CB for certification according to the current CC scheme:

**1. Collect required documents**

The sponsor is responsible to prepare all the required documents for applying the evaluation. The required documents may be assisted by EB. The required documents are listed below in the next section, **2. File a certification application**.

**2. File a certification application**

The sponsor fills in the CC Certification Application Form [CB-4-FRM-CertAppl]. The application is completed with the following documents:

1) the Security Target (ST),
2) the time schedule for the evaluation activity planned,
3) listing of product development and production sites of the TOE,
4) listing of cryptographic mechanisms used in the TOE (i.e. algorithms and communication protocols),
5) the TOE user manuals (if available).

In case the sponsor applies for re-certification of a TOE he adds the following documents,

6) an impact analysis report (IAR) of the changes made to the TOE after the last certification,
7) a configuration list of the TOE

In order for the CB to judge the impartiality of the EB the sponsor adds

8) a description of consulting services provided by the EB for the TOE and information about the relationship between the EB and the sponsor or the developer.

Note: All documents required in addition to the certification application form may be prepared by the EB as a service to the sponsor.

Finally, the sponsor sends his completed application to the QCCS CB.

### 3. Confirm certification application

The CB confirms the receipt of the application to the sponsor.

Note: The signed certification application form [CB-4-FRM-CertAppl] is a binding statement by the sponsor that he will accept the QCCS CB regulations and the CC scheme in particular.

### 4. Review application

**ISO/IEC 17065 clause 7.3 Application review**

The QCCS CB reviews the application according to the following criteria:

- The application includes sufficient information about the sponsor and the TOE and includes all documents required,
- QCCS CB and sponsor agree on and obviously understand the applied evaluation standards and the scheme certification procedure (this document)
- The sponsor provides or commits himself to provide all evidence required by the QCCS CB and the EB for evaluation and certification,
- The QCCS CB either confirms or rejects an application by the sponsor or the EB to reuse results from former certifications (for criteria see section 4.5),
- The QCCS CB has the technical capability and staff capacity to conduct the certification sought by the sponsor.
- The proposed EB by the sponsor in the certification application form is able to perform evaluation

Based on the review steps, the QCCS CB either confirms or rejects the certification application to the sponsor in writing. A confirmation can include stipulations the sponsor or the EB have to follow during the evaluation procedure.

Note: Written notification as ‘in writing’ may include writing through email, formal electronic letter or hardcopy letter.

### 5. Issue a unique certification ID

When the QCCS CB accepts a certification application, it issues a unique certification ID to the begin the certification process.

### 6. Confirm or reject application

In the event that the application does not fulfill the application criteria in **4.Review application** above, the QCCS CB have full right to reject the application from the sponsor and not proceed to the next step. In case of a rejection the QCCS CB informs the sponsor why the TOE cannot be certified.

### 4.2.3 Evaluation phase

Sponsor and EB detail the time schedule prepared earlier in the process and send it to the QCCS CB for reference.

Based on the type of certification selected by the sponsor, the following sub-procedures apply:

- Generic CC certification of products (section 4.2.3.1)
- CC certification based on cPPs (section 4.2.3.2)
- CC certification of PPs (section 4.2.3.3)
- CC site certification (section 4.2.3.4)

### 4.2.3.1 Generic CC certification of products

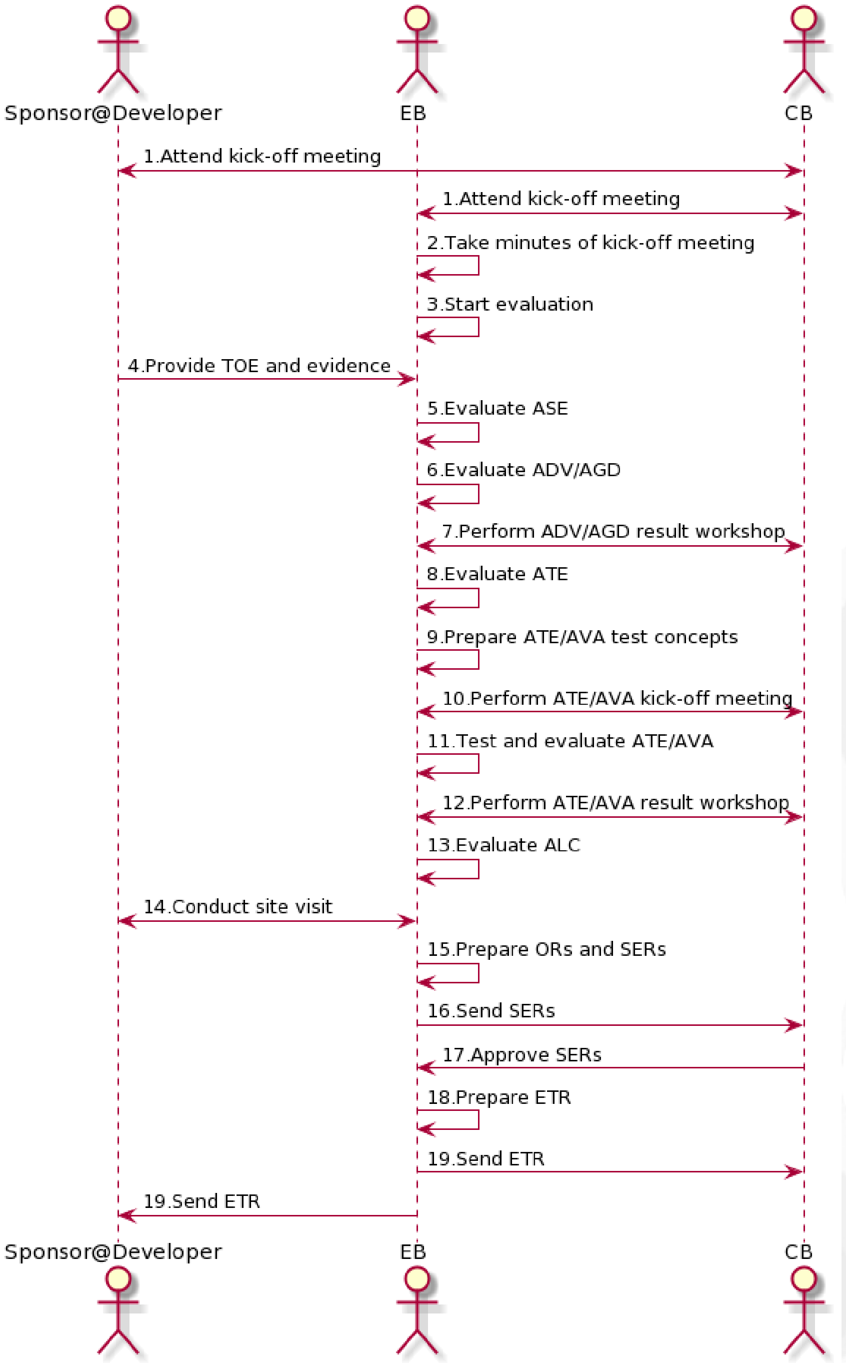
Sponsor@Developer
EB
CB
1.Attend kick-off meeting
1.Attend kick-off meeting
2.Take minutes of kick-off meeting
3.Start evaluation
4.Provide TOE and evidence
5.Evaluate ASE
6.Evaluate ADV/AGD
7.Perform ADV/AGD result workshop
8.Evaluate ATE
9.Prepare ATE/AVA test concepts
10.Perform ATE/AVA kick-off meeting
11.Test and evaluate ATE/AVA
12.Perform ATE/AVA result workshop
13.Evaluate ALC
14.Conduct site visit
15.Prepare ORs and SERs
16.Send SERs
17.Approve SERs
18.Prepare ETR
19.Send ETR
19.Send ETR
Sponsor@Developer
EB
CB

