# Site Security Target - Lite

AUSTRIA**CARD**

Version 4.0-Lite

2026-09-21

# Table of Contents

Table of Contents ..... 2
1 Document Introduction ..... 5
1.1 SST Reference ..... 5
2 SST Introduction ..... 5
3 Site Reference ..... 5
3.1 Site Description ..... 5
3.1.1 Physical Scope ..... 5
3.1.2 Logical Scope ..... 6
4 Conformance Claim ..... 6
5 Security Problem Definition ..... 7
5.1 Assets ..... 7
5.2 Threats ..... 8
5.3 Organizational Security Policies ..... 8
5.4 Assumptions ..... 9
6 Security Objectives ..... 10
6.1 Security Objectives Rationale ..... 13
7 Extended Assurance Components Definition ..... 15
7.1 ALC_FLR.4 Flaw remediation with distinction between security and functional flaws (Extended) ..... 15
7.2 Software Bill of Materials (ALC_SBM) – Extended ..... 17
7.3 Periodic Security Review and Testing (ALC_PSR) – Extended ..... 19
8 Security Assurance Requirements ..... 21
8.1 Application Notes and Refinements ..... 22
8.1.1 CM Capabilities (ALC_CMC.4) ..... 22
8.1.2 CM Scope (ALC_CMS.5) ..... 22
8.1.3 Delivery (ALC_DEL.1) ..... 22
8.1.4 Developer Environment Security (ALC_DVS.2) ..... 23
8.1.5 Life-cycle Definition (ALC_LCD.1) ..... 23
8.1.6 Tools and Techniques (ALC_TAT.2) ..... 23
8.1.7 Flaw Remediation (ALC_FLR.3) ..... 23
8.1.8 Flaw remediation separation (ALC_FLR.4) ..... 23
8.1.9 Software bill of materials (ALC_SBM.1) ..... 23

8.1.10 Periodic security review and testing (ALC_PSR.1) ..... 23
8.2 Security Requirements Rationale ..... 23
8.2.1 Dependencies ..... 23
8.2.2 Mapping ..... 24
9 Site Summary Specification ..... 33
9.1 Preconditions required by the Site ..... 33
9.2 Services of the Site ..... 34
9.3 Objectives Rationale ..... 34
9.4 Assurance Measure Rationale ..... 38
9.4.1 O.Config_IT-env ..... 38
9.4.2 O.LifeCycle-Doc ..... 38
9.4.3 O.Physical-Access ..... 39
9.4.4 O.Security-Control ..... 39
9.4.5 O.Alarm-Response ..... 40
9.4.6 O.Internal-Monitor ..... 40
9.4.7 O.Maintain-Security ..... 40
9.4.8 O.Network-Separation ..... 40
9.4.9 O.Logical-Access ..... 40
9.4.10 O.Logical-Operation ..... 40
9.4.11 O.Config-Items ..... 40
9.4.12 O.Config-Process ..... 41
9.4.13 O.Staff-Engagement ..... 41
9.4.14 O.Zero-Balance ..... 41
9.4.15 O.Flaw-Remediation-Monitor ..... 42
9.4.16 O.Flaw-Remediation-External ..... 42
9.4.17 O.Security-Review ..... 43
9.4.18 O.Component-Lists ..... 43
9.4.19 O.Transport ..... 43
9.4.20 O.Data-Transfer ..... 43
9.5 Mapping of the Evaluation Documentation ..... 43
10 References ..... 44
10.1 Literature ..... 44
10.2 Definitions ..... 45

10.3 List of Abbreviations ..... 45
10.4 Revision History ..... 46

# 1 Document Introduction

## 1.1 SST Reference

| | |
|---|---|
| Title: | Site Security Target - Lite, Austria Card Vienna |
| Version: | 4.0-Lite |
| Date: | 2026-09-21 |
| Company: | Austria Card |
| Name of Site: | AUSTRIA CARD - Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Vienna (short name Austria Card Vienna) |
| EAL: | SARs taken from EAL5 augmented with ALC_DVS.2, ALC_FLR.3, ALC_FLR.4 (extended), ALC_SBM.1 (extended) and ALC_PSR.1 (extended) |

# 2 SST Introduction

The Chapters Document Introduction to References of this document are based on the Eurosmart Site Security Target Template [1] with adaptations such that it fits the site.

# 3 Site Reference

The site is located at:

Austria Card, Lamezanstrasse 4-8, 1230 Vienna, Austria

Only parts of the building are within the scope of this SST located in the ground and first floor. The areas within the scope of the evaluation are given in Section 3.

## 3.1 Site Description

### 3.1.1 Physical Scope

The following stations (facility/building/site) of the site, specified in the Site Reference, are in the scope of the SST:

- Reception,
- Security Office,
- Development Environment,
- Server Rooms hosting the CM system, Backups, Firewall, CCTV, Alarm- and Access Control,
- Shipment and Reception areas for physical goods.

The location(s) listed above contain security areas with restricted access under control of Austria Card where only authorised persons can enter.

Only authorised employees are entitled to access sensitive information like physical samples, source code, libraries, tools, and documentation. To enforce such access restrictions, a combination of physical, procedural, personnel and logical measures have been installed.

### 3.1.2 Logical Scope

The following life cycle phase as defined in the Protection Profile (PP) [2], and also defined in a similar way in the referred PPs [2] to [12] which is subject of the SST:

- Phase 1: IC Embedded Software Development.

The following services and/or processes provided by Austria Card are in the scope of the site evaluation process:

- Secure software development,
- Testing (debugging, functional verification),
- Documentation relating to the developed software (e.g. functional and security specifications, software architecture, design, implementation and interface documentation, test specifications, test data and test reports, application notes, configuration management documentation, vulnerability handling and flaw remediation documentation, security advisories and corrective-action guidance, and SBOMs or component lists)
- Secure management and handling of transport, authentication and key protection[1] keys for smartcards and similar devices,
- Secure delivery and reception of code, tools, documentation, keys and other data.

# 4 Conformance Claim

This SST is conformant with Common Criteria (CC) CC:2022 Revision 1:

- Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, CC:2022 Revision 1, November 2022 [13]
- Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance components, CC:2022 Revision 1, November 2022 [15]

For the evaluation, the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation (CEM): CEM:2022 Revision 1, November 2022 [16]

All claims take into account the

- Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, 2025-10-15 [30],

where applicable.

The SST is CC Part 3 extended.

The evaluation of the site comprises the following Security Assurance Components (SAR):

- ALC_CMC.4,
- ALC_CMS.5,

[1] e.g. keys for protection of integrity and confidentiality of (pre-)personalization keys

- ALC_DEL.1,
- ALC_DVS.2,
- ALC_FLR.3,
- ALC_FLR.4 (extended),
- ALC_SBM.1 (extended),
- ALC_PSR.1 (extended),
- ALC_LCD.1,
- ALC_TAT.2[2].

The chosen assurance components are derived from the assurance level EAL5 augmented with ALC_DVS.2, ALC_FLR.3, ALC_FLR.4, ALC_SBM.1 and ALC_PSR.1 of the assurance class 'Life-cycle Support'. For the assessment of the security controls attackers with ***high attack potential*** are assumed. Therefore, this site supports product evaluations up to EAL5 augmented with ALC_DVS.2, ALC_FLR.3, ALC_FLR.4, ALC_SBM.1 and ALC_PSR.1 and AVA_VAN.5.

# 5 Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site.

## 5.1 Assets

This section describes the assets together with their default[3] asset classification according to "EUCC State-of-the-Art document: Application of Attack Potential to Smartcards" [18] handled at the site. They can be grouped within the following categories:

- Physical security objects:
  The site has physical security objects (samples, printed documents, etc.) in relation to developed TOEs. Both, the integrity and the confidentiality of these must be protected - default asset classification is Critical.
- Development data:
  The site has access to (and optionally copies thereof) electronic development data (source code, IC dedicated software for ROM or Flash memories, libraries, functional specifications, etc.) in relation to developed TOEs. Both, the integrity and the confidentiality of these electronic data must be protected - default asset classification is Critical.
  Transport keys for encryption of developed software - default asset classification is Critical+.
  Authentication keys for authentication at flashloaders - default asset classification is Critical+.
  Key protection keys - default asset classification is Critical+.
- Development Tools:
  To perform its development activities the site uses tools to compile source code and

[2] The site does not contribute to the aspect ALC_TAT. The aspect has been claimed in order to ensure the assessment of related items during the evaluation process and to support the reuse of the evaluation results in a product evaluation accordingly.

libraries. The integrity of these tools must be protected - default asset classification is Restricted.

