Giesecke+Devrient

Site Security Target Lite for Giesecke+Devrient (China) Huangshi Branch

Version 2.3/24.04.2025

Rating : **PUBLIC**

© Copyright 2025
Giesecke+Devrient ePayments GmbH
Prinzregentenstraße 161
D-81677 München

Table of Contents

List of tables

1. Document information

1.1 Overview

This document is the Site Security Target Lite for Giesecke+Devrient (China) Huangshi Branch. It is based on the Eurosmart Site Security Target Template [5] with the modifications necessary to correctly describe the sites named above.

1.2 Site reference

Title of document: Site Security Target Lite for Giesecke+Devrient (China) Huangshi Branch

Version/Date: Version 2.3/24.04.2025

Applying Company: Giesecke+Devrient (China) Technologies Co., Ltd. Huangshi Branch

Name of the site: Giesecke+Devrient (China) Technologies Co., Ltd. Huangshi Branch

Site identification: GDCN Huangshi

Product Type: Smart Card Production

2.

2.

2. SST introduction

2.1 Identification of the site

The site under evaluation is a smartcard production site of Giesecke+Devrient (China) Technologies Co., Ltd., called Giesecke+Devrient (China) Technologies Co., Ltd. Huangshi Branch (short GDCN Huangshi) located at:

151 Hangzhou West Road,
Huangshi City Hubei Province, 435000 P.R. of China

The production area of the site is located on a fenced and guarded area that is owned by Giesecke+Devrient (China) Technologies Co., Ltd. and is not shared with other companies.

When not in production, Smart Cards and Smart Card modules are securely stored in the main vault and sensitive materials vault. The vaults are located in the warehouse inside of the high security area at the ground floor of the building.

The server infrastructure is located in a dedicated server room. Physical Security Management, IT and the local IT administrators are located at the site.

2.2 Site description

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

- Secure reception, identification, registration and storage of Smart Card modules and Smart Cards.
- Secure reception and storage of initialisation data for Smart Card products.
- Cryptographic key management (the key management is only performed as far as it is required for authentication towards the IC and secure loading of the initialisation data).
- Card body manufacturing, chip module embedding, connection of antenna to chip, initialisation.
- Secure delivery (internal shipment and external delivery) of Smart Card modules and Smart Cards. Delivery includes delivery for secure destruction.

- Secure storage and secure destruction of scrap.

The site evaluation covers the above named services for STARCOS products, Sm@rtCafé Expert products and other customer secure products.

Secure reception comprises a verification of the correctness of the delivered items with respect to the delivery documents and - if applicable - the verification of integrity of seals for secure transport.

Secure storage is done in specially secured vaults with restricted access. The items are tracked from reception up until delivery.

Products that require EMVCo related type approvals are produced and handled in the same environment following the same procedures.

2.2.1 Smart Card Production

The site hosts a secure storage area and a secure production area. The site is located on a fenced and monitored area with only one entrance. The site can either be accessed by foot passing a turnstile secured by a card reader or in a vehicle. All vehicles and drivers information are backed up in the Guard House of Security, the authorisation for entering the site in a vehicle is under the control of permanently present security staff. On site access to the security areas is restricted to authorised persons only. The access to the security areas is secured by a mantraps which can only be entered by successful authorisation by card (company badge or visitor’s badge). Access rights on access cards are granted and revoked by the responsible for physical site security.

After the last production step the Smart Cards are delivered either to another site which performs further production steps, or to the Card Issuer. Not all possible production steps have to be carried out at this site. Initialisation is optional. Delivery of Smart Cards to a another site prior to the end of the initialisation is possible.

After reception of Smart Cards or Smart Card modules, the items are either processed immediately or securely stored in the secure storage area. They are only kept outside the secure storage area for the purpose of production or delivery.

The client’s data for production can be received in different ways according to the technical and security needs of the client.

2.2.2 Supporting Services

The services provided by other sites of Giesecke+Devrient used by this site are listed in [11].

The supporting services provided by the company headquarters GDM comprise Corporate Security Office, IT security and IT services, hosting of CM system databases, all located at a regularly audited secure area with restricted access.

2.3 Life-Cycle Phases

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 PP-0084 [6], chap. 1.2.3. This site covers phase 4 (chip module embedding and initialisation) and phase 5 (composite product finishing, preparation and shipping to the personalisation line).