**Figure 4: Evaluation phase: Generic CC certification of products**

### ISO/IEC 17065 clause 7.4 Evaluation

### 1.Attend kick-off meeting

The QCCS CB invites sponsor and EB to a kick-off meeting. In the meeting, the parties will

- present information about the CC requirements and the TOE,
- agree on relevant CC requirements for the TOE and the development sites,
- agree on reuse of existing evaluation results (e.g. platform or site certifications),
- discuss the use of cryptographic mechanisms in the TOE (if available),
- discuss available and to be prepared documentation for the TOE,
- discuss possible site visits,
- present the documents prepared so far and
- discuss and agree on the time schedule,
- discuss and agree on the ST.

### 2.Take minutes of kick-off meeting

The EB takes minutes of the meeting for later reference. This also applies to all other meetings which will come later on. The minutes of meeting shall be shared to all attendees.

### 3.Start evaluation

After the meeting, the EB starts the evaluation of the TOE. This involves the sponsor and the EB as follows:

- the sponsor (or the developer) provides the TOE including required updates, patches, test tools and the documented evidence as required in the CC requirement set (**4.Provide TOE and evidence**),
- the EB evaluates the TOE according to the CC aspects,
- the EB performs technical tests of the TOE (e.g. penetration tests),
- the EB conducts a site visit (audit) of the developer's sites,
- the EB prepares observation reports about its evaluation, testing or auditing results according to CC requirements
- the EB sends the ORs (Observation Reports) and the SERs (Single Evaluation Reports) to the sponsor and the CB for reference

The QCCS CB evaluates the reports provided by the EB to make sure that the evaluation is conducted according to the requirements of the scheme. The QCCS CB reserves the right to instruct the EB and the sponsor to change an ongoing evaluation or to end it prematurely when the QCCS CB reaches the conclusion that the evaluation is not properly done.

In order to support evaluations, workshops will be held to discuss the results of the various CC aspect evaluations:

- ADV/AGD result workshop

- ATE/AVA kick-off meeting
- ATE/AVA result workshop

In these workshops, QCCS CB, EB and sponsor discuss results of completed evaluation steps and the setup of the TOE tests for the CC aspects ATE and AVA.

Based on the typical structuring of the CC requirements, although it is not mandatory to follow the sequence, the following order of aspect evaluations was found useful for CC evaluations:

1. ASE evaluation (**5.Evaluate ASE**)
2. ADV/AGD evaluation (**6.Evaluate ADV/AGD**)
3. ADV/AGD result workshop (**7.Perform ADV/AGD result workshop**)
4. ATE evaluation (**8.Evaluate ATE**)
5. ATE/AVA preparation of test concepts (**9.Prepare ATE/AVA test concepts**)
6. ATE/AVA kick-off meeting (**10.Perform ATE/AVA kick-off meeting**)
7. ATE/AVA testing and evaluation (**11.Test and evaluate ATE/AVA**)
8. ATE/AVA result workshop (**12.Perform ATE/AVA result workshop**)

The ALC aspect is usually evaluated in parallel with a site visit (audit) but planned independently from the other evaluations.

- ALC evaluation and site visit (**13.Evaluate ALC, 14.Conduct site visit**)

After ALC evaluation and site visit, the EB will have to:

- **15.Prepare ORs and SERs**
- **16.Send SERs** (to QCCS CB and to sponsor for reference)

When the evaluation is finally completed, the QCCS CB approves the SERs (**17.Approve SERs**).

Afterwards, the EB prepares the ETR (**18.Prepare ETR**) as the collection of SERs and sends it to the sponsor and the QCCS CB (**19.Send ETR**). The ETR is the basis for evaluation and certification decision taken by the QCCS CB.

#### 4.2.3.2 CC certification based on cPPs

The overall procedure for a certification according to a cPP is similar to the generic CC certification of products, see section 4.2.3.1 above.

