Common.SECC

Process Description

Best Practice to perform a CC-Evaluation of POI Platforms

Annex 1

Version 1.2

16 January, 2018

Content

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

1 Introduction

Common Criteria (CC) is a vendor driven evaluation standard focusing on the interfaces of the IT security product. Therefore CC is strong in evaluating software if the software is complex and the evaluator steps cannot be easily identified. EAL POI provides more or less the same level of assurance as e.g. PCI PTS in the area of hardware evaluation.

CC is vendor driven because the verdict of the evaluators is based on the evidence and rationale given by the vendor. Only the area of independent testing and penetration testing is evaluator driven.

A vendor who wants to know what is expected by the evaluator may read the [CEM] to find the work units of the evaluators. Seeing what the evaluator has to do, the vendor should understand what the vendor has to provide. Additional information can be found in [DEV CC].

It is therefore recommended that a vendor benefits from this approach by providing the exact evidence that is needed for the evaluation. For CC a well documented product will lead most probably to the most cost and time efficient evaluation whereas negligently provided evidence will very probably lead to increased costs and time.

2 Target of Evaluation (TOE)

The TOE is the **t**arget **o**f **e**valuation and thus the specific part of the product which is going to be evaluated. The TOE can be a subset of a product. In order to identify the TOE, the subset of the product shall meet all functional security requirements of the PP (SFRs). The functional security requirements are claiming what the product itself (hardware, software, guidance) has to meet. Thus, the TOE covers the security functionality of the product.

E.g. a printer can be excluded from the TOE because it does not contribute to the SFRs. Or a PIN-Pad is not sufficient to cover the SFRs related to the protection of the payment transaction data which are also processed in the non-PIN-Pad part. Thus a whole standard POS-Terminal is expected to be the TOE in the POI-COMPREHENSIVE configuration where external peripherals, e.g. a printer, can be excluded.

3 Security Target

Preliminary Note: Parties exist who do not see a benefit in writing a Security Target because Security Targets from different products are not significantly different. Even the TOE summary specification does not really include detailed technical information.

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

However, according to the CC point of view the TOE description gives technical information about the POI, the SFRs include technical details in their assignments (e.g. the Random Number Generator to be selected or cryptographic algorithms). Other SFRs may be iterated i.e. being applied more than one time. The ST also refers to guidance documents in order that the user knows which guidance documents were evaluated. According to the CC point of view a Security Target is therefore a necessary document to address the exact security requirements met by the POI and to give security related information about the evaluated POI on a more general level.

The Protection Profile offers configuration options for an evaluation. The PPs used by GBIC are CC conformant evaluation methodology implementations of the EPC security requirements [Volume]. The vendors have to ask the approval bodies which options are required for approval. The POI-COMPREHENSIVE configuration covers the full set of functional security requirements, thus an evaluation according to that would meet the expectation of a comprehensive user group.

Note: Pilot CC evaluations according to the POI-COMPREHENSIVE PP v2 have been published under [VER CC1], [VER CC2], [ING CC] and [SE CC].

The Security Target can be derived from the Protection Profile. To do that the following steps have to be done:

1. The configuration has to be selected and all parts in the PP have to be deleted which are not related to the chosen configuration. E.g. if POI-COMPREHENSIVE is chosen, the POI-CHIP-ONLY parts are to be deleted. It has not been evaluated whether by deletion a consistent subset remains. But the authors have written the PP in the way to allow a consistent deletion. Information about how to choose a configuration is found in the first chapters of the PP.

2. A TOE Overview/ TOE Description has to be written as the introductory part of the ST. Usually that part can be easily derived from the product data sheet of the POI.

3. The vendor has to work on the SFR part. The SFRs (Security Functionality Requirements) of the PP are taken from the CC standard part 2. The SFRs are formal templates to allow the PP author a precise definition of the functional security requirements. Because of the formal structure of the SFR it is not always easy to understand the content of the SFR. Therefore some examples are outlined to enhance the understandig as follows.