## 5.2 Threats

| | |
|---|---|
| T.Smart-Theft | An attacker tries to access sensitive areas of the site or equipment for manipulation or theft of assets: (1) physical security objects, (2) development data, (3) development tools. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered. |
| T.Rugged-Theft | An attacker with specialized equipment for burglary, who may be paid to perform the attack, tries to access sensitive areas or equipment and manipulate or steal assets. |
| T.Computer-Net | A possibly paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to<br>(1) development data with the intention to violate confidentiality and possibly integrity<br>(2) development computers with the intention to modify the development process. |
| T.Accident-Change | An employee, contractor or student trainee may exchange samples or software of different clients during development/qualification by accident. |
| T.Unauthorised-Staff | Employees or subcontractors not authorized to get access to assets violating the confidentiality and possibly the integrity of products. |
| T.Staff-Collusion | An attacker tries to get access to assets by getting support from one employee through extortion or bribery. |
| T.Attack-Transport | An attacker tries to get access to shipped physical security objects when shipped in or out of the site. The target is to compromise confidential information or violate the integrity of the products during the stated internal shipment and/or the external delivery process to allow a modification, cloning or the retrieval of confidential information after further production steps. Confidential information comprises design data, client data like code, data (including and/or transport and authentication keys) and/or classified product documentation. |

## 5.3 Organizational Security Policies

| | |
|---|---|
| P.Config_IT-env | In addition to the used software on development workstations and servers, the site uses configuration management systems for file versioning and problem tracking. For file versioning, the team members are assigned to project specific, centralized repositories to |

| | |
|---|---|
| | support proper management of multiple products and the site internal procedures. The team members are requested to use only project related IT equipment with the provided tools. |
| P.LifeCycle-Doc | The site follows the life cycle documentation that describes:<br>(1) Description of configuration management systems and their usage;<br>(2) A configuration items list;<br>(3) Site security;<br>(4) The development process;<br>(5) The development tools. |
| P.Vulnerability-Handling | The site is in charge of handling vulnerabilities including security flaw remediation.<br>The procedures in place within the site must show how flaw remediation is managed and supported giving assurance on the following topics:<br>(1) acceptance and acting upon all reports of security flaws and requests for corrections to those flaws.<br>(2) flaw remediation guidance to address the TOE users and distribution of corrections to clients.<br>(3) ensuring periodic security reviews and testing for defined timeframes and intervals and scope defined by the client<br>(4) maintaining all component dependencies (component lists) and delivering them to the client in a defined format |
| P.Organise-Product | Additionally, specifications, necessary for the development flow may come from the client for dedicated and specialized software development processes. For keys, relevant for the life cycle or configuration data, security, appropriate measures must be in place. This includes the requirement that the site shall be able to handle in a way that knowledge of sensitive keys shall be split to at least two different persons (as an option, if requested). Furthermore, technical measures like cryptography, separation of network, split access permission and secure storage shall be implemented for this kind of data. |

## 5.4 Assumptions

| | |
|---|---|
| A.Product-Setup | The site participates in the development of products. To define the participation of the site in the development while maintaining quality, for each product the client has to manage the activities to be performed by the site, the specifications of the input for the site and |

| | |
|---|---|
| | the acceptance of the results by the client. In addition the client may define dedicated classification levels for all assets[3].<br>The client has to define the product-dependent development tools and documentation, make them accessible (or support the site getting access to the tools and documentation from a third party), and has to support the site if necessary.<br>The client has to define a plan (e.g. begin, end, interval) for periodic security reviews suitable for the product type or agree with the default plan of the site for that product type. |
| A.Shipment | The client is responsible for defining the secure packaging and delivery procedures for physical security objects, according to their classification, the necessary addresses for delivery are part of the project setup.<br>For delivery of development data and tools an appropriately secure communication, according to their classification, has to be established, which includes key exchange and, if required, definition of encryption/signature method. This is part of the project setup. |
| A.Transport-keys | Any kind of cryptographic keys used to protect software during the transport from developer to the client are not usable in the operational phase, i.e. they cannot be used by end users for any purpose. |

# 6 Security Objectives

| | |
|---|---|
| O.Config_IT-env | In addition to the software used on development workstations and servers, the site uses configuration management systems for file versioning and problem tracking. For file versioning, unique repositories are used to support proper management of multiple products and the site-internal procedures. Only project-related tools and IT equipment are used. |
| O.LifeCycle-Doc | The site follows the life cycle documentation that describes:<br>(1) Description of configuration management systems and their usage;<br>(2) A configuration items list;<br>(3) Site security;<br>(4) The development process;<br>(5) The development tools;<br>(6) The component lists. |

[3] The site applies a default classification for each asset type (see 5.1) when not defined explicitly by the client.

| | |
|---|---|
| O.Physical-Access | The combination of physical partitioning between the different access control levels together with technical and organisational security measures allows a sufficient separation of employees to enforce the “need to know” principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorised people. The access control measures ensure that only registered employees can access restricted areas. When certain types of assets are handled outside of the restricted areas additional technical (two factor authentication, hardware seals) and additional organisational measures (work instructions) are applied to control access to the assets. |
| O.Security-Control | Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers. The site has established dedicated work instructions that ensure the protection of assets. |
| O.Alarm-Response | The technical and organisational security measures ensure that an alarm is generated before an unauthorised person gets access to any asset. After the alarm is triggered the unauthorised person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack. |
| O.Internal-Monitor | The site performs security management meetings at least every six months. The security management meetings are used to review security incidents, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures. |
| O.Maintain-Security | Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorised employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems. |
| O.Network-Separation | The development network of the site exists within the secured areas of the site only. It is connected only to:<br>(1) the development workstations;<br>(2) Additional equipment (e.g. a printer). |

| | |
|---|---|
| O.Logical-Access | The site enforces a logical separation between the internal network and the internet including a firewall. The security measures ensure that only defined services and defined connections are accepted on the internal network. The internal network is appropriately separated to prevent interference between the different environments (office and development environments). Access to the development network and associated systems is restricted to authorised employees working in the related area or involved in the configuration tasks of the used environment. Every user of an IT system has his/her own user account and password. Transport, authentication keys, key protection keys and other specialized sensitive data for development, transport or authentication can be generated and stored securely at the development site. |
| O.Logical-Operation | Development workstations enforce that every user authenticates using a password and has a unique user ID. For certain types of development workstations multifactor authentication is mandatory. |
| O.Config-Items | The site has a configuration management system that manages products and parts used. A unique internal identification is assigned to each product to uniquely identify configuration items and allow an assignment to a client. Also, the internal procedures and guidance are covered by the configuration management. |
| O.Config-Process | The site controls its services and/or processes using a configuration management plan. The configuration management is controlled by tools and procedures for the development, for the management of flaws and optimizations of the process flow as well as for the documentation that describes the services and/or processes provided by a site. |
| O.Staff-Engagement | All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job. |
| O.Zero-Balance | The site ensures that all physical assets are separated and traced. Automated controls and/or acknowledgements by two employees are required during handover of functional and defective material. |
| O.Flaw-Remediation-Monitor | All security flaws discovered by development teams or reported by TOE users must be monitored and managed. |
| O.Flaw-Remediation-External | Corrections and guidance on corrective actions for security flaws with consequences for TOE users are provided to TOE users. |
| O.Security-Review | The site ensures that security review and testing is performed periodically with a defined scope, as defined or agreed by the client. |

| | |
|---|---|
| O.Component-Lists | The site produces and delivers formal records to the client containing all third-party components used by the TOE to support vulnerability identification. |
| O.Transport | The recipient of a physical security object is identified by the assigned address. The shipment procedure is applied to the physical asset. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the client. For every sensitive physical asset, the protection measures against manipulation are defined. |
| O.Data-Transfer | Sensitive electronic assets (development data or tools in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated transport keys must be assigned to individuals to ensure that only authorised employees are able to extract these assets. Keys for authentication are securely exchanged and they are sufficiently protected. Data and keys are securely imported / exported, and therefore ensuring integrity and confidentiality. |

## 6.1 Security Objectives Rationale

| Threat | Security Objective(s) | Rationale |
|---|---|---|
| T.Smart-Theft | O.LifeCycle-Doc<br>O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security | The combination of structural, technical and organisational measures detects unauthorised access and allows for appropriate response on the threat. |
| T.Rugged-Theft | O.LifeCycle-Doc<br>O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security | The combination of structural, technical and organisational measures detects unauthorised access and allows for appropriate response on the threat. |
| T.Computer-Net | O.Config_IT-env<br>O.LifeCycle-Doc<br>O.Physical-Access<br>O.Internal-Monitor<br>O.Maintain-Security<br>O.Network-Separation<br>O.Logical-Access<br>O.Logical-Operation<br>O.Staff-Engagement<br>O.Data-Transfer. | The development network is not connected to anything that an attacker could use to set up a remote connection.<br>For data transfers dedicated procedures exist that allow for secure communication and import/export of data. |
| T.Accident-Change | O.Config_IT-env<br>O.Network-Separation<br>O.Logical-Access | A strict separation of data from different clients is applied. All |

| Threat | Security Objective(s) | Rationale |
|---|---|---|
| | O.Logical-Operation<br>O.Config-Items<br>O.Staff-Engagement<br>O.Zero-Balance | employees are trained regarding handling of secure objects.<br>Zero balancing and tracing of single items further enables to detect such errors. |
| T.Unauthorised-Staff | O.Config_IT-env<br>O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security<br>O.Network-Separation<br>O.Logical-Access<br>O.Logical-Operation<br>O.Staff-Engagement | Physical and logical access control prohibits unauthorised access to assets. |
| T.Staff-Collusion | O.Config_IT-env<br>O.LifeCycle-Doc<br>O.Physical-Access<br>O.Internal-Monitor<br>O.Maintain-Security<br>O.Staff-Engagement | The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees limits unauthorised access to assets. |
| T.Attack-Transport | O.LifeCycle-Doc<br>O.Staff-Engagement<br>O.Zero-Balance<br>O.Transport<br>O.Data-Transfer. | The shipment method and the organisational measures ensure that integrity changes of shipped objects are detected and appropriately responded to. |

Table 1: Mapping between Threats and Security Objectives

| OSP | Security Objective(s) | Rationale |
|---|---|---|
| P.Config_IT-env | O.Config_IT-env<br>O.Config-Process | The Security Objectives directly enforce the OSP. |
| P.LifeCycle-Doc | O.LifeCycle-Doc<br>O.Component-Lists | The Security Objective O.LifeCycle-Doc directly enforce the OSP. O.Components-Lists address the production of lists of components as a part of the development process documented in the life-cycle documentation. |
| P.Vulnerability-Handling | O.Flaw-Remediation-Monitor<br>O.Flaw-Remediation-External<br>O.Security-Review<br>O.Component-Lists | The Security Objectives directly enforce the OSP. |
| P.Organise-Product | O.Logical-Access<br>O.Transport<br>O.Data-Transfer | The Security Objectives directly enforce the OSP. |

| OSP | Security Objective(s) | Rationale |
|---|---|---|
| | O.Security-Review | |

Table 2: Mapping between OSPs and Security Objectives

# 7 Extended Assurance Components Definition

The following extended assurance components are defined in this Security Target, taken from [27] resp. [28].

