



Giesecke+Devrient

Site Security Target Lite for Giesecke+Devrient (Jiangxi) Technology Co., Ltd.

Version 3.4/25.09.2024

Author : Alfons Martin

Rating : G+D PUBLIC

File : ASE_SST_GDCNMS_NAN_lite.docx

© Copyright 2024
Giesecke+Devrient Mobile Security GmbH
Prinzregentenstraße 161
D-81677 München

This document as well as the information or material contained is copyrighted. Any use not explicitly permitted by copyright law requires prior consent of Giesecke+Devrient Mobile Security GmbH. This applies to any reproduction, revision, translation, storage on microfilm as well as its import and processing in electronic systems, in particular.

The information or material contained in this document is property of Giesecke+Devrient Mobile Security GmbH and any recipient of this document shall not disclose or divulge, directly or indirectly, this document or the information or material contained herein without the prior written consent of Giesecke+Devrient Mobile Security GmbH.

All copyrights, trademarks, patents and other rights in connection herewith are expressly reserved to Giesecke+Devrient Mobile Security GmbH and no license is created hereby.

All brand or product names mentioned are trademarks or registered trademarks of their respective holders.

Table of Contents

1.	Document Information	5
1.1	SST reference	5
1.2	Overview	5
1.3	Change History	5
1.4	Document ID.....	6
2.	SST Introduction	7
2.1	Identification of the Site	7
2.2	Site description	8
2.2.1	Wafer initialization and pre-personalisation	9
2.2.2	Embedded devices initialization, pre-personalisation and personalization	9
2.2.3	Supporting Services	9
2.2.4	Life-Cycle Phases	10
3.	Conformance Claim	11
4.	Security Problem Definition.....	12
4.1	Assets.....	12
4.2	Threats	12
4.3	Organisational Security Policies.....	14
4.4	Assumptions	15
5.	Security Objectives	17
5.1	Security Objectives Rationale	20
5.1.1	Mapping of Security Objectives	20
5.1.2	Justification for Threats and OSPs	23
6.	Extended Assurance Components Definition	28
7.	Security Assurance Requirements	29
7.1.1	Overview regarding CM capabilities (ALC_CMC)	29
7.1.2	Overview regarding CM scope (ALC_CMS)	30
7.1.3	Overview regarding Delivery procedure (ALC_DEL)	30
7.1.4	Overview regarding Development Security (ALC_DVS)	30
7.1.5	Overview regarding Life-cycle definition (ALC_LCD).....	30
7.2	Security Assurance Rationale	31
7.2.1	Rationale for ALC_CMC.5.....	31
7.2.2	Rationale for ALC_CMS.5.....	34
7.2.3	Rationale for ALC_DEL.1	35
7.2.4	Rationale for ALC_DVS.2.....	35
7.2.5	Rationale for ALC_LCD.1.....	37
8.	Site Summary Specification	40
8.1	Preconditions required by the site.....	40
8.2	Services of the site	40
8.3	Objectives rationale	41
8.4	SAR Rationale	47
8.4.1	ALC_CMC.....	47
8.4.2	ALC_CMS.....	48
8.4.3	ALC_DEL	49
8.4.4	ALC_DVS	49
8.4.5	ALC_LCD.....	50
8.5	Assurance Measures Rationale	50
8.6	Mapping of the Evaluation Documentation.....	56
8.6.1	Mapping for ALC_CMC.5	56
8.6.2	Mapping for ALC_CMS.5	57
8.6.3	Mapping for ALC_DEL.1	57
8.6.4	Mapping for ALC_DVS.2.....	58
8.6.5	Mapping for ALC_LCD.1	58

8.6.6	Mapping for AST_INT.1	59
8.6.7	Mapping for AST_CCL.1	59
8.6.8	Mapping for AST_SPD.1	60
8.6.9	Mapping for AST_OBJ.1	60
8.6.10	Mapping for AST_ECD.1	61
8.6.11	Mapping for AST_REQ.1	62
8.6.12	Mapping for AST_SSS.1	63
9.	References	64
9.1	Bibliography	64
9.2	Terminology	65
9.3	Abbreviations	65

List of tables

Table 1:	Security problem definition to security objectives mapping	23
Table 2:	Rationale for ALC_CMC.5	34
Table 3:	Rationale for ALC_CMS.5	35
Table 4:	Rationale for ALC_DEL.1	35
Table 5:	Rationale for ALC_DVS.2	37
Table 6:	Rationale for ALC_LCD.1	37
Table 7:	Rationale for Security Objectives	39
Table 8:	Relation between Security Objectives and Threats and OSPs	42
Table 9:	Mapping for ALC_CMC.5	57
Table 10:	Mapping for ALC_CMS.5	57
Table 11:	Mapping for ALC_DEL.1	58
Table 12:	Mapping for ALC_DVS.2	58
Table 13:	Mapping for ALC_LCD.1	59
Table 14:	Mapping for AST_INT.1	59
Table 15:	Mapping for AST_CCL.1	60
Table 16:	Mapping for AST_SPD.1	60
Table 17:	Mapping for AST_OBJ.1	61
Table 18:	Mapping for AST_ECD.1	62
Table 19:	Mapping for AST_REQ.1	63
Table 20:	Mapping for AST_SSS.1	63

1. Document Information

1.1 SST reference

Title of document: Site Security Target Lite for Giesecke+Devrient (Jiangxi) Technology Co., Ltd.

Version/Date: Version 3.4/25.09.2024

Applying Company: Giesecke+Devrient (Jiangxi) Technology Co., Ltd.

Name of the site: Giesecke+Devrient (Jiangxi) Technology Co., Ltd.

Abbreviation of the site: GDCNMS NAN

Product Type: Initialisation and pre-personalisation of dies on wafer and initialisation, pre-personalisation and personalisation of embedded devices.

1.2 Overview

This document is the Site Security Target Lite for Giesecke+Devrient (Jiangxi) Technology Co., Ltd.. It is based on (1) with the modifications necessary to correctly describe the sites named above.

