Common Security Evaluation &
Certification Consortium
of GBIC and UKF

Annex 2

Common.SECC
Security Evaluation & Certification Consortium

Security Requirements for POI Site Audits

Version 1.8

16 January 2018

Document History

Version	Date
0.9	11.11.2015
1.0	13.01.2015
1.1	29.01.2016
1.2	03.02.2016
1.3	01.03.2016
1.4	04.07.2016
1.5	04.08.2016
1.6	05.10.2016
1.7	23.01.2017
1.71	03.02.2017
1.72	01.01.2018
1.8	16.01.2018

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

Table of Contents

1 Introduction

A CC evaluation to be performed for the Common Security Evaluation & Certification Consortium requires according to the PPs used [JTEMS PP V2] and [JTEMS PP V4] audits of the sites for the initial key loading and for the final assembly of the POI.

This document shortly explains which attack scenarios are faced by these audits and lists state of the art requirements for these sites to be checked and assessed when performing the audits. These requirements will be analysed in the scope of the according assets that are identified by the auditor. All information given in this document should give laboratories and vendors a guidance to be compliant to the ALC_DVS.2 refinements given in the Point of Interaction Protection Profile [JTEMS PPV4].

Once a site has been assessed this is deemed to be valid for three years (unless there are any reported changes).

2 Requirements of the JTEMS PPs

2.1 Criteria

In the [JTEMS PPV2]and [JTEMS PPV4] the following aspects are outlined:

- "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**."[JTEMS PPV2]

- Refinement for the developer: „The development environment stands for the design, manufacturing, assembling and maintenance environments of TOE components, including the final assembly and the Initial Key Loading facilities. The Initial Key Loading is defined as the point where responsibility for the TOE security-related components falls to the acquirers. The initial key here is *not* the Acquirer key, but is the key that assures the authentication of the hardware device independent of the its ultimate purpose and destination" [JTEMS PPV4]

- 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. Further explanations are given in chapter 4.Explanation

The audit of the initial key loading facility is required to prove the integrity of authentic POI and exclude opportunities for compromise. The attacker could tamper initial keys despite this audit, because the key generation is not in scope of the audit. Key generation is however evaluated based on documentation.

The audit of the final assembly site is required to prevent manipulations of the POI during manufacturing. An attacker can try to compromise the POI during the manufacturing phase, e.g. by installing a „PIN disclosing bug". Such compromises can damage POI specific cryptographic keys and PINs. The attacker could of course also compromise the POI by performing manipulations outside of the final manufacturing phase. It is more likely, however, that the compromise performed in this phase is effectively installed.

These audits in addition, enable the evaluator to assess whether the vendor is trustworthy and reliable.

3 Asset based approach

Requiring site audits the Common Security Evaluation & Certification Consortium does neither target at simple checklists to be ticked off nor at minimum requirements to be covered by an audit. Instead an audit shall provide a good assurance that the POI produced in the sites are authentic and secure. Therefore the Common Security Evaluation & Certification Consortium requires an asset based approach which requires that the auditor starts with a problem definition describing clearly and comprehensively all the assets to be protected by the implementation of the sites. This problem definition determines the scope of the site visit.

The following steps must be concluded to ensure that the assets that are in scope of the site visit are protected.

1. Produce a list of identified assets,
2. Identify the according security measures to protect the assets,
3. Assess the proper implementation of these security measures,

3.1 Asset List

The asset list is based on the lifecycle documentation provided by the developer.

The following example is given to avoid misunderstandings to define assets:

Example:

Aspect of the Lifecycle: Key Confidentiality

Assets identified: Keys

- Authenticity of the public keys
- Confidentiality of the initial keys

3.2 Security Measures

The identified assets must be mapped to adequate security measures that will be analysed. To identify the security measures the assets outlined in chapter 3.1 are taken into account to ensure a detailed assessment in the next step.

The same examples as outlined in chapter 3.1 are used in the following text:

Example:

Assets identified: Keys

- Authenticity of the public keys
- Confidentiality of the initial keys

Considered security measures may be:

- Site Identification
- Responsible staff
- Physical Security
- Human Resources
- Secure Room
- Audits

- Company Standards
- Distribution
- IT-Security
- Device Returns

3.3 Assessment of the proper implementation of the security measure

After having identified the proper security measures the site visit is conducted to assess the implemented measures and the evidence provided by the developer. This assessment is conducted in accordance to the requirements outlined in chapter 4. The results of the site visit are summarized in a complete audit report.