3. Conformance Claim

The evaluation is based on Common Criteria (CC), CC:2022, Revision 1:

Conformance of this ST with respect to CC Part 1 (Introduction and general model) [1].

Conformance of this ST with respect to CC Part 3 (Security Assurance components) [2] is CC Part 3 conformant.

For Common Methodology for Information Technology Security Evaluation [3] will be applied.

This Site Security Target covers the following CC assurance components:

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

The chosen assurance components are taken from the definition of the EAL5 package defined in CC Part 3 [2], augmented with ALC_DVS.2.

ALC_TAT.2 is omitted because development activities are out of scope of the certification of this site.

To support product claims of AVA_VAN.5, attackers with high attack potential as defined in [3] are assumed for the assessment of security measures.

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 the products and the security management of the site.

4.1 Assets

The assets handled at the site are:

- sensitive products (Smart Card modules or Smart Cards):
    - unfinished products
    - finished products
    - defective or rejected products
- sensitive production systems or configuration systems;
- security relevant production processes;
- sensitive configuration data or items;
- cryptographic keys for secure initialisation.

4.2 Threats

All threats endanger the integrity and confidentiality of the products and the representation of parts of the products as long as they are not self-protected. During the development and production, the products and the representation of parts of the products are assumed to be vulnerable to such attacks.

The term 'sensitive configuration item' used in [5] is replaced by 'sensitive data or items' in this document to address the security of sensitive configuration items and of other data kept outside the configuration management system (e.g. cryptographic keys).

Threat	Description
T.Smart-Theft	An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive configuration 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

Threat	Description
	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 configuration 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 access to sensitive configuration data or items or modify security relevant production processes.
T.Accident-Change	An employee or freelancer of G+D may exchange products of different production lots or different clients during production by accident.
T.Unauthorised-Staff	Employees, freelancer of G+D or non G+D employee not authorised to get access to products or systems used for production get access to sensitive configuration data or items or products or affect production systems or configuration systems, so that the confidentiality and/or the integrity of the product is violated. This can apply to the initialisation and any sensitive configuration data or item of the finished product as well as to the finished product, its configuration data or other sensitive data (e.g. cryptographic keys).
T.Staff-Collusion	An attacker tries to get access to sensitive configuration 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 configuration data or items, specifications or products during the internal shipment or the external delivery. The target is to compromise confidential information or violate the integrity of the products during the stated internal shipment or the external delivery process to allow a modification, cloning or the retrieval of confidential information. Confidential information comprises

Threat	Description
	design data, customer or consumer data like code and data (including cryptographic keys) stored in the NVM or classified product specifications.

Table 1: Threats to the security of the site

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).

OSP	Description
P.Config-Items	The configuration management system shall be able to uniquely identify sensitive configuration data or items. This includes the unique identification of sensitive configuration data or items that are created, generated, developed or used at a site as well as the received and transferred and provided sensitive configuration data or items.
P.Config-Control	The procedures for setting up the production process for a new product as well as the procedure that allows changes of the initial setup for a product 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. The procedure for the initial set up of a development or production process ensures that sufficient information is provided by the client.
P.Config-Process	The services and processes provided by the site are controlled in the configuration management plan. This comprises tools used for the production of the product, 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 sensitive configuration data or

	items done at the site ensures that the received sensitive configuration data or items comply with the properties stated by the client.
P.Accept-Product	If required by the client, release tests are performed to ensure the compliance with the specification of the client.
P.Zero-Balance	For each hand over of sensitive configuration data or items, either an automated or an organisational “two-employees-acknowledgement” (“four-eyes principle”) is applied for functional and defective products. According to the released production process the defective items are either sent back to the client or customer and/or consumer or to another production facility (depending on the production-setup).
P.Organise-Product	The configuration or initialisation process is applied as specified by the client. Performing the initialisation is an optional production step. If the data includes sensitive items like cryptographic keys relevant for the life-cycle or sensitive configuration data that affect the security of the product, appropriate measures must be in place. This includes the requirement that the knowledge of cryptographic keys shall be split to at least two different persons. Furthermore, technical measures like crypto-boxes, separation of network, split access permission and secure storage shall be implemented for this kind of sensitive configuration data.
P.Product-Transport	Technical and organisational measures shall ensure the correct labelling of the product. A controlled internal shipment and/or the external delivery 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 product during transport. In case the product is protecting itself after conclusion of a specific production step - i.e. after initialisation - no specific protection during transport might be necessary.

