G+D Mobile Security

Site Security Target Lite Giesecke+Devrient Development Center Spain (DCS)

Version 2.7/23.03.2023

Table of Contents

List of tables

1 Document Information

1.1 Reference

Title: Site Security Target Lite Giesecke+Devrient Development Center Spain (DCS)

Version/Date: Version 2.7/23.03.2023

Company: Giesecke+Devrient Mobile Security Iberia

Name of the site: Giesecke+Devrient Development Center Spain (DCS)

Product Type: Smart Card Software Development and administrative services

1.2 Overview

This document is the Site Security Target Lite Giesecke+Devrient Development Center Spain (DCS). It is based on [5] with the modifications necessary to correctly describe the sites named above.

2 SST Introduction

This chapter is divided into the sections "Identification of the Site" and "Site description".

This security target refers to the following sites:

Giesecke+Devrient Development Center Spain (DCS)

The sites are used for Smart Card Software Development.

2.1 Identification of the Site

1.) The G+D development site is located at

Giesecke+Devrient Mobile Security Iberia S.A.

Carrer del Número 114, nº 27 , Polígon Pratenc

E-08820 El Prat de Llobregat

Barcelona

Spain

which will be abbreviated by 'DCS' (Development Center Spain) throughout the rest of the document.

The site covers one building where CC relevant development is performed: BCN2. DCS is located in building BCN2. *Building BCN2 is used by G+D exclusively.* The site is used for development of Smart Card software and testing. Development and testing activities are restricted to the designated development area. The server infrastructure including the CM system is located in a dedicated server room. Administrative services, physical security management and central IT-services are also located in this building.

For multisite development, services provided by the administration may also be fully or partly be provided to other development sites. The services provided by this site to other sites of Giesecke+Devrient are listed in the document 'Services provided to other G+D sites by Giesecke+Devrient Development Center Spain'. The services provided by other sites of Giesecke+Devrient used be the site defined in chap. 2.1 are listed in the

document 'Services provided by other G+D sites used by Giesecke+Devrient Development Center Spain'.

2.2 Site description

The following areas of the plant specified in Chap. 2.1 are in the scope of the SST:

1.) DCS

The following services and/or processes provided by Giesecke+Devrient Development Center Spain (DCS) are in the scope of the site evaluation process:

Smart Card Software Development (Smart Card OS Development, Smart Card Applet and Application Development, Testing, Release of developed components).

The site evaluation covers the development of products based on the following operating systems:

- Sm@rtSIM CX
- SmartCafe Expert
- Convego JOIN
- STARCOS
- Sm@rtSIM Next Generation

In addition, product lines which require EMVCo related type approvals are developed in the same environment following the same procedures as the products named above.

Supporting services at DCS:

- Management of physical security and IT-Security
- IT-Services (storage, backup, etc.)
- Administrative Services (e.g. Human Resources related services)

2.2.1 Smart Card Software Development

The Smart Card Software Development area is a security area with restricted access. Only authorised persons are allowed to enter this area. The security area is secured by mantraps which can only be entered after successful authentication by card (company

badge, visitor badge). Access rights on access cards are granted and revoked by the responsibles for physical site security.

For the development of the Smart Card Software a configuration management system is used. Access to the software development storage servers is restricted to authorised persons. Successful authentication by login name and password or access card and password is required for access to the software development storage servers.

2.2.2 Supporting Services

Supporting Services are provided from the building BCN2, but from outside the actual development area. The supporting services comprise physical site security, IT security, IT services, HR related services, etc.

2.2.3 Multisite Development

The following sites are used for multisite development projects (not all sites have to be part of each multisite development project):

1.) Giesecke+Devrient Development Center Germany (DCG)

Giesecke+Devrient GmbH

Prinzregentenstr. 159

81677 München

Germany

2.) Giesecke+Devrient Development Center India (DCI)

Giesecke+Devrient India Pvt. Ltd.

Padale Prime, Plot No 9/1A

411004 Pune

India

3.) Giesecke+Devrient Development Center China (DCC)

Giesecke+Devrient China Pvt. Ltd.

2F Zhuoming Plaza, 1069 Huihenan Street, Banbidian Village, Gaobeidian Town,

Chaoyang District, Beijing,

100123 China

China

2.3 Typical Life Cycle of supported TOEs

The site under evaluation supports the Life Cycle phase Development of a TOE in the sense of the CC. A more detailed description of the Life Cycle of a typical TOE is given here for clarity.

A Smart Card which is ready to use by the final cardholder usually consists of the underlying HW (IC), the Smart Card Operating System, some or all of the applications residing in the card together with the user data in the file system and the related guidance documentation. The underlying HW is a Smart Card chip that consists either of ROM and EEPROM memory or Flash memory.

An ICC consisting of ROM and EEPROM memory requires the delivery of the ROM mask to the HW manufacturer. The chips or modules containing the processed ROM mask are then either delivered back to the development site and are forwarded to a smart card production facility or are delivered from the HW manufacturer directly to the smart card production facility. The EEPROM data required for installation or preparation of the final smart card (e.g. EEPROM part of the Smart Card OS, fixed parts of the file system) is delivered from the development site to the smart card production facility.

For ICCs using flash technology the flash image containing the completed Smart Card OS is delivered to the flash loading site. The ICCs are delivered from the HW manufacturer to the flash loading site directly or via G+D. In addition, flash loading can be performed by the HW manufacturer.

The Life Cycle phase Development refers to the generation and compilation of source code files (usually into hex images) as well as generation the evaluation documentation.

It is assumed that product certifications which refer to this Site Security Target are related to a TOE that follows a TOE life-cycle according to [11], chap. 1.2.3. The Giesecke+Devrient Development Center covers Phase 1 (IC Embedded Software Development) according to [11].

Since a site certification formally does not cover 'TOEs' in the sense of CC but only sites which handle items related to a TOE in a product certification, the term 'TOE related item' is widely used instead of TOE in this document. This comprises all items that

belong to a future TOE like source code files, guidance documentation, cryptographic keys, etc. Please note that a reference to 'TOE related items' in this document might not necessarily covers all TOE related items but only some of them. When the document refers to a TOE which is expected to be developed at this site the term 'future TOE' is used.

3 Conformance Claim

The evaluation is based on Common Criteria Version 3.1, Revision 5 [1], [2]. For the evaluation the methodology in [3] will be used. The SST is CC Part 3 conformant.

This Site Security Target covers the following CC assurance components:

ALC_CMC.4, ALC_CMS.5, ALC_DVS.2 and ALC_LCD.1 as defined in [2]. Please note that ALC_DEL.1 has been excluded from this SST since the site referenced in chap. 2.1 does not perform external deliveries and ALC_DEL.1 is therefore not applicable.

