Common Security Evaluation & Certification Consortium of GBIC and UKF

Common Security Evaluation & Certification Consortium

Process Description

Certification Scheme

Version 1.5

16 January 2018

Contents

1 Introduction....5
2 Security Requirements / Protection Profiles / Supporting Documents....5
3 First Evaluation....6
4 Maintenance....7
4.1 Variants....7
4.2 Delta-Evaluation....8
4.3 Surveillance....8
5 Contacts....9
6 Annexes....9
7 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
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 consortium web site - Clarification of delta-evaluation rules - Description of surveillance process according to consortium web site - 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	16 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
			- Enhancement of the surveillance description regarding the validity periods.

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 have 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].

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 the vendor makes use of the opportunity for this multiple recognition is left to him.

This document, which is also known as the “Playbook”, 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 hard- 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 chose 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 PPV2] or [JTEMS PPV4]. Evaluations according to [JTEMS PPV4] using the chip only module PP must be agreed on with UK Finance on a case by case basis.

- GBIC mandates the security requirements according to [SECPUR] which are covered by all JTEMS PPs. For the acceptance of the evaluation by both GBIC and UK Finance currently [JTEMS PPV2] or [JTEMS PPV4] must be used. All requirements of [SECPUR], which are not covered by the above mentioned PPs, 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.

For all evaluation reports being delivered to the Consortium from 1st March 2017 onwards the documents "Attack Methods for POIs, 01.95, February 2015" [JTEMS_Attacks] and "JIL Application of Attack Potential to POI, Version 1.92" [JTEMS_Potential] including all new attacks being known since the publication of these documents, e.g. described in the JTEMS minutes, are mandatory. This rule applies independent of the use of [JTEMS PPv2] or [JTEMS PPv4].

ETRs of evaluations for Common.SECC certification must be registered with [JTEMS PPV4] from 1 September 2017 onwards. Registrations of evaluations before this date can be performed with PPs v2. For the registration of upcoming evaluations the registration form offered under "https://common-secc.org/certification/" must be used. 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 and Annex 4.

3 First Evaluation

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

1. The vendor registers at the CCB for a CC security evaluation using the Consortium's Registration Form mentioned above.
2. The vendor selects an eligible CC evaluator and orders a CC evaluation to evidence the security requirements according to the PPs 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 the annexes 2, 3 and 4 as well as [JTEMS_Potential] and [JTEMS_Attacks].

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

4. The formal conformity of the ETR to the PPs mandated by GBIC and UK Finance are checked by the CCB.
5. The contents of the ETR is assessed by the CCB.
6. If both, the results of the formal ETR check and the security assessment of the CCB are positive the CCB issues a Security Certificate, which the vendor can use to achieve a GBIC and/or a UK Finance approval.

Common.SECC issues certificates for a POI whenever the delivered ETR strictly claims a Protection Profile being declared valid by Common.SECC. Beyond this rule certification letters can be issued for other POI basing on these Protection Profiles but not providing for all assets defined in the PPs. These letters can be used to achieve approval of GBIC and UK Finance on their own individual decision.

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 Variants

For the maintenance of Consortium's POI certificates the following use cases are defined.

Use Case 1:

The vendor changes an already certified POI, but these changes do not impact the implementation of the security requirements of GBIC and UK Finance. In this case the CCB does not have to be informed and the issued certificate is not impacted. If the vendor, however, wishes to receive a certificate for the changed new POI version, he can officially confirm to the CCB that the changes performed do not impact the implementation of the requirements of the Consortium. For this confirmation [Variant Application Form] must be used.

It is up to the vendor to strengthen his confirmation by an evaluator statement.

The CCB will in this case complete the certificate already issued adding the variants by referring to the vendor confirmation (and evaluator statement, if present) and issue separate, actually dated certificates.

Use Case 2:

Use Case 2 is identical to Use Case 1, the ETR to which the vendor refers to is however older than 24 months.

In this case the CCB requires an evaluator statement in addition stating that the POI platform still meets the security requirements according to the state of the art.

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

If this statement cannot be presented, a Delta-Evaluation must be performed.

4.2 Delta-Evaluation

The following Use Case is defined:

The vendor changes an already certified POI in a way that impacts the certified implementation of the security requirements of the Consortium. In this case the vendor is obliged to perform a delta-evaluation of the changes performed in order to receive a new certificate for the new version of the POI. The vendor must present the necessary evidences to the evaluator for delta-evaluation.

To simplify the process for evaluation and certification the evaluator must use the original ETR, indicate at the beginning of the report that this is a delta-evaluation and explain the changes made including the rationale for the changes. This new text must be marked with revision marks in the ETR.

The evaluator must investigate the changes according to [Assurance].

The ETR of the re-evaluation will be checked by the CCB. Having a positive result a new certificate will be issued to the vendor. This process must also be performed in cases of emergency for already deployed POI when e.g. new attack methods are published and the changes of the POI to meet them impact the implementation of security requirements of GBIC and UK Finance.

4.3 Surveillance

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

a) 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 certified three years ago still meets the Common.SECC security requirements. The re-assessment should preferably be delivered by the evaluator that carried out the original assessment of the TOE. If the re-assessment is delivered after three years this will be shown on the Common.SECC web page device library. If the re-assessment is not delivered after three years this will be indicated on the Common.SECC web page device library as “Re-assessment Missed”.

b) This applies to all TOE versions included in the originally issued certificate. If an already Common.SECC certified TOE is changed in a security relevant way it needs delta-evaluation and a new certificate will be issued for this new version of the TOE. For this newly issued certificate the process described under a) applies accordingly. The three and six year validity dates of such a delta certificate will be the same as for the original certificate for the product.

5 Contacts

Stakeholders using the Consortium's process should contact

Bill Reding, UK Finance, One Angel Court, 30 Throgmorton Street, London EC2R 7HJ
(Bill.Reding@ukfinance.org.uk)

6 Annexes

Annex 1: Common Criteria Evaluation of POIs – Best Practice, Common Security Evaluation Consortium, v1.2, 16 January 2018

Annex 2: Requirements on Site Audits, Common Security Evaluation Consortium, Version 1.8, 16 January.2018

Annex 3: Rules to perform a POI Platform CC-Evaluation, Common Security Evaluation Consortium Version 1.3, 16 January 2018

Annex 4: Common.SECC Source Code Analysis Requirements, version 0.91 (for trial use), 16 January 2018

[Variant Application Form] Confirmation to achieve a variant certificate, version 2, 16 January 2018

7 References

[Assurance] Assurance Continuity: CCRA REQUIREMENTS VERSION 2.1, June 2012 www.sogisportal.eu

[JTEMS_Attacks] Attack Methods for POIs, 01.95, February 2015

[JTEMS_Potential] JIL Application of Attack Potential to POI, Version 1.92

[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".