Table 2: Organisational Security Policies addressed by the site

4.4 Assumptions

The following assumptions are considered to be applicable to the operational environment associated with the site.

Assumption	Description
A.Prod-Specification	The client must provide appropriate information in order to ensure an appropriate production process. This includes the delivery of correct data for production, secured by appropriate means against modification and/or disclosure, if necessary.
A.Prod-Release	The client is responsible for the release of the products to be produced.
A.Item-Identification	Each sensitive configuration data or item received by the site can be uniquely identified.
A.External-Delivery	The recipient (consumer) of the product is identified by the address provided by the client. The address of the consumer is part of the product setup. Alternatively, deliveries to the client (Card Issuer) or other production facilities are possible. Every recipient of the items is identified by the address provided by the client.
A.Internal-Shipment	The recipient (client) of the product is identified by the address of the client site for physical items and by corresponding information (e.g. email address) for electronic items.
A.Init-Data	The requirements on the scripts for the configuration and initialisation process are specified or provided by the client of the product.
A.Product-Integrity	The self-protecting features of the smart cards in production are fully operational and it is not possible to influence the configuration and behaviour of the devices based on insufficient operational conditions

	or any command sequence generated by an attacker or by accident.
A.Destruct-Scrap	In case scrap configuration items are not destroyed under the supervision of the site, scrap configuration items are transferred to another site and they are securely destroyed at the receiving site so that they are useless for an attacker.
A.Used-Services	If services provided by other G+D sites related to production and development of products which undergo Common Criteria certification are used then these sites are CC certified.

Table 3: Assumptions for the site

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.

Objective	Description
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 site shall enforce two levels (level 1 and level 2) of access control to sensitive areas of the site. The access control measures ensure that only registered employees and visitors can access restricted areas. Sensitive products 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 configuration data or item. 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 audit is performed at least every year to verify the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure a sufficient protection.
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. The firewall ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into a production network and an office network. Additional specific networks for production and configuration are physically or logically separated from any internal network to enforce access control. Access to the production network and related systems is restricted to authorised employees that work in the related area or that are involved in the configuration tasks or the production systems. 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.
O.Logical-Operation	All network segments and the computer systems are kept up-to-date (software updates, security patches, virus 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 product to uniquely identify products.
O.Config-Control	The site applies a released procedure for the setup of the production process for each new product. In addition, the site has a process to classify and introduce changes for services and/or processes of released products. A designated team is responsible for integration of new products into the configuration management system.
O.Config-Process	The site controls its services and/or processes using a configuration management plan. The configuration management is supported by tools and procedures for the production of the product, for the management of flaws and optimisations of the process flow as well as for the documentation that describes the services and/or processes provided by the site.
O.Accept-Product	Upon request of the client, release tests are performed to ensure the compliance with the specification of the client.
O.Organise-Product	For the configuration or initialisation process it is ensured that the specified process is applied. Performing the initialisation is an optional production step. Data integrity is either ensured by technical means, cryptographic means or is verified at the site. Security relevant cryptographic keys can only be constructed in plaintext or used for cryptographic operations by at least two employees. Other

	sensitive data can only be constructed in plaintext by at least two employees. Use of security relevant cryptographic keys is restricted to crypto-boxes (e.g. Hardware Security Modules, HSM) or similar devices (e.g. smartcards). The update of already released products is done according to a controlled process.
O.Staff-Engagement	All employees who have access to sensitive configuration data or items and who can move parts of the product 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.Zero-Balance	Automated control and/or two employees acknowledgement during hand over of sensitive items is applied for functional and defective products. According to the agreed production flow the defect products are either destroyed at the site or sent to the client or the consumer.
O.Reception-Control	Upon reception of a physical product an incoming inspection is performed. The inspection comprises the received amount of products and the identification according to the documentation of the supplier. For electronic items that require authenticity, the authenticity is verified upon reception.
O.Internal-Shipment	The recipient of a physical configuration item is identified by the assigned client address. The recipient(s) of an electronic configuration 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 configuration data or 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 configuration data or

	items during internal shipment. For every sensitive configuration data or item, the protection measures against manipulation are defined (e.g. sealed boxes, encryption, integrity protection).
O.External-Delivery	The recipient of a physical configuration item is identified by the assigned consumer address. The recipient(s) of an electronic configuration item (e.g. initialization data, response data) can be identified in different ways. The specific way is defined in the external delivery procedure. The external delivery procedure is applied to all sensitive configuration data or items. The recipient for shipment can only be changed by a controlled process. The packaging (if any) is also part of the defined process and applied as agreed with the client or the consumer. The forwarder supports the tracing of sensitive configuration data or items during external delivery. For every configuration data or item, the protection measures against manipulation are defined (if necessary).
O.Transfer-Data	Sensitive electronic configuration 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 configuration 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. The site has measures in place to securely destroy Smart Card modules and Smart Cards.