The assurance components chosen for the Site Security Target are taken from the definition of the EAL5 package defined in [2], because the levels EAL4 and EAL5 are usually applied in smart card evaluations. Since some protection profiles require augmentation by ALC_DVS.2 instead of ALC_DVS.1 as in the original package definitions of EAL4 and EAL5, for this Site Security Target also ALC_DVS.2 has been selected instead of ALC_DVS.1.

For the assessment of the security measures attackers with high attack potential are assumed. This allows an evaluation of products using this site according to the assurance component AVA_VAN.5.

4 Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site and security problems derived from the configuration management requirements. The configuration management covers the integrity of TOE related items and the security management of the site.

The Security Problem Definition comprises two major so called security problems. The first set of security problems comprises all kind of attacks regarding theft (e.g. samples) or disclosure (e.g. design data) or manipulation of assets. These security problems are described in terms of threats. The second set of security problems comprises the requirements for the configuration management (e.g. controlled modification) and the control of security measures. These security problems are described in terms of Organisational Security Policies (OSP).

4.1 Assets

The following section describes the assets handled at the site as well as the type of asset and the protection required:

- software specifications (type: electronic documentation; protection: confidentiality, integrity)
- source code in any form (ROM code, EEPROM code, Flash code) (type: electronic source files; protection: confidentiality, integrity)
- pre-personalisation data (including binaries for ROM mask processing, EEPROM content, flash images) (type: electronic binary files; protection: confidentiality, integrity)
- sensitive data or items (this comprises software specifications, source code in any form, pre-personalisation data) (see above)
- security relevant processes such as the development process at the site (type: electronic documentation; protection: confidentiality, integrity)
- development systems and configuration systems (type: system, combination of hardware and software; protection: integrity)
- confidential product documentation (type: electronic documentation; protection: confidentiality, integrity)

All assets of a product line belong to the development team of this product line and access to these assets is restricted to the dedicated development team.

4.2 Threats

All threats endanger the integrity and confidentiality of TOE related items. Future TOEs protect themselves after conclusion of the personalisation phase. However, during the development and production TOE related items are vulnerable to such attacks.

Remark: The term 'sensitive configuration item' has been replaced by 'sensitive data or items', because not only the theft or modification of sensitive configuration items but also of other data kept outside the configuration management system (e.g. personalisation data) might compromise the security of TOE related items or future TOEs. In addition, some threats limited to the production phase in [5] have been extended to the development phase.

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive data or items. 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. In addition, the attacker may be able to use specific working clothes of the site to camouflage the intention.

T.Rugged-Theft: An experienced thief with specialised equipment for burglary, who may be paid to perform the attack tries to access sensitive areas and manipulate or steal sensitive data or items.

T.Computer-Net: A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get data such as source code or sensitive data or modify security relevant processes such as the development process at the site.

T.Unauthorised-Staff: Employees or subcontractors not authorised to get access to products or systems used for development get access to sensitive data or items or affect development systems or configuration systems, so that the confidentiality and/or the integrity of TOE related items is violated. This can apply to development and any TOE related item as well as to the future TOE, its configuration or other sensitive data.

T.Staff-Collusion: An attacker tries to get access to sensitive data or items stored or processed at the site. The attacker tries to get support from one or more employees through an attempted extortion or an attempt at bribery.

T.Attack-Transport: An attacker might try to get sensitive data or items or software specifications during the internal shipment. The target is to compromise confidential information or violate the integrity of TOE related items or future TOEs during the stated internal shipment to allow a modification, cloning or the retrieval of confidential product documentation.

4.3 Organisational Security Policies

The following policies are introduced by the requirements of the assurance components of ALC for the assurance level EAL5+ (augmented by ALC_DVS.2). The chosen policies shall support the understanding of the development and production flow and the security measures of the site. In addition, they shall allow an appropriate mapping to the Security Assurance Requirements (SAR).

P.Config-Items: The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of items that are created, generated, developed or used at a site as well as the received and transferred and provided items.

P.Config-Control: The procedures for setting up the development process for a future TOE as well as the procedure that allows changes of the initial setup for a future TOE shall only be applied by authorised personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes.

P.Config-Process: The services and processes provided by the site are controlled in the configuration management plan. This comprises tools used for the development of the future TOE, the management of flaws and optimisations of the process flow as well as the documentation that describes the services and processes provided by the site.

P.Reception-Control: The inspection of incoming requirements specifications from the client done at the site ensures that developed future TOEs comply with the requirements specified by the client. The inspection of incoming requirements from the HW manufacturer (i.e. datasheets and security manuals) at the site ensures that the developed future TOEs comply with the requirements specified by the HW manufacturer.

P.Accept-Product: In case the client requires formal release of the developed items, the quality control of the site ensures that the released future TOEs comply with the specification agreed with the client. The acceptance process is supported by automated measures. Records are generated for the acceptance process of TOE related items. Thereby, it is ensured that the properties of the future TOE are ensured when internally shipped or externally delivered.

P.Organise-Product: The development process is applied as specified by the site's quality management documentation. If the related data includes sensitive items appropriate measures must be in place.

P.Product-Transport: Technical and organisational measures shall ensure the correct labelling of the future TOE. A controlled internal shipment process shall be applied. The transport supports traceability up to the acceptor. If applicable or required this policy shall include measures for packing if required to protect the future TOE during transport.

In case the future TOE is protecting itself after conclusion of a specific production step - i.e. after personalisation - no specific protection during transport might be necessary.

4.4 Assumptions

Each site operating in a development or production flow must rely on preconditions provided by the previous site. Each site has to rely on the information received by the previous site/client. This is reflected by the assumptions that must be defined for the interface.

The following assumption is considered to be applicable to all sites.

A.Prod-Specification: The client must provide appropriate information (e.g. Stakeholder requirements specification) in order to ensure an appropriate development process. The provided information includes the classification of the documents and future TOE. Default values might be defined with the clients (e.g. "all documents are regarded as public/company confidential/strictly confidential unless a specific classification is provided"). The provided information has to clarify which documents or items developed by the site have to undergo a release process (if any).

A.Item-Identification: Each configuration item shipped from the client to the development site is uniquely labelled by the client to ensure the identification of the configuration item.

A.Internal-Shipment: The recipient (client) of the future TOE is identified by the address of the client site for physical items and by corresponding information (e.g. email address) for electronic items.