## 7.1 ALC_FLR.4 Flaw remediation with distinction between security and functional flaws (Extended)

### *Objectives*

Flaw remediation requires that discovered security flaws be tracked and corrected by the developer. Although future compliance with flaw remediation procedures cannot be determined at the time of the TOE evaluation, it is possible to evaluate the policies and procedures that a developer has in place to track and correct flaws, and to distribute the flaw information and corrections. [4]

### *Component levelling*

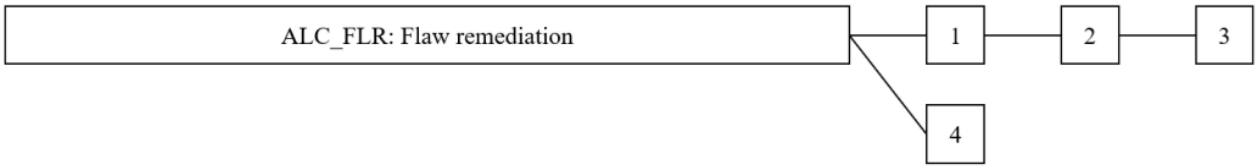



Figure 1: component levelling of ALC_FLR family (extended)

The components in this family are levelled on the basis of the increasing extent in scope of the flaw remediation procedures and the rigour of the flaw remediation policies.[5]

A non-hierarchical component aims to require separation in the developer's procedures between the procedures used to handle security flaws and those used to address other issues (e.g., functional) in the TOE.

### *Application notes*

This family provides assurance that the TOE will be maintained and supported in the future, requiring the TOE developer to track and correct flaws in the TOE. Additionally, requirements are included for the distribution of flaw corrections. However, this family does not impose evaluation requirements beyond the current evaluation.

The TOE user is considered to be the focal point in the user organization that is responsible for receiving and implementing fixes to security flaws. This is not necessarily an individual user, but may be an organisational representative who is responsible for the handling of security flaws. The use of the term TOE user recognizes that different organisations have different procedures for

[4] text of the objectives for the ALC_FLR family, as in [15] section 12.6.1 inserted
[5] text of the component levelling for the ALC_FLR family, as in [15] section 12.6.2 inserted

handling flaw reporting, which may be done either by an individual user, or by a central administrative body.

The flaw remediation procedures should describe the methods for dealing with all types of flaws encountered. These flaws may be reported by the developer, by users of the TOE, or by other parties with familiarity with the TOE. Some flaws may not be reparable immediately. There may be some occasions where a flaw cannot be fixed and other (e.g. procedural) controls must be taken. The documentation provided should cover the procedures for providing the operational sites with fixes and providing information on flaws where fixes are delayed (and what to do in the interim) or when fixes are not possible.

Changes applied to a TOE after its release render it unevaluated; although some information from the original evaluation may still apply. The phrase “release of the TOE” used in this family therefore refers to a version of a product that is a release of a certified TOE, to which changes have been applied.[6]

The extension of this family with the component ALC_FLR.4 intends to introduce in the assessment of the developer’s flaw remediation methods particular verifications to ensure that the actions taken into remediating flaws, especially when it comes to distribution of corrective actions in the form of updates, are organized in a way that ensures separation between correction of security flaws and other types of flaws, such as functional flaws.

### *ALC_FLR.4 Flaw remediation with distinction between security and functional flaws*

Hierarchical to: None.

Dependencies: ALC_FLR.1 Basic flaw remediation

Developer action elements:

ALC_FLR.4.1D **The developer shall document and provide flaw remediation procedures addressed to TOE developers**.

Content and presentation elements:

ALC_FLR.4.1C **The flaw remediation procedures documentation shall describe how a separation is established in the distribution of flaw corrections to TOE users, separating corrections of security flaws from other flaws that address non-security flaws.**

Evaluator action elements:

ALC_FLR.4.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence**.

### *Evaluation work units for ALC_FLR.4.1 (Extended)*

Action ALC_FLR.4.1E

ALC_FLR.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### *General*

[6] text of the application notes for the ALC_FLR family, as in [15] section 12.6.3 inserted

ALC_FLR.4.1C: The flaw remediation procedures documentation shall describe how a separation is established in the distribution of flaw corrections to TOE users, separating corrections of security flaws from other flaws that address non-security flaws.

Work unit ALC_FLR.4-1

The evaluator **shall examine** the flaw remediation procedures documentation to determine that it describe how a separation is established in the distribution of flaw corrections to TOE users, separating corrections of security flaws from other flaws that address non-security flaws.

Work unit ALC_FLR.4-1 indicates that, when a flaw is discovered not to be security-relevant, then there is no need for the flaw remediation procedures to track it further. However, the remediation procedures for security-flaws shall describe how they are separated, e.g., prioritized or handled through a different internal fixing pipeline, with respect to those that aren't security related.

When a flaw is categorized as security-relevant, then the procedures describe how the subsequent actions are designed and conducted in a way ensuring that, when the flaw requires a corrective action to be distributed to TOE users, for example through the distribution of a patch, then that corrective action is separated from and not mixed with other corrections that aren't security-relevant.

The separation in the distribution between security-related corrections and security-non-relevant corrections to users can be evidenced in various ways. First, the written procedures support this separation, for example by enforcing that the generation of patches or other types of corrections that address security-related flaws don't include in any case other type of features, e.g., functional. Second, the updates themselves may contain a distinguished naming convention, e.g., in the filename or in the description provided to users, that clearly identifies if the patch consist in security updates or in other type of updates. The dissemination methods may also establish separate paths depending on the type of correction.

The evaluator may also review, whenever they are available, records of the flaw remediation procedures that were conducted e.g., in previous versions of the TOE in order to judge whether the aforementioned separation has been exercised in past releases of corrections to previous versions of the TOE.

## 7.2 Software Bill of Materials (ALC_SBM) – Extended

*Objectives*

This family includes a component that requires the developer to provide a Software Bill Of Materials (SBOM), which is a formal record containing details and supply chain relationships of components included in the software/firmware elements of a product with digital elements. This list usually translates into a list of third-party components (e.g. libraries) used by the TOE, identifying their version and their origin (e.g. developer, or if it's open source code). By providing this evidence, it is possible to maintain a record of third-party components that can be examined at any point in time to determine whether vulnerabilities have been found in any of them.

Moreover, this family requires that the SBOM is provided in a machine-readable format that supports automation when searching for vulnerabilities in the used third-party components.

*Component levelling*

This assurance family contains only one component.

| | |
|---|---|
| ALC_SBM: Software bill of materials | 1 |

Table 3: component levelling for ALC_SBM family

### *Application notes*

The software bill of materials does not necessarily need to match with the parts of the TOE contemplated in ALC_CMS.2 or higher. The fact that the third-party software elements are not consistently listed as parts that compose the TOE (especially those that are linked statically and do not result in a separate binary upon TOE generation), in addition to the fact that the format in which the bill of materials provided needs to be machine readable, make ALC_CMS components not suitable to cover the objectives of ALC_SBM in all situations.

### *ALC_SBM.1: Software bill of materials (Extended)*

Hierarchical to: No other components.

Dependencies: No dependencies

Developer action elements:

ALC_SBM.1.1D **The developer shall elaborate the SBOM including the developer and SBOM Uniform Resource Identifier, containing its email address, and the SBOM compilation timestamp in an ISO 8601 format.**
ALC_SBM.1.2D **The developer shall provide the SBOM to TOE users.**
**Content and presentation elements:**

ALC_SBM.1.1C **The SBOM shall contain at least the top-level third-party software components used by the TOE including, for each, at least its name, version, developer's URI, SPDX-ID structure licence and hash value of the executable component.**
ALC_SBM.1.2C **The SBOM shall be provided in machine readable format, using CycloneDX in version 1.4 or higher or Software Package Data eXchange (SPDX) in version 2.3 or higher.**
Evaluator action elements:

ALC_SBM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### *Evaluation work units for ALC_SBM.1 (Extended)*

#### *Action ALC_SBM.1.1E*

ALC_SBM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### *General*

ALC_SBM.1.1C The SBOM shall contain at least the top-level third-party software components used by the TOE including, for each, at least its name, version, developer's URI, SPDX-ID structure licence and hash value of the executable component.

Work unit ALC_SBM.1-1

The evaluator ***shall examine*** the SBOM to determine that it contains at least the top-level third-party component used by the TOE and that, for each, it includes at least name, version, developer's URI, SPDX-ID structure licence and hash value of the executable component.

For TOEs comprised purely by hardware, without any software or firmware in them, this work unit is not applicable.

For more detail regarding the expected parameters to be included for each third-party component, refer to section 5 in [25].

ALC_SBM.1.2C The SBOM shall be provided in machine readable format, using CycloneDX in version 1.4 or higher or Software Package Data eXchange (SPDX) in version 2.3 or higher.