4 Requirements for Sites to be assessed

An important part of the laboratory's assessment is the site visit to cover manufacturing, initial key loading, possible warehouse storage and distribution. Not all site visits are the same and some flexibility must be expected in dealing with and reacting to the environment found.

It is recommended to integrate any report for multiple sites into one document.

It is a principal requirement to gain assurance that any declared policies and procedures relevant to the manufacturing of the POI, including final assembly and key loading are in place, within a secure environment and properly followed.

Site Audits of different manufacturing sites are required, if the life cycle states that

- the relevant lifecycle steps are not located at the same site,.
- the used sites are not handled by the same QMS.

If several used sites are handled by the same QMS at least one site has to be audited.

All measures that are provided to ensure the secure Manufacturing and delivery of POIs are focused on a Product.

For a manufacturing site visit report the headings below represent requirements that are expected to be covered within a comprehensive review. The headings represent a broad and high-level template of requirements expected to be covered by a site visit within a CC evaluation. If some of these requirements are not satisfying or inadequate the product may not be able to receive an approval.

The following subchapters represent report headings, defined for structuring a site visit report. It represents requirements derived from the [JILMINSSR] document.

The site visit is based on the developer documentation for each requirement in the subchapters. During the site visit the evidence to proof the statements outlined in this documentation is gathered and summarized in a final report by referencing interview partners and documenting the proven aspects.

There are examples outlined in the subchapters below, which represent security measures that can be used on a site in accordance to the security level that needs to be provided. Each and every site can be different and therefore needs different security measures.

According to the Protection Profiles required by JTEMS there are two types of sites that are relevant for the POI evaluation

- POI manufacturing site or Manufacturing line within a site where in the final assembly step tamper mechanisms are switched on.
- POI Manufacturing site or area where the initial key(s) for authentication are imported into a POI

All procedures and information must be analysed before the site visit based on the lifecycle documentation and must further on analysed during the site visit.

4.1 Site Identification

This chapter consists of organisational aspects like address; number of sites to be visited, relevance of each and any inter-relationship between sites.

a) The location where manufacturing occurs and description of the manufacturing performed, along with the security measures applied. If there is more than one site used in the lifecycle, secure transports between different locations must be identified. For example, manufacturing and key injection could occur in different rooms within a single building, multiple buildings at the same site, or at multiple sites.

b) The main parameters for each location are:
    - location including complete address
    - purpose (manufacturing, initial key loading)
    - interaction between sites in scope of the audit (asset transfer)
    - security measures

4.2 Responsible staff

This chapter identifies particular requirements for any responsible staff within a secure manufacturing environment including names, positions and roles being responsible in the lifecycle of the target of evaluation.

a) The security roles and responsibilities of employees, contractors and third party users must be documented in accordance with the organization's security policy, e.g. in project plans or contracts.
b) Especially roles like security manager, key distributors and HSM administrator’s need to be outlined the names of backup personnel.
c) There must be a translation into Roman alphabet if the names are only available in other fonts.

4.3 Physical Security

This chapter contains requirements concerning perimeter security, CCTV, security guards and visitor policies. The analysis of the physical security requirements is based on documentation and the site visit itself.

4.3.1 Physical security perimeter

The physical security perimeter is a final manufacturing site where the final assembly steps of the POI are performed. The key injection room to inject keys for authentication can be part of this site or is located on an additional site.

a) Manufacturing areas (final assembly and initial key loading sites) where integrity could be impaired shall be properly secured.

Example:

In a typical setup, the premises manufacturing are located within a manufacturing building with other manufacturing lines surrounded with a fence or wall. Buildings are constructed with concrete or stonework walls, ceilings and floors. Controlled doors are strong (including frames), close automatically, and are monitored with magnetic contacts and CCTV.

Windows are secured with irremovable metal grid or with magnetic contacts and glass breakage sensors. Where the site may not be fenced an IR curtain can be deployed or the outer skin of the building is monitored by digital CCTV with motion detection (“Telemat”) or is patrolled by security guards 24/7.

b) The first protection layer of the manufacturing areas shall have at least two lines of defence, a detection layer and a stop layer. These layers shall separate authorized from unauthorized people, including employees. In case that no physical manifestation is handled and solely logical access to electronic data is present a stop layer may also be a logical one. In case of a natural disasters the physical security measurements should uphold.