A.Requirements_Specification: Development projects are initiated by a project manager or product manager of G+D. If requirements from the client are not sent directly to the development staff, then requirements are sent from the client to the product manager or project manager. The specification of requirements is sent to the product manager or project manager secured against unauthorised modification. For specifications with confidential content these specifications have to be delivered protected against disclosure. The product manager or project manager is then responsible for the transfer

of the client's requirements to the development area. The product manager or project manager does not necessarily have to forward the original requirements of the customer to the development staff.

A.Multisite_Development: In case TOE development is performed together with other development sites (i.e. 'multisite development'), all other sites have to cover all CC assurance components as defined in chap. 3 (or higher). In addition, the site has to be resistant to attackers with high attack potential (i.e. AVA_VAN.5). A trusted communication channel must exist to the remote sites.

5 Security Objectives

The Security Objectives are related to physical, technical and organisational security measures, the configuration management as well as the internal shipment and the external delivery.

O.Security-Documentation: The security of the site is maintained according to the sites security documentation covering all physical and logical measures to ensure the security of the site.

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 and visitors can access restricted areas. Sensitive TOE related items are handled in restricted areas only.

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 video control, 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.

O.Alarm-Response: The technical and organisational security measures ensure that an alarm is generated before an unauthorised person gets access to any sensitive TOE related item (asset). After the alarm is triggered the unauthorised person still has to overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack.

O.Internal-Monitor: The site performs security management meetings on a regular basis. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audits are performed on a regular basis to verify 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.Logical-Access: The site enforces a logical separation between the internal network and the internet by a firewall-system. The firewalls ensure that only defined services and defined connections are accepted. Every user of an IT system has its own user account and password. All computer systems with access to sensitive data require successful authentication either by user name and password or identification token (e.g. company badge) and password. Users have no direct access to the internet from within the internal network. In case of multisite development secure connections to other development sites are established and only appropriately secured connections to other development sites are used. In case administrative services are provided to other development sites (e.g. remote administration of local IT infrastructure this is done via a secured connection.

O.Logical-Operation: All network segments and the computer systems are kept up-to-date (software updates, security patches, virus protection, spyware protection). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.

O.Config-Items: The site has a configuration management system that assigns a unique internal identification to each configuration item. In addition, any future TOE consisting of several configuration items can be uniquely identified by unique labels.

O.Config-Control: The site applies a release procedure for each new future TOE on request of the client. In addition, the site has a process to classify and introduce changes for released future TOEs. A designated team is responsible for the release of new future TOEs and for the classification and release of changes.

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 of future TOEs and for the management of security flaws.

O.Acceptance-Test: The site delivers TOE related items that fulfil the specified properties. The formal prove for that will be provided by the site upon request of the client. Upon request of the client, functional and/or visual checks and tests are performed to ensure the compliance with the specification. The test results are logged to support tracing and the identification of systematic failures. The test results may be logged and transferred to the client, so investigation of the logfiles, verification of compliance with the specification, identification of systematic failures and storage of the logfiles might be shifted to the client (upon request of the client).

O.Organise-Product: For the development process it is ensured that the specified process and implementation standards are applied.

O.Staff-Engagement: All employees who have access to sensitive TOE related items and who can move them out of the defined production flow are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.

O.Reception-Control: Upon reception of a requirements specification from a client by the development staff the authenticity of the specification is verified..

O.Internal-Shipment: The recipient of a physical TOE related item is identified by the assigned client address. The recipient(s) of an electronic TOE related item (e.g. source code) can be identified in different ways. The specific way is defined in the internal shipment procedure. The internal shipment procedure is applied to all shipped TOE related items. The recipient for shipment can only be changed by a controlled process. The packaging (if any) is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of TOE related items during internal shipment. For every sensitive TOE related item, the protection measures against manipulation are defined (e.g. sealed boxes, encryption, integrity protection, electronic signature).

O.Transfer-Data: Sensitive electronic TOE related items (data or documents in electronic form) are protected by applying cryptographic algorithms to ensure confidentiality and/or integrity (whatever is required) during internal shipment and external delivery. In case asymmetric cryptographic algorithms are applied, the associated cryptographic keys must be assigned to individuals to ensure that only authorised employees are able to extract the sensitive electronic TOE related items. Alternatively, symmetric key or password based exchanges methods might be used (e.g. symmetric key encrypted files, password encrypted archives) which don't allow assignment of individuals. In the latter case it has to be ensured that only authorised users have access to the cryptographic keys or passwords. The cryptographic keys and/or passwords are exchanged based on secure measures and they are sufficiently protected.

O.Control-Scrap: The site has measures in place to destroy sensitive documentation and erase electronic media.

O.Multisite_Development: The site provides measures for regular synchronisation of development repositories between sites in case of multisite development. The site provides measures to merge versions of configuration items resulting from concurrent use on different sites between synchronisation periods. Access control meachanisms applied to the configuration management system are also active during synchronisation and merging. Access from other development sites to local development repositories are restricted to multisite development repositories. Other development sites cannot access

local single development repositories. Multisite development repositories have to be explicitely set-up as multisite development repositories.

5.1 Security Objectives Rationale - Coverage of threats and OSPs

The SST includes a Security Objectives Rationale. This includes a tracing which shows how the threats and OSPs for the development site are covered by the Security Objectives. In addition, it includes a justification that shows that all threats and OSPs for the development site are effectively addressed by the Security Objectives. This part of the security objective rationale refers to the requirements of AST_OBJ.1-3 and AST_OBJ.1-4.

5.1.1 Mapping of Security Objectives

Threat and OSP	Security Objective	Note
T.Smart-Theft	O.Security-Documentation O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organisational measures detects unauthorised access and allow for appropriate response on any threat.
T.Rugged-Theft	O.Security-Documentation O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organisational measures detects unauthorised access and allow for appropriate response on any threat.
T.Computer-Net	O.Security-Documentation O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement	The technical and organisational measures prevent unauthorised access to the internal network.

T.Unauthorised-Staff	O.Security-Documentation O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement	Physical and logical access control limits the access to sensitive data to authorised persons.
T.Staff-Collusion	O.Security-Documentation O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Transfer-Data O.Control-Scrap	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees prevent unauthorised access to sensitive data or items.
T.Attack-Transport	O.Internal-Shipment O.Transfer-Data	The applied security measures on sensitive data during internal shipment prevent modification or disclosure of any sensitive data during transport. The applied security measures on physical items during internal shipment allow detection of attempted attacks.
P.Config-Items	O.Config-Items O.Multisite_Development	All relevant items are covered by the control.
P.Config-Control	O.Config-Items O.Config-Control O.Logical-Access O.Multisite_Development	The scope of the configuration control comprises the development process.
P.Config-Process	O.Config-Process	The scope comprises the development process.