Work unit ALC_SBM.1-2

The evaluator ***shall examine*** the SBOM to determine that it is provided in machine readable format using CycloneDX in version 1.4 or higher or Software Package Data eXchange (SPDX) in version 2.3 or higher.

The format is defined in the specifications below:

CycloneDX – https://cyclonedx.org/specification/overview/
Software Package Data eXchange (SPDX)- https://spdx.dev/specifications/
For TOEs comprised purely by hardware, without any software or firmware in them, this work unit is not applicable.

## 7.3 Periodic Security Review and Testing (ALC_PSR) – Extended

### *Objectives*

This family defines a component that requires the developer to perform periodic security review and testing of the TOE. This review and testing are different from that performed during the evaluation during AVA_VAN assessment and it doesn't necessarily overlap either with the testing performed as part of ATE assurance class, which is oriented to functional verification of the TOE behaviour rather than security-oriented. The security review and testing required by this family shall be carried out periodically, and not only when changes are introduced in the TOE (e.g. when releasing new functionality or modifying existing one). The intention of the periodical review and testing is twofold:

To regularly verify that no new vulnerabilities have been found for the TOE or its parts.
To ensure no new attack techniques have appeared, that make the TOE vulnerable, since the previous TOE testing which did not reveal any exploitable vulnerabilities.

### *Component levelling*

This assurance family contains only one component.

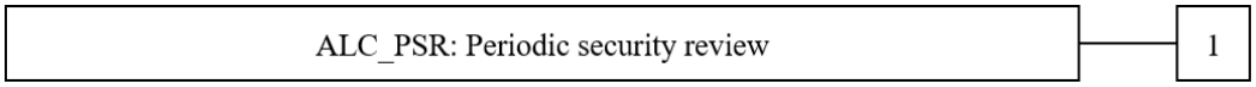



Figure 2: component levelling of ALC_PSR assurance family

### *Application notes*

The evaluation activities linked to this family require the evaluator to examine the security review and testing procedures in order to verify that they require the developer to perform regular security review and testing, and also include review of the developer's records demonstrating that the procedure has been exercised at some moment in the past prior or during the evaluation.

### *Periodic Security Review and Testing of the TOE (ALC_PSR.1) - Extended*

Hierarchical to: No other components.

Dependencies: No dependencies

Developer action elements:

ALC_PSR.1.1D **The developer shall provide the procedures for periodic security review and testing of the TOE.**

ALC_PSR.1.2D **The developer shall provide evidence of exercising the procedures for periodic security review and testing of the TOE**.

Content and presentation elements:

ALC_PSR.1.1C **The procedures for periodic security review and testing of the TOE shall require the developer to perform security review and security testing of the TOE with a periodicity of at most once a year and for a period of time covering, at least, five years from the end of the evaluation.**

ALC_PSR.1.2C **The evidence provided by the developer shall demonstrate that the TOE undergoes security review and testing with the periodicity specified in the procedures.**

Evaluator action elements:

ALC_PSR.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

### *Evaluation work units for ALC_PSR.1 (Extended)*

### *Action ALC_PSR.1.1E*

ALC_PSR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### *General*

ALC_PSR.1.1C The procedures for periodic security review and testing of the TOE shall require the developer to perform security review and security testing of the TOE at regular intervals, with a periodicity of at most once a year.

Work unit ALC_PSR.1-1

The evaluator ***shall examine*** the procedures for periodic security review and testing of the TOE to determine that they require the developer to perform security review and security testing of the TOE at regular intervals, with a periodicity of at most once a year and for a period of time covering, at least, five years from the end of the evaluation.

These periodical tests most commonly include vulnerability assessments. They play a crucial role in periodically reviewing and testing the security of a TOE to verify the absence of new vulnerabilities. This may involve using automated vulnerability scanning tools to scan the TOE and its components for known vulnerabilities. These scans should encompass the entire technology stack, including third-party components and dependencies. Special attention should be paid to

third-party components by cross-referencing them with CVE databases to check for any known vulnerabilities associated with these components.

Other periodical and more in-dept technics may include: Assessing the settings, options, and parameters within the TOE to ensure that they align with established security best practices and organizational policies. Executing red-team exercises, which operates with the goal of finding and exploiting vulnerabilities, providing valuable insights into the TOE's security resilience. Making code reviews, where cybersecurity experts examine the product's source code, searching for coding errors, vulnerabilities, and potential security issues.

The developer's procedures for periodic security review and testing should outline how the manufacturer would react upon the finding of a vulnerability during the review, or point to the applicable ALC_FLR flaw remediation procedures.

Regarding the period of time during which the periodical security review and testing is performed, evaluators shall review the developer's evidence and use as a reference date, that in which it is expected to conclude the evaluation. Evaluators shall review the verdict assigned to this work unit before issuing the final verdict of the evaluation to ensure that the five-year period is still covered at the conclusion of the evaluation.

ALC_PSR.1.2C The evidence provided by the developer shall demonstrate that the TOE undergoes security review and testing with the periodicity specified in the procedures.

Work unit ALC_PSR.1-2 The evaluator **shall examine** the evidence provided by the developer to determine that the TOE undergoes security review and testing with the periodicity specified in the procedures.

When possible, the vendor evidence should be provided in the form of records of exercising the procedures in the past.

It may be the case of a newly developed TOE that the security review and testing procedures have yet to be exercised.

If the developer has produced other similar products, then an examination of records for these procedures in their use may be useful in providing assurance.

# 8 Security Assurance Requirements

The security assurance requirements selected for the site shall support evaluations according to the assurance level EAL5 augmented with ALC_DVS.2, ALC_FLR.3, ALC_FLR.4 (extended), ALC_SBM.1 (extended) and ALC_PSR.1 (extended). These security assurance include the augmentations defined in the PP [2].

The Security Assurance Requirements are:

- ALC_CMC.4,
- ALC_CMS.5,
- ALC_DEL.1,
- ALC_DVS.2,

- ALC_FLR.3,
- ALC_FLR.4 (extended),
- ALC_SBM.1 (extended),
- ALC_PSR.1 (extended),
- ALC_LCD.1, and
- ALC_TAT.2.

The Security Assurance Requirements listed above fulfill the requirements of [13] because hierarchically higher components than the defined minimum site requirements (ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, see section 3.2.3 of [17]) are used in this Site Security Target.

## 8.1 Application Notes and Refinements

The description of the site certification process [17] includes specific application notes. The main item is that a product that is considered as intended TOE is not available during the evaluation. Since the term “TOE” is not applicable in the Site Security Target, the associated processes for the handling of products, or “intended TOEs” are in the scope of this Site Security Target and are described in this document. These processes are subject of the evaluation of the site.

### 8.1.1 CM Capabilities (ALC_CMC.4)

Refer to subsection ‘Application Notes for Site Certification’ in [17] 5.1 ‘Application Notes for ALC_CMC’.

Note: Due to the PP refinements in [2] for ALC_CMS (see PP [2] (see Section 6.2.2.4) not being applicable those for ALC_CMC are also not applicable.

### 8.1.2 CM Scope (ALC_CMS.5)

Refer to subsection ‘Application Notes for Site Certification’ in [17] 5.2 ‘Application Notes for ALC_CMS’.

Note: Due to these application notes the refinements from the PP [2] (see Section 6.2.2.3) are not applicable.

### 8.1.3 Delivery (ALC_DEL.1)

The CC assurance components of the family ALC_DEL (Delivery) refer to the external delivery of (i) the TOE or parts of it (ii) to the recipient or recipient’s site. The CC assurance component ALC_DEL.1 requires procedures and technical measures to maintain the confidentiality and integrity of the product. The means to detect modifications and prevent any compromise of the Initialization Data and/or Configuration Data may include supplements of the Security IC Embedded Software.

The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3 or in later phases of the Security IC product life cycle.

The developer of the Security IC Embedded Software must apply protection to ensure the security of the Security IC Embedded Software. This relates to providing the IC Embedded Software itself or any authentication data required to enable the download of software. This includes the delivery (exchange) procedures for Phase 1.

The client is responsible for secure handling after delivery.

As already outlined in the application notes of the PP [2] the external delivery of the TOE may require additional transfers between the product manufacturer and the client or recipient. These do not address the internal deliveries between sites involved in the life cycle of the intended TOE. Since the assurance component ALC_DEL is only applicable to the external delivery to the recipient, the component cannot be used for internal shipment. Internal shipment is covered by ALC_DVS.

Also, refer to subsection ‘Application Notes for Site Certification’ in [17] 5.3 ‘Application Notes for ALC_DEL’.

#### 8.1.4 Developer Environment Security (ALC_DVS.2)

Refer to subsection ‘Application Notes for Site Certification’ in [17] 5.4 ‘Application Notes for ALC_DVS’.

The assessment of ALC_DVS.2 follows EUCC Scheme State-of-the-Art Document Minimum Site Security Requirements [29].

#### 8.1.5 Life-cycle Definition (ALC_LCD.1)

Refer to subsection ‘Application Notes for Site Certification’ in [17] 5.6 ‘Application Notes for ALC_LCD’.

#### 8.1.6 Tools and Techniques (ALC_TAT.2)

Refer to subsection ‘Application Notes for Site Certification’ in [17] 5.7 ‘Application Notes for ALC_TAT’. Since the used tools and techniques are well defined upfront by the client (see A.Product-Setup) they are TOE specific and cannot be seen as product type specific as stipulated by [17]. Therefore ALC_TAT is not applicable for this SST.

#### 8.1.7 Flaw Remediation (ALC_FLR.3)

Refer to subsection ‘Application Notes for Site Certification’ in [17] 5.5 ‘Application Notes for ALC_FLR’.