Table 4: Security Objectives of the site

5.1 Security Objectives Rationale

The SST includes a tracing which shows how the threats and OSPs for a development site are covered by the Security Objectives.

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	The technical and organisational measures prevent unauthorised access to the internal network.

	O.Logical-Access O.Logical-Operation O.Staff-Engagement	
T.Accident-Change	O.Config-Items O.Accept-Product O.Config-Control O.Config-Process	The automated measures and the control and verification procedures avoid accidental changes of sensitive items.
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. In addition, organisational measures prevent uncontrolled access to products or product related items.
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.External-Delivery O.Transfer-Data	The applied security measures on sensitive data during internal shipment and external delivery prevent modification or disclosure of any sensitive data during transport. The applied security measures on physical items during internal shipment and external delivery

		allow detection of attempted attacks.
P.Config-Items	O.Reception-Control O.Config-Items	All relevant items are covered by the control.
P.Config-Control	O.Config-Items O.Config-Control O.Logical-Access O.Reception-Control	The scope of the configuration control comprises the production process.
P.Config-Process	O.Config-Process	The scope comprises the production process.
P.Reception-Control	O.Reception-Control	The incoming control on physical items ensures that only authentic items of correct quantity are accepted. The incoming control on electronic items ensures that only authentic items are accepted.
P.Accept-Product	O.Accept-Product O.Config-Process O.Config-Control	On request of the client release tests are performed.
P.Zero-Balance	O.Zero-Balance O.Control-Scrap	The handling of correct and defective products ensure that no unexpected missing items or left-over items occur.
P.Organise-Product	O.Logical-Operation O.Logical-Access O.Config-Control O.Config-Process O.Organise-Product	The application of the production processes is ensured by O.Organise-Product supported by technical and organisational means.

P.Product-Transport	O.Config-Items O.Internal-Shipment O.External-Delivery O.Transfer-Data	The controlled shipment and delivery procedures ensure correct shipment and delivery of items.

Table 5: Security problem definition to security objectives mapping

5.1.2 Justification for Threats and OSPs

This part of the rationale was removed in the (public) lite version of the Site Security Target.

6.

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 EAL4+ and EAL5+ (AVA_VAN.5). 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 EAL4 and EAL5 in CC Part 3 [2]. Because ALC_DVS.2 is the hierarchically higher component to ALC_DVS.1 this Site Security Target is also suitable for EAL4 and 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_DEL.1 (Delivery)

ALC_DVS.2 (Development security)

ALC_LCD.1 (Life-cycle definition)

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]. In addition, the minimum set of assurance requirements is extended by assurance requirements of the assurance component for delivery (ALC_DEL.1).

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_DEL.1: 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 does not cover product specific information of the life-cycle definition.

7.1 Application Notes and Refinements

The description of the site certification process [4] 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 SST the associated processes for the handling of products 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 'product' or 'configuration item'.

7.1.1 Overview regarding CM capabilities (ALC_CMC)

All products that can be initialised at the site are defined in SAP. Each product is defined as a combination of materials which are also defined in SAP. Each material and each product can be uniquely identified in the SAP system. The single production steps are controlled via the SAP system (e.g. if the first step is not marked as completed in SAP, the second step cannot be started). Evaluation documents (e.g. this document, ALC_xxx documents) and local policies and procedures are managed with Bitbucket.

7.1.2 Overview regarding CM scope (ALC_CMS)

The configuration list [13] contains all evaluation documentation for the certification of this site as well as the development tools used for production.

7.1.3 Overview regarding Delivery procedure (ALC_DEL)

The delivery aspect refers to the delivery of Smart Card modules, inlays, Smart Cards and related data and documentation to the production site as well as all deliveries of Smart Card related products, data and documentation from the Smart Card Production site to the client (i.e. the Card Issuer) or to other production facilities.