P.Reception-Control	O.Reception-Control	The incoming control on client's specifications ensures that only authentic items are accepted.
P.Accept-Product	O.Config-Control O.Config-Process O.Acceptance-Test	The proper future TOE release is ensured by O.Acceptance-Test supported by the means of the configuration management system.
P.Organise-Product	O.Logical-Operation O.Logical-Access O.Config-Control O.Config-Process O.Organise-Product	The application of the development processes is ensured by O.Organise-Product supported by technical and organisational means.
P.Product-Transport	O.Config-Items O.Internal-Shipment O.Transfer-Data	The controlled shipment and delivery procedures ensure correct shipment and delivery of items.

Table 1: Security problem definition to security objectives mapping

6 Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

7 Security Assurance Requirements

The security assurance requirements for this Site Security Target shall support an evaluation according to the assurance level EAL5+. In some cases, this evaluation assurance level is augmented by the security assurance requirement ALC_DVS.2. Therefore this security assurance requirement is also used in this Site Security Target instead of ALC_DVS.1 as defined for the package EAL5 in [2]. Because ALC_DVS.2 is the hierarchically higher component to ALC_DVS.1 this Site Security Target is also suitable for EAL5 evaluations using ALC_DVS.1.

The assurance requirements for the Life-Cycle support are:

ALC_CMC.4 (CM capabilities)

ALC_CMS.5 (CM scope)

ALC_DVS.2 (Development security)

ALC_LCD.1 (Life-cycle definition)

Please note that ALC_DEL.1 is not applicable for the site since no external deliveries are performed by the site.

The assurance requirements listed above fulfil the requirements of [4] because hierarchically higher components are used in this Site Security Target compared to the Minimum Requirements in [4].

The dependencies for the assurance requirements named above are as follows:

ALC_CMC.4: ALC_CMS.1, ALC_DVS.1, ALC_LCD.1

ALC_CMS.5: None

ALC_DVS.2: None

ALC_LCD.1: None

The following dependencies are not fulfilled or not completely fulfilled:

ALC_LCD.1: ALC_LCD.1 is part of this Site Security Target but doesn't cover TOE specific information of the life-cycle definition.

ADV_IMP.1: ADV_IMP.1 relates to TOE specific implementation representations and is therefore not part of this Site Security Target. Therefore this dependency is not satisfied.

7.1 Application Notes and Refinements

The description of the site certification process [4] includes specific application notes. The main item is that a future TOE is not available during the evaluation. Since the term “TOE” is not applicable in the SST the associated processes for the handling of TOE related items are in the focus and described in this SST. These processes are subject of the evaluation of the site.

Refinements regarding Security Assurance Requirements as defined in CC Part 3 [2] are written in *italic*. The term 'TOE' is replaced by 'TOE related items' or 'future TOE', depending on the specific case.

7.1.1 Overview regarding CM capabilities (ALC_CMC)

A configuration management system is used to manage all source files of a future TOE under development.

According to [4] the processes rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below. Since the application notes in [4] are defined for ALC_CMC.5 but this SST claims ALC_CMC.4 only the relevant content elements are adapted.

The use of the configuration management system and the application of a defined change process for the procedures of the site under evaluation are mandatory. The control process must include all procedures that have an impact on the evaluated development processes as well as on the site security measures.

All items listed as assets in chap. 4.1 are kept within the configuration management system.

7.1.2 Overview regarding CM scope (ALC_CMS)

The scope of the configuration management for a site certification process is limited to the documentation relevant for the SAR for the claimed life-cycle SAR and the TOE related items handled at the site.

For this site all items listed as assets in chap. 4.1 are kept within the configuration management system.

7.1.3 Overview regarding Development Security (ALC_DVS)

The CC assurance components of family ALC_DVS refer to (i) the “development environment”, (ii) to the “TOE” or “TOE design and implementation”. The component ALC_DVS.2 “Sufficiency of security measures” requires additional evidence for the suitability of the security measures.

The manufacturer of the future TOEs must ensure that the development and production of the future TOEs is secure so that no information is unintentionally made available for the operational phase of the future TOEs. The confidentiality and integrity of design information, test data, configuration data and pre-personalisation data must be guaranteed, access to any kind of samples, development tools and other material must be restricted to authorised persons only.

Based on these requirements the physical security as well as the logical security of the site are in the focus of the evaluation. Beside the pure implementation of the security measures also the control and the maintenance of the security measures must be considered.

In addition, internal shipment between two development sites has to be covered by ALC_DVS.

7.1.4 Overview regarding Life-cycle definition (ALC_LCD)

The site is not necessarily equal to the entire development environment. Therefore, the ALC_LCD criteria are interpreted in a way that only those life-cycle phases have to be evaluated which are in the scope of the site. For this site the Life Cycle phases 'Development' and 'Production' are relevant.

7.2 Security Assurance Requirements Rationale

The security assurance requirements rationale maps the content elements of the selected assurance components of [2] to the security objectives defined in this Site Security Target. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of future TOEs. If the site already receives TOE related items, this process is based on the assumption that the delivered TOE related items are appropriately labelled and identified, refer to A.Item-Identification.

Note: The content elements that are changed from the original CEM [3] according to the application notes in the process description [4] are written in italic. The term 'TOE' can be replaced by 'TOE related items'.

7.2.1 Rationale for ALC_CMC.4

Security Assurance Requirement	**Security Objective**	**Rationale**
ALC_CMC.4.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*	O.Config-Items O.Reception-Control	Upon reception of an item from another site O.Reception-Control ensures that authenticity is verified for the shipped item. With this it is ensured that the item has been labeled before delivery. After integration into the CM system O.Config-Items ensures appropriate and consistent labeling as well as unique identification of the item.
ALC_CMC.4.2C: The CM documentation shall describe the method used to	O.Config-Items	see ALC_CMC.4.1C

uniquely identify the configuration items.		
ALC_CMC.4.3C: The CM system shall uniquely identify all configuration items.	O.Config-Items O.Multisite_Development	see ALC_CMC.4.1C, O_Multisite_Development ensures the synchronisation of configuration items between all development locations.
ALC_CMC.4.4C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	O.Config-Control O.Logical-Access	All configuration items are kept under configuration control by O.Config-Control. O.Config-Control is supported by O.Logical-Access that requires the authentication of each user before any change can be applied to a configuration item.
ALC_CMC.4.5C: The CM system shall support the production of the *future TOE* by automated means.	O.Config-Process O.Config-Control O.Acceptance-Test	The production phase comprises the compilation of a set of configuration items into image files. The automated selection of a specific set of configuration items for a specific future TOE is supported by the uniquely labeled configuration items in the CM system. Therefore O.Config-Process and O.Config-Control support the automated production of the future TOE. The relation between a specific future TOE and the specific set of configuration items is