#### 8.1.8 Flaw remediation separation (ALC_FLR.4)

No refinement.

#### 8.1.9 Software bill of materials (ALC_SBM.1)

No refinement.

#### 8.1.10 Periodic security review and testing (ALC_PSR.1)

No refinement.

### 8.2 Security Requirements Rationale

#### 8.2.1 Dependencies

For the selected SARs, the following dependencies are defined according to [15]:

- ALC_CMC.4: ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
- ALC_CMS.5: None
- ALC_DEL.1: None
- ALC_DVS.2: None
- ALC_FLR.3: None

- ALC_FLR.4 (extended): ALC_FLR.1
- ALC_LCD.1: None
- ALC_PSR.1 (extended): None
- ALC_SBM.1 (extended): None
- ALC_TAT.2: ADV_IMP.1

The following dependencies are not (completely) fulfilled:

- ALC_LCD.1: This dependency is only partly fulfilled as the site does not represent the entire development environment. This is in-line with and further explained in [17].
- ADV_IMP.1: This dependency is not fulfilled as there is no specific TOE. This is in-line with and further explained in [17].

### 8.2.2 Mapping

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| ALC_CMC.4.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling. | O.Config_IT-env<br>O.LifeCycle-Doc<br>O.Config-Items | Appropriate and consistent labeling is ensured through the application of the CM-Plan (O.LifeCycle-Doc) and the use of the configuration management systems (O.Config_IT-env). The configuration management system manages all TOE relating hardware, software and information (O.Config-Items). |
| ALC_CMC.4.2C: The CM documentation shall describe the method used to uniquely identify the configuration items. | O.LifeCycle-Doc<br>O.Config-Items<br>O.Config-Process | The method used to uniquely identify the configuration items is described in the CM Plan (O.LifeCycle-Doc). Each item gets an internal unique identification for identification (O.Config-Items). The configuration items are tracked throughout the life cycle of the TOE (O.Config-Process). |
| ALC_CMC.4.3C: The CM system shall uniquely identify all configuration items. | O.Config_IT-env<br>O.LifeCycle-Doc<br>O.Config-Items | Unique identification of all CIs is realized by performing the CM activities in accordance with the CM-Plan (O.LifeCycle-Doc) using the Configuration management systems (O.Config_IT-env). Each item gets an internal unique identification for identification (O.Config-Items). |
| ALC_CMC.4.4C: The CM system shall provide automated controls such | O.Config_IT-env<br>O.LifeCycle-Doc<br>O.Logical-Access | The configuration management systems (O.Config_IT-env) used according to the CM-Plan |

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| that only authorized changes are made to the configuration items. | O.Logical-Operation<br>O.Config-Items<br>O.Config-Process | (O.LifeCycle-Doc) enforces automated controls such that only authorized changes are made to the configuration items. Only authorised changes can be made to the CM system (O.Logical-Access). An authentication is necessary to get access to the system (O.Logical-Operation). The configuration management system manages all TOE relating hardware, software and information (O.Config-Items). The configuration items are tracked throughout the life-cycle of the TOE (O.Config-Process). |
| ALC_CMC.4.5C: The CM system shall support the production of the product by automated means. | O.Config_IT-env<br>O.LifeCycle-Doc<br>O.Config-Process<br>O.Zero-Balance | The software on the development computers (O.Config_IT-env) supports automated production of products when used in accordance with the CM-Plan (O.LifeCycle-Doc). The configuration items are tracked throughout the life cycle of the TOE (O.Config-Process). The zero balancing prevents an unnoticed loss of secure objects by dedicated internal processes (O.Zero-Balance). |
| ALC_CMC.4.6C: The CM documentation shall include a CM plan. | O.LifeCycle-Doc<br>O.Config-Process | The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan. The procedures may be detailed in the CM plan (O.Config-Process). |
| ALC_CMC.4.7C: The CM plan shall describe how the CM system is used for the development of the product. | O.LifeCycle-Doc<br>O.Config-Process | The life cycle documentation (O.LifeCycle-Doc) describes how the CM system is used for the development of the product. The procedures may be detailed in the CM plan (O.Config-Process). |
| ALC_CMC.4.8C: The CM plan shall describe the procedures used to accept modified or newly created | O.LifeCycle-Doc<br>O.Config-Process | The acceptance procedures for modified or newly created configuration items are described in the CM-Plan (O.LifeCycle-Doc). The |

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| configuration items (as part of the product). | | configuration items are tracked throughout the life cycle of the TOE. The procedures may be detailed in the CM plan (O.Config-Process). |
| ALC_CMC.4.9C: The evidence shall demonstrate that all configuration items are being maintained under the CM system. | O.LifeCycle-Doc<br>O.Config-Items<br>O.Config-Process<br>O.Zero-Balance | All configuration items are listed in the CI-list (O.LifeCycle-Doc). This is also described in the developer documentation (O.LifeCycle-Doc). The configuration items are tracked throughout the life cycle of the TOE (O.Config-Process). Each item gets an internal unique identification for identification (O.Config-Items). The contributed zero balancing prevents an unnoticed loss of secure objects by dedicated internal processes (O.Zero-Balance). |
| ALC_CMC.4.10C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan. | O.Config_IT-env<br>O.LifeCycle-Doc<br>O.Config-Items<br>O.Config-Process | The CI-list (O.LifeCycle-Doc) is generated from the configuration management systems (O.Config_IT-env). This is also described in the developer documentation (O.LifeCycle-Doc). The configuration items are tracked throughout the life cycle of the TOE. Each item gets an internal unique identification for identification (O.Config-Items). The procedures may be detailed in the CM plan (O.Config-Process). |

Table 4: Rationale for ALC_CMC.4

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| ALC_CMS.5.1C:<br>The configuration list includes the following: the intended TOE itself; the evaluation evidence required by the SARs in the SST; the parts that comprise the intended TOE; the implementation | O.Config_IT-env<br>O.LifeCycle-Doc<br>O.Config-Items<br>O.Config-Process | The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan and a CI-List with the items required by ALC_CMS.5.1C. This is generated from the configuration management systems (O.Config_IT-env). The developer documentation |

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan. | | contains all necessary and TOE relating information (O.LifeCycle-Doc). The configuration items are tracked throughout the life cycle of the TOE. Each item gets an internal unique identification for identification (O.Config-Items). The procedures may be detailed in the CM plan (O.Config-Process). |
| ALC_CMS.5.2C:<br>The configuration list shall uniquely identify the configuration items. | O.Config_IT-env<br>O.LifeCycle-Doc<br>O.Config-Items | Unique identification of all CIs is realized by performing the CM activities in accordance with the CM-Plan (O.LifeCycle-Doc) using the Configuration management systems (O.Config_IT-env). Each item gets an internal unique identification for identification (O.Config-Items). |
| ALC_CMS.5.3C:<br>For each configuration item, the configuration list shall indicate the developer/subcontractor of the item. | O.Config_IT-env<br>O.LifeCycle-Doc<br>O.Config-Items | The CI-List (O.LifeCycle-Doc) indicates the developer / subcontractor for each configuration items as described in the CM-Plan (O.LifeCycle-Doc). All items are managed by the CM system (O.Config_IT-env). Each item gets an internal unique identification for identification (O.Config-Items). |

Table 5: Rationale for ALC_CMS.5

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| ALC_DEL.1.1C:<br>The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the intended TOE to the recipient. | O.LifeCycle-Doc,<br>O.Transport,<br>O.Data-Transfer. | The developer environment security documentation (O.LifeCycle-Doc) describes all measures which have to be considered for delivering the Embedded Software.<br>The definition of the secure transport procedures for physical security objects and development data and tools ensure confidentiality and integrity of all transported assets. |

Table 6: Rationale for ALC_DEL.1

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| ALC_DVS.2.1C:<br>The developer environment security documentation shall describe all the physical, logical, procedural, personnel, and other security controls that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment. | O.LifeCycle-Doc<br>O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security<br>O.Network-Separation<br>O.Logical-Access<br>O.Logical-Operation<br>O.Staff-Engagement | The developer environment security documentation (O.LifeCycle-Doc) describes the physical (O.Physical-Access, O.Security-Control, O.Alarm-Response), procedural (O.Internal-Monitor, O.Maintain-Security), personnel (O.Staff-Engagement), and other (O.Network-Separation, O.Logical-Access, O.Logical-Operation) security controls that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. |
| ALC_DVS.2.2C:<br>The developer environment security documentation shall justify that the security controls provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE. | O.LifeCycle-Doc<br>O.Zero-Balance | The developer environment security documentation (O.LifeCycle-Doc) justifies that the security controls provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. The contributed zero balancing prevents an unnoticed loss of secure objects by dedicated internal processes (O.Zero-Balance). |

Table 7: Rationale for ALC_DVS.2

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| ALC_LCD.1.1C:<br>The life-cycle definition documentation shall describe the processes used to develop and maintain the intended TOE. | O.LifeCycle-Doc<br>O.Config-Process | The processes used to develop the TOE are described in the life cycle documentation (O.LifeCycle-Doc). The configuration items are tracked throughout the life cycle of the TOE (O.Config-Process). |
| ALC_LCD.1.2C:<br>The life-cycle model shall provide for the necessary control over the development and | O.LifeCycle-Doc<br>O.Config-Process<br>O.Zero-Balance | The life cycle model as described in the life cycle documentation (O.LifeCycle-Doc) provides for the necessary control over the development and maintenance of the TOE. The configuration items are |

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| maintenance of the intended TOE. | | tracked throughout the life cycle of the TOE (O.Config-Process). The contributed zero balancing prevents an unnoticed loss of the TOE and TOE components by dedicated internal processes (O.Zero-Balance). |