1.3 Change History

Version	Date	Changes	Author	Reviewer	Approver
0.1	29.06.22	Draft version for FOR-002 submission to CCN – still changes will occur	fth	haf	haf
1.0	28.07.22	Initial version for pre-audit	fth	haf	haf
1.1	02.09.22	Review comments from Yauhen incorporated	fth	haf	haf
1.2	12.01.2023	Updates according to OR001-AST	haf	fth	Fth
1.3	31.01.2023	Updates according to OR003-AST	haf	fth	Fth
1.4	22.02.2023	Updates according to OR004-	haf	fth	Fth

		ALC			
2.0	15.06.2023	Rename the site of NAN	haf	fth	fth
2.1	21.08.2023	Update for 2023 recertification Update bibliography (9.1) General formatting in whole document Replace ClearCase by BitBucketDoc in 7.1.1	maa	haf	haf
2.2	20.11.2023	Update locations in 2.2.2	maa	wak	wak
2.3	13.12.2023	Editorial updates, e.g. references and biography. Sm@rtSIM NextGen added.	kwa		
2.4	22.12.2023	Update references to latest version Update GDM site certificate	maa	kwa	kwa
3.0	27.03.2024	Include an additional clean room Add ALC_DEL.1 and phase 5 (personalization) in scope	maa	fes	fes
3.1	04.07.2024	Fix sections 7 and 8 based on lab's feedback. Include embedded devices production in scope. Rework production in scope.	maa	fes	fes
3.2	10.07.2024	Include scrap in sections 2.2 and 8. Clarify section 2.2. Fix minor issues reported.	maa	fes	fes
3.3	19.08.2024	Update references to latest	maa	fes	fes
3.4	25.09.2024	References in Bibliography section 1.9 corrected.	kwa	maa	maa

1.4 Document ID

Document ID	ASE_SST_GDCNMS_NAN_lite
-------------	-------------------------

2. SST Introduction

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

This security target refers to the following site:

Giesecke+Devrient (Jiangxi) Technology Co., Ltd.

The site is used for initialisation and pre-personalisation of dies on wafer and initialisation, pre-personalisation and production of embedded devices.

2.1 Identification of the Site

The Giesecke+Devrient (Jiangxi) Technology Co., Ltd. is located at

399 Huoju Avenue, High-New Tech Development Zone,
Nanchang City, Jiangxi Province, 330096 P.R.China.

The production area of GDCNMS NAN is located in a fenced and guarded site that is leased by Giesecke+Devrient (Jiangxi) Technology Co., Ltd. under a lease agreement and is not shared with other companies. There is a three floors office building and a one floor production building. There are cameras monitoring the whole fences with electronic walls on the physical fences.

The areas belonging to the assets include loading bay, vault, main embedded devices production room, both clean rooms, embedded devices workshop (packaging station included), security control centre, product storage area and server room are located in the production building.

Data gen room is in the second floor of office building. Mantraps control access to data gen room and production areas. Cameras and alarm control system monitor the activities in the production building and Data gen room.

Giesecke+Devrient (Jiangxi) Technology Co., Ltd. provides services for initialisation and pre-personalisation of dies as well as initialisation, pre-personalisation and personalization of embedded devices and is abbreviated by 'GDCNMS NAN'.

When not in initialisation or pre-personalisation, dies on wafer are securely stored in the vault. Same happens for embedded devices, including personalisation. The vault is in the warehouse inside of the high security area at the first 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 GDCNMS NAN.

The supporting IT services are provided by GDM (Giesecke+Devrient München) located at a secure area with restricted access which has been audited.

2.2 Site description

The following services and/or processes provided by Giesecke+Devrient (Jiangxi) Technology Co., Ltd. are in the scope of the site evaluation process:

- Secure reception, storage and transportation of dies on wafer (the term 'wafer' is used throughout the rest of this document describing either single dies or dies on wafer) and embedded devices' modules and devices. Delivery includes transportation for secure destruction.
- Secure reception and storage of initialisation, pre-personalisation data for wafer and initialisation, pre-personalisation and personalisation data for embedded devices production.
- Secure reception and storage of cryptographic keys, derivation of wafer specific pre-personalisation keys and embedded devices pre-personalisation and personalisation keys.
- Wafer initialisation and pre-personalisation.
- Embedded devices production comprising initialisation, pre-personalisation and personalisation.
- Secure destruction of defective/broken embedded devices.

The site evaluation covers only the handling and production of wafer and embedded devices with Sm@rtSIM CX and Sm@rtSIM NextGen.

The term 'handling' in this regard comprises secure reception, storage and shipment of wafers and embedded devices as well as secure reception and storage of data for wafer initialisation and pre-personalisation or for embedded devices initialisation, pre-personalisation and personalisation.

The reception of wafer and embedded modules comprises a verification of the correctness of the shipped items with respect to the transportation documents and - if applicable - the verification of integrity of seals used for secure transportation of items.

The storage of wafer and embedded devices is done in a specially secured vault at GDCNMS NAN with restricted access. The number of items is tracked from reception of the items until the shipment of the items.

2.2.1 Wafer initialization and pre-personalisation

The production site hosts (beside others) a secure storage area for wafer as well as a secure initialization and pre-personalisation area for initialisation and pre-personalisation of wafer. The production 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 is finished the wafer are transported back to the manufacturer of the wafer.

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

2.2.2 Embedded devices initialization, pre-personalisation and personalization

The embedded devices production site follows the same principals described in section 2.2.1, with the particularity that personalisation is also done in the site. During the production process, the sample never leave the production machine until it is personalized.

The client's data for embedded devices production (including personalisation) can be received in different ways according to the technical and security needs of the client.

2.2.3 Supporting Services

The location for Supporting Services is GDM in Munich, a security area with restricted access. A company badge or visitor badge has to be presented for access to this area. Access rights on access cards are granted and revoked by the responsible for physical

site security. At the site for supporting services no Smart Card Software Development is performed. Therefore no configuration management system is necessary for the site GDM. The supporting services comprise Corporate Security Office, IT security and IT services, for details see (2) Services_Used_From_Other_Sites_GDCNMS NAN.

2.2.4 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 (3), chap. 1.2.3.