		established within the acceptance procedure for the future TOE according to O.Config-Control which is supported by O.Acceptance-Test.
ALC_CMC.4.6C: The CM documentation shall include a CM plan.	O.Config-Process	CM process documentation is available and maintained according to O.Config-Process.
ALC_CMC.4.7C: The CM plan shall describe how the CM system is used for the development of the *future TOE*.	O.Config-Process	CM process documentation is available and maintained according to O.Config-Process.
ALC_CMC.4.8C: The CM plan shall describe the procedures used to accept modified or newly created configuration items (as part of the *future TOE*).	O.Config-Control O.Config-Process	Process descriptions are covered by O.Config-Process, including modification or new generation of configuration items. Product release and handling of change management for released future TOEs is covered by O.Config-Control.
ALC_CMC.4.9C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Config-Items O.Config-Control	All configuration items are kept under configuration control according to O.Config-Items and O.Config-Control.

ALC_CMC.4.10C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.Config-Process	The operation of the CM system in accordance to the CM plan is ensured by O.Config-Process.

Table 2: Rationale for ALC_CMC.4

7.2.2 Rationale for ALC_CMS.5

Security Assurance Requirement	**Security Objective**	**Rationale**
ALC_CMS.5.1C: The configuration list shall include the following: *clear instructions how to consider these items in the list;* the evaluation evidence required by the SARs of *the life-cycle*; *development and production tools.*	O.Config-Items O.Config-Control O.Config-Process	The unique identification of all configuration items is ensured by O.Config-Items. O.Config-Process contains the CM documentationincluding clear instructions how to consider the configuration items in the configuration list. O.Config-Control coveres the handling and identification of released future TOEs.
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config-Items O.Config-Control O.Config-Process	The unique identification of all configuration items is ensured by O.Config-Items. O.Config-Control coveres the handling and identification of released future TOEs. O.Config-Process contains the CM documentation.
ALC_CMS.5.3C: For each *configuration item*, the configuration	O.Config-Process	O.Config-Process contains the CM documentation including clear instructions how to consider the

list shall indicate the developer of the item.		configuration items in the configuration list (including developer information - no subcontractors are used).

Table 3: Rationale for ALC_CMS.5

7.2.3 Rationale for ALC_DVS.2

Security Assurance Requirement	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the *future TOE* design and implementation in its development environment.	O.Security-Documentation O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Internal-Shipment O.Transfer-Data O.Control-Scrap O.Multisite_Development	The development security documentation from O.Security-Documentation describes all physical measures according to O.Physical-Access supported by O.Security-Control and O.Alarm-Response. In addition, all logical measures are described according to O.Logical-Access and O.Logical-Operation. These measures are supported by the security awareness of the staff according to O.Staff-Engagement and the measures that ensure the functionality of the technical security measures of the site according to O.Maintain-Security. Security during internal shipment is ensured by O.Internal-Shipment, O.Multisite_Development and O.Transfer-Data. O.Control-Scrap ensures that no unauthorised access to future

		TOEs is possible for an attacker.
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *future TOE*.	O. Security-Documentation O.Internal-Monitor O.Internal-Shipment O.Transfer-Data O.Multisite_Development	The security measures of the site are in agreement with the security documentation of O.Security-Documentation. Sufficiency of the security measures is verified according to O.Internal-Monitor. Security during internal shipment is ensured by O.Internal-Shipment, O.Multisite_Development and O.Transfer-Data.

Table 4: Rationale for ALC_DVS.2

7.2.4 Rationale for ALC_LCD.1

Security Assurance Requirement	**Security Objective**	**Rationale**
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the *future TOE*.	O.Config-Control O.Config-Process O.Organise-Product	The processes used for development and maintainance of the future TOE are defined in the documentation related to O.Config-Control, O.Config-Process and O.Organise-Product
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the *future TOE*.	O.Acceptance-Test O.Config-Process O.Organise-Product	Control over the development and maintenance of the future TOE is maintained by O.Process-Config and O.Organise-Product supported by the quality

		assurance measures defined by O.Acceptance-Test

Table 5: Rationale for ALC_LCD.1

The guidance on Site Certification [4], chap. 4.8 requires that this rationale shows that all security objectives are effectively addressed by the SARs. The results are summarised in the following table.

Security Objective	**Security Assurance Requirements**
O.Security-Documentation	ALC_DVS.2.1C, ALC_DVS.2.2C
O.Physical-Access	ALC_DVS.2.1C
O.Security-Control	ALC_DVS.2.1C
O.Alarm-Response	ALC_DVS.2.1C
O.Internal-Monitor	ALC_DVS.2.2C
O.Maintain-Security	ALC_DVS.2.1C
O.Logical-Access	ALC_CMC.4.4C, ALC_DVS.2.1C
O.Logical-Operation	ALC_DVS.2.1C
O.Config-Items	ALC_CMC.4.1C, ALC_CMC.4.2.C, ALC_CMC.4.3C, ALC_CMC.4.9C, ALC_CMS.5.1C, ALC_CMS.5.2C
O.Config-Control	ALC_CMC.4.4C, ALC_CMC.4.5C, ALC_CMC.4.8C, ALC_CMC.4.9C, ALC_CMS.5.1C, ALC_CMS.5.2C, ALC_LCD.1.1C
O.Config-Process	ALC_CMC.4.5C, ALC_CMC.4.6C, ALC_CMC.4.7C, ALC_CMC.4.8C, ALC_CMC.4.10C, ALC_CMS.5.1C, ALC_CMS.5.2C, ALC_CMS.5.3C, ALC_LCD.1.1C, ALC_LCD.1.2C
O.Acceptance-Test	ALC_CMC.4.5C, ALC_LCD.1.2C

O.Organise-Product	ALC_LCD.1.1C, ALC_LCD.1.2C
O.Staff-Engagement	ALC_DVS.2.1C
O.Internal-Shipment	ALC_DVS.2.1C, ALC_DVS.2.2C
O.Transfer-Data	ALC_DVS.2.1C, ALC_DVS.2.2C,
O.Reception-Control	ALC_CMC.4.1C
O.Control-Scrap	ALC_DVS.2.1C
O.Multisite_Development	ALC_CMC4.3C, ALC_DVS.2.1C, ALC_DVS.2.2C

Table 6: Rationale for Security Objectives

8 Site Summary Specification

8.1 Preconditions required by the site

This section provides background information on the assumptions defined in chap. 4.4.