However, the procedure has to be agreed with the QCCS CB. The QCCS CB may require additional evaluation steps or other deviations from the generic procedure as required in the cPP for the particular product class.

#### 4.2.3.3 CC certification of PPs

The sponsor sends the Protection Profile to the EB and the QCCS CB for reference.

The EB evaluates the PP according the requirements in CC aspect APE. During the evaluation, the EB may contact the sponsor for updates to the PP.

The EB prepares an ETR with the final evaluation result and sends it to the sponsor and the QCCS CB.

#### 4.2.3.4 CC site certification

Sponsor and QCCS CB have to agree on the procedure for a site certification before any activity is started.

Site certifications are based on a site visit (audit) by the EB and a resulting OR written by the EB.

### 4.2.4 Certification

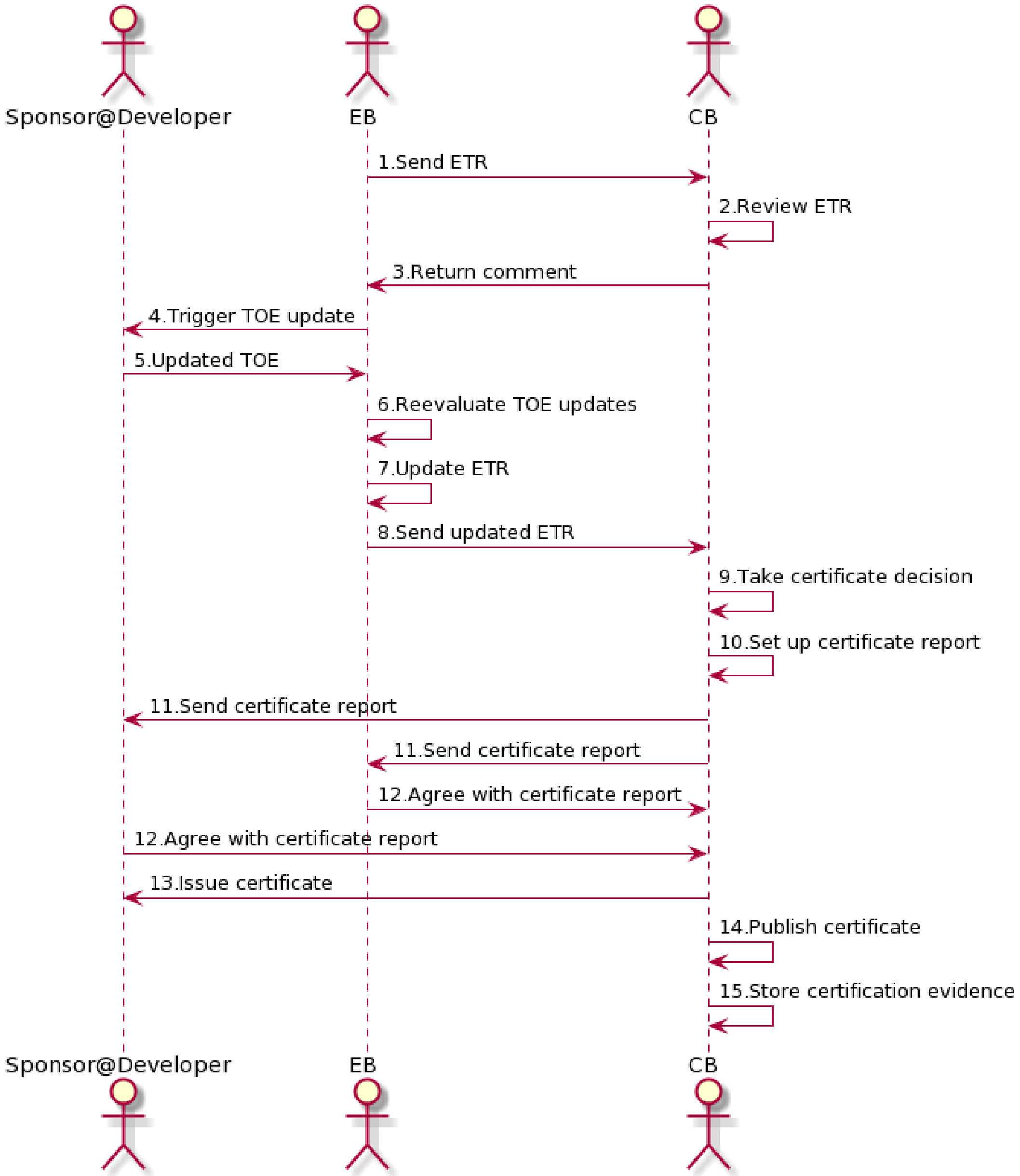

**Figure 5: Certification phase**

## ISO/IEC 17065 clause 7.5 Review

### 1.Send ETR

The certification phase starts when the Evaluation Technical Report (ETR) is delivered by the EB to QCCS CB. It is up to the EB whether to share the ETR with sponsor or not.

### 2.Review ETR

The QCCS CB reviews the ETR based on the requirements listed in section 2.1 of this document.

### 3.Return comment

The QCCS CB documents the results of the review and return any comments to the EB.

When the QCCS CB detects formal nonconformities in the ETR, the CB will provide feedback to the EB.

### 4.Trigger TOE update

There will be cases when nonconformities found in ETR where EB needs to inform sponsor or developer to update the TOE based on the nonconformities.

### 5.Updated TOE

When sponsor or developer updates the TOE, they shall inform the TOE changes to the EB. This may trigger changes to the document evidences of the TOE.

### 6.Re-evaluate TOE updates

Based on the requirements in section 2.1, the EB may have to re-evaluate the updated TOE accordingly.

### 7.Update ETR

Based on the latest changes, test results and evidences, the EB will update the ETR.

