



**Common Security Evaluation &
Certification Consortium**
of GBIC and UKF

**Common
Security Evaluation & Certification
Consortium**

Common.SECC

Rule Book

Version 1.6

29-11-2018

Contents

1	Introduction.....	5
2	Security Requirements / Protection Profiles / Supporting Documents	5
3	First Evaluation.....	6
4	Maintenance.....	7
	4.1 Delta-Report in Case of Re-Evaluation.....	7
	4.2 Surveillance.....	8
5	Particular Rules	8
	5.1 Re-Usage of Site Audit Reports.....	8
	5.2 Usage of Device Names.....	9
6	Contacts	9
7	Annexes	9
8	References.....	9

Please note that the Common Security Evaluation & Certification Consortium should only be referred to using the shortened version “Common.SECC”.

Change History

Version	Date	Author	Changes compared to former version 1.3
1.4	1st September 2017	Common.SECC Coordination Committee	<ul style="list-style-type: none"> - New Logo integrated - Integration of the Footnote explaining the abbreviation - Integration of migration period to PP v4 as announced by email to vendors and labs on 17th May, 2017 - Integration of mandate to use the registration form offered on www.CSEC-consortium.org - Clarification of delta-evaluation rules - Description of surveillance process according to www.CSEC-consortium.org - Integration of rules to issue certificates and certification letter - Replacement of “UKCA” with “UK Finance” - Limitation of the contacts to the Common.SECC Secretary - Integration of Annex 4 Source Code Analyses for trial use (see also Annex 3) - Integration of mandate to use the BSI Template (see also Annex 3) - Integration of a change history
1.5	1 st January 2018	Common.SECC Coordination Committee	<ul style="list-style-type: none"> - New logo integrated (UK Finance) - Integrate new URL www.Common-SECC.org - Change of secretariat to Bill Reding

Please note that the Common Security Evaluation & Certification Consortium should only be referred to using the shortened version “Common.SECC”.

Version	Date	Author	Changes compared to former version 1.3
			<ul style="list-style-type: none"> - Dating all reference documents to 1st January 2018 including new versioning.
1.6	29 th November 2018	Common.SECC Coordination Committee	<ul style="list-style-type: none"> - Deletion of Variant Certification (former chapter 4.1) - Clarification of delta-evaluations in chapters 2 , 3 and 4.1. - Clarifications in chapter 4.2 Surveillance process - Integration of new version of Annex 2: JTEMS Evaluation Framework, Requirements on Site Audits, Version 2.0, 29 November 2018 in chapter 6. - Integration of new version of Annex 3: Rules to perform a POI Platform CC-Evaluation, Common Security Evaluation Consortium Version 2.0, 29 November 2018 - Integration of new version of Annex 5 Re-Assessment Statement - Integration of Annex 6 Common.SECC Modular Evaluation Guidance, Version 1.0 29 November 2018 - Clarification on surveillance and maintenance, and introduction of new arrangements - Integration of new chapter 5 Particular Rules for the re-usage of Site Audits and the usage of product names.

Please note that the Common Security Evaluation & Certification Consortium should only be referred to using the shortened version “Common.SECC”.

1 Introduction

UK Finance and GBIC signed a Consortium Agreement to establish and maintain a common POI security certification scheme. They named the common certification scheme “Common Security Evaluation & Certification Consortium“, the shortened version of which is “Common.SECC”. The Consortium is based on ISO 15408 Common Criteria as the evaluation methodology to be used for evidence.

Eligible evaluators have to be accredited by a SOGIS-CC-Certification Body¹ for the technical domain “Hardware Devices with Security Boxes“².

According to the above mentioned agreement POI security certificates will only be issued by the Common Certification Body (CCB) of the Consortium formed by representatives of GBIC and UK Finance. The Consortium’s security certificates can be used by the vendors to achieve approvals of both GBIC and UK Finance. Both approval bodies will accept the certificates within their own approval schemes. Whether vendors make use of the opportunity for this multiple recognition is left to them.

This document describes how the common process of the Consortium works.

2 Security Requirements / Protection Profiles / Supporting Documents

GBIC and UK Finance mandate the use of JTEMS Protection Profiles and supporting documents for POI platform-security evaluations. The SOGIS certified Protection Profiles cover the POI hardware and firmware which is called “POI platform” in this document. The payment application is not covered by these PPs.

UK Finance and GBIC did not change their security requirements within the Consortium:

¹ “Senior Officials Group Information Systems Security“ (for further information see www.SOGIS.org).