The client must provide appropriate specification regarding the requested development services. This will usually be a Stakeholder requirements specification. All documents provided by the client have to be classified as 'confidential', 'company confidential', 'strictly confidential' or similar classification if they require protection against disclosure. All documents with no classification as confidential document are regarded as 'public'. (Remark: All development documents and source code developed by the site are regarded as confidential by default).

For composite future TOEs a user guidance manual and data sheet for the underlying hardware is required from the hardware manufacturer.

For every internal shipment expected from the development site by the client, the client has to provide the site with appropriate address data. This shall be address data for physical items and equivalent address data (e.g. email address) for the delivery or shipment of electronic items.

Details on the requirements for the secure exchange of physical and electronic items are summarised in the confidential document 'Confidential_Preconditions_DCS.doc'.

In case the TOE is developed in a multisite environment the code must be protected at all sites with access to the TOE's source code and the level of protection must be sufficiently high at all sites.

8.2 Services of the site

This site provides the service of secure development of Smart Card software for future TOEs based on the Sm@rtSIM CX, SmartCafe Expert, STARCOS and Convego JOIN based operating system. This comprises Smart Card OS development and application development as well as generation of data for completion, initialisation and personalisation of Smart Cards (e.g. initialisation tables). In addition, the same services are also provided for future TOEs which require EMVCo related type approvals. The site provides secure storage for the source code and related documentation with respect to

confidentiality and integrity in a configuration management system. This data is stored on servers in the site's central computer centre. In case of a multisite development environment the data is only exchanged via sufficiently secured connections and exchanged only with sites which provide a sufficient level of protection for the assets exchanged.

This site also provides the service of compiling Smart Card software into images ready for flash loading for future TOEs based on the Sm@rtSIM CX, SmartCafe Expert, STARCOS and Convego JOIN based operating system and for future TOEs which require EMVCo related type approvals.

The site provides the service of performing a release of future TOEs according to the client's specifications in agreement with the site's quality management system which is certified according to ISO 9001.

This site provides the service of secure delivery of compiled images for Sm@rtSIM CX, SmartCafe Expert, STARCOS and Convego JOIN based future TOEs and for future TOEs which require EMVCo related type approvals to other parties for further processing (ROM mask processing, completion, initialisation and personalisation, flash loading).

8.3 Security objectives rationale - Tracing of security objectives to threats and OSPs

The following rationale provides a justification that shows that all threats and organisational security policies are effectively addressed by the security objectives. This part of the security objective rationale refers to the requirements of AST_OBJ.1-2

The following table shows which security objectives cover which threats and OSPs.

Security Objective	Threats and OSPs
O.Security-Documentation	T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion

O.Physical-Access	T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff
O.Security-Control	T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff
O.Alarm-Response	T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff
O.Internal-Monitor	T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion
O.Maintain-Security	T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion
O.Logical-Access	T.Computer-Net, T.Unauthorised-Staff, P.Config-Control, P.Organise-Product
O.Logical-Operation	T.Computer-Net, T.Unauthorised-Staff, P.Organise-Product
O.Config-Items	P.Config-Items, P.Config-Control, P.Product-Transport
O.Config-Control	P.Config-Control, P.Accept-Product, P.Organise-Product
O.Config-Process	P.Config-Process, P.Accept-Product, P.Organise-Product
O.Acceptance-Test	P.Accept-Product
O.Organise-Product	P.Organise-Product
O.Staff-Engagement	T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion
O.Internal-Shipment	T.Attack-Transport, P.Product-Transport
O.Transfer-Data	T.Staff-Collusion, T.Attack-Transport, P.Product-Transport
O.Reception-Control	P.Reception-Control
O.Control-Scrap	T.Staff-Collusion
O.Multisite_Development	P.Config-Items, P.Config-Control

Table 7: Relation between Security Objectives and Threats and OSPs

O.Security-Documentation

The security of the site is maintained according to the sites security documentation covering all physical and logical measures to ensure the security of the site.

These security measures are necessary to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unautorised-Staff and T.Staff-Collusion.

O.Physical-Access

The development site is operated by G+D only and is not shared with other companies. The site is separated into different security levels.

Only authorised users are allowed within the development part of the site.

All other measures are internal to the site and are therefore not provided in the lite version of the SST.

These measures prevent access to sensitive areas for any unauthorised person and therefore prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff.

O.Security-Control

Trained security staff is in charge of operating all security related systems. This especially holds for monitoring surveillance cameras, granting access rights. etc. Visitors are escorted by the company's security staff or collected by company internal staff from the company's security staff.

Therefore the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff are addressed by management of the security related systems like the access control system.

O.Alarm-Response

Several alarm and detection sensors are installed to provide a warning system for entering the premises by T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff. The trained security staff is able to monitor and access the situation throughout surveillance cameras. Security personnel is dispatched to the location where presence is needed. Security staff is present at any location 24/7.

O.Internal-Monitor

The security officer performs meetings with all security staff on a regular basis. During this meeting security procedures are reviewed and corrective actions are initiated (if necessary). In case security related incident occurred since the last security meeting, they will be addressed. In addition, internal audits are performed on a regular basis to ensure the application of the security measures.

The monitoring and protection of the IT system (including network) is handled by the IT departments under supervision of the IT security manager of the company's security staff.

These measures prevent T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion.

O.Maintain-Security

All security related alarm and detection systems are checked on a regular basis. Logs for building access or site access as well as access to especially secured areas are stored and checked on a regular basis. Network security is monitored permanently by the IT-department.

These measures prevent T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion.

O.Logical-Access

The IT network is logically separated from the outside world by a firewall system consisting of several firewalls which ensures that only authorised connections from and to the IT network are possible. At least two firewalls (i.e. outer firewall and inner firewall) are present between the outside world and any internal network. Communication between all sites which are not on the same premises are secured by end-to-end encrypted connections.

Each user has an individual account. To access data on the company's network every user has to authenticate himself either by login name and password or token and password. Multiple successive failed authentication attempts lead to a blocked the account. The number of retries depend on the authentication method.

Access rights to all network resources are set according to a need-to-know or need-to-have basis, respectively. Access rights of users who do not need access to a network share any longer (e.g. change of jobs) are revoked. In particular, all accounts of employees who leave the company are deactivated.

These measures prevent T.Computer-Net and T.Unauthorised-Staff and support the OSPs P.Config-Control and P.Organise-Product.

O.Logical-Operation

Virus protection and patch management for operating systems and applications ensure the correct operation of the systems and prevent the systems from malfunction. They ensure that protective measures of the IT workplaces are up-to-date (virus definitions, security patches of operating system, security patches of programs, etc.). In addition, regular backups are applied to all network shares related to the configuration management system to prevent loss of data. Backup tapes are securely stored protected against unauthorised modification and disclosure.