### 8.Send updated ETR

The EB fixes the errors and returns the updated version of the ETR to the CB.

Note: Technical nonconformities may prevent the QCCS CB from issuing a certificate. In this case, the QCCS CB has to inform the sponsor about these nonconformities and about additional evaluation work required to re-evaluate the TOE after the nonconformities are fixed by the sponsor. The QCCS CB halts the certification phase until the sponsor presents an updated TOE together with an updated ETR by the EB.

## ISO/IEC 17065 clause 7.6 Certification decision

### 9.Take certification decision

When the ETR finally passes the QCCS CB review, the QCCS CB takes a positive certification decision. The certification decision (and the certificate) may restrict the validity area of the certificate.

Note: Since sponsor, EB and QCCS CB are in permanent communication, it is unlikely that the QCCS CB has to take an official negative certification decision because the cooperation may terminate prematurely should the sponsor for some reason refuse to change the TOE as required by the QCCS CB in the earlier phase.

## ISO/IEC 17065 clause 7.7 Certification documentation

### 10.Set up certification report

The certification decision is documented in a certification report with the following contents but not limited to:

- Reference to the CC requirement set the evaluation was based on
- Technical description of the TOE and its security functions with version and completion date
- Evaluated configuration of the TOE
- Description of one or more PPs the certification may be based on
- Summary of the evaluation results
- Hints or stipulations for the secure use of the TOE

### 11.Send certification report

The QCCS CB sends the certification report to sponsor and EB. Sponsor or EB are allowed to comment on the certification report and suggest changes. The QCCS CB may accept or decline these changes and issue an update of the certification report.

### 12.Agree with certification report

The EB and sponsor shall make sure all the information in the certification report are correct and they agreed on the contents written. Otherwise they shall be returned to the CB as in (section **11.Send certification report**) process above.

### 13.Issue certificate

When sponsor and EB agree with the certification report, the QCCS CB issues a certificate and sends it to the sponsor. The sponsor may use the certification mark in his public product communication according to the rules laid down in [CCRA].

The certificate may contain the following information:

- Name and address of the CB
- Date of issuance of the certificate
- Unique certification ID or certificate serial ID
- Name and address of the sponsor
- Scope of the certification with information about
    - The certified product
    - The evaluation assurance levels
    - The certification scheme
- Expiry date of the certificate
- Signature by the CB

(See CCRA requirements; Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology [CCRA] annex J for further details)

For the validity period of CC certificates please refer to section 4.2.5 of this document.

**ISO/IEC 17065 clause 7.8 Directory of certified products**

**CCRA Annex C C.11**

### 14.Publish certificate

QCCS CB publishes certificates together with the ST and the certification report. The QCCS CB also updates its public list of certified products with the current TOE.

However, in the certification application [CB-4-FRM-CertAppl] the sponsor may refuse publication of the certificate. If this is the case, the certificate will not appear on the website or other public media of the QCCS CB.

### 15.Store certificate evidence

Finally, the QCCS CB stores all evidence collected during the certification procedure from the sponsor or the EB (i.e. certification application, meeting protocols, reports, reviews, certification decision, certificate, certification mark) for later reference.

**ISO/IEC 17065 clause 7.9 Surveillance**

**CCRA Annex C C.9g, C.14**

The CC do not require the CB to do active surveillance of the certified products.

The QCCS CB randomly check whether

- the sponsor uses the certificate as laid down in section 4.8 of this document,
- the sponsor uses the certification mark as laid down in [CCRA],

- any other party uses certificates or certification marks without authorization.

When the QCCS CB detects deviations, the sponsor or respective party receives a note from the CB and is prompted for change. Failure to do as instructed will result in certificate to be withdrawn.