   SFRs which are not part of the chosen configuration have to be deleted.

   The “selection” and “assignment” operation have to be processed. For that purpose the vendor has to fill the brackets in order to give the specific information for his product. E.g. in FCS_COP the supported cryptographic algorithms and the key length

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

have to be written into the SFR. E.g. in FDP_RIP the sensitive information has to be given which is deleted. There is also an operation called “iteration”. If a SFR is not sufficient to describe the fulfillment of the SFRs by the product, a second SFR can be added to the ST (or a third, a forth, …). These iterations are normally identified by a slash ‘/’.

Please note that the application note is the essential information for the interpretation of the SFR. It is not the intention of the PP authors to go beyond the EPC security requirements. Thus the SFRs have always to be understood as the CC implementation of the EPC security requirements.

Please download the STs of the pilot evaluations from the CC schemes’ homepages [VER CC1], [VER CC2], [ING CC], [SE CC] to see how the SFRs are implemented there. Please note that the optional SRED module was not used during the pilot evaluations.

4. The vendor has to work on the TOE Summary Specification. During that step the vendor explains the technical features of the POI implementing the SFRs. The TOE Summary Specification has to give a rationale how the SFRs are implemented. For this purpose the SFRs shall be immediately referred to the TOE Summary Specification. The TOE Summary Specification can be developed based on the security objectives. The security objectives are already linked to the SFRs thus the SFR compliance rationale is very easy. The security objectives shall be extended by the technical means of the POI implementing the SFRs. Please download the STs of the pilot evaluations from the CC schemes’ homepages [VER CC1], [VER CC2], [ING CC], [SE CC] to see how the TOE Summary Specification has been written there.

4 Functional Specification (FSP)

The FSP is the crucial aspect of the CC evaluation. In order to understand what is required in the FSP the concept of the TSF has to be understood by the vendor (see [CC WS PRE]). From this concept the TOE Security Functional Interfaces (TSFI) are derived.

The vendor has to identify the TSFI of the TOE. The TSFI can be classified in

- TSFI by which the TOE can be attacked (non-interfering), but these TSFI does neither support nor enforce the implementation of the SFRs. For these TSFI the vendor has to provide design information to the evaluator (“purpose”, “method of use”, “parameters”, see definition in the CC standard).
- There are also supporting TSFI. For these TSFI the vendor has to provide information like for non-interfering TSFIs.

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

- More information has to be provided for TSFI which enforce the implementation of the SFR. E.g. the interfaces where the encrypted PIN is sent to the smartcard or to the background system, are SFR-enforcing TSFI. For these TSFIs the vendor has to provide more information (in addition “actions”, “error messages”).

What are the interfaces of the TOE in the POIs? Not only hardware but also logical interfaces must be considered. Therefore also the transport layer as well as the application layers can be TSFIs and the evidence has to be provided accordingly.

It has to be noted that the current PPs provides requirements for a platform evaluation. Thus software running on the platform (e.g. apps) can be excluded from the TOE and thus interfaces of the software only running on the platform need not necessarily to be TSFIs. Instead the API of the platform belongs to the external interfaces of the TOE. Thus the evaluator has to provide the related evidence for the API.

If the API supports security functions which are not meeting the SFRs, e.g. the API supports Single-DES, this information has to be made public to the developer of the software running on the platform. This is usually done in a security guidance which is evaluated, too. The developer of the software running on the platform has to be informed about each API call which is not conformant with the PP. In either case the vendor has to provide the API call meeting the SFR but is also allowed to provide API calls not meeting the SFRs if the developer of the software is informed about it. Certainly, it must not be possible to attack the SFR-enforcing API by any non-PP conformant API call.