These measures prevent T.Computer-Net and T.Unauthorised-Staff and support the OSP P.Organise-Product.

O.Config-Items

All configuration items are identified by a unique version number by the configuration management system. The configuration management system allows unique labelling of any set of configuration items in the configuration management system. By this different future TOEs and configurations thereof can be identified. This ensures that only correct version of TOE related items or future TOE are internally shipped or externally delivered.

By this the OSPs P.Config-Items, P.Config-Control and P.Product-Transport are addressed.

O.Config-Control

The site can either be responsible for development of specific TOE related items for the customer or for the development of complete future TOEs. A future TOE release can be performed on request of the client. This will be done by the site's quality management staff. Released future TOEs are identified by a unique identification assigned by the quality management staff member who is performing the release process. In case the client requests changes to a future TOE that has already been released, these change request will be assessed by the quality management staff. After approval the changes are implemented and applied to the future TOE by the development staff. A new release of the modified future TOE will be performed by the quality management staff. By this the OSPs P.Config-Control, P.Accept-Product and P.Organise-Product are addressed.

O.Config-Process

Configuration items are stored in the configuration management system according to the site's configuration managment plan. In addition, security flaws are also managed through the configuration management system. By this the OSPs P.Config-Process, P.Accept-Product and P.Organise-Product are addressed.

O.Acceptance-Test

On request of the client release of the developed future TOE or developed TOE related items are subjected to a release process under supervision of the site's quality management staff. By this the OSP P.Accept-Product is addressed.

O.Organise-Product

The development process are defined and applied according to the site's quality management system. By this the OSP P.Organise-Product is addressed.

O.Staff-Engagement

All employees working at the site and having access to sensitive information or data habe to sign a non-disclosure agreement to provide legal liability to protect sensitive information against disclosure. In addition, all employees are trained regarding security to support the security awareness. All employees have to pass a security check before they are hired. These measures prevent T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

O.Internal-Shipment

Security relevant physical items are internally shipped either by security transport (e.g. sealed boxes) or in person by company's internal staff. Security relevant electronic items are internally shipped using secure communication measures. This might be signed and/or encrypted emails or similar (e.g. SSL secured web portals) or shared network systems (e.g. shared configuration management system). This prevents T.Attack-Transport and covers also P.Product-Transport.

O.Transfer-Data

Sensitive electronic TOE related items are protected against modification and/or disclosure by cryptographic means during transfer. Either symmetric means, asymmetric means or password protection are applied (as appropriate). Cryptographic keys and password used for secure communication are sufficiently protected against unauthorised access and disclosure. This prevents T.Staff-Collusion, T.Attack-Transport and covers also P.Product-Transport.

O.Reception-Control

Upon reception of a requirements specification from a client, authenticity of this item is verified (e.g. verification of a PGP signature when sent via email). By this the OSP P.Reception-Control is addressed.

O.Control-Scrap

Security relevant items (e.g. documentation and electronic media that contain confidential information) are securely destroyed if no longer required. By this no employee could get uncontrolled access to scrap which might be helpful to support an attack. This prevents T.Staff-Collusion.

O.Multisite_Development

The regular synchronisation between sites and the measures for merging configuration items are necessary to ensure unique identification of all configuration item according to P.Config-Items. These measures have to be set up in a way that the access control mechanisms to configuration items according to P.Config-Control are applied at all times.

8.4 SAR Rationale

The Security Assurance Requirements rationale does not explicitly address the developer action elements defined in [2] because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the preparation for the site visit. In addition, this includes that the procedures are applied as written and explained in the documentation.

Note: The content elements that are changed from the original CEM [3] according to the application notes in the process description [4] are written in italic. The term TOE can be replaced by 'TOE related items' in most cases. In specific cases it is replaced by 'future TOE'.

8.4.1 ALC_CMC

ALC_CMC.4.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling* (refined for Site Certification).

ALC_CMC.4.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C: The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C: The CM system shall support the production of the *future TOE* by automated means.

ALC_CMC.4.6C: The CM documentation shall include a CM plan.

ALC_CMC.4.7C: The CM plan shall describe how the CM system is used for the development of the *future TOE*.

ALC_CMC.4.8C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *future TOE*.

ALC_CMC.4.9C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.

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

The security assurance requirements of the assurance class "CM capabilities" listed above are suitable to support the secure and efficient development of future TOEs due to the formalized acceptance process and the automated support. The identification of all configuration items allows a parallel development of different future TOEs. The requirement for authorized changes support the integrity and confidentiality required for the future TOEs. Therefore this assurance level meets the requirements for the configuration management.

8.4.2 ALC_CMS

ALC_CMS.5.1C: The configuration list shall include the following: *clear instructions how to consider these items in the list;* the evaluation evidence required by the SARs *of the life-cycle; development and production tools* (refined for site certification).

ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.

ALC_CMS.5.3C: For each *configuration item*, the configuration list shall indicate the developer of the item.

The security assurance requirements of the assurance class "CM scope" listed above are suitable to define a controlled environment for the future TOE development. This includes the documentation of the site security and the procedures for the configuration management. Since the site certification process focuses on the processes based on the absence of a concrete TOE these assurance requirements are considered to be suitable.

8.4.3 ALC_DVS

ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the *future TOE* design and implementation in its development environment.

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *future TOE*.

The security assurance requirements of the assurance class "Development security" listed above are required since a high attack potential is assumed for potential attackers. The information used at the site during the development of the future TOE can be used by potential attackers for the development of attacks. This information is needed to apply an attack within considerable time and effort.

8.4.4 ALC_LCD

ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the *future TOE*.

ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the *future TOE*.

The security assurance requirements of the assurance class "Life-cycle definition" listed above are suitable to support the controlled development process and maintenance of already developed future TOEs. This includes the documentation of these processes and the procedures for the configuration management. The site supports only the phases development and production (in the sense of the CC) of the described life cycle. The assurance requirements are considered to be suitable for this site.

8.5 Assurance Measures Rationale

O.Security-Documentation

ALC_DVS.2.1C, requires that the developer shall have a security documentation and ALC_DVS2.2C requires the justification that the described measures are appropriate to provide the necessary level of protection. Therefore this objective contributes to meet the Security Assurance Requirements.

O.Physical-Access

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

O.Security-Control

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

O.Alarm-Response

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

O.Internal-Monitor

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the future TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Maintain-Security

ALC_DVS.2.1C: The development security documentation shall describe the security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Logical-Access

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation including the initialization in its development and production environment. ALC_CMC.4.4C requires that only authorised changes are made to the TOE related items. Thereby this objective is suitable to meet the Security Assurance Requirements.