### 4.2.5 Maintenance phase

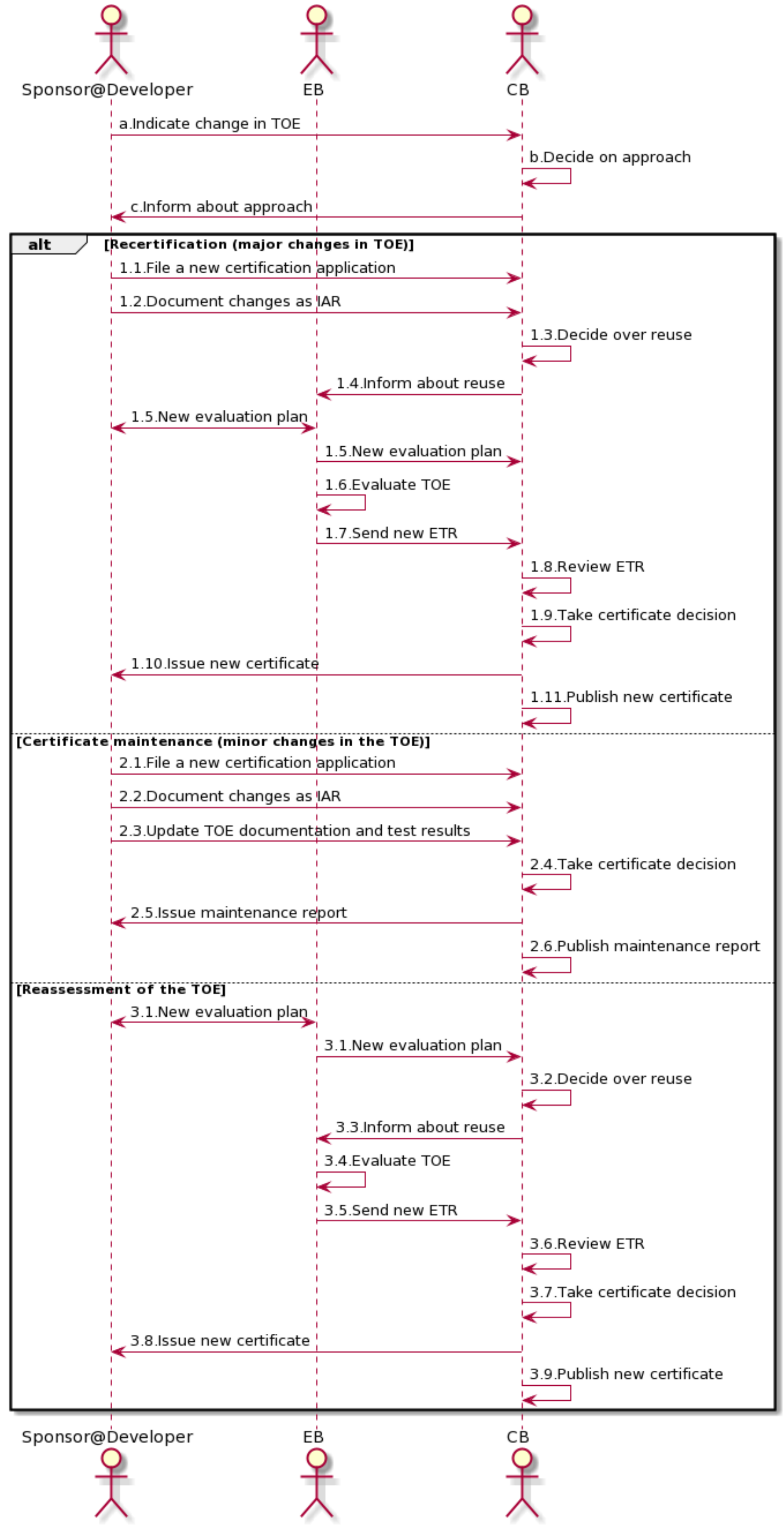
Sponsor@Developer
EB
CB
a.Indicate change in TOE
b.Decide on approach
c.Inform about approach
alt
[Recertification (major changes in TOE)]
1.1.File a new certification application
1.2.Document changes as IAR
1.3.Decide over reuse
1.4.Inform about reuse
1.5.New evaluation plan
1.5.New evaluation plan
1.6.Evaluate TOE
1.7.Send new ETR
1.8.Review ETR
1.9.Take certificate decision
1.10.Issue new certificate
1.11.Publish new certificate
[Certificate maintenance (minor changes in the TOE)]
2.1.File a new certification application
2.2.Document changes as IAR
2.3.Update TOE documentation and test results
2.4.Take certificate decision
2.5.Issue maintenance report
2.6.Publish maintenance report
[Reassessment of the TOE]
3.1.New evaluation plan
3.1.New evaluation plan
3.2.Decide over reuse
3.3.Inform about reuse
3.4.Evaluate TOE
3.5.Send new ETR
3.6.Review ETR
3.7.Take certificate decision
3.8.Issue new certificate
3.9.Publish new certificate
Sponsor@Developer
EB
CB

**Figure 6: Maintenance phase** (above)

QCCS CB certificates are only valid for the TOE version, TOE configuration and TOE use environments as documented in the certification report. Site certificates are only valid for the site indicated.

Certificates have the following validity periods:

- Product certificates expire five (5) years after issuance,
- Site certificates expire two (2) years after issuance,
- PP certificates are valid for ten (10) years.

### ISO/IEC 17065 clause 7.10 Changes affecting certification

When the QCCS CB changes the current CC scheme and this change affects sponsors holding certificates for their products, the QCCS CB informs the sponsors about the change. The QCCS CB takes any action required by the scheme and verifies that the sponsors correctly implement the required changes.

Changes made to the TOE, its environment or technical progress, during the validity period of the certificate, may jeopardize the validity of the certificate. It is the sponsor's responsibility to inform the QCCS CB of the changes made to the TOE. However, this action is not mandatory for the sponsor.

**a.Indicate change in TOE**

The sponsor is obliged to indicate such changes to the QCCS CB and to follow the QCCS CB's instructions on how to maintain the validity of the certificate.

**b.Decide on approach**

Based on CCRA Assurance Continuity [2012-06-01_Assurance Continuity] the QCCS CB decides about the proper approach to treat the changes in question.

**c.Inform about approach**

One of following approaches may be applied:

- Recertification (major changes in the TOE)
- Certificate maintenance (minor changes in the TOE)
- Reassessment of the TOE

#### 4.2.5.1 Recertification (major changes in the TOE)

When the developer or sponsor made major changes to the TOE, its configuration or its use environment, the QCCS CB may require a recertification of the TOE.

### 1.1.File a new certification application

For a recertification, the sponsor has to file a new certification application [CB-4-FRM-CertAppl].

### 1.2.Document changes as IAR

The sponsor or developer is responsible to document the changes of the TOE in an Impact Analysis Report (IAR). Preparation of this IAR can be assisted by a consultant or an EB in separate arrangement with the sponsor.

### 1.3.Decide over reuse

In some cases, the sponsor may submit previous evidence to be reuse. The QCCS CB need to decide whether it can be reuse or not.

### 1.4.Inform about reuse

The QCCS CB then inform to the EB that the previous evidence can be reuse.

### 1.5.New evaluation plan

Based on this information, QCCS CB, EB and sponsor set up a new evaluation plan. The plan has to cover all CC aspects that have been affected by the changes. However, the QCCS CB reserves the right to decide about reuse of results from former evaluations when the particular TOE properties are not changed since the last evaluation.

### 1.6.Evaluate TOE

Because this phase is considered as major changes, this is where the EB will need to evaluate the TOE as per the requirement in section 2.1 of this document.

### 1.7.Send new ETR

New ETR will be submitted by the EB to QCCS CB according to evaluation made on the latest TOE.

### 1.8.Review ETR

QCCS CB will review the ETR to ensure consistencies on the latest changes and evidence submitted for the TOE.