Giesecke+Devrient (Jiangxi) Technology Co., Ltd. Derives:

- Initialisation from phase 3 by loading a secure operating system to the wafer or embedded device.
- Pre-personalisation from phase 4 (Pre-personalisation) by loading pre-personalisation data to the wafer or embedded device.
- Personalisation from phase 6 (Personalizer) data to the embedded device.

Note: Phase 5 (Composite Product Manufacturer) is implicit, as phase 4 and phase 6 happen at the same time, thus phase 5 is not performed as an intermediate step.

3. Conformance Claim

The evaluation is based on Common Criteria Version 3.1, Revision 5 (4), (5). For the evaluation the methodology in CEM (6) will be used. The SST is CC Part 3 conformant.

This Site Security Target covers the following CC assurance components:

ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2 and ALC_LCD.1.

The assurance components chosen for the Site Security Target are taken from the definition of the EAL6 package defined in (5).

Note that the site does not provide services that are covered by ALC_TAT.3. This component is rejected because development activities as those defined in PP0084 are out of scope of the certification of this site.

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 the products 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. For simplification the term 'get access' covers all three before mentioned security problems. 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:

- sensitive products:
 - unfinished wafer or embedded device
 - finished wafer or embedded device
 - defective or rejected wafer or embedded device
- sensitive production systems or configuration systems
- security relevant production processes
- sensitive configuration data or items
- cryptographic keys to secure initialisation and/or pre-personalisation and/or personalisation

4.2 Threats

All threats endanger the integrity and confidentiality of the products and the representation of parts of the products. The products protect themselves after conclusion of the initialisation phase. However, during the development and production the products and the representation of parts of the products 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. cryptographic keys) might compromise the security of a product.

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 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 GDCNMS NAN may exchange products of different production lots or different clients during production by accident.

T.Unauthorised-Staff: Employees freelancer of GDCNMS NAN or non GDCNMS NAN 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 completion, initialisation or pre-personalisation or personalisation 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 shipment. The target is to compromise confidential information or violate the integrity of the products during the stated shipment process to allow a modification, cloning or the retrieval of confidential information. Confidential information comprises design data, customer or consumer data like code and data (including cryptographic keys) stored in the ROM, Flash or EEPROM or classified product specifications.

4.3 Organisational Security Policies

The following policies are introduced by the requirements of the assurance components of ALC for the assurance level EAL6 (with limitations explained in chapter 3). The chosen policies shall support the understanding of the 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 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 products are either sent back to the client or another wafer or embedded device Production facility (depending on the production-setup).

P.Organise-Product: The configuration, completion, initialisation or pre-personalisation or personalisation process is applied as specified by the client. 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 shipment 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.

4.4 Assumptions

Each site operating in a 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 assumptions are considered to be applicable to all sites.

A.Prod-Specification: The client must provide appropriate information in order to ensure an appropriate production process. This includes the provisioning 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: Deliveries to the recipient (client) or other embedded devices production facilities are possible. Every recipient of the product is identified by the address provided by the client.

A.Shipment: Applicable only for internal deliveries. 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, initialisation, pre-personalisation and personalisation process are specified or provided by the client of the product.

A.Product-Integrity: The self-protecting features of the dies on the wafer or embedded devices received are operational and it is not possible to influence the configuration and behaviour of the devices without access credentials.

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.¹

¹ As mentioned in sec. 2.2.2, GDCNMS NAN uses services from GDM, which are part of the certificate BSI-DSZ-CC-S-0261.

5. Security Objectives

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

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 username 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.Acceptance-Test: The site delivers configuration 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 configuration, completion, initialisation or pre-personalisation or personalisation process it is ensured that the specified process is applied. The 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 sent to the client or another wafer or embedded device manufacturing site.

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.Shipment: Applicable only for internal deliveries. 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, initialization data, response data) can be identified in different ways. The specific way is defined in the shipment procedure. The shipment procedure is applied to all shipped sensitive 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 sensitive configuration data or items during 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 shipment. 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. Wafers which should be destroyed are sent to another site for destruction or to the client for destruction so that they don't support an attacker. The site has measures in place to securely destroy embedded devices.

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 O.Logical-Access O.Logical-Operation O.Staff-Engagement	The technical and organisational measures prevent unauthorised access to the internal network.
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	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy

	O.Transfer-Data O.Control-Scrap	employees prevent unauthorised access to sensitive data or items.
T.Attack-Transport	O.Shipment O.Transfer-Data O.External-Delivery	The applied security measures on sensitive data during shipment prevent modification or disclosure of any sensitive data during transport. The applied security measures on physical items during shipment 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.Acceptance-Test 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.Shipment O.Transfer-Data O.External-Delivery	The controlled shipment procedure ensure correct shipment of items.

Table 1: Security problem definition to security objectives mapping

5.1.2 Justification for Threats and OSPs

T.Smart-Theft

O.Security-Documentation specifies all security measures of the site and is therefore the very basis to counter all attacks to the assets of the site.

The physical countermeasures defined by O.Physical-Access prevent that an attacker can get access to the site.

The security control mechanisms like access control and surveillance cameras and the work of the security staff as defined by O.Security-Control ensure that any attempts of unauthorised access to the site are detected and alarms are triggered. In that case O.Alarm-Response ensures that an attacker undertaking an unauthorised access attempt cannot get access to sensitive areas of the site for manipulation or theft of sensitive data or items.

The internal assessments defined by O.Internal-Monitor and the maintenance measures defined by O.Maintain-Security ensure that the required level of security to prevent unauthorised access attempts is established at all times.

Therefore the combination of O.Security-Documentation, O.Physical-Access, O.Security-Control, O.Alarm-Response, O.Internal-Monitor and O.Maintain-Security are sufficient to cover T.Smart-Theft.

T.Rugged-Theft

See justification for T.Smart-Theft which also applies to T.Rugged-Theft.

T.Computer-Net

O.Security-Documentation specifies all security measures of the site and is therefore the very basis to counter all attacks to the assets of the site.