O.Logical-Operation

ALC_DVS.2.1C: The development security documentation shall describe the security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation in its development environment. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Config-Items

ALC_CMC.4.1C requires a documented process ensuring an appropriate and consistent labelling of the future TOEs. In addition, ALC_CMC.4.3C requires that the CM system uniquely identifies all configuration items. ALC_CMC.4.9C requires that the evidence demonstrates that all configuration items are being maintained under the CM system. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs of the life-cycle, development and production tools. ALC_CMS.5.2C requires that all configuration items are identified uniquely. The objective meets the set of Security Assurance Requirements.

O.Config-Control

ALC_CMC.4.2C requires the CM documentation to describe the method used to uniquely identify the configuration items. ALC_CMC4.4C requires that the CM system shall provide automated measures such that only authorised changes are made to configuration items. ALC_CMC.4.5C requires that the CM system supports the production of the future TOE by automated means. ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items as part of the future TOE. ALC_CMC.4.9C requests evidence to demonstrate that all configuration items are being maintained under the CM system. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs of the life-cycle, development and production tools. ALC_CMS.5.2C requires that all configuration items are identified uniquely. The objective meets the set of Security Assurance Requirements.

O.Config-Process

The provision of automated measures is required by ALC_CMC.4.5C. ALC_CMC.4.6C requires that the CM documentation includes a CM plan. ALC_CMC.4.7C requires that the CM plan describes how the CM system is used for the development of the future TOE. ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items as part of the future TOE. ALC_CMC.4.10C requires that the evidence demonstrates that the CM system is being

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 of the life-cycle, development and production tools. ALC_CMS.5.2C requires that all configuration items are identified uniquely. ALC_CMS.5.3C requires that for each configuration item the developer is indicated in the configuration list.

ALC_LCD1.1C requires a description of the model used to develop and maintain the future TOE. ALC_LCD.1.2C requires that the life-cycle model provides the necessary control over the development and maintenance or the future TOE. The objective meets the set of Security Assurance Requirements.

O.Acceptance-Test

The testing of the future TOEs is considered as automated procedure which is supported by the CM system according to ALC_CMC.4.5C. In addition ALC_LCD.1.2C requires control over the development and maintenance of the future TOE. Thereby the objective fulfils this combination of Security Assurance Requirements.

O.Organise-Product

ALC_LCD1.1C requires a description of the model used to develop and maintain the future TOE. ALC_LCD.1.2C requires that the life-cycle model provides the necessary control over the development and maintenance or the future TOE.

Thereby the objective fulfils this combination of Security Assurance Requirements.

O.Staff-Engagement

ALC_DVS.2.1C requires the description of personnel security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation in its development environment. Thereby the objective fulfils this combination of Security Assurance Requirements.

O.Internal-Shipment

ALC_DVS.2.1C requires that the development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation in its development environment. ALC_DVS2.2C requires the justification that the described measures are appropriate to provide the necessary level of protection. This protection also includes internal shipments. Thereby the objective is suitable to meet this combination of Security Assurance Requirements.

O.Transfer-Data

ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation in its development environment. ALC_DVS2.2C requires the justification that the described measures are appropriate to provide the necessary level of protection. This protection also includes internal shipments. Thereby this objective is suitable to meet the combination of Security Assurance Requirements.

O.Reception-Control

ALC_CMC.4.1C requires that the CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling. Newly created configuration items are also items that are received by another development site which have to be integrated into the site's CM system. Thereby this objective is suitable to meet this Security Assurance Requirement.

O.Control-Scrap

The controlled destruction of scrap is necessary to ensure the confidentiality and integrity of future TOEs as required by ALC_DVS.2.1C.

O.Multisite_Development

ALC_CMC.4.3C requires that the CM system uniquely identifies all configuration items. The synchronisation between sites supports this and thereby the objective supports this Security Assurance Requirement.

ALC_DVS.2.1C requires that the development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation in its development environment. ALC_DVS2.2C requires the justification that the described measures are appropriate to provide the necessary level of protection. This protection also includes internal shipments. The synchronisation between sites is a special type of internal shipment which is covered by O.Multisite_Development. Thereby the objective supports these Security Assurance Requirements.

8.6 Mapping of the Evaluation Documentation

The scope of the evaluation according to the assurance class ALC_CMS comprises the future TOE related configuration items, the complete documentation of the site provided for the evaluation and the security flaw reports and their resolution status. The specifications and descriptions provided by the client are not part of the configuration management at the site.

The mapping between the internal site documentation and the Security Assurance Requirements is only available within the full version of the Site Security Target.

Therefore the following part will be removed for the Site Security Target Lite.

9 References

9.1 Literature

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, CCMB-2017-04-001, April 2017

[2] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 5, CCMB-2017-04-003, April 2017

[3] Common Methodology for Information Technology Security Evaluation: Evaluation methodology; Version 3.1, Revision 5, CCMB-2017-04-004, April 2017

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

[5] Site Security Target Template, Eurosmart, Version 1.0, 21.06.2009

[6] Configuration Management documentation Giesecke+Devrient Development Center Spain (DCS), Version 2.3, 09.03.2023

[7] reference deleted from document, enumeration kept for clarity

[8] Development Security Giesecke+Devrient Development Center Spain (DCS), Version 2.3, 15.12.2020

[9] Life Cycle Definition Giesecke+Devrient Development Center Spain (DCS), Version 2.3, 02.12.2020

[10], [10a] n.a.

[10b] n.a.;

Remark: [10] is used to identify the combination of references [10a] and [10b]

[11] Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, Version 1.0, 19.02.2014

[12] Configuration List Site Certification DCS, Version 2.0, 23.03.2023

[13] Site Security Target Lite Giesecke+Devrient Development Center Spain (DCS), Version 2.7/23.03.2023

[14] Additional Information for Giesecke+Devrient Development Center Spain (DCS), Version 1.4, 03.12.2023

9.2 Terminology

client — The word 'client' is used if the site operates as development site on request of another development site. The ordering development site is denoted as 'client'. The word client is used here instead of 'customer' , because the words 'customer' and 'consumer' are reserved in Common Criteria.

9.3 Abbreviations

CC	Common Criteria.
EAL	Evaluation Assurance Level.
IC	Integrated circuit.
IT	Information Technology.
SST	Site Security Target
ST	Security Target.
TOE	Target of Evaluation.
TSF	TOE Security functions.
TSP	TOE Security Policy.
CM	Configuration Management