Example:

A Detection Layer may consist of at least one or more of the following and, where implemented, proper operational review processes must be evidenced:

- Fence with sensor (vibration, ultrasonic, motion, etc.)
- IR curtain
- Digital CCTV with motion detection
- Wall with alarm tapestry or vibration sensor
- 24/7 guard post

A Stop Layer is a constructive measure which needs time to overcome in accordance to the location (country) and attack risks identified:

- Concrete or brick stone wall
- dry walling construction enforced with inside metal grid (> 8mm diameter, <100 mm grid distance) or enforced with steel plate (> 3mm thickness)
- windows in a stop layer are either protected with metal bars (> 8 mm diameter) or made with bullet proof glass
- door hardware must be properly installed, locked door blades fixed at floor and ceiling, door locks are still working by default even when power loss is happening.

c) In case buildings ot rooms are used for security relevant activities, e.g. key injection, the layers shall separate the different activities to avoid modification and manipulation during the manufacturing steps.

d) In general, the POI relevant areas should provide

- perimeter protection
- protection of the outer skin of the building
- protection of the outer skin of the security area
- protection within the security areas

e) The resistance time value of the stop layer shall exceed the reaction time of supporting forces. This should be supported by the construction.

Example:

If supporting forces need at least 5 mins to reach the secure area after detecting an attacker, a wall or door should withstand this attacker until supporting forces arrive.

h) Unauthorized use of photo and video cameras or audio recording equipment shall be prohibited.

i) Site should be secured by security personnel 365 days a year /24 hours a day in accordance to the attack potential on the location. For example there could be an intruder alarm system if the protection layer provides a resistance until security personnel reacts and is reaching the security area.

4.3.2 Physical entry controls

a) Secure manufacturing areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed to access.

b) Access requests shall be submitted in written or via an electronic work flow system. Access rights shall only be granted to employees and contractors on a need-to-know basis. A process shall be in place to ensure that access rights can only be granted after approval of responsible people, e.g. the manager of the applicant, the owner of the area, and the Security Manager.

c) Segregation of duty should ensure that setting access rights in the access control system is separated from producing and issuing ID/badges. Any withdrawal of a badge shall be logged.

d) The access control system shall provide full traceability. All access attempts shall be logged at least 6 months, tailgating shall be effectively prevented, and unauthorized access attempts should be analysed.

Example:

In a typical setup, access to the building is controlled by electronic badge access. Security areas (e.g. laboratory, data centre, security control rooms; key injection rooms) have dual authentication, e.g. badge with PIN.

4.3.3 Public access, delivery and loading areas

a) Access points such as delivery and loading areas of the products, and other points where unauthorized persons may enter the premises shall be controlled and isolated from processing facilities to avoid unauthorized access.

b) Visitors shall have only predefined, controlled access to the manufacturing areas.

c) Delivery and loading areas shall be monitored by CCTV. The recordings shall provide clear pictures enabling identification of any unintended unloading and loading. CCTV recordings should be available for at least one year.

d) Incoming material for manufacturing /final assembly shall be registered on entry, and inspected before delivery to the point of use. This can be done by e.g. checking a bill of materials. If the final assembly site and the personalisation site are on different locations the secure delivery process between the sites is checked

e) Transfer of security relevant materials within a physically secured area shall be logged in order to provide full traceability.

f) Devices shall be protected against tampering or theft during transit between physically separated sites. The protective mechanism shall enable the recipient to detect if tampering or theft has taken place.

4.4 Human resources (Employees)

This chapter identifies requirements for access control management, security policies, security training, hiring and dismissal procedures, and contracts with third party companies that are relevant for the POI.

a) Physical protection and guidelines for working in secure areas shall be designed andapplied to the personnel that is working with the POI.

b) Personnel that is working with the POI shall be aware that information may only be shared on a need-to-know basis.

c) People from external parties (e.g. customers, development partners, Manufacturing partners, housekeeping, vendors, suppliers, carriers) shall not work in POI relevant areas without supervision of approved internals (e.g. host, owner of area, guard). This rule does not apply to externals which work as internal team members and are subject to the same security rules as internals

d) The developer shall grant access to the POI or its parts only to trustworthy people. That objective should be accomplished by appropriate hiring and termination procedures which ensure careful selection of trustworthy staff.

e) Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant local laws, regulations and ethics, and proportional to the business requirements, the classification of the information and material to be accessed, and the perceived risks.