The authors of the PP assumed that transport layer interfaces are fully processed by the platform. Thus the authors assumed that software running on the platform accesses the external transport layer interface via the platform API only. However, if there is a need that a software running on the platform implements a specific interface not being part of the platform, this can be done in a way being conformant to the PP. The reason for that is that application separation is also required by the PP. Thus if the external interface can be implemented in a way not harming any other application, it is possible to extend the TOE by that external interface for field application without harming the CC approval.

For the external interfaces there may be secure and insecure configuration. There must be documents available for the user of the POI or for the developer of the software running on the platform to use the platform in a secure way. Thus if there are insecure configuration e.g. the security guidance shall address them and say that it is not allowed to use them in the certified configuration (e.g. this can hold for an insecure SSL version). Any configuration which is allowed to be used by the user of the POI/ the developer of the software running on the platform has to be described according to the requirements of FSP.

There are SFRs which cannot be mapped to TSFIs. The implementation of such SFRs has no external interfaces. This holds e.g. for SFRs related to hardware protection but also for SFRs related to the deletion of internal data. In order that the evaluator gets design infor-

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

mation for these SFRs, too, the vendor has to provide the information in the security architecture (see future chapter for the evaluation of the security architecture).

5 Security Architecture (ARC)

The vendor has to provide a security architecture to the evaluator. The vendor has to explain in that document why he is convinced that the product meets the functional security requirements. The security architecture is the vendor counterpart of the evaluator's vulnerability analysis. CC already indicates via the related content requirements what is expected at a minimum in a security architecture: i.e. descriptions of

a) security domains,

b) initialisation process

c) self-protection

d) non-bypassability

ad a) Security domains define areas where the processing of sensitive data is separated from other functionality when the POI supports domain separation.. Such a domain separation can be provided logically or physically by a security chip and its operating system. Another security domain separation may be provided by a two processor architecture the separation between an application processor and a security processor.

Ad b) For the initialisation process a description of any initialisation process of the POI is expected like e.g. the start-up.

Ad c) Self-protection from a hardware perspective summarizes the usual physical means which are provided by a POI (tamper-responsiveness, switches, security modules, …). However, self-protection applies also to software means like self-test or a secure update mechanisms.

Ad d) For non-bypassability the vendor has to give a rationale why he is convinced that the security requirements cannot be bypassed. Logically this is usually a reflection of the external interfaces in order that all external interfaces are listed and rationales are given why this interfaces cannot be misused (e.g. a SFR-enforcing interface is well designed and tested according to the provided vendor evidence for FSP and ATE, an interface is not a TSFI because of architectural means e.g. a printer interface,…).

In addition, the security architecture has always to give a rational for security requirements where no TSFI has been assigned in the FSP. It has to be kept into consideration that SFRs may exist where no TSFI can be addressed (thus not external interface). This may hold for physical mechanisms like tamper-responsive mechanisms which do not have external inter-

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

faces per definition. Why such mechanisms without any external interface are effective has to be described in the security architecture.

Please note that a vendor questionnaire being available for a PCI PTS evaluation may be a good input to provide a security architecture. This holds especially for the hardware means provided by the POI where vendor questionnaire hardware evidence can be used.

The vendor may provide any other arguments in the security architecture to show why he is convinced that his product meets the security requirements. E.g. logically it is expected that he is basing his rationale on a check of the CVE entries or that he is describing his efforts hardening his operating system (this would especially hold for Android or Linux).

But also other arguments are possible like the usage of static analysis tool. Note: It is expected that the JTEMS user group will work in that item to harmonize the content of the security architecture.

Information what is expected in a security architecture can be derived from the [CEM] as well as from [DEV CC].

6 TOE Design (TDS)

The vendor has to provide information about the TOE design for that aspect. Whereas FSP reflects the external interfaces and the security architecture focuses on the security means this aspect shall provide information about the internals of the TOE in general.