### 1.9.Take certification decision

When the EB finished the evaluation and the QCCS CB reaches a positive certification decision based on the new ETR, it will update the certification report.

### 1.10.Issue new certificate

QCCS CB will issue a new certificate because this a major changes, where previous certificate will be considered as invalid immediately.

### 1.11.Publish new certificate

New certificate will be published by the QCCS CB to inform the existence of new certificate for the respective TOE.

#### 4.2.5.2 Certificate maintenance (minor changes in the TOE)

### 2.1.File a new certification application

Certificate maintenance may be applied when only minor changes were made to the TOE, its configuration or the use environment. In this case, a certificate maintenance procedure is started. The sponsor has to file a new certification application [CB-4-FRM-CertAppl].

### 2.2.Document changes in IAR

When there is any changes to the TOE it will be documented in IAR and inform to QCCS CB.

### 2.3.Update TOE documentation and test results

Certificate maintenance requires the sponsor to update the product documentation and the test results produced during the TOE evaluation. In contrast to a recertification, the sponsor is not required to involve the EB in a certification maintenance procedure.

### 2.4.Take certification decision

The QCCS CB takes its maintenance decision based on the evidence provided by the sponsor.

### 2.5.Issue maintenance report

When the QCCS CB reaches a positive decision in a certification maintenance procedure, QCCS CB will provide a maintenance report.

### 2.6.Publish maintenance report

QCCS CB publishes maintenance report together with the original certification report. The original certificate remains valid (may be issued with the new certificate as addendum).

#### 4.2.5.3 Reassessment of the TOE

A reassessment will be triggered when the technical progress (e.g. emerging of new vulnerabilities, new attack scenarios, weakening strength of crypto algorithms) requires to repeat an assessment of the TOE. Any sponsor may voluntarily refuse for this activity if their TOE is affected, which will result of their certificate to be withdrawn.

### 3.1.New evaluation plan

For a reassessment, QCCSCB and EB set up an evaluation plan that focusses on the AVA aspects of the CC and new attack scenarios.

### 3.2.Decide over reuse

The QCCS CB may allow to reuse results from former evaluations when the particular TOE properties are not affected by technical progress.

### 3.3.Inform about reuse

The QCCS CB will inform EB if reuse of previous evidence is suitable

### 3.4.Evaluate TOE

This phase is yet to confirm as major or minor changes, this is where the EB will need to evaluate the TOE as per the requirement in section 2.1 of this document.

### 3.5.Send new ETR

New ETR will be submitted by the EB to QCCS CB according to evaluation made on the latest TOE.

### 3.6.Review ETR

QCCS CB will review the ETR to ensure consistencies on the latest changes and evidence submitted for the TOE.

### 3.7.Take certificate decision

When the EB finished the evaluation and the QCCS CB reaches a positive certification decision based on the new ETR, it will update the certification report

### 3.8.Issue new certificate

QCCS CB will issue a new certificate because based on the certification decision, where previous certificate is considered as invalid.

### 3.9.Publish new certificate

New certificate will be published by the QCCS CB to inform the existence of new certificate for the respective TOE.

Note: When the TOE is not evaluated with positive result, the QCCS CB may withdraw the original certificate or issue a new certificate that documents a lower attack resistance of the TOE.

## 4.3 Documentation standard

When preparing documents for the certification process, the EB may have to follow a common documentation standard in order to communicate evaluation results in a fixed and proven format. The format reflects the structuring of the CC evaluation aspects and makes sure that the ISO/IEC 17025 and CCRA reporting requirements are fulfilled.

Each EB may have their own unique documentation standard structure, however they shall comply to the CCRA requirement.

When the EB reports on test results, this has to happen in a comprehensive way:

- Detailed description of the test setting and the preconditions required for the test
- Complete test results

Based on a CC test report, a competent third party has to be able to repeat the tests and to reproduce the same test results.

When issuing a certificate, the QCCS CB uses internal document templates for

- Certification Report
- Certificate

## 4.4 Certificate ID schema

The QCCS CB uses the following ID schema for its certificates:

QCCS-CERT-CXXX-ZZZ-YYYY

with CXXX being the certification ID, ZZZ as running number within a year and YYYY the year of issuance of the certificate.

Example:

“QCCS-CERT-C001-001-2020” - indicates project certification ID C001, certificate number 001 in year 2020. If there is any maintenance certificate being release, it will use Mxxx, eg; M001.

## 4.5 Reuse of evaluation results

In general, EBs are allowed to reuse evaluation results established for one TOE as evidence in evaluations of other TOEs. However, to be able to reuse evidence from former evaluations, the EB must have access to all evaluation reports from these evaluations in order to decide what results can be reused for what evaluations.

Note: Reuse of evaluation results is most effective when two or more TOEs from one developer are evaluated by one EB.

Note: Site visit results may be shared in different evaluations when evaluating several products from one developer.

Note: TOEs may be developed by adding specific functionality to an already certified platform product. In this case, evaluation of the TOE can rely on the platform certification and can be restricted to the functions added to the platform. The CC aspect ACO has to be followed in such evaluations.

Note: The QCCS CB only allows reuse of evaluation results from previously completed certifications issued by the CB itself before the sponsor applied for the current certification.

Note: Be aware that the QCCS CB has to decide on reuse of evaluation evidence in every single case.

## 4.6 Confidentiality and document exchange

The sponsor or the developer may require that highly sensitive information about the TOE design is not allowed to leave its secured environment. If this is the case, the EB and the QCCS CB may evaluate the information inside this environment on the sponsor's or the developer's premises. However, the sponsor has to explain the reasons for this difficulty and to bear any additional cost (e.g. additional travel expenses) incurred by QCCS CB.