7.1.4 Overview regarding Development Security (ALC_DVS)

The site must ensure that the handling and storage of *products* is secure so that no information is unintentionally made available for the operational phase and no unauthorised modifications of security relevant parameters is possible. The confidentiality and integrity of configuration data and initialisation data must be guaranteed, access to any kind of *products* and related data and documentation 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.

Internal shipment within the site has to be covered by ALC_DVS.

7.1.5 Overview regarding Life-cycle Definition (ALC_LCD)

The life-cycle phase covered by the site is the 'Preparation Phase' in the sense of the Common Criteria. G+D uses a quality management system and is certified according to ISO9001.

7.2 Security Assurance Rationale

The security assurance requirements rationale maps the content elements of the selected assurance components of CC Part 3 [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 the products.

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 *configuration items* or *product*.

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*	O.Reception-Control O.Config-Items	Upon reception of an item from another site O.Reception-Control ensures that authenticity is verified for

appropriate and consistent labelling.		the shipped item. With this it is ensured that the item has been labelled before delivery. After integration into the CM system O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the item.
ALC_CMC.4.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Config-Items	see ALC_CMC.4.1C
ALC_CMC.4.3C: The CM system shall uniquely identify all configuration items.	O.Config-Items	see ALC_CMC.4.1C
ALC_CMC.4.4C: The CM system shall provide automated controls 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 according to 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 *product*	O.Config-Process	The ERP system supports automated production of products.

by automated means.		
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 *product*.	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 *product*.	O.Config-Control O.Config-Process	Process descriptions are covered by O.Config-Process, including modification or new generation of configuration items. Handling of change management for released products 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 6: 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*; security flaw reports and resolution status; *development and production tools and related information.*	O.Config-Items O.Config-Process	The unique identification of all configuration items is ensured by O.Config-Items. O.Config-Process contains the CM documentation including clear instructions how to consider the configuration items in the configuration list.
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config-Items O.Config-Process	The unique identification of all configuration items is ensured by O.Config-Items. O.Config-Process contains the CM documentation.
ALC_CMS.5.3C: *Requires a process ensuring that subcontractors involved in developing configuration items are listed in the configuration list.*	O.Config-Process	O.Config-Process contains the CM documentation including clear instructions how to consider the configuration items in the configuration list (no subcontractors are used).

Table 7: Rationale for ALC_CMS.5

7.2.3 Rationale for ALC_DVS.2

Security Assurance	**Security Objective**	**Rationale**

Requirement		
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security controls that are necessary to protect the confidentiality and integrity of the *product* 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.Zero-Balance O.Maintain-Security O.Internal-Shipment O.Transfer-Data O.Control-Scrap	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 controls are described according to O.Logical-Access and O.Logical-Operation. These controls 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 controls of the site according to O.Maintain-Security. Security during internal shipment is ensured by O.Internal-Shipment and O.Transfer-Data. O.Control-Scrap and O.Zero-Balance ensure that no unauthorised access to products is possible for an attacker.
ALC_DVS.2.2C: The development security documentation shall justify that the security controls provide the	O. Security-Documentation O.Internal-Monitor O.Internal-Shipment O.Transfer-Data	The security controls of the site are in agreement with the security documentation of O.Security-Documentation. Sufficiency of the security

necessary level of protection to maintain the confidentiality and integrity of the *product or at least are followed during the development and maintenance of the product.*		controls is verified according to O.Internal-Monitor. Security during internal shipment is ensured by O.Internal-Shipment and O.Transfer-Data.

Table 8: Rationale for ALC_DVS.2

AIS47 [14] justifies the exclusion of ALC_DVS.2.3C which is mandated by [4].

7.2.4 Rationale for ALC_DEL.1

Security Assurance Requirement	**Security Objective**	**Rationale**
ALC_DEL.1.1C: The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the *product* to the consumer.	O.External-Delivery O.Transfer-Data	All external deliveries are according to O.External-Delivery and O.Transfer-Data.