The logical security measures defined by O.Logical-Access prevent an attacker from unauthorised remote access to sensitive data. The measures defined by O.Logical-Operation ensure that the IT systems are kept up-to-date and by this ensure that the security measures defined by O.Logical-Access continuously provide a sufficient security level. This is supported by O.Internal-Monitor and O.Maintain-Security.

The measures defined by O.Staff-Engagement ensure that staff with access to sensitive items has the required skills not to compromise the security measures established at the site.

Therefore the combination of O.Security-Documentation, O.Logical-Access, O.Logical-Operation, O.Internal-Monitor, O.Maintain-Security and O.Staff-Engagement are sufficient to cover T.Computer-Net.

T.Accident-Change

O.Config-Items and O.Accept-Product together with the defined process of O.Config-Process and O.Config-Control prevents the accidental changes of sensitive items.

Therefore the combination of O.Config-Items, O.Accept-Product, O.Config-Process and O.Config-Control is sufficient to cover T.Attack-Transport.

T.Unauthorised-Staff

O.Security-Documentation specifies all security measures of the site and is therefore the very basis to counter all attacks to the assets of the site.

The physical countermeasures defined by O.Physical-Access ensure that only authorised persons can get access to the site and security related areas therein.

The security control mechanisms like access control and surveillance cameras and the work of the security staff as defined by O.Security-Control ensure that any attempts of unauthorised access to the site are detected and alarms are triggered. In that case O.Alarm-Response ensures that a person undertaking an unauthorised access attempt cannot get access to sensitive areas of the site for manipulation or theft of sensitive data or items.

The logical security measures defined by O.Logical-Access ensure that only authorised users can get access to sensitive data. The measures defined by O.Logical-Operation ensure that the IT systems are kept up-to-date and by this ensure that the security measures defined by O.Logical-Access continuously provide a sufficient security level. The internal assessments defined by O.Internal-Monitor and the maintenance measures defined by O.Maintain-Security ensure that the required level of security to prevent unauthorised access attempts is established at all times.

The measures defined by O.Staff-Engagement ensure that staff with access to sensitive items has the required skills not to compromise the security measures established at the site.

Therefore the combination of O.Security-Documentation, O.Physical-Access, O.Security-Control, O.Alarm-Response, O.Internal-Monitor, O.Maintain-Security, O.Logical-Access, O.Logical-Operation and O.Staff-Engagement are sufficient to cover T.Unauthorised-Staff.

T.Staff-Collusion

O.Security-Documentation specifies all security measures of the site and is therefore the very basis to counter all attacks to the assets of the site.

The measures defined by O.Staff-Engagement ensure that staff with access to sensitive items has the required skills not to compromise the security measures established at the site and to understand the risk of supporting an external attacker.

It is ensured that the security level of the site is maintained at all times by the security measures defined in O.Internal-Monitor and O.Maintain-Security including background checks during hiring of personnel and defined exit procedures for dismissed employees (e.g. deactivation of accounts).

O.Transfer-Data ensures the security of sensitive data during transfer.

The security measures defined by O.Control-Scrap ensure that an attacker cannot get access to sensitive data when they are no longer required at the site.

Therefore the combination of O.Security-Documentation, O.Internal-Monitor, O.Maintain-Security, O.Staff-Engagement, O.Transfer-Data and O.Control-Scrap are sufficient to cover T.Staff-Collusion.

T.Attack-Transport

The security measures defined by O.Shipment and O.External-Delivery ensures that an attacker cannot get access to sensitive physical or electronic data or items during shipment. For electronic items this is supported by the security measures defined by O.Transfer-Data.

Therefore the combination of O.Shipment, O.External-Delivery and O.Transfer-Data is sufficient to cover T.Attack-Transport.

P.Config-Items

The Security Objective O.Config-Items directly enforces P.Config-Items. The measures defined by O.Reception-Control support this policy by assuring the correct usage of items.

P.Config-Control

The Security Objective O.Config-Control enforces P.Config-Control. The Security Objective O.Logical-Access prevents unauthorised changes of the CM system and the configuration items stored therein. O.Config-Items support the enforcement of P.Config-Control by ensuring that each configuration item is uniquely identified in the CM system. The measures defined by O.Reception-Control support O.Config-Items by assuring the correct usage of items.

P.Config-Process

The Security Objective O.Config-Process directly enforces P.Config-Process.

P.Reception-Control

The Security Objective O.Reception-Control directly enforces P.Reception-Control.

P.Accept-Product

The Security Objectives O.Accept-Product and O.Acceptance-Test enforce P.Accept-Product. This is supported by O.Config-Process, which ensures that a configuration management plan is in place, and by O.Config-Control, which ensures the application of the required procedures for the product release.

P.Organise-Product

The Security Objective O.Organise-Product enforces P.Organise-Product. This is supported by O.Config-Process, which ensures that a configuration management plan is in place, and by O.Config-Control, which ensures the application of the required

procedures for the product release. The security objectives O.Logical-Access and O.Logical-Operation provide the necessary security measures to protect sensitive items.

P.Product-Transport

P.Product-Transport is directly enforced by O.Shipment for shipments, O.External-Delivery for external shipments and O.Transfer-Data for transfer of sensitive electronic configuration items. This enforcement is supported by O.Config-Items which ensures the correct labelling of the product.

P.Zero-Balance

P.Zero-Balance is directly enforced by O.Zero-Balance and for the defective items it is enforced by O.Control-Scrap

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 EAL6.

The assurance requirements for the Life-Cycle support are:

ALC_CMC.5 (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 (7) because hierarchically higher components are used in this Site Security Target compared to the Minimum Requirements in (7).

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

ALC_CMC.5: ALC_CMS.1, ALC_DVS.2, 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 doesn't cover product specific information of the life-cycle definition.

7.1.1 Overview regarding CM capabilities (ALC_CMC)

Wafer or embedded devices that can be completed, initialised and personalised at GDCNMS NAN are defined in the CM tool 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). This document together with all ALC_XXX documents are managed with BitBucketDoc.

7.1.2 Overview regarding CM scope (ALC_CMS)

The configuration list (8) 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 wafers, embedded modules, embedded devices and related data and documentation to the Production site as well as all deliveries of embedded device related products, related data and documentation from the Production site to the consumer, client (i.e. the Device manufacturer) or other Embedded Production facilities.