Example:
Respecting privacy regulations, the developer shall make a reasonable effort to gainconfidence in the integrity of the staff, e.g. through

- careful check of job applications regarding completeness, conclusiveness, and authenticity,
- check of indicated references, and
- criminal record check ("Clearance Certificate", "Criminal Records Bureau check", "Casier judiciaire", "Polizeiliches Führungszeugnis" etc.).

f) As part of their contractual obligation, employees, contractors and third party users that are working with the POI shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for security. Contracts with all employees (permanent, temporary, subcontractors, students etc.) shall contain a confidentiality clause which remains valid after expiration/termination of the contract; third party users respectively shall sign a non-disclosure agreement (NDA).

g) All employees of the organization, where relevant, contractors and third party users that are working with the POI shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. That can be face to face or online training. Records of training shall be kept, including date, attendances and content. An Initial and regular (annual) security training program shall make the development team members aware of their responsibilities, e.g. handling of documents and information, behaviour in public, and encourage them to act pro-actively when problems occur.

h) All employees, contractors and third party users that are working with the POI shall return all of the developer's assets in their possession upon termination of their employment contract or agreement. The same shall apply when they leave the developer's organization due to change of job assignment or dismissal due to disciplinary reasons. This process should be supported by a checklist for employees leaving employment in order to make sure that all relevant tasks, e.g. return of company properties, deletion of access rights are completed.

4.5 Secure Room

This chapter identifies the requirements for secure rooms for personalisation or key injection.

a) Secure rooms shall be protected by appropriate entry controls to ensure that only authorized personnel that is allowed to work with the POI has access.

Example:

In a typical setup, access to the building is controlled by electronic badge access. Security areas (e.g. laboratory, data centre, security control rooms) have dual authentication, e.g. badge with PIN. A separate access room (manlock) should be used to enforce the dual control mechanism of two authorized employees.

b) The access control system shall provide full traceability. All access attempts shall be logged, tailgating shall be effectively prevented, and unauthorized access attempts should be analysed.

c) The design and layout of sites and premises should avoid secure rooms next to public areas. The routes and walkways designated to visitors should be designed to ensure that visitors will not see restricted areas or information unintentionally.

d) All openings towards the secure rooms (air conditioning, cable ducts, etc.) shall be protected in order to effectively prevent intrusion, e.g. with a welded metal grid.

e) Secure rooms should be alarmed and locked when unattended. Access controlled doors should be monitored with magnetic contacts and CCTV, and the secure rooms should be monitored with motion detection.

d) Any storage objects like safes must be set up so that it cannot be removed until security forces arrive.

4.6 Audits

This chapter identifies requirements for internal or external security audits including their evidence and time interval.

a) The organization should conduct internal or external audits at planned intervals to determine whether the processes and procedures of its POI manufacturing including all components:
   - conform to the requirements of this Requirement Document;
   - conform to the identified security needs of the POI;
   - are effectively implemented and maintained; and
   - are performed as expected.

b) An audit program should be completed once a year, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods should be defined. The selection of auditors and conduct of audits should ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

c) The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities should include the verification of the actions taken and the reporting of verification results.

4.7 Company Standards & Procedures

In this chapter written standards for the manufacturing especially for the firmware of a POI are identified. Authentication and storage during manufacturing, including change control logs, and firmware validation procedures are part of the following requirements.

a) An automated configuration management System must be used to automatically maintain and control the firmware. The CM system shall ensure the integrity of the firmware from the early design stages through all subsequent maintenance efforts, that the firmware is correct and complete before it is installed into a POI and preventing unauthorized modification, addition, or deletion of any firmware parts.
b) Access rights to the CM system should be controlled and restricted to authorized personnel.
c) There must be documented processes for the manufacturing of all components of a POI, e.g. the firmware including validation procedures.
d) manufacturing machines and all classified digital information to conduct the secure POI manufacturing must be located in a secured network environment.

4.8 Distribution

Transportation between sites are part of the following requirements if the final assembly and initial key loading are conducted on different locations.

a) The whole transport chain from final assembly area to shipment of the POI to the initial key loading site shall be controlled. Transport shall be monitored for security violations and any incidents shall be responded to and acted upon immediately.
b) Transports of parts of the POI or the unfinished POI between different sites, , are to be covered by security measures, e.g. transport keys between interacting sites.
c) The security measures during transit shall correspond to
integrity and authenticity and should be defined in a written document. This includes reliable contracts with the courier company to track devices during transit.