Table 9: Rationale for ALC_DEL.1

7.2.5 Rationale for ALC_LCD.1

Security Assurance Requirement	**Security Objective**	**Rationale**
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the process used to develop and maintain the *product*.	O.Config-Control O.Config-Process O.Accept-Product O.Organise-Product	During production no development takes place. Therefore only the maintenance of products is relevant for this site. Maintenance is done

		according to O.Config-Control, O.Config-Process and O.Organise-Product. On request of the customer, release tests are performed according to O.Accept-Product.
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the *product*.	O.Config-Control O.Config-Process O.Accept-Product O.Organise-Product	see ALC_LCD.1.1C

Table 10: 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.4.2C, 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.4.8C, ALC_CMC.4.9C, ALC_LCD.1.1C, ALC_LCD.1.2C
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.Accept-Product	ALC_LCD.1.1C, ALC_LCD.1.2C
O.Organise-Product	ALC_LCD.1.1C, ALC_LCD.1.2C
O.Staff-Engagement	ALC_DVS.2.1C
O.Zero-Balance	ALC_DVS.2.1C
O.Reception-Control	ALC_CMC.4.1C
O.Internal-Shipment	ALC_DVS.2.1C, ALC_DVS.2.2C
O.External-Delivery	ALC_DEL.1.1C
O.Transfer-Data	ALC_DVS.2.1C, ALC_DVS.2.2C, ALC_DEL.1.1C
O.Control-Scrap	ALC_DVS.2.1C

Table 11: Rationale for Security Objectives

8. Site Summary Specification

8.1 Preconditions required by the site

This section provides background information for the assumptions defined in section 4.4.

The client provides appropriate information for the secure production of ordered products, this includes the scripts or the specification of requirements on the scripts for the configuration and initialisation of the product. The client is responsible for the release of the products. The client provides a method of unique identification for all items shipped to the site. The client provides appropriate information for the delivery of produced goods and electronic data. This information shall at least comprise address data for physical items.

The self-protection features of the *products* are fully operational during production.

Scrap parts are either destroyed under supervision of the site or delivered to the client or another production site for secure destruction. In the latter case, the client or the other production site is responsible for the secure destruction of scrap parts.

Details on the requirements for the secure exchange of physical and electronic items are summarised in [12].

If services provided by other G+D sites related to production and development of products which undergo Common Criteria certification are used, then these sites are CC certified.

8.2 Services of the site

Secure reception, storage and delivery of Smart Card modules and Smart Cards and related goods, secure reception and storage of data for Smart Card production as well as secure destruction of Smart Card modules and Smart Cards.

The reception of Smart Card modules and Smart Cards comprises a verification of the correctness of the delivered items with respect to the delivery documents and - if applicable - the verification of integrity of seals used for secure transportation of items.

The storage of Smart Card related items, including scrap, is done in a specially secured environment on G+D premises with restricted access. The number of items is tracked from reception of the items until the delivery of the items.

The site provides the service of initialisation of Smart Card products based on operating systems listed in section 2.2, and performs cryptographic key management for initialisation.

Secure destruction of Smart Card modules (either several single modules from reel or modules formally part of a Smart Card) with a shredder and additional grinding of the plastic card body of a Smart Card (without module) with a shredder.

8.3 Security Objectives Rationale

The following rationale provides a justification that shows that all threats and organisational security policies are effectively addressed by the security objectives.

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

Security Objective	**Threats and OSPs**	**Rationale**
O.Security-Documentation	T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion	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	T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff	Removed in the public version of the SST.
O.Security-Control	T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff	Trained security staff is in charge of operating all security related systems. This especially holds 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.