7.1.4 Overview regarding Development Security (ALC_DVS)

The site must ensure that the handling and storage of wafer or embedded device related 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, initialisation data, pre-personalisation and personalisation data must be guaranteed, access to any kind of wafer or embedded device related 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.

In addition, shipment within and between Production site has to be covered by ALC_DVS.

7.1.5 Overview regarding Life-cycle definition (ALC_LCD)

Applicable life-cycles are as defined in chapter 2.2.4. GDCNMS NAN 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 (5) 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 (6) according to the application notes in the process description (6) are written in *italic*. The term TOE can be replaced by configuration items or product.

7.2.1 Rationale for ALC_CMC.5

Security Assurance Requirement	Security Objective	Rationale
ALC_CMC.5.1C: <i>The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.</i>	O.Reception-Control O.Config-Items	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 labelled before shipment. After integration into the CM system O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the item.
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Config-Items O.Config-Control	O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the item. All configuration items are kept under configuration control according to O.Config-Control.
ALC_CMC.5.3C: The CM	O.Config-Control	O.Config-Control ensures that all

documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	O.Acceptance-Test	changes to configuration items are done according to the procedures setup for the product with reviews of the changes and O.Acceptance-Test ensures that all changes are compliant to the specification.
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.Config-Items	O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the item.
ALC_CMC.5.5C: 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 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.5.6C: The CM system shall support the production of the <i>product</i> by automated means.	O.Config-Process O.Config-Control O.Acceptance-Test	The ERP system supports automated production of products. O.Config-Process and O.Config-Control support the automated production of the product. The relation between a specific product and the specific set of configuration items is established within the acceptance procedure for the product according to O.Config-Control which is supported by O.Acceptance-Test.
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a	O.Config-Control	O.Config-Control ensures that a designated team is responsible to integrate the changes into the CM system.

configuration item into CM is not the person who developed it.		
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the <i>product</i> .	O.Config-Items	O.Config-Items ensures that every configuration item that comprises the product is uniquely identified.
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the <i>product</i> by automated means, including the originator, date, and time in the audit trail.	O.Config-Process	O.Config-Process ensures that audit trail exist for all changes to the TOE
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O.Config-Process	O.Config-Process ensures by automated means that interdependencies between different configuration items are identified.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the <i>product</i> is generated.	O.Config-Process	O.Config-Process ensures by use of appropriate tools the identification of the version of the implementation representation from which the product is generated
ALC_CMC.5.12C: 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.5.13C: The CM plan shall describe how the CM system is	O.Config-Process	CM process documentation is available and maintained according to O.Config-Process.

used for the development of the <i>product</i> .		
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the <i>product</i> .	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.5.15C: 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.5.16C: 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.5

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: <i>clear instructions how to consider these items in the list</i> ; the evaluation evidence required by the SARs of <i>the life-cycle</i> ; security flaw reports and resolution status; <i>development and production</i>	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.

<i>tools and related information.</i>		
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: <i>Requires a process ensuring that subcontractors involved in developing configuration items are listed in the configuration list.</i>	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 3: Rationale for ALC_CMS.5

7.2.3 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 <i>product</i> to the client.	O.External-Delivery O.Transfer-Data	All external deliveries are according to O.External-Delivery and O.Transfer-Data.

Table 4: Rationale for ALC_DEL.1

7.2.4 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	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	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

confidentiality and integrity of the <i>product</i> design and implementation in its development environment.	O.Shipment O.Transfer-Data O.Control-Scrap	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 shipment is ensured by O.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 measures provide the necessary level of protection to maintain the confidentiality and integrity of the <i>product or at least are followed during the development and maintenance of the product. The evidence shall justify that the security measures provide</i>	O.Security-Documentation O.Internal-Monitor O.Shipment O.Transfer-Data	The security measures of the site are in agreement with the security documentation and their evidences of O.Security-Documentation. Sufficiency of the security measures and the evidences is verified according to O.Internal-Monitor. Security during shipment is ensured by O.Shipment and O.Transfer-Data.

<i>the necessary level of protection to maintain the confidentiality and integrity of the product.</i>		
--	--	--

Table 5: Rationale for ALC_DVS.2

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 model used to develop and maintain the <i>product</i> .	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 <i>product</i> .	O.Config-Control O.Config-Process O.Accept-Product O.Organise-Product	see ALC_LCD.1.1C

Table 6: Rationale for ALC_LCD.1

The guidance on Site Certification (7), 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.5.5C, ALC_DVS.2.1C
O.Logical-Operation	ALC_DVS.2.1C
O.Config-Items	ALC_CMC.5.1C, ALC_CMC.5.2C, ALC_CMC.5.4C, ALC_CMC.5.8C, ALC_CMC.5.15C, ALC_CMS.5.1C, ALC_CMS.5.2C
O.Config-Control	ALC_CMC.5.2C, ALC_CMC.5.3C, ALC_CMC.5.5C, ALC_CMC.5.6C, ALC_CMC.5.7C, ALC_CMC.5.14C, ALC_CMC.5.15C, ALC_LCD.1.1C, ALC_LCD.1.2C
O.Config-Process	ALC_CMC.5.6C, ALC_CMC.5.9C, ALC_CMC.5.10C, ALC_CMC.5.11C, ALC_CMC.5.12C, ALC_CMC.5.13C, ALC_CMC.5.14C, ALC_CMC.5.16C, 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.Acceptance-Test	ALC_CMC.5.3C, ALC_CMC.5.6C
O.Staff-Engagement	ALC_DVS.2.1C
O.Zero-Balance	ALC_DVS.2.1C
O.Reception-Control	ALC_CMC.5.1C

O.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 7: 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 information for the secure production of ordered products. The client is responsible for the release of the products (e.g. by buying released products). The client provides a method of unique identification for all items shipped to the site. The client provides appropriate information for the shipment of produced goods as well as electronic data to be delivered. This information shall at least comprise address data for physical items.

The self-protection features of the wafer and embedded device to be initialised and pre-personalized 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 the confidential document 'Confidential_Preconditions_GDCNMS NAN.doc'.