² Vendors can choose an evaluator out of this framework (see www.sogis.org). It is recommended to choose evaluators which are active members of JTEMS (see www.Common-SECC.org). The Consortium will also accept evaluators performing a POI CC evaluation the first time for SOGIS accreditation.

Please note that the Common Security Evaluation & Certification Consortium should only be referred to using the shortened version “Common.SECC”.

- UK Finance currently mandates the requirements according to [JTEMS PPV4]. Whether evaluations can be performed according to [JTEMS PPV4] using the chip only module PP in order to be accepted by UK Finance must be agreed on with UK Finance from case to case.
- GBIC mandates the security requirements according to [SECPUR]. For the acceptance of the certification by both GBIC and UK Finance currently [JTEMS PPV4] must be used. All requirements of [SECPUR], which are not covered by this PP, must be evaluated using the current GBIC specific evaluation methodology. This rule applies to the security requirements which are to be implemented
 - by the POI payment application and the EMV-Kernel and
 - in the personalization site to import the girocard network provider encryption keys.

These GBIC mandates are not covered in the Consortium's cooperation and are therefore out of scope of this document. The Open Protocol Package of [JTEMS PPV4] does not apply. The requirements to be met by a Common.SECC ETR are defined in Annex 2, Annex 3, Annex 4 and Annex 6 (if applicable).

3 First Evaluation

The following process has to be followed for the first platform evaluation:

1. The vendor / laboratory registers at the CCB for a CC security evaluation using the Consortium's Registration Form published on www.Common-SECC.org.
2. The vendor selects an eligible CC evaluator and orders a CC evaluation to evidence the security requirements according to the PP mentioned above.
3. The evaluator performs the CC evaluation and delivers the ETR to the vendor. Vendors are encouraged to use the Consortium's Best Practice document (see Annex 1) for support; evaluators have to use annexes 2, 3 4 and 6, if applicable..
4. The ETR is presented to Common.SECC.
5. The formal conformity of the ETR to the PP and the other Common.SECC requirements mandated by GBIC and UK Finance is checked by the Common.SECC CCB.
6. The contents of the ETR are assessed by the Common.SECC CCB.
7. If both the results of the formal checks and the security assessment of the CCB are positive the Common.SECC CCB issues a Security Certificate, which the vendor can use to achieve a GBIC and/or a UK Finance approval or an approval of other approval bodies willing to accept it.

Common.SECC issues certificates for a POI whenever the delivered ETR strictly claims a Protection Profile being declared valid by Common.SECC. Beyond this policy certification is performed by

Please note that the Common Security Evaluation & Certification Consortium should only be referred to using the shortened version "Common.SECC".

Common.SECC for other POIs based on these Protection Profiles but not providing for all assets defined in the PPs. For these evaluations Annex 6 must be used. For innovative concepts or architectures Common.SECC also accepts ETRs including residual vulnerabilities. The residual vulnerabilities may be addressed in claims in the Security Target and the evaluator may wish to re-evaluate the device based on these claims and this may result e.g. in the change of the scope of the TOE to solve the residual vulnerabilities.

These certificates can be used to achieve approval of GBIC and UK Finance on their own individual decision or other approval bodies willing to accept it.

Note: Registrations for POI approval (not certification) are handled separately within the approval schemes of GBIC and UK Finance and are therefore out of scope of this document.

4 Maintenance

4.1 Delta-Report in Case of Re-Evaluation

If the vendor changes an already certified POI the vendor is according to [Assurance] obliged to deliver an Impact Analysis Report IAR to the laboratory outlining the changes made. The IAR is to be delivered to the evaluator who must investigate the changes according to [Assurance]:

- If the changes are assessed as minor, these changes are evaluated resulting in a new certificate for the new versions of the platform using the same expiry date as the original certificate.
- If the changes are identified as major, a re-evaluation must be performed resulting in a new certificate issued with a new six years' validity.

In both cases a delta report must be delivered. To simplify the process for assessment of the ETR and certification it is recommended that the evaluator uses the original ETR as the basis for the delta-report.

The delta-report must outline the high level results of the vendor's IAR explaining what changes were made and why, and explaining whether they are assessed as minor or major changes. The text must be marked with revision marks if the original ETR is used as the basis for the delta-report. This can be done in a [JTEMS PPv2] report if the original ETR used [JTEMS PPv2].

To achieve a new six year validity of the certificate the delta-report must demonstrate that the changes identified in the IAR are evaluated and that there is no impact on the already certified parts of the product and that the whole platform remains secure. A clear re-evaluation verdict for the whole re-evaluated platform is required. If this verdict is also delivered in the delta-report for the old already certified POI this POI is also included in the new certificate issued with a new six year validity. If applicable, variants that the vendor does not want to carry forward, can be dropped in the delta-report. This must be explicit via the revision marks and in the text of the delta report, and will be made explicit in the certificate.