In contrast, when sponsor or developer decide to disclose confidential information to other parties besides QCCS CB or EB (e.g. customers, commercial partners), this may have an effect on the vulnerability assessment of the TOE. This is because within a larger group of informed persons, there is a bigger chance that potential attackers may receive information about vulnerabilities of the TOE.

Any information exchange between the parties has to be encrypted with an agreed type of encryption. By default, QCCS CB will use PGP and share public keys to the only authorized personnel they will be communicated with.

## 4.7 International recognition of CC certificates

The QCCS CB conducts CC certifications according to the international CC standard (see [CCPart1], [CCPart2], [CCPart3]) and the CEM methodology (see [CEM]). Furthermore, the Qatar QCCS CB is the member of the international CC recognition agreement (see [CCRA]).

Therefore, products certified by QCCS CB receive a CCRA test mark and will be recognized as being certified by other countries as set forth in [CCRA].

Vice versa, the QCCS CB will recognize certificates issued by other country's CBs as described in [CCRA].

## 4.8 Publication of certificates

The QCCS CB publishes certificates by default. The sponsor is allowed to refuse the publication of his certificate.

Note: CCRA recognition of a certificate requires that the certificate is published by the CB. When the sponsor refuses publication of his certificate, it will not be recognized by other national CBs. This shall be known and accepted in prior by the sponsor.

Based on the information available from the QCCS CB website, certificates issued by the QCCS CB will also appear on the CCRA website http://www.commoncriteriaportal.org. This publication is governed by the CCRA regulation (see [CCRA]).

## 4.9 Termination, reduction, suspension or withdrawal of certificates

**ISO/IEC 17065 clause 7.11 Termination, reduction, suspension or withdrawal of certification**

**CCRA Annex C C.15**

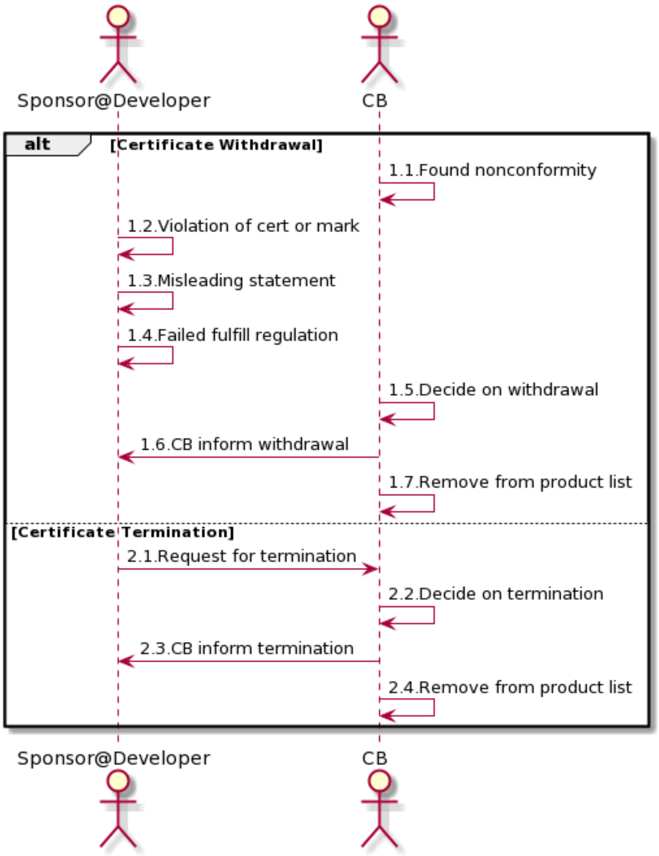
Sponsor@Developer
CB
alt
[Certificate Withdrawal]
1.1.Found nonconformity
1.2.Violation of cert or mark
1.3.Misleading statement
1.4.Failed fulfill regulation
1.5.Decide on withdrawal
1.6.CB inform withdrawal
1.7.Remove from product list
[Certificate Termination]
2.1.Request for termination
2.2.Decide on termination
2.3.CB inform termination
2.4.Remove from product list
Sponsor@Developer
CB

**Figure 7: Withdrawal and termination** (above)

## Certificate withdrawal

The QCCS CB may consider withdrawing a certificate when

- **1.1.Found nonconformity** - the QCCS CB substantiates a nonconformity of the product with the CC scheme requirements (either because of changes to the product or the certification requirements),
- **1.2.Violation of cert or mark** - the sponsor uses or permits use of the certificate or the CC certification mark in a wrong or misleading way,
- **1.3.Misleading statement** - the sponsor makes or permits misleading statements about the certification of the product,
- **1.4.Failed fulfill regulation** - the sponsor fails to fulfil the organizational regulations in the CC scheme,

### 1.5.Decide on withdrawal

When the above situations occur, the QCCS CB may decide on withdrawal

### 1.6.CB inform withdrawal

After decision made, QCCS CB shall inform the withdrawal of certificate to the sponsor. Upon a withdrawal, the QCCS CB informs the sponsor in writing about the decision taken, possible action to prevent the withdrawal and any further action required by the certification scheme.

### 1.7.Remove from product list

The product certificate shall be considered as invalid and shall be removed from QCCS CB external product list. An internal record can be kept for historical purpose.

## Certificate termination

### 2.1.Request for termination

A certificate termination can only be requested by the sponsor.

### 2.2.Decide on termination

Certificate terminations or withdrawals have to be conducted in accordance with the requirements in the current scheme.

### 2.3.CB inform termination

Since the termination was requested by the sponsor, the QCCS CB shall abide to it and the QCCS CB urges the sponsor to discontinue the use of the certificate immediately.

### 2.4.Remove from product list

When a certificate is terminated or withdrawn, the QCCS CB takes care that the product is no longer listed in its internal and public documents as being certified. An internal record can be kept for historical purpose.