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.²

8.2 Services of the site

This site provides the service of secure reception, storage and transportation of wafers and embedded devices and related goods as well as secure reception and storage of data for wafer initialisation and pre-personalisation and embedded devices initialisation, pre-personalisation and personalisation. On top, secure destruction or shipment of defective products is performed on site.

² As mentioned in sec. 2.2.2, GDCNMS NAN uses services from GDM, which is part of the certificate BSI-DSZ-CC-S-0261.

The reception of wafers and embedded device comprises a verification of the correctness of the delivered items with respect to the shipment documents and - if applicable - the verification of integrity of seals used for secure transportation of items.

The storage of wafers and embedded devices is done in a specially secured environment on GDCNMS NAN premises with restricted access. The number of items is tracked from reception of the items until the shipment of the items.

The site securely receives and stores initialization and pre-personalisation data for wafer initialisation and pre-personalisation, as well as initialisation, pre-personalisation and personalisation data for embedded devices initialisation, pre-personalisation and personalisation.

Cryptographic keys are securely received and stored, wafer specific pre-personalisation and embedded device specific pre-personalisation and personalisation keys are securely derived and stored.

In addition, this sites provides the service of wafer initialisation and pre-personalisation, as well as embedded devices initialisation, pre-personalisation and personalisation for the Sm@rt SIM CX and Sm@rtSIM NextGen operating systems.

Secure destruction of embedded devices modules (either several single modules from reel or modules formally part of an embedded device) with a shredder and additional grinding or the plastic card body of an embedded device (without module) with a shredder. In case of wafers, they are stored and sent back to the manufacturer for secure destruction at their site.

8.3 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
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	T.Accident-Change, P.Config-Items, P.Config-Control, P.Product-Transport
O.Config-Control	T.Accident-Change, P.Organise-Product, P.Config-Control, P.Accept-Product
O.Config-Process	T.Accident-Change, P.Config-Process, P.Accept-Product, P.Organise-Product
O.Accept-Product	T.Accident-Change, P.Accept-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.Zero-Balance	P.Zero-Balance
O.Reception-Control	P.Config-Items, P.Config-Control, P.Reception-Control
O.Shipment	T.Attack-Transport, P.Product-Transport
O.External-Delivery	T.Attack-Transport, P.Product-Transport
O.Transfer-Data	T.Staff-Collusion, T.Attack-Transport, P.Product-Transport
O.Control-Scrap	T.Staff-Collusion, P.Zero-Balance

Table 8: 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.Unauthorised-Staff and T.Staff-Collusion.

O.Physical-Access

The production site is operated by GDCNMS NAN only and is not shared with other companies. The site is separated into different security levels. Only authorised users are allowed within the production 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 granting access rights, etc. Visitors are escorted by the company's security staff or internal 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. Security staff will start to investigate any alarm immediately.

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.

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 GDCNMS NAN's internal network.

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 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. Hard disks 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. By this different products can be identified. By this the threat T.Accident-Change is countered and the OSPs P.Config-Items, P.Config-Control and P.Product-Transport are addressed.

O.Config-Control

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. By this the OSPs P.Organise-Product, P.Accept-Product and P.Config-Control are addressed. In addition, the threat T.Accident-Change is covered.

O.Config-Process

Configuration items are stored in the configuration management system according to the site's configuration management plan. By this the threat T.Accident-Change and the OSPs P.Config-Process, P.Accept-Product and P.Organise-Product are addressed.

O.Accept-Product

On request of the client release tests are performed for the corresponding products. By this the threat T.Accident-Change is countered and the OSP P.Accept-Product is addressed.

O.Acceptance-Test

On request of the client tests are performed, that proves the delivered configuration items fulfil the specified properties. By this the threat T.Accident-Change is countered and the OSP P.Accept-Product is addressed.

O.Organise-Product

The development processes 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 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. These measures prevent T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

O.Zero-Balance

Automated means and/or the application of a 4-eyes-principle ensures a continuous tracking of wafer or embedded devices during the whole production process. By this the OSP P.Zero-Balance is addressed.

O.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. By this the OSPs P.Config-Items, P.Config-Control and P.Reception-Control are addressed.

O.Shipment

Applicable only for internal deliveries. Security relevant physical items are shipped either by security transport (e.g. sealed boxes) or in person by company's internal staff or collected by the client as long as the security functions of the item are not sufficient to protect itself. Security relevant electronic items are shipped using secure communication measures. This might be signed and/or encrypted emails or similar (e.g. SSL secured webportals) or shared network systems (e.g. shared configuration management system). This prevents T.Attack-Transport and covers also P.Product-Transport.

O.External-Delivery

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 webportals). This prevents T.Attack-Transport and covers also P.Product-Transport.

O.Transfer-Data

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. This prevents T.Staff-Collusion, T.Attack-Transport and covers also P.Product-Transport.

O.Control-Scrap

Wafers scrap is securely transferred to another site capable of secure destruction of scrap or securely shipped to a different site or the client for destruction. Embedded devices scrap is destroyed under the supervision of the site. By this no employee could get uncontrolled access to scrap which might be helpful to support an attack. This prevents T.Staff-Collusion and covers P.Zero-Balance.

8.4 SAR Rationale

The Security Assurance Requirements rationale does not explicitly address the developer action elements defined in (5) 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.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling* (refined for Site Certification).

ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.5.3C: The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.

ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.

ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.5.6C: The CM system shall support the production of the *product* by automated means.

ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.

ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the product.

ALC_CMC.5.9C: The CM system shall support the audit of all changes to the *product* by automated means, including the originator, date, and time in the audit trail.

ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.

ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the *product* is generated.

ALC_CMC.5.12C: The CM documentation shall include a CM plan.

ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the *product*.

ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *product*.

ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.5.16C: 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: 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*.

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

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

8.4.3 ALC_DEL

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.

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.

8.4.4 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 *product* 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 *product* or *at least are followed during the development and maintenance of the product*. *The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity 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, initialization, pre-personalisation and personalisation 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, pre-personalisation and personalisation process also

support the security during the shipment. Therefore the handling is applied to split keys and a special storage of electronic keys is implemented.