Table 8: Rationale for ALC_LCD.1

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| ALC_FLR.3.1C:<br>The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the<br>TOE. | O.LifeCycle-Doc | The life cycle documentation (O.LifeCycle-Doc) together with the documentation of the development tools unambiguously defines flaw remediation procedures. |
| ALC_FLR.3.2C:<br>The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw. | O.Flaw-Remediation-Monitor<br>O.Flaw-Remediation-External | The monitoring of flaws (O.Flaw-Remediation-Monitor) lead to a monitoring and management of each discovered flaw. If this flaw was relevant for the TOE user, corrections and guidance of corrective actions are provided to the TOE user (O.Flaw-Remediation-External). |
| ALC_FLR.3.3C:<br>The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws. | O.Flaw-Remediation-Monitor<br>O.Flaw-Remediation-External | The monitoring of flaws (O.Flaw-Remediation-Monitor) lead to a monitoring and management of each discovered flaw. If this flaw was relevant for the TOE user, corrections and guidance of corrective actions are provided to the TOE user (O.Flaw-Remediation-External). |
| ALC_FLR.3.4C:<br>The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users. | O.Flaw-Remediation-Monitor<br>O.Flaw-Remediation-External | The monitoring of flaws (O.Flaw-Remediation-Monitor) lead to a monitoring and management of each discovered flaw. If this flaw was relevant for the TOE user, corrections and guidance of corrective actions are provided to the TOE user (O.Flaw-Remediation-External). |

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| ALC_FLR.3.5C:<br>The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE. | O.Flaw-Remediation-External | For all TOE user relevant flaws, guidance and corrections are provided to the TOE user (O.Flaw-Remediation-External). |
| ALC_FLR.3.6C:<br>The flaw remediation procedures shall include a procedure requiring timely response and the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw. | O.Flaw-Remediation-Monitor | All security flaws are distributed automatically by using a management system (O.Flaw-Remediation-Monitor). |
| ALC_FLR.3.7C:<br>The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users. | O.Flaw-Remediation-Monitor<br>O.Flaw-Remediation-External | The monitoring of flaws (O.Flaw-Remediation-Monitor) lead to a monitoring and management of each discovered flaw. If this flaw was relevant for the TOE user, corrections and guidance of corrective actions are provided to the TOE user (O.Flaw-Remediation-External). |
| ALC_FLR.3.8C:<br>The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws. | O.Flaw-Remediation-External | Each corrective action is documented and evaluated by the developer for functionality and side effects (O.Flaw-Remediation-External). |
| ALC_FLR.3.9C:<br>The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE. | O.Flaw-Remediation-External | For all TOE user relevant flaws, guidance and corrections are provided to the TOE user (O.Flaw-Remediation-External). |
| ALC_FLR.3.10C<br>The flaw remediation guidance shall describe a means by which TOE users | O.Flaw-Remediation-External | All relating TOE users get informed about security flaws and corrective actions by the |

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| may register with the developer, to be eligible to receive security flaw reports and corrections. | | developer (O.Flaw-Remediation-External). |
| ALC_FLR.3.11C:<br>The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE. | O.Flaw-Remediation-Monitor<br>O.Flaw-Remediation-External | The monitoring of flaws (O.Flaw-Remediation-Monitor) lead to a monitoring and management of each discovered flaw. If this flaw was relevant for the TOE user, corrections and guidance of corrective actions are provided to the TOE user (O.Flaw-Remediation-External). |

Table 9: Rationale for ALC_FLR.3

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| ALC_FLR.4.1C:<br>The flaw remediation procedures documentation shall describe how a separation is established in the distribution of flaw corrections to TOE users, separating corrections of security flaws from other flaws that address non-security flaws. | O.LifeCycle-Doc<br>O.Flaw-Remediation-Monitor<br>O.Flaw-Remediation-External | The life cycle documentation (O.LifeCycle-Doc) and the flaw remediation procedures define the Security Flaw classification in the Configuration management system and describe possibility of generation of separate correction or release packages for security-related and non-security-related corrections. Records in the CM systems provide evidence of the classification and processing (O.Flaw-Remediation-Monitor). Security corrections are delivered to the client as a separate delivery. (O.Flaw-Remediation-External). |

Table 10: Rationale for ALC_FLR.4

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| ALC_SBM.1.1C:<br>The SBOM shall contain at least the top-level third-party software components used by the TOE including, for each, at least its name, | O.Component-Lists<br>O.LifeCycle-Doc | The life cycle documentation (O.LifeCycle-Doc) together with the documentation of the vulnerability handling unambiguously defines how the components of the TOE and |

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| version, developer's URI, SPDX-ID structure licence and hash value of the executable component. | | their necessary details are tracked and how component lists are generated. |
| ALC_SBM.1.2C:<br>The SBOM shall be provided in machine readable format, using CycloneDX in version 1.4 or higher or Software Package Data eXchange (SPDX) in version 2.3 or higher | O.Component-Lists<br>O.LifeCycle-Doc | The life cycle documentation (O.LifeCycle-Doc) unambiguously defines the document formats supported by the site. |

Table 11: Rationale for ALC_SBM.1

| SAR | Security Objective(s) | Rationale |
|---|---|---|
| ALC_PSR.1.1C:<br>The procedures for periodic security review and testing of the TOE shall require the developer to perform security review and security testing of the TOE with a periodicity of at most once a year and for a period of time covering, at least, five years from the end of the evaluation. | O.Security-Review | The vulnerability handling documentation defines the default scope and periodicity for a product type. |
| ALC_PSR.1.2C:<br>The evidence provided by the developer shall demonstrate that the TOE undergoes security review and testing with the periodicity specified in the procedures. | O.Security-Review | The vulnerability handling documentation defines the output of the security review and testing. |

Table 12: Rationale for ALC_PSR.1

# 9 Site Summary Specification

## 9.1 Preconditions required by the Site

The site performs development and test services for secure IC embedded software. In order to perform these services in a secure way, the client of the site needs to support the security processes of the site. The following description summarizes the preconditions clients have to fulfil to ensure the security measures of the site in order to protect its assets.

| Precondition | Assumption |
|---|---|
| For each project setup, the client needs to agree on the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results from the site.<br>The client has to provide and support tools and their documentation which are needed to develop software for this dedicated client. The amount and description of these tools must be defined and communicated by the client.<br>Further, for each project setup, the client may either a) explicitly define the classification for each asset type depending on his security requirements and in consultation with the site[7] or b) accept the default classification[8] by not providing his own definition.<br>If the client uses the service of Periodic Security Review the client defines the scope, intervals, periodicity and timeframe for the product type or the client agrees to the default plan provided by the Site for that product type. | A.Product-Setup |
| In case of physical shipment of security relevant items between the client and the site, the client needs to agree about the shipment details and procedures.<br>To be able to exchange development data and tools securely it is necessary to establish a secure channel. Therefore, the types of encryption and signature have to be agreed upon and the necessary keys have to be exchanged. | A.Shipment |
| In case of transport, the developed software will be encrypted by using dedicated transport keys. Also for authentication at platforms (e.g. by flash loader) TOE keys are in use. The keys have to be shared with the opposite communication partner in a secure way. If requested by the client the knowledge of sensitive keys can be split in at least two parts and separately transferred to at least two different persons. | A.Transport-keys |

Table 13: Mapping of preconditions to assumptions

[7] A template is provided by the site
[8] See 5.1 for all asset types and assigned default levels

## 9.2 Services of the Site

The following services and/or processes provided by Austria Card are in the scope of the site evaluation process:

- IC Embedded Software Development and testing (Phase 1).

as defined in the Protection Profile [2] and also defined in a similar way in the referred PPs [2] to [12].

Development and handling of assets is performed according to their classification. The site provides development according to the asset classification and restricted access under control of Austria Card. Secure areas, which are established by a combination of physical, procedural, personnel and logical measures, are allowing only authorized employee access to assets like physical samples, source code, libraries, tools, keys and documentation.

Development comprises the specification of embedded operating systems- and application products, the source code of embedded software, the test specifications and the related test vectors and the creation of development related documents. Some of the data sheet and application note material is also produced at this site. The site manages software and hardware dependencies and produces corresponding documentation in machine readable formats.

Validation comprises the execution of the tests foreseen by the test specification using the defined test vectors.

The site is also used to generate and set up cryptographic keys used to protect the developed software during transport and for authentication at platforms (e.g. via flash loader).

The site offers secure management and handling of keys, as well as the secure delivery and reception of code, tools, documentation, keys and other data.

The site offers an additional optional service for periodic security review according to CRA [26] requirements.

## 9.3 Objectives Rationale

The following rationale provides a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives:

O.Config_IT-env: The site uses strict versioning and project separated management of project relating information. This directly addresses the OSP P.Config_IT-env. Further, the threats T.Computer-Net, T.Accident-Change, T. Unauthorisied-Staff and T.Staff-Collusion can be prevented.

O.LifeCycle-Doc: Dedicated documents exist for the site which defines the use and the management of the configuration management systems, the configuration item list, the site security, the development process and the development tools. The site follows the procedures and instructions of these documents. This directly addresses the OSP P.LifeCycle-Doc and P.Vulnerability-Handling (for component-lists). Further, the

threats T. Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.StaffCollusion and T.Attack-Transport can be prevented.

O.Physical-Access: The site implements a “need to know” principle by separation measures using a combination of physical partitioning together with technical and organisational security measures. The access control measures support the enforcement of the separation and the “need to know” principle. The handling of assets is restricted to separate security areas. By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion can be prevented.