Example of different measures to ensure transport security in accordance to attack risk:
During transportation, the POI is attended at any time except while locked in an airplane. Therefore the following rules apply to ground transportation

- packed in sealed transport boxes with unpredictable seal number (seal, plumb, or security tape)
- transport in a locked vehicle
- point-to-point transport without additional payload or hub/relation
- Two-man rule shall be applied during the entire transportation and the vehicle shall not be unattended at any time
- the transport should be equipped with mobile phone and GPS based Surveillance
- In order to prevent attacks shipment information may be encrypted.
- Tamper detection activated a parcel service may be enough

d) A recipient should be provided with all information necessary to verify the integrity and authenticity of the shipment. The following information should be included.
   - Number of boxes
   - Seal number(s) of transport box(es)
   - Number of pieces packed

   Additionally, it may be useful to provide
   - Route and schedule
   - Drivers name, truck license plate number

4.9 IT Security

This chapter includes requirements according to signing procedures and encryption, access to sensitive information, equipment maintenance, system back-up (onsite / offsite), sensitive information uniqueness in scope of the POI manufacturing.

a) Only authorized people shall have access to electronic information and data related to the POI.
b) Security relevant hardware such as HSMs and or other tools to establish signing or distribute keys must be located in a secure room and operated under dual control.
c) It should not be possible to view and/or modify security items from outside a defined security area, even from within the corporate network. A strong authentication scheme shall be defined for network access.
d) Adequate back-up facilities shall be provided to ensure that all essential information and software can be recovered following a disaster or media failure while maintaining confidentiality and integrity of the POI and its part. Beside all information and data related to the POI, e.g. design data and CM system, access control and administrator log files shall be backed-up.
e) All equipment and cryptographic implementations, shall be correctly maintained to ensure its continued integrity and – for security systems - availability.
f) A defined network plan with security mechanism shall be provided that includes at least the following information according to the assets in the data flow:
   - on overview of network segments,
   - the boundary and interfaces of each network segment,
   - overview of network infrastructure (router, firewall, storage system, etc.),
   - the administration concept including security relevant configuration and maintenance of network components (e.g. workstations, backup machines, firewalls, intrusion detection systems, intrusion prevention systems, production machines)
g) A defined policy for classified digital information must be provided (e.g. BOM for Manufacturing)

   Example for Information classification:
   - public (e.g. marketing information)
   - restricted (e.g. Security awareness documents)
   - sensitive (e.g. BOM)
   - critical and above (e.g. Network plan, third party contracts)

4.10 Device Returns and End of Life

This chapter defines requirements to aspects of devices that are returned at end-of-life including re-cycling or destruction, repair, storage and inspection procedures if this is applicable in the scope of the site that is audited.

a) Finished goods, semi-finished goods, rejected material, or parts of the POI that are no longer needed should be destroyed in a way that the remains cannot be used in any meaningful way that might affect the confidentiality of the POI.

Example:

- Packaged chips with key material are shredded in a rolling mill so that every edge of each and any die is cut 3 times.
- Masks/Reticules are re-etched in order to remove the pattern or shredded in a rolling mill.
- The destruction process is recorded on CCTV.
- Confidential and strictly confidential documentation of the POI on paper or optical disks are shredded according to at least 2 mm strips or 4 x 30mm particles.
- Files on re-writable data carriers (HDD, SSD, USB sticks) are sanitized or degaussed.

b) If there is a repair process the storage of POIs must be traceable from the moment they are in an unsecure state until a new firmware or key is injected. All security measures must up-hold as if the POI is a complete new produced device.

c) The related processes shall be designed to provide full traceability of every piece of any tangible form of the POI or its parts.

5 References

[JTEMS PPV2] Point of Interaction Protection Profile, POI Comprehensive, 26.11.2010, Version 2.0 sogis.org/uk/pp_pages/poi/pp_poi_comprehensive.html,

[JTEMS PPV4] Point of Interaction Protection Profile, POI-CHIP-ONLY base PP, 06.03.2015, Version 4.0 www.commoncriteriaportal.org/pps/

[JILMINSSR] Joint Interpretation Library Minimum Site Security Requirements, Version 1.1 (for trial use), July 2013