O.Alarm-Response	T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff	Several alarm and detection sensors are installed to provide a warning system for entering the premises. Security staff will start to investigate any alarm immediately.
O.Internal-Monitor	T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion	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.
O.Maintain-Security	T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion	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.
O.Logical-Access	T.Computer-Net, T.Unauthorised-Staff, P.Config-Control, P.Organise-Product	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. 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. The production network is additionally separated from the rest of G+D's internal network.
O.Logical-Operation	T.Computer-Net, T.Unauthorised-Staff, P.Organise-Product	Virus protection and patch management for operating systems and applications shall 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 prevent loss of data. Backup tapes are securely stored protected against unauthorised modification and disclosure.
O.Config-Items	T.Accident-Change, P.Config-Items, P.Config-Control, P.Product-Transport	All configuration items are identified by a unique version number by the configuration management system. By this different products can be identified.
O.Config-Control	T.Accident-Change, P.Organise-Product, P.Config-Control, P.Accept-Product	The application of released procedures for the setup of the production process for each product and the controlled introduction of changes ensures a production according to clients' specifications. Procedures for setting up the production process as well as changes to the initial setup are done only by authorised personnel. The production process is supported by automated systems.
O.Config-Process	T.Accident-Change, P.Config-Process, P.Accept-Product, P.Organise-Product	Configuration items are stored in the configuration management system according to the site's configuration management plan.
O.Accept-Product	T.Accident-Change, P.Accept-Product	On request of the client release tests are performed for the corresponding products.
O.Organise-Product	P.Organise-Product	The development processes are defined and applied according to the site's quality management system.
O.Staff-Engagement	T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion	All employees working at the site and having access to sensitive information or data have 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.
O.Zero-Balance	P.Zero-Balance	Automated means and/or the application of a 4-eyes-principle ensures a continuous tracking of smart cards and smart card modules during the whole production process.
O.Reception-Control	P.Config-Items, P.Config-Control, P.Reception-Control	Upon reception of an electronic item relevant to security from a different site, authenticity of this item is verified (e.g. verification of a PGP signature when sent via email). Identification is performed if necessary (i.e. requested by the client; the client has to provide information how to identify the item). In case items are shared by a shared configuration management system between different sites or shared network drives, authenticity is implicitly assumed.
O.Internal-Shipment	T.Attack-Transport, P.Product-Transport	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).
O.External-Delivery	T.Attack-Transport, P.Product-Transport	Security relevant physical items are externally delivered either by security transport (e.g. sealed boxes), in person by company's internal staff or collected by the client or the consumer as long as the security functions of the item are not sufficient to protect itself. Security relevant electronic items are externally shipped using secure communication measures. This might be signed and/or encrypted emails or similar (e.g. SSL secured web portals).
O.Transfer-Data	T.Staff-Collusion, T.Attack-Transport, P.Product-Transport	Sensitive electronic configuration 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.
O.Control-Scrap	T.Staff-Collusion, P.Zero-Balance	Scrap is either destroyed under supervision of the site, securely transferred to another site of Giesecke+Devrient capable of secure destruction of scrap or securely shipped to a different site for destruction. By this no employee could get uncontrolled access to scrap which might be helpful to support an attack.

Table 12: Relation between Security Objectives and Threats and OSPs

8.4 SAR Rationale

The Security Assurance Requirements rationale does not explicitly address the developer action elements defined in CC Part 3 [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.

8.4.1 ALC_CMC

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

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 controls such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C (Refined): The CM system shall support the production of the *product* by automated means.

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

ALC_CMC.4.7C (Refined): The CM plan shall describe how the CM system is used for the development of the *product*.

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

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 production of high volumes due to the automated support. The identification of all configuration items allows a parallel production of several products. The requirement for authorized changes support the integrity and confidentiality required for the products. Therefore this assurance level meets the requirements for the configuration management.

8.4.2 ALC_CMS

ALC_CMS.5.1C (Refined): 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 SST*; *development and production tools and related information.*

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

ALC_CMS.5.3C (Refined): *Requires a process ensuring that subcontractors involved in developing configuration items are listed in the configuration list.*

8.4.3 ALC_DVS

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

ALC_DVS.2.2C (Refined): The development security documentation shall justify that the security controls provide the necessary level of protection to maintain the confidentiality and integrity of the *product or at least are followed during the development and maintenance of the product*.

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 production and initialization of the product can be used by potential attackers during the development of attacks. Based on the assumed self-protection of the products the information is needed to apply an attack within considerable time and effort. The keys used during the initialization process also support the security during the shipment or delivery. Therefore the handling is applied to split keys and a special storage of electronic keys is implemented.

8.4.4 ALC_LCD

ALC_LCD.1.1C (Refined): The life-cycle definition documentation shall describe the model used to develop and maintain the *product*.

ALC_LCD.1.2C (Refined): The life-cycle model shall provide for the necessary control over the development and maintenance of the *product*.

The security assurance requirements of the assurance class "Life-cycle definition" listed above are suitable to support the controlled production maintenance and development process. This includes the documentation of these processes and the procedures for the configuration management. The site supports only one phase of the described life-cycle for the category of products. However the assurance requirements are considered to be suitable for this site.

8.4.5 ALC_DEL

ALC_DEL.1.1C (Refined): The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the *product* to the consumer.

The security assurance requirement of the assurance class "Delivery" listed above is suitable to define a controlled environment and controlled processes for shipping procedures. The confidentiality and integrity of the product is addressed by this assurance class.