It is expected that the vendor decomposes the product ins so-called subsystems. There is no requirement how many subsystems have to be provided. However, it has to be a meaningful separation. Thus the vendor is not allowed to provide one subsystem. In that case there would not any decomposition. If he provides two subsystems this may be sufficient however there has to be a good rationale why no additional decomposition has been provided. A good number of subsystems may be 6 to 10.

Subsystems can be physical only (hardware), logical only (software) or a subsystem can be both.

One idea to decompose the TOE into subsystems can be to do that based on the level of protection. Thus the area where the protection level is high (keypad, key protection) could be one subsystem, the area where the protection level is low (application processor) could be another subsystem.

All in all it depends on the rationale for the decomposition and whether the evaluator is satisfied by the decomposition of subsystems chosen by the vendor.

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

It has to be kept in consideration that the interfaces between the subsystems has also be part of the evidence provided by that aspect. This is one reason why CC requires a TOE design. If the POI is separated between an application processor and a security processor the TOE design would give internal information about the internal interface between the application processor and the security processor.

It has to be noted that the TOE design is the lowest level of internal information which has to be presented independent from the analysis of the evaluator. The JTEMS user group decided not to mandate the next level ADV_IMP for the evaluation because of the dependencies of ADV_IMP. These dependencies would lead to much higher assurance levels in other aspects like FSP which were not wished by the group. However, the evaluators had to do code analysis if they are convinced that without any code analysis they cannot prove that a security requirement is met (e.g. to check buffer overflows or the deletion of sensitive data after usage cannot be done without a code analysis). In addition, hardware drawings are necessary to allow the evaluators to perform hardware penetration tests and to rate them. However, such information has to be provided outside the TOE Design aspect during the vulnerability analysis of the evaluators (AVA_POI).

7 Life-Cycle (ALC)

The life-cycle aspect related to the configuration management system (ALC_CMC.2), the coverage of the configuration management in relation to the POI (ALC_CMS.2), the delivery procedures (ALC_DEL.1) and the sufficiency of security measures (ALC_DVS.2) are the assurance requirements of ALC. In addition refinements compared to CC are defined for the mentioned assurance requirements. These refinements are caused by life-cycle PCI security requirements the PP claim to comply with. From the available description only additional information seem to be necessary for ALC_DVS.2 which is done in the following.

ALC_DVS.2 requires site visits (see below), but only for the initial-key loading and for the final manufacturing step. Any other development environment shall only be described paper based but no site visit is necessary for that development environment. ALC_DVS.2 requires:

ALC_DVS.2.2E The evaluator shall confirm that the security measures are being applied.

CAS E9: The evaluator shall confirm that the security measures are being applied by examination of the developer's documentation and evidences. The security measures involving the final assembly and the Initial Key Loading facilities shall be checked during a site visit.

According to the OSeC decision from 31st October 2012 the following holds: “Initial Key Loading Facility and the Final Assembly Facility sites are to be audited. The definition of the precise sites to be audited for both functions depends on the individual life cycle, which must be provided by the vendor. If several sites exist, handled by the same quality management

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

system, and therefore similar procedures, the vendor must propose at least one site for auditing. If no agreement on the sites can be achieved the approval body can be contacted for escalation and decision." Therefore at least one site visit has to be performed. These requirements are more precisely explained as follows: The site visit has to be performed by a representative of an ITSEF which is recognized by GBIC. Thus the site audit has not necessarily to be performed during a CC evaluation and not necessarily by the lab which is doing the product evaluation.