8.4.5 ALC_LCD

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

ALC_LCD.1.2C: 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.

8.5 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. *The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.*

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 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 measures that are necessary to protect the confidentiality and integrity of

the product design and implementation including the initialization, pre-personalisation and personalisation 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 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 measures 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. *The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.*

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 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 measures that are necessary to protect the confidentiality and integrity of the product design and implementation including the initialization, pre-personalisation and personalisation in its development and production environment. ALC_CMC.5.5C 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 measures 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.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. In addition, ALC_CMC.5.2C requires that the CM documentation describe the method to uniquely identifies the configuration items, ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items and ALC_CMC.5.8C requires that all the product comprising configuration items are identified. ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the CM system. The configuration list (8) 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.5.2C requires the CM documentation to describe the method used to uniquely identify the configuration items. ALC_CMC5.5C requires that the CM system shall provide automated measures such that only authorised changes are made to configuration items and ALC_CMC.5.3C requires adequate reviews of these changes. ALC_CMC.5.6C requires that the CM system shall support the production of the TOE by automated means. ALC_CMC.5.7C requires that the person responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the product. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_LCD.1.1C requires that the life-cycle definition documentation describe 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.Config-Process

The provision of automated measures is required by ALC_CMC.5.6C. ALC_CMC.5.12C requires that the CM documentation includes a CM plan. ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development of the product.

ALC_CMC.5.9C requires that the CM system shall support the audit of all changes to the *product* by automated means. ALC_CMC.5.10C requires that the CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.11C requires that the CM system shall be able to identify the version of the implementation representation from which the *product* is generated. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the product. ALC_CMC.5.16C requires that the evidence demonstrates that the CM system is being operated in accordance with the CM plan.

The configuration list (8) 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 of the product. The objective meets the set of Security Assurance Requirements.

O.Organise-Product

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 of 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 measures 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 wafer or embedded devices 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.5.1C 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.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 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.

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 shipments. It also requires that the shipment documentation shall describe all procedures that are necessary to maintain security when distributing versions of the product to the client. 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.

O.Acceptance-Test

ALC_CMC.5.3C requests that the CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.

ALC_CMC.5.6C requests that the CM system shall support the production of the *product* by automated means.

8.6 Mapping of the Evaluation Documentation

8.6.1 Mapping for ALC_CMC.5

Security Assurance Requirement	Aspects	References
ALC_CMC.5.1C: <i>The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.</i>	all	(9) chap. 2.1
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	all	(9) chap. 2.1
ALC_CMC.5.3C The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	all	(9) chap. 3.2
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	all	(9) chap. 2.1
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	all	(9) chap. 2.1
ALC_CMC.5.6C: The CM system shall support the production of the <i>product</i> by automated means.	all	(9) chap. 2.1.4
ALC_CMC.5.7C The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	all	(9) chap. 3
ALC_CMC.5.8C The CM system shall identify the configuration items that comprise the <i>product</i> .	all	(9) chap. 2.1
ALC_CMC.5.9C The CM system shall support the audit of all changes to the <i>product</i> by automated means, including the originator, date, and time in the audit trail.	all	(9) chap. 2.1.4
ALC_CMC.5.10C The CM system shall provide an automated means to	all	(9) chap. 2.1

identify all other configuration items that are affected by the change of a given configuration item.		
ALC_CMC.5.11C The CM system shall be able to identify the version of the implementation representation from which the <i>product</i> is generated.	all	(9) chap. 2.1
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	all	(9) chap. 3
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the <i>product</i> .	all	(9) chap. 3
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the <i>product</i> .	all	(9) chap. 3
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	all	(9)
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	all	(9)

Table 9: Mapping for ALC_CMC.5

8.6.2 Mapping for ALC_CMS.5

Security Assurance Requirement	Aspects	References
ALC_CMS.5.1C: The configuration list shall include the following: <i>clear instructions how to consider these items in the list</i> ; the evaluation evidence required by the SARs of <i>the life-cycle</i> ; security flaw reports and resolution status, <i>development and production tools and related information</i> .	all	(8)
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	all	(8)
ALC_CMS.5.3C: <i>Requires a process ensuring that subcontractors involved in developing configuration items are listed in the configuration list.</i>	all	(8)

Table 10: Mapping for ALC_CMS.5

8.6.3 Mapping for ALC_DEL.1

Security Assurance Requirement	Aspects	References
ALC_DEL.1.1C: The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the <i>product</i> to the consumer.	all	(10), chap. 2

Table 11: Mapping for ALC_DEL.1

8.6.4 Mapping for ALC_DVS.2

Security Assurance Requirement	Aspects	References
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 <i>product</i> design and implementation in its development environment.	Physical Security	(11) chap. 4.1
ALC_DVS.2.1C	Personnel Security	(11) chap. 4.2
ALC_DVS.2.1C	Logical Security, IT-Security	(11) chap. 4.3
ALC_DVS.2.1C	Security of Production Process	(11) chap. 3
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 <i>product</i> or at least are followed during the development and maintenance of the product. The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.	all	(11) chap. 5

Table 12: Mapping for ALC_DVS.2

8.6.5 Mapping for ALC_LCD.1

Security Assurance Requirement	Aspects	References
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the <i>product</i> .		(12) whole document
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the <i>product</i> .		(12) whole document

Table 13: Mapping for ALC_LCD.1

8.6.6 Mapping for AST_INT.1

Security Assurance Requirement	Aspects	References
AST_INT.1.1C: The SST introduction shall contain an SST reference, a Site reference and a Site description.	SST introduction	This document, chapter 1 and 2
AST_INT.1.2C: The SST reference shall uniquely identify the SST.	SST introduction	This document, chapter 1
AST_INT.1.3C The Site reference shall identify the Site.	SST introduction	This document, chapter 2
AST_INT.1.4C The Site description shall describe the physical scope of the Site.	SST introduction	This document, chapter 2
AST_INT.1.5C The Site description shall describe the logical scope of the Site.	SST introduction	This document, chapter 2