O.Security-Control: The site is using dedicated personnel for guard services. These personnel are responsible for operation of the access control systems, for the enforcement of the access control, for the surveillance of the technical alarm sensors and the responses to incidents and for the escort of visitors. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff.

O.Alarm-Response: In case of an access attempt to an asset by an unauthorised person the site has an alarm system in place. After the alarm is triggered the unauthorised person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff.

O.Internal-Monitor: The established security measures of the site are regularly reviewed by security management meetings and internal audits. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff and T.Staff-Collusion.

O.Maintain-Security: Technical security measures are maintained regularly. This ensures that the systems are working correctly and are configured as required to ensure the protection of the networks and computer systems. In addition all employees are trained regularly. Hence, this helps to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

O.Network-Separation: The development networks of the site are located in a dedicated secured area. These networks are connected only to dedicated trustworthy systems. The networks as well as the CM system

implement separation based on asset classifications which allows additionally separation of critical (strictly confidential) assets and above from lower classified assets. This prevents the threats T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff.

O.Logical-Access:The development network is strictly separated from the other internal networks and the internet by using a firewall. The different projects inside the developer network are separated by logical directory structure. The access to the different project information is protected by user account and password. By considering the “need-to-know” principle, only authorised persons have access to the project relating information. Each user has his/her own user account and password. Based on their classification assets are in addition only processed in the according logical security area with regard to the implemented access security measures (e.g. asset storage in dedicated container secured by multifactor-authentication). This prevents the threats T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff.

O.Logical-Operation:The used workstations for development purposes are using authentication measures for the users of these systems. Authentication may include multifactor authentication depending on the type of the development workstation. Hence the threats T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff is prevented.

O.Config-Items: A configuration management system is in use which manages all TOE relating hardware, software and information. Each item gets an internal unique identification for identification. The threat T.Accident-Change is prevented and the security policy P.Config_IT-env is fulfilled.

O.Config-Process: The configuration items are tracked throughout the life cycle of the TOE. The procedures may be detailed in the CM plan. The threat T.Unauthorised-Staff is prevented and the security policy P.Config_IT-env is fulfilled.

O.Staff-Engagement: The site has established personnel security measures: All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job. This helps to prevent the threats T.Computer-Net, T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion and T-Attack-Transport.

| | |
|---|---|
| O.Zero-Balance: | The site executes zero balancing to monitor that no secure object gets lost onsite or during transport. Therefore the amount of incoming and outgoing objects is managed and monitored by the CM system. This helps to prevent the threat T.Attack-Transport. |
| O.Flaw-Remediation-Monitor: | If any kind of flaw is discovered during development or test processes, defined procedures to monitor the flaw and inform the client are executed. This addresses the OSP P.Vulnerability-Handling. |
| O.Flaw-Remediation-External: | In case a flaw remediation has to be executed, all necessary information to enhance the guidance or to prevent the flaw is provided to the client. This addresses the OSP P.Vulnerability-Handling. |
| O.Security-Review | To address vulnerability handling over the whole product life cycle the site offers a periodic security review and testing service described in the vulnerability handling documentation. The scope and periodicity as well as the timeframe are defined by the client for the product type. The site has default values per product type. This addresses the OSP P.Vulnerability-Handling. |
| O.Component-Lists | The site produces and securely delivers component-lists to the client for each TOE as described in the life cycle documentation by tracking all components and compiling corresponding lists. Component-Lists one the one hand support the vulnerability handling in charge of the client and on the other hand enable the client and downstream parties to perform their vulnerability handling. This addresses the OSP P.Vulnerability-Handling. |
| O.Transport | All necessary information regarding the transport has to be shared during the project setup with the client. All received objects are entered in the configuration management system for traceability. This helps to prevent the threat T.Attack-Transport. |
| O.Data-TransferFor secure data transfer, transport and authentication keys are handed over to the client. All secure information is transferred in encrypted form. The client gets informed if a new release is available. If requested by the client the transfer keys are conducted by split the relating key in at least two parts which are transferred to at least two different persons. Furthermore, technical measures like cryptography, separation of network, split access permission and secure storage shall be implemented for this kind of data. This helps to prevent | |

| | |
|---|---|
| | the threats T.Computer-Net, T.Attack-Transport and addresses the OSP P.Organise-Product and P.Vulnerability-Handling (by ensuring secure transfer of vulnerability related information resp. their corrections and remediations and component lists). |

## 9.4 Assurance Measure Rationale

### 9.4.1 O.Config_IT-env

ALC_CMC.4.1C: requires a documented process ensuring an appropriate and consistent labeling of the products.

ALC_CMC.4.3C requires that the CM system uniquely identifies all configuration items.

ALC_CMC.4.4C requires that the CM system provides automated controls so that only authorized changes are made to the configuration items. The configuration list required by ALC_CMC.4.5C requires that the CM system supports the production by automated means.

ALC_CMC.4.10C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan.

ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.4.3C.

ALC_CMS.5.3C requires that the developer of each TSF relevant configuration item is indicated in the configuration list.

The objective meets the set of Security Assurance Requirements.

### 9.4.2 O.LifeCycle-Doc

ALC_CMC.4.1C: requires a documented process ensuring an appropriate and consistent labeling of the products.

ALC_CMC.4.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.

ALC_CMC.4.3C requires a unique identification of all configuration items by the CM system.

ALC_CMC.4.4C requires that the CM system provides automated controls so that only authorized changes are made to the configuration items.

ALC_CMC.4.5C requires that the CM system supports the production by automated means.

ALC_CMC.4.6C requires a CM documentation that includes a CM plan.

ALC_CMC.4.7C requires that the CM plan describes how the CM system is used for the development (production) of the TOE.

ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C requests evidence to demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan.

ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information.

ALC_CMS.5.2C requires that the CL uniquely identify the configuration items.

ALC_CMS.5.3C requires that for each configuration item, the configuration list indicates the developer/subcontractor of the item.

ALC_DVS.2.1C requires that the developer environment security documentation describes all the physical, logical, procedural, personnel, and other security controls that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C requires that the developer environment security documentation justifies that the security controls provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_LCD.1.1C requires that the life-cycle definition documentation describes the processes used to develop and maintain the TOE.

ALC_LCD.1.2C requires that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

All these content elements of the mentioned SARs require dedicated content of the CM documentation and the configuration list, properties of the CM system, content of the developer environment security documentation and of the life cycle documentation.

ALC_FLR.3.1C requires a documentation of the procedures how to track all reported security flaws in each release of the TOE.

ALC_FLR.4.1C requires flaw remediation procedures that describe the separation of security-related and non-security-related corrections. In the CM-System artefacts (e.g. as requests and tasks) are classified in the CM system by the Security Flaw flag. A correction containing at least one Security Flaw element is treated as security-relevant, and security-related and non-security-related corrections are generated as separate correction or release packages through the normal CM process.

Thereby these SARs are suitable to meet the security objective.

### 9.4.3 O.Physical-Access

ALC_DVS.2.1C requires the developer to describe all physical security controls that are necessary to protect the integrity and confidentiality of the product design and implementation in its development environment. Thereby this Security Assurance Requirement contributes to meet the objective.

### 9.4.4 O.Security-Control

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security controls that are necessary to protect the confidentiality and integrity of the product design and implementation including the initialization in its development environment. Thereby this Security Assurance Requirement contributes to meet the objective.

### 9.4.5 O.Alarm-Response

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security controls that are necessary to protect the confidentiality and integrity of the TOE design and implementation including the initialization in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

### 9.4.6 O.Internal-Monitor

ALC_DVS.2.2C: The developer environment security documentation shall justify that the security controls provide the necessary level of protection to maintain the confidentiality and integrity of the product. Thereby this Security Assurance Requirement contributes to meet the objective.

### 9.4.7 O.Maintain-Security

ALC_DVS.2.1 requires that the developer shall describe all personnel, procedural and other security controls that are necessary to protect the confidentiality and integrity of the product design and implementation. Thereby this Security Assurance Requirement contributes to meet the objective.

### 9.4.8 O.Network-Separation

ALC_DVS.2.1C requires that the developer environment security documentation describes all the physical, logical, procedural, personnel, and other security controls that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

### 9.4.9 O.Logical-Access

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security controls that are necessary to protect the confidentiality and integrity of the product design and implementation including the initialization in its development environment. ALC_CMC.4.4C requires that only authorised changes are made to the configuration items.

Thereby these Security Assurance Requirements contribute to meet the objective.

### 9.4.10 O.Logical-Operation

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security controls that are necessary to protect the confidentiality and integrity of the TOE design and implementation including the initialization in its development environment.

ALC_CMC.4.4C requires that only authorised changes are made to the configuration items. Thereby these Security Assurance Requirements contribute to meet the objective.

### 9.4.11 O.Config-Items

ALC_CMC.4.1C requires a documented process ensuring an appropriate and consistent labelling of the products. A method used to uniquely identify the configuration items is required by ALC_CMC.4.2C.

ALC_CMC.4.3C requires that the CM system uniquely identifies all configuration items.

ALC_CMC.4.4C requires that the CM system provides automated controls so that only authorised changes are made to the configuration items. Further

ALC_CMC.4.9C requires that the evidence shall demonstrate that all configuration items are being maintained under the CM plan.

ALC_CMC.4.10C requires the evidence to demonstrate that the CM system is being operated in accordance with the CM plan.

ALC_CMS.5.1C requires that the configuration list shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.4.3C.

ALC_CMS.5.3C requires for each TSF relevant configuration item, that the configuration list indicated the developer of the item.