**Note:** CC certificates are not suspended or reduced in this scheme in any case.

## 4.10 Complaints and appeals

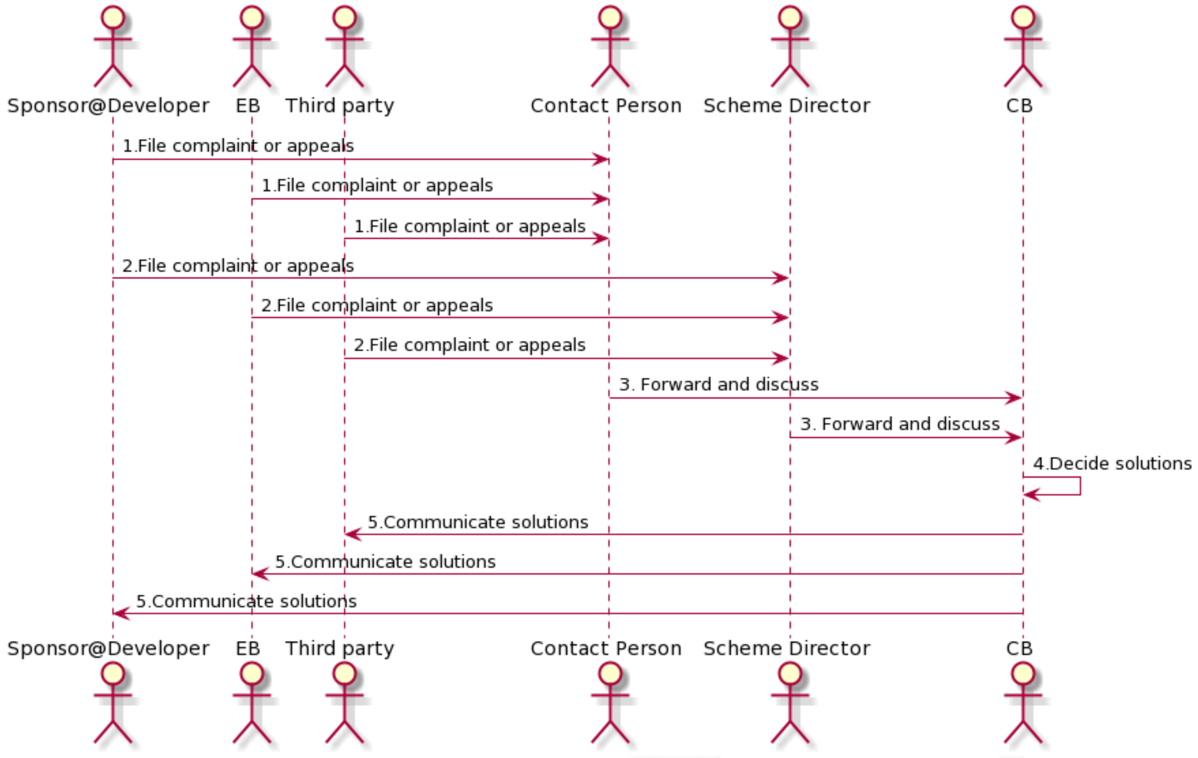

**Figure 8: Complaint and appeals**

The QCCS CB has a formal procedure to deal with complaints or appeals issued by the sponsor, the EB or any third party (anyone) that has a justified interest in the certification of a particular product or the certification procedure itself. They are as in below steps:

### 1.File complaint or appeals

In the first place, complaints or appeals should be filed to the contact person responsible for the respective project or certification scheme.

**2.File complaint or appeals**

However, the complainant or appellant may also contact the Scheme Director directly.

**3.Forward and discuss**

The contact person and Scheme Director will forward and discuss the issue inside the QCCS CB.

**4.Decide solutions**

Since the QCCS CB is interested in joint solutions, it will in many cases consult the complainant or appellant in order to consider his viewpoint.

**5.Communicate solutions**

The QCCS CB will then suggest a solution to the issue.

The QCCS CB finally communicates the solution in writing to the complaining or appealing party through electronic communication.

# 5 Terms and abbreviations

## 5.1 Terms

The current manual uses terms as defined in ISO/IEC17065 and CCRA.

## 5.2 Abbreviations

| | |
|---|---|
| ACO | CC assurance class composition |
| ADV | CC assurance class development |
| AGD | CC assurance class guidance documents |
| ALC | CC assurance class live-cycle support |
| APE | CC assurance class protection profile evaluation |
| ATE | CC assurance class tests |
| ASE | CC assurance class security target evaluation |
| AVA | CC assurance class vulnerability assessment |
| CB | Certification Body |
| CC | Common Criteria for Information Technology Security Evaluation (http://www.commoncriteriaportal.org) |
| cPP | Common Protection Profile |
| EB | Evaluation body |
| ETR | Evaluation technical report |
| IAR | Impact analysis report |
| OR | Observation report |
| PP | Protection profile |
| SER | Single evaluation report |
| ST | Security target |
| CCRA | Common Criteria Recognition Arrangement |
| TOE | Target of Evaluation |

# 6 History

| Version | Date | Comments | Author |
|---|---|---|---|
| 0.1 | 2015/07/27 | First Draft | TÜViT |
| 0.2 | 2015/08/27 | Additions | TÜViT |
| 0.3 | 2015/08/31 | Additions | TÜViT |
| 0.65 | 2015/10/04 | Additions | TÜViT |
| 0.7 | 2015/10/24 | Additions | TÜViT |
| 0.8 | 2019/11/20 | Additions | TÜViT |
| 0.9 | 2019/11/28 | Name and reference changes | MoTC |
| 0.91 | 2020/03/24 | Updated review | MoTC |
| 0.92 | 5.8.2020 | Comments-Additional templates, forms, workflows, flowcharts are required | CB/MOTC |
| 1.0 | 2020/08/27 | Final – Update document template | MoTC |

## End of Document