Common Security Evaluation &
Certification Consortium
of GBIC and UK Finance

Common.SECC
Rule Book

Version 2.0

19 December 2023

Contents

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 versions
1.4	1st September 2017	Common.SECC Coordination Committee	- 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	1st January 2018	Common.SECC Coordination Committee	- 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 versions
			- Dating all reference documents to 1st January 2018 including new versioning.
1.6	29th November 2018	Common.SECC Coordination Committee	- 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.
1.7	10th May 2019	Common.SECC Coordination Committee	- Inclusion of NO CVM PP and alignment of PP versions - Modification for re-evaluations - Mandate for SER templates in Annex 3

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 versions
			- Editorial changes
1.8	30 July 2020	Common.SECC Coordination Committee	- Inclusion of Annex 7 - Inclusion of optional POI payment applications as evaluation and certification objects, Annex 8 - Editorial adjustments
1.81	22 December 2020	Common.SECC Coordination Committee	- Editorial changes to references
1.9	1 April 2022	Common.SECC Coordination Committee	- Inclusion of a paragraph in section 3 about evaluator change - Inclusion of a sentence in section 4.2 about the issuance of a new six year certificate following to the re-assessment statement.
1.91	7 October 2022	Common.SECC Coordination Committee	- Inclusion of a new section 4.1.2 to address patches and the use of wildcards - Inclusion of a sentence in section 4.2 to explain that is the vendor's responsibility to arrange a surveillance evaluation - Replacement of 'device' by 'product' as appropriate
2.0	23 October 2023	Common.SECC Coordination Committee	- Changes to allow for Software POIs and to refer to the Software POI PP. - Changes to address security patches - Editorial changes in section 5.2, changes to name of Annex 7, corrections to links in section 7

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 Body[1] for the technical domain **“**Hardware Devices with Security Boxes**“**[2] or “All products”.

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 by both GBIC and UK Finance. Both approval bodies will accept the certificates within their own approval schemes.[3] 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.

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

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

[2] Vendors can chose an evaluator out of this framework (see www.sogis.eu). It is recommended that evaluators 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.

[3] Each approval body may have additional requirements, and deployment will also be subject to compliance with scheme rules.

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

2 Security Requirements / Protection Profiles / Supporting Documents

2.1 POI Platform Evaluations

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

Within Common.SECC the following Protection Profiles can be used:

- [JTEMS PP V4 COMPREHENSIVE]
- [JTEMS PP V4 COMPREHENSIVE_SRED]
- [JTEMS PP V4 Chip Only]
- [JTEMS PP No CVM]
- [JTEMS PP Software Payment - draft for trial use]

It is the vendor’s responsibility to make sure that their product suits the approval requirements of the relevant approval schemes. Common.SECC is not responsible in this regard.

The Open Protocol Package included in the above mentioned PPs is not applicable for certification by Common.SECC as by using CC evaluation methodology the requirements of this package are covered implicitly.

The requirements to be met by a Common.SECC Evaluation Test Report (ETR) are defined in Annex 2, Annex 3, Annex 4 and Annex 6 (if applicable).

A Common.SECC Certificate based on a full evaluation of a product is valid for three or six years from its date of issuance: six years for a hardware-based product and three years for a software (COTS-based) product.

2.2 POI Payment Application Evaluation

In addition to the POI platform Common.SECC offers the security evaluation and certification of the Payment Application of the POI as an option.

The requirements to perform this application evaluation and to receive an application certificate are described in Annex 8.

A Common.SECC application Certificate is valid for six years from its date of issuance.

3 First Evaluation

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

1. The vendor / laboratory registers at the CCB for a CC security evaluation using the Consortium's Registration Form published on the www.Common-SECC.org website.
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 and 8, 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.

In principle, Common.SECC issues certificates for a POI whenever the delivered ETR strictly claims a Protection Profile being declared as valid by Common.SECC.

Beyond this policy, certification may be possible 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 vulnerabilities. The vulnerabilities may be addressed in claims in the Security Target and the evaluator may wish to re-evaluate the product based on these claims. This may result e.g. in the change of the scope of the TOE to solve the vulnerabilities. These certificates can be used to achieve approval of GBIC and UK Finance at their discretion or other approval bodies willing to accept them.

Common.SECC does not interfere in the vendor-evaluator relationship. However, it is recommended that vendors take care to clearly define the terms and conditions in their evaluation contracts in case they may wish to change the evaluator for subsequent activity to allow them the necessary insights and access.

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 Re-Evaluation

4.1.1 Delta-Report based on Impact Analysis Report (IAR)

If the vendor changes an already certified POI the vendor is obliged to deliver an IAR to the laboratory outlining the changes made. The evaluator investigates whether the changes are security relevant and need evaluation.

If the evaluator assesses the changes to be security relevant a delta report must be delivered to the Common Certification Body. 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. 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].

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 to the POI to meet them impact the implementation of the security requirements of GBIC and UK Finance.

4.1.2 Validity of certificates

To achieve a new certificate with a full validity period the delta-report must demonstrate that the changes identified in the IAR are evaluated, that no impact on the already certified parts of the product does apply and that the whole platform/application remains secure. In this case the following re-evaluation verdict for the whole re-evaluated platform/application is required:

> "The platform/application versions <all platform/application versions covered by the delta evaluation> pass all security requirements of <PP version used for the evaluation> and resist all known state-of-the-art attack methods at the time of re-evaluation."