Table 14: Mapping for AST_INT.1

8.6.7 Mapping for AST_CCL.1

Security Assurance Requirement	Aspects	References
AST_CCL.1.1C: The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the SST and the Site claim conformance.	Conformance claims	This document, chapter 3

AST_CCL.1.2C: The CC conformance claim shall describe the conformance of the SST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.	Conformance claims	This document, chapter 3
AST_CCL.1.3C: The CC conformance claim shall be consistent with the extended components definition.	Conformance claims	This document, chapter 3
AST_CCL.1.4C: The CC conformance claim shall identify the SARs.	Conformance claims	This document, chapter 3

Table 15: Mapping for AST_CCL.1

8.6.8 Mapping for AST_SPD.1

Security Assurance Requirement	Aspects	References
AST_SPD.1.1C: The security problem definition shall describe the threats.	Security problem definition	This document, chapter 4
AST_SPD.1.2C: All threats shall be described in terms of a threat agent, an asset, and an adverse action.	Security problem definition	This document, chapter 4
AST_SPD.1.3C: The security problem definition shall describe the OSPs.	Security problem definition	This document, chapter 4

Table 16: Mapping for AST_SPD.1

8.6.9 Mapping for AST_OBJ.1

Security Assurance Requirement	Aspects	References
AST_OBJ.1.1C: The statement of security objectives shall describe the security objectives for the development environment.	Security objectives	This document, chapter 5
AST_OBJ.1.2C: The security objectives rationale shall trace each security objective	Security objectives	This document,

for the development environment back to threats countered by that security objective and OSPs enforced by that security objective.		chapter 5
AST_OBJ.1.3C: The security objectives rationale shall demonstrate that the security objectives counter all threats.	Security objectives	This document, chapter 5
AST_OBJ.1.4C: The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.	Security objectives	This document, chapter 5

Table 17: Mapping for AST_OBJ.1

8.6.10 Mapping for AST_ECD.1

Security Assurance Requirement	Aspects	References
AST_ECD.1.1C: The statement of security requirements shall identify all extended security requirements.	Extended Components Definition	This document, chapter 6
AST_ECD.1.2C: The extended components definition shall define an extended component for each extended security requirement.	Extended Components Definition	This document, chapter 6
AST_ECD.1.3C: The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.	Extended Components Definition	This document, chapter 6
AST_ECD.1.4C: The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.	Extended Components Definition	This document, chapter 6
AST_ECD.1.5C: The extended	Extended Components	This document,

components shall consist of measurable and objective elements such that compliance or noncompliance to these elements can be demonstrated.	Definition	chapter 6
--	------------	-----------

Table 18: Mapping for AST_ECD.1

8.6.11 Mapping for AST_REQ.1

Security Assurance Requirement	Aspects	References
AST_REQ.1.1C: The statement of security requirements shall describe the SARs.	Security requirements	This document, chapter 7
AST_REQ.1.2C: The statement of security requirements shall identify all operations on the security requirements.	Security requirements	This document, chapter 7
AST_REQ.1.3C: The statement of security requirements shall identify all operations on the security requirements.	Security requirements	This document, chapter 7
AST_REQ.1.4C: All operations shall be performed correctly.	Security requirements	This document, chapter 7
AST_REQ.1.5C: Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.	Security requirements	This document, chapter 7
AST_REQ.1.6C: The statement of security requirements shall contain only SARs drawn from components in the ALC class.	Security requirements	This document, chapter 7
AST_REQ.1.7C: The statement of security requirements shall contain ALC_DVS.1, ALC_CMC.3 and ALC_CMS.1 or hierarchically higher	Security requirements	This document, chapter 7

SARs.		
AST_REQ.1.8C: The security requirements rationale shall trace each SAR back to the security objectives for the development environment.	Security requirements	This document, chapter 7
AST_REQ.1.9C: The security requirements rationale shall demonstrate that the SARs meet all security objectives for the development environment.	Security requirements	This document, chapter 7

Table 19: Mapping for AST_REQ.1

8.6.12 Mapping for AST_SSS.1

Security Assurance Requirement	Aspects	References
AST_SSS.1.1C: The Site summary specification shall identify all evidence for the SARs.	Site summary specification	This document, chapter 8
AST_SSS.1.2C: The Site summary specification shall describe aspects of how the Site meets the SARs.	Site summary specification	This document, chapter 8
AST_SSS.1.3C: The Site summary specification shall trace the aspects to the evidence.	Site summary specification	This document, chapter 8

Table 20: Mapping for AST_SSS.1

9. References

9.1 Bibliography

1. **Eurosmart.** *Site Security Target Template, Version 1.0.* 21.06.2009.
2. **G+D.** *Services provided by other G+D sites used by Giesecke+Devrient (Jiangxi) Technology Co., Ltd., Version 1.5.* 08.07.2024.
3. **Eurosmart.** *Security IC Platform Protection Profile with Augmentation Packages Version 1.0, BSI-CC-PP-0084-2014.* 19.02.2014.
4. **Common Criteria.** *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; v3.1 Revision 5, CCMB-2017-04-001.* April 2017.
5. —. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; v3.1, Revision 5, CCMB-2017-04-003.* April 2017.
6. —. *Common Methodology for Information Technology Security Evaluation: Evaluation methodology; Version 3.1, Revision 5, CCMB-2017-04-004.* April 2017.
7. —. *Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001.* October 2007.
8. **G+D.** *Configuration list v1.6.* 27.09.2024.
9. —. *Configuration Management Documentation for Giesecke+Devrient (Jiangxi) Technology Co. Ltd., Version 1.8.* 25.09.2024.
10. —. *Delivery Documentation for Giesecke+Devrient (Jiangxi) Technology Co., Ltd., Version 1.0.* 17.06.2024.
11. —. *Development Security Documentation for Giesecke+Devrient (Jiangxi) Technology Co. Ltd., Version 1.8.* 25.09.2024.
12. —. *Life-Cycle Definition for Giesecke+Devrient (Jiangxi) Technology Co. Ltd., Version 1.8.* 25.09.2024.

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.

9.3 Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
GDM	Giesecke+Devrient München
G+D	Giesecke+Devrient
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