Thereby these Security Assurance Requirements contribute to meet the objective.

#### 9.4.12 O.Config-Process

ALC_CMC.4.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.

The provision of automated controls such that only authorised changes are made to the configuration items, as required by ALC_CMC.4.4C.

ALC_CMC.4.5C requires that the CM system supports the production by automated means. ALC_CMC.4.6C requires that the CM documentation includes a CM plan.

ALC_CMC.4.7C requires that the CM plan describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C requests evidence to demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan.

The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information.

ALC_LCD.1.1C requires that the life-cycle definition documentation describes the processes used to develop and maintain the products.

ALC_LCD.1.2C requires control over the development and maintenance of the TOE.

The objective meets the set of Security Assurance Requirements.

#### 9.4.13 O.Staff-Engagement

ALC_DVS.2.1C requires the description of personnel security controls that are necessary to protect the confidentiality and integrity of the product design and implementation in its development environment. Thereby this Security Assurance Requirement contributes to meet the objective.

#### 9.4.14 O.Zero-Balance

ALC_CMC.4.5C requires that the CM system supports the production of the TOE by automated means.

ALC_CMC.4.9C requires evidence that all configuration items are being maintained under the CM system.

ALC_DVS.2.2C requires security controls that are necessary to protect the confidentiality and integrity of the TOE.

ALC_LCD.1.2C requires control over the development and maintenance of the TOE.

Thereby this objective is suitable to meet the Security Assurance Requirement

### 9.4.15 O.Flaw-Remediation-Monitor

ALC_FLR.3.2C requires a description of the nature and effect of each security flaw and its status of finding and correction.

ALC_FLR.3.3C requires that for each security flaw a corrective action is identified.

ALC_FLR.3.4C requires a description of the methods to provide flaw information, corrections and guidance on corrective actions.

ALC_FLR.3.6C requires a timely response and an automated distribution of security flaw reports and associated corrections to affected registered users.

ALC_FLR.3.7C requires that any reported flaws are remediated and that the remediation procedures are issued to the TOE users.

ALC_FLR.3.11C requires a that the guidance identify the specific points of contact for all reports and enquiries about security issues involving the TOE.

ALC_FLR.4.1C is supported by the CM system, in which individual artefacts (e.g. requests or tasks) are marked with the Security Flaw flag. A correction containing marked elements is classified and monitored as a security-relevant correction.

### 9.4.16 O.Flaw-Remediation-External

ALC_FLR.3.2C requires a description of the nature and effect of each security flaw and its status of finding and correction.

ALC_FLR.3.3C requires that for each security flaw a corrective action is identified.

ALC_FLR.3.4C requires a description of the methods to provide flaw information, corrections and guidance on corrective actions.

ALC_FLR.3.5C requires a description how the developer receives reports and enquiries of suspected security flaws from the user.

ALC_FLR.3.7C requires that any reported flaws are remediated and that the remediation procedures are issued to the TOE users.

ALC_FLR.3.8C requires that any corrections to a security flaw do not introduce any new flaws.

ALC_FLR.3.9C requires a description in the guidance where the TOE user report any suspected security flaws in the TOE to the developer.

ALC_FLR.3.10C requires a description in the guidance how TOE users can register by the developer to receive security flaw reports and corrections.

ALC_FLR.3.11C requires that the guidance identify the specific points of contact for all reports and enquiries about security issues involving the TOE.

ALC_FLR.4.1C requires security-related and non-security-related corrections to be distributed separately. The site tracks all security relevant artefacts in the CM system and provides separate correction or release packages through the normal CM process.

#### 9.4.17 O.Security-Review

ALC_PSR.1.1C requires procedures for periodic security review and testing of the TOE, with a periodicity of at most once a year and for a period of time covering at least five years from the end of the evaluation.

ALC_PSR.1.2C requires evidence demonstrating that the TOE undergoes security review and testing with the periodicity specified in the procedures.

#### 9.4.18 O.Component-Lists

ALC_SBM.1.1C requires that the SBOM (which is part of the component lists described in the life cycle and in the vulnerability handling documentation) contains at least the top-level third-party software components used by the TOE including, for each, at least its name, version, developer's URI, SPDX-ID structure licence and hash value of the executable component.

ALC_SBM.1.2C requires that the SBOM (which is part of the component lists described in the life cycle and in the vulnerability handling documentation) is provided in machine readable format, using CycloneDX in version 1.4 or higher or Software Package Data eXchange (SPDX) in version 2.3 or higher.

#### 9.4.19 O.Transport

ALC_DEL.1.1C requires that the delivery documentation describe all procedures that are necessary to maintain security during TOE distribution.

#### 9.4.20 O.Data-Transfer

ALC_DEL.1.1C requires that the delivery documentation describe all procedures that are necessary to maintain security during TOE distribution.

## 9.5 Mapping of the Evaluation Documentation

| SAR | Evaluation Documentation |
|---|---|
| ALC_CMC.4 | Configuration Management System Documentation [19]. |
| ALC_CMS.5 | Life Cycle Documentation [21]. |
| ALC_DEL.1 | Development Security and Delivery Documentation [20]. |
| ALC_DVS.2 | Development Security and Delivery Documentation [20]. |
| ALC_FLR.3 | Vulnerability Handling documentation [22], Vulnerability Disclosure Policy [23]. |
| ALC_FLR.4 (extended) | Vulnerability Handling documentation [22]. |
| ALC_SBM.1 (extended) | Life Cycle Documentation [21], Vulnerability Handling documentation [22]. |

| | |
|---|---|
| ALC_PSR.1 (extended) | Vulnerability Handling documentation [22]. |
| ALC_LCD.1 | Life Cycle Documentation [21]. |

# 10 References

## 10.1 Literature


[1] Site Security Target Template, Version 1.0, published by Eurosmart, 2009-06-21.

[2] Security IC Platform Protection Profile with Functional Packages, Version 2.0, BSI-CC-PP-0084-V2-2026, Eurosmart, 2025.

[3] Common Criteria Protection Profile, Java Card System – Open Configuration Protection Profile, Version 3.2, BSI-CC-PP-0099-V3-2024, July 2024

[4] Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application", Basic Access Control, Version 1.10, BSI-CC-PP-0055-2009.

[5] Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application", Extended Access Control, Version 1.10, PSI-CC-PP-0056V2-2012.

[6] Common Criteria Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP), Version 1.0, BSI-CC-PP-0068-V2-2011.

[7] Common Criteria Protection Profile, Protection profiles for secure signature creation device - Part 2: Device with key generation, BSI-CC-PP-0059-2009-MA-02

[8] Common Criteria Protection Profile, Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application, Version 1.0.1, BSI-CC-PP-0071-2012.

[9] Common Criteria Protection Profile, Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application, Version 1.0.1, BSI-CC-PP-0072-2012.

[10] Common Criteria Protection Profile, Schutzprofil Smart Meter Gateway, Version 1.3, BSI-CC-PP-0073-2014.

[11] Common Criteria Protection Profile Configuration, Java Card System Multi-Assurance PP Configuration, Protection Profile Module for Firewall ADV_SPM, November 2025, Version 3.2M

[12] Common Criteria Protection Profile, Protection profiles for secure signature creation device - Part 3: Device with key import, Version 1.0.2, BSI-CC-PP-0075-2012.

[13] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, CC:2022 Revision 1, November 2022.

[14] Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, CC:2022 Revision 1, November 2022.

[15] Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance components, CC:2022 Revision 1, November 2022.

[16] Common Methodology for Information Technology Security Evaluation (CEM): CEM:2022 Revision 1, November 2022.

[17] Supporting Document Guidance, Site Certification, October 2007, Version 1.0, Revision 1, CCDB-2007-11-001

[18] EUCC State-of-the-Art document: Application of Attack Potential to Smartcards, Version 2 (final), applicable version 16 December 2025.

[19] Configuration Management System Documentation.

[20] Development Security and Delivery Documentation.

[21] Life Cycle Documentation.

[22] Vulnerability Handling Documentation.

[23] Vulnerability Disclosure Policy

[24] BSI, Technische Richtlinie TR-03183: Cyber-Resilienz-Anforderungen an Hersteller und Produkte. Teil 2: Software Bill of Materials (SBOM). Version 1.0, 2023-07-12.

[25] BSI, Technical Guideline TR-03183-2: Cyber Resilience Requirements for Manufacturers and Products – Part 2: Software Bill of Materials (SBOM). Version 2.1.0, 2025-09-03.

[26] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Official Journal of the European Union, 20 November 2024.

[27] Cyber Resilience Act implementation via EUCC and its applicable technical elements, Annexes, Final Version 27/01/2025

[28] prEN 18330, Cybersecurity requirements for smartcards or similar devices, including secure elements - Application layer, Publication date: Jan 20, 2026

[29] EUCC Scheme State-of-the-Art Document, Minimum Site Security Requirements, Version 2, February 2025.

[30] CCMB, Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, 2025-10-15

## 10.2 Definitions

Client — The site providing the Site Security Target may operate as a subcontractor of the TOE manufacturer. The term “client” is used here to define this business connection. It is used instead of customer since the terms “customer” and “recipient” are reserved in CC. In this document, the terms “customer” and “recipient” are only used in the sense of the CC.

## 10.3 List of Abbreviations

| | |
|---|---|
| SST | Site Security Target |
| SSM | Site Security Manual |
| PP | Protection Profile |

| | |
|---|---|
| CC | Common Criteria |
| SAR | Security Assurance Requirement |

## 10.4 Revision History

| Version | Changes |
|---|---|
| 4.0-Lite | SST-Lite derived from SST Version 4.0 |