If the verdict in the delta-report includes the already certified platforms/applications these POI versions are also included in the new certificate issued with a new full validity period. 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.

If the above mentioned verdict is not included in the delta report because the re-evaluation has not re-considered the complete TOE and/or known state-of-the-art attack methods, a certificate is issued using the same expiry date as the original certificate.

4.2 Surveillance

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

- For a hardware-based product, 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 still meet(s) the Common.SECC security requirements and resists all known state-of-the-art attacks. In order to achieve the same level of assurance a re-assessment for surveillance must also be performed for re-evaluations which resulted in a certificate using the same expiry date as the original certificate within three years after the date of issuance of the original certificate.
- For a software (COTS-based) product, one year after the date of issuance a re-assessment of the evaluator is required confirming that the TOE version(s) certified a year ago still meet(s) the Common.SECC security requirements and resists all known state-of-the-art attacks. In order to achieve the same level of assurance a re-assessment for surveillance must also be performed for re-evaluations which resulted in a certificate using the same expiry date as the original certificate within a year after the date of issuance of the original certificate.

The re-assessment should preferably be delivered by the evaluator that carried out the original evaluation of the TOE. It is the vendor's responsibility, as the applicant for the certificate, to arrange for the re-assessment to be performed.

If the re-assessment is delivered within the required period this will be shown on the Common.SECC web page product library. If the re-assessment is not delivered in time this will be indicated on the Common.SECC web page product 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.

The Re-Assessment statement gives the product a new 6-year or 3-year certificate as appropriate.

4.3 Patch management

Any patch update that has a direct impact on the Security Functionality Requirements (SFRs) listed in the Security Target (ST) must be advised to Common.SECC and must be expressed by a patch version number. Wildcards are not allowed in these cases.

Security patches to fix publicly announced vulnerabilities in third-party products, with a direct impact on SFRs, are an exception to this rule. They should be applied as soon as possible, to avoid the exploitation of a vulnerability, and must be advised to Common.SECC. Products with such security patches applied since the last full evaluation should be reassessed annually by a laboratory as described under section 4.2 Surveillance. Version numbers following these patches may be included in wildcards as shown on the website and in certificates.

Patches to such vulnerabilities must be reported to Common.SECC as soon as they are applied, or at least annually. Information provided should give the vulnerability identifier, the names and identifiers of the parts of the product that were affected, an identifier for the patch, and the date it was applied.

Patches to the vendor's own software should also be applied as soon as possible. In this case they must be checked by the developer (e.g. as part of the POI life cycle (ALC)) to determine whether the patch affects the SFRs or not. If this review confirms that an impact exists, a re-evaluation to obtain a new certificate must be pursued, as described in section 4.1 Re-evaluation. For this purpose, the developer may also consult the expert advice of an ITSEF.

The above rules apply for all future certifications.

5 Particular Rules

5.1 Re-Usage of Site Audit Reports

All Protection Profiles listed in the References require site audits which shall be performed according to Annex 2.

Site audits can be re-used for three years. Within the following two 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.

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

5.2 Usage of Product Names, and Co-listing of Products

The combination of vendor name and product name must be unique for Common.SECC purposes. If a vendor has two distinct products 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 first, second and subsequent product names for the purpose of listing on its web site, naming in certificates, and referring to products for surveillance, maintenance and so on.

A product may be listed under more than one name on the website, if the vendor wishes. More detail on this is given in Annex 7.

6 Annexes

Annex 1: Best Practice to perform a CC-Evaluation of POI Platforms, version 1.4, 22-12-2020

Annex 2: Security Requirements for Site Audits, version 2.1, 30-07-2020

Annex 3: Evaluator Rules to perform a CC-Evaluation of POI Platforms, Version 3.2, 08-03-2022

Annex 4: Source Code Analysis Requirements, version 0.91 (for trial use), 30-07-2020

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

Annex 6: Modular Evaluation Guidance, version 1.1, 08-03-2022

Annex 7: Co-listing of Products, version 0.2, 19-12-2023

Annex 8: Evaluation of the Payment Application, version 0.9, 30-03-2020.

7 References

[JTEMS PP V4 Chip Only], see: https://common-secc.org/documents-links/ and http://sogis.eu/uk/pp_pages/poi/pp_poi_comprehensive.html

[JTEMS PP V4 COMPREHENSIVE], see: https://common-secc.org/documents-links/ and http://sogis.eu/uk/pp_pages/poi/pp_poi_comprehensive.html

[JTEMS PP V4 COMPREHENSIVE_SRED], see: https://common-secc.org/documents-links/ and http://sogis.eu/uk/pp_pages/poi/pp_poi_comprehensive.html

[JTEMS PP No CVM] NO-CVM Point of Interaction Protection Profile, version 1.0, 2019-04-01, see: https://common-secc.org/documents-links/

[JTEMS PP Software Payment] Software Payment Point of Interaction Protection Profile, version 1.0, date 2023-10-23 - draft for trial use – see https://common-secc.org/documents-links/

[Registration] Product Registration Form, https://common-secc.org/documents-links/

[JTEMS PPV2] Point of Interaction POI Comprehensive, https://www.ssi.gouv.fr/uploads/IMG/certificat/ANSSI-CC-cible_PP-2010-10en.pdf