1) The vendors are asked to base their site visit on the related CEM annex.
2) According to the OSeC decision from 31st October 2012 the following holds: "The initial key in no cases is the acquirer key, but is the key, which assures the authentication of the hardware device independent on the purpose it is used for later on."
3) Final assembly is seen as the final step in the POI manufacturing process. Until now there is no more precise definition. Please note that the attack potential required to counter attacks on the final assembly (general protection of the manufacturing step) is lower than the attack potential required to counter attacks on the initial-key loading site (key protection).
4) The site where the initial key is generated needs not necessarily to be the place where the initial key is loaded. The place where the key is generated needs not to be audited. Depending on the individual validation of the risk assessment it may be assessed as more important to perform a site visit where the initial key has been generated. The current decision is based on a risk assessment where the payment schemes came to the conclusion not to require a site visit of initial key generation.
5) Initial key generation and distribution is expected to be documented and to be evaluated based on the provided evidence. Details depend on the implementation and life-cycle of the POI.
6) The 'Minimum Site Visit Requirements' provided by the smart card group ISCI are not applicable to POI evaluations. The security needs of a smart card evaluation are different from the security needs of a POI evaluation.
7) It has been discussed that a production environment may be changed after a site visit or that the auditors probably will not see security related measures but more the production environment. Therefore a site visit probably would not meet the expectations. The experiences of certification bodies and the risk assessment of payment schemes showed however that site visits improve assurance because deviations from paper work could be found and because auditors know where to look.
8) Best Practice for site visits is considered.

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

8 Functional Testing (ATE)

The FSP is the basis for the functional testing aspect.

The vendor has to test all TSFI and has to provide the evidence to the evaluator. In the area of testing discussions are ongoing in JTEMS (see [IMP PRE]). Vendors are asked to investigate whether categories of TSFI can be identified showing similar requirements in order to use standardized test tools.

The vendor has to test especially the SFR-enforcing TSFIs thus the vendor has to prove by testing that the SFRs are implemented.

E.g. for PIN encryption it has to be proven by testing that PIN encryption works as expected by the FSP. Such tests may be already performed by functional tests like EMV Level 1 or 2. However, the focus of CC is the security behavior of the interfaces and thus it is not guaranteed that security behavior is really tested during functional tests.

9 References

[CC WS PRE] CC-Workshop presentation, GBIC Common Criteria, Point of Interactions, Security Evaluation, 27.01.2015

[IMP PRE] Improvement presentation, Improving the JTEMS Evaluation Methodology, 25.09.2014

[PP ST] PP/ST Guide, Anleitungen zur Erstellung von Protection Profiles and Security Targets, Anleitungen zur Erstellung von Protection Profiles and Security Targets, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_41_BSI_PP_ST_Guide_pdf.pdf?__blob=publicationFile

[JTEMS PP V2] Point of Interaction Protection Profile, PP V2.0 – JTEMS PP

[JTEMS PP V4] Point of Interaction Protection Profile, PP V2.10 – JTEMS PP V4.0)

[CC P1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, July 2009, Version 3.1, Revision 4

[CC P2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, July 2009, Version 3.1, Revision 4

[CC P3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, July 2009, Version 3.1, Revision 4

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

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1, Revision 4

[DEV CC] Guidelines for Developer Documentation according to Common Criteria Version 3.1, Version 1.0, http://www.commoncriteriaportal.org/files/ccfiles/CommonCriteriaDevelopersGuide_1_0.pdf

[ING CC] Common Criteria JTEMS Evaluation of an Ingenico POI in the German CC Scheme, search for BSI-DSZ-CC-0859-2013 at www.bsi.bund.de

[VER CC1] Common Criteria JTEMS Evaluation of a VeriFone POI in the German CC Scheme, search for BSI-DSZ-CC-0865-2013 at www.bsi.bund.de

[VER CC2] Common Criteria JTEMS Evaluation of a VeriFone POI in the Netherland CC Scheme, http://www.tuv-nederland.nl/nl/37/view_certificate.html?cert_id=62

[SE CC] Common Criteria JTEMS Evaluation of a SecureElectrans Payment Device in the United Kingdom CC Scheme, http://www.cesg.gov.uk/finda/Pages/CCITSECProduct.aspx?PID=185&backpage=CCITSECResults.aspx?post=1&status=Certified&sort=name

[Volume] SEPA Cards Standardisation Volume Version 8.0 01.03.17; /www.e-csg.eu/scs-volume-v8

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