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 controls 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 controls that are necessary to protect the confidentiality and integrity of the product 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 controls that are necessary to protect the confidentiality and integrity of the product 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 controls that are necessary to protect the confidentiality and integrity of the product 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 controls provide the necessary level of protection to maintain the confidentiality and integrity of the *product or at least are followed during the development and maintenance of the product.* 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 controls that are necessary to protect the confidentiality and integrity of the product 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 controls that are necessary to protect the confidentiality and integrity of the product 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 configuration 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 controls that are necessary to protect the confidentiality and integrity of the product 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 products and ALC_CMC.4.2C requires a methodology description. 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.4.4C and ALC_CMC.4.8C requires that the CM system provides automated controls that only authorised changes are made. A controlled setup is necessary to ensure that the resulting products are compliant with the customers' specifications which supports the maintenance of products according to ALC_CMC.4.9C, ALC_LCD.1.1C and ALC_LCD.1.2C.

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 product. ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items as part of the product. 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, security flaw reports and resolution status, development and production tools and related information. ALC_CMS.5.2C requires that all configuration items are identified uniquely. ALC_CMS.5.3C *requires a process ensuring that subcontractors involved in developing configuration items are listed in the configuration list.*

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

O.Organise-Product

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

Thereby the objective fulfils this combination of Security Assurance Requirements.

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 the objective fulfils this combination of Security Assurance Requirements.

O.Zero-Balance

Ensuring that no unidentified losses of Smart Cards and Smart Card modules can occur, prevents an attacker from getting access to samples of products to investigate potential vulnerabilities. This is necessary to ensure the confidentiality and integrity of products as required by ALC_DVS.2.1C.

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.Internal-Shipment

ALC_DVS.2.1C requires that the development security documentation shall describe all the physical, procedural, personnel, and other security controls that are necessary to protect the confidentiality and integrity of the product 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.External-Delivery

ALC_DEL.1.1C: The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the product to the consumer. Thereby this objective is suitable to meet the Security Assurance Requirement.

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 product 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. ALC_DEL.1.1C requires that the delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the product to the consumer (external delivery). Thereby this objective is suitable to meet the combination of Security Assurance Requirements.

O.Control-Scrap

The controlled destruction of scrap is necessary to ensure the confidentiality of products as required by ALC_DVS.2.1C.

O.Accept-Product

In ALC_LCD.1.1C and in ALC_LCD.1.2C it is requested that the life-cycle documentation and the life-cycle model supports the correct development and maintenance of the product. Thereby the objective is suitable to meet this combination of Security Assurance Requirements.

8.6 Mapping of the Evaluation Documentation

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

9.
9.
9.
9.
9.
9.
9.
9.
9.
9.
9.
9.
9.

9. References

9.1 Literature

[1] Common Criteria, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC:2022, Revision 1, November 2022, CCMB-2022-11-001

[2] Common Criteria, Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CC:2022, Revision 1, November 2022, CCMB-2022-11-003

[3] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CC:2022, Revision 1, November 2022, CCMB-2022-11-004

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

[7] ALC_CMC Configuration Management Documentation for Giesecke+Devrient China Huangshi Branch, Version 1.6, 24 April 2025

[8] ALC_DEL Delivery Documentation for Giesecke+Devrient China Huangshi Branch, Version 1.3, 04 December 2024

[9] ALC_DVS Development Security Documentation for Giesecke+Devrient China Huangshi Branch, Version 1.7, 04 December 2024

[10] ALC_LCD Life-Cycle Definition for Giesecke+Devrient China Huangshi Branch, Version 1.3, 04 December 2024

[11] Services provided by other G+D sites used by Giesecke+Devrient China Huangshi Branch, Version 1.7 / 7 April 2025

[12] Confidential Preconditions GDCN Huangshi, Version 1.3, 04 December 2024

[13] ALC_CIL Configuration Items List for Giesecke+Devrient China Huangshi Branch, Version 1.2 / 24 April 2025

[14] AIS 47 Guidance for Site Certification, Version 1.1, 2013-12-04.

[15] Services_Provided_To_Other_Sites_GDCN_Huangshi Version 1.3/04.12.2024

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.

initialisation Initialisation means loading of a flash image including a secure embedded software onto the secure ICs.

9.3 Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
GDM	Giesecke+Devrient München
IC	Integrated circuit
IT	Information Technology
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation
CM	Configuration Management