Please note that the Common Security Evaluation & Certification Consortium should only be referred to using the shortened version "Common.SECC".

This process must also be performed in cases of emergency for already deployed POI when, for example, new attack methods are published and the changes of the POI to meet them impact the implementation of the security requirements of GBIC and UK Finance.

4.2 Surveillance

The Consortium uses a surveillance process for POI security to protect consumers and merchants. It works as follows:

A Common.SECC Certificate is valid for six years from its date of issuance. Three years after the date of issuance a re-assessment of the evaluator is required confirming that the TOE version(s) certified three years ago including all subsequent re-evaluations of minor changes still meets the Common.SECC security requirements.

The re-assessment should preferably be delivered by the evaluator that carried out the original evaluation of the TOE.

If the re-assessment is delivered within three years this will be shown on the Common.SECC web page device library. If the re-assessment is not delivered within three years this will be indicated on the Common.SECC web page device library as “Re-assessment Missed”. The wording to be used in a re-assessment statement is defined in Annex 5. This applies to all TOE versions included in the originally issued certificate unless stated differently in the statement.

Surveillance re-assessment applies only where a product has not been subject to a re-evaluation during the past three years.

5 Particular Rules

5.1 Re-Usage of Site Audit Reports

[JTEMS PPv4] requires site audits which shall be performed according to Annex 2.

Site audits can be re-used for three years. Within the following 2 years an Impact Analysis Report IAR produced by the vendor can be used by the evaluator to investigate the security impact of the changes. The IAR must include an evaluable description of all changes made after the original site audit. The lab’s security assessment may indicate that

- no security relevant changes are described. In this case the lab does not perform a new Site Audit and will ask the developer to confirm the changes in a formal and signed statement letter to which the lab will refer in the ALC part of the ETR.
- the changes are security relevant. Depending on the assessed nature and impact of the changes the lab will perform a new site audit or will perform an assessment based on the IAR to which it will refer in the ALC part of the ETR.

Please note that the Common Security Evaluation & Certification Consortium should only be referred to using the shortened version “Common.SECC”.

This procedure only applies if the IAR assessment is performed by the same evaluator which performed the original site audit.

5.2 Usage of Device Names

The combination of vendor name and device name must be unique for Common.SECC purposes. If a vendor has two distinct devices with the same name that the vendor wishes Common.SECC to treat separately, then the laboratory should determine that. In such cases Common.SECC will append a version identifier to the second and subsequent device names for the purpose of listing on its web site, naming in certificates, and referring to devices for surveillance, maintenance and so on.

6 Contacts

Stakeholders needing further information on the Consortium's process should contact common-secc@ukfinance.org.uk.

7 Annexes

Annex 1: Common Criteria Evaluation of POIs – Best Practice, Common Security Evaluation Consortium, version 1.2, 01-01-2018

Annex 2: Common.SECC Requirements on Site Audits, version 2.00, 29-11-2018

Annex 3: Common.SECC Rules to perform a POI Platform CC-Evaluation, Common Security Evaluation Consortium Version 2.0, 29-11-2018

Annex 4: Common.SECC Source Code Analysis Requirements, version 0.91 (for trial use), 01-01-2018

Annex 5: Wording for a Re-assessment Statement, version 1.0, 29-11-2018

Annex 6: Common.SECC Modular Evaluation Approach, version 1.0, 29-11-2018

8 References

[Assurance] Assurance Continuity: CCRA REQUIREMENTS VERSION 2.1, June 2012
<https://www.commoncriteriaportal.org/files/operatingprocedures/2012-06-01.pdf>

Please note that the Common Security Evaluation & Certification Consortium should only be referred to using the shortened version “Common.SECC”.

[JTEMS PPV2] Point of Interaction POI Comprehensive, sogis.org/uk/pp_pages/poi/pp_poi_comprehensive.html, www.sogisportal.eu

[JTEMS PPV4] Point of Interaction Protection Profile, POI-CHIP-ONLY base PP, www.commoncriteriaportal.org/pps/

[SECPUR] Criteria for the Evaluation and Construction of electronic cash-systems - Security requirements for terminals in the purely chip-based girocard payment system, Version 1.0, 2013-02-20

[Registration] Consortium Registration Form, www.Common-SECC.org.

Please note that the Common Security Evaluation & Certification Consortium should only be referred to using the shortened version “Common.SECC”.