

REVISION HISTORY

Date	Revision	Requestor	ECN #	Description Of Change
2025.9.5	0	Psyche.Jiang	NA	Initial version
2025.11.14	1	Psyche.Jiang	NA	Modify layout



Site Security Target Lite for
JCET Group JCAP and JSCC
site

Rev_1



Table of Contents

1	Document Information	5
1.1	Reference	5
2	SSTL Introduction	6
2.1	Identification of the Site	6
2.2	Site Description	6
2.2.1	Physical Scope	6
2.2.2	Logical Scope	6
3	Conformance Claim.....	9
4	Security Problem Definition	10
4.1	Assets	10
4.2	Threats	10
4.3	Organizational Security Policies.....	11
4.4	Assumptions.....	12
5	Security Objectives.....	14
5.1	Security Objectives	14
5.2	Security Objectives Rationale.....	16
6	Extended Assurance Components Definition.....	21
7	Security Assurance Requirements.....	22
7.1	Application Notes and Refinements.....	22
7.1.1	Overview and Refinements regarding CM Capabilities (ALC_CMC).....	22
7.1.2	Overview and Refinements regarding CM Scope (ALC_CMS)	23
7.1.3	Overview and Refinements regarding Delivery Procedure (ALC_DEL)	23
7.1.4	Overview and Refinements regarding Development Security (ALC_DVS).....	23
7.1.5	Overview and Refinements regarding Life-Cycle Definition (ALC_LCD)	24
7.1.6	Overview and Refinements regarding Tools and Techniques (ALC_TAT).....	24
7.2	Security Assurance Requirements Rationale	24
7.2.1	ALC_CMC.5	24
7.2.2	ALC_CMS.5	25
7.2.3	ALC_DVS.2	26
7.2.4	ALC_LCD.1	26



7.2.5	ALC_DEL.1.....	26
7.2.6	ALC_TAT.3.....	26
7.3	Security Assurance Rationale.....	27
8	Site Summary Specification.....	32
8.1	Preconditions Required by the Site.....	32
8.2	Services of the Site.....	33
8.3	Security Assurance Requirement Aspects.....	34
9	References.....	42
9.1	Literature.....	42
9.2	Definitions.....	42
9.3	List of Abbreviations.....	43



1 Document Information

1.1 Reference

Title: Site Security Target Lite for *JCET Group JCAP and JSCC site*

Version: 1

Date: 2025.11.14

Company: *JCET Group Co. Ltd.*

Name of the site: *JCET Group JCAP and JSCC site*

Site type: *IC manufacturing and packaging*

EAL-Level: *Site supports product evaluations up to EAL6*



2 SSTL Introduction

The Site Security Target Lite refers to JCET Group JCAP and JSCC site that describes the security features and defines the scope of the site.

This chapter is divided into the sections “Identification of the Site” and “Site Description”.

2.1 Identification of the Site

The site [JCET Group JCAP and JSCC site] is located at:

[No. 78, ChangShan Road, JiangYin City, JiangSu Province, P.R. China]

2.2 Site Description

The JCET Group JCAP and JSCC site is located at No. 78, ChangShan Road, JiangYin City, JiangSu Province, P.R. China. The site is a part of the JCET (JCET Group Co., Ltd) Jiangyin East Site Industrial Park. The JCET Jiangyin East Site Industrial Park consists of various buildings occupied by different companies. The site is a manufacturer with Security IC packaging, testing and pre-personalisation if necessary. The site provides services for both security and non-security products, including pre-assembly (Bumping and Backside Metallization), assembly (advanced Packaging, flip chip and wire bonding), testing (wafer probing and IC testing), scrap management and reliability & failure analysis.

2.2.1 Physical Scope

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

- 1st, 2nd, 3rd floors of B2 Building
- 1st and 2nd floors of B2B Building
- 1st, 2nd, 3rd floors of AB Building
- 1st, 2nd, 3rd, 4th floors of DEFM Building

The site is inside the JCET Industrial Park, which is protected by surveillance and secured by security guards of JCET Industrial Park, restrictions and access controlled from main and back gates.

The site comprises the production facilities, warehousing and material dispatch, customer service, equipment maintenance, engineering, as well as the IT office for the site.

The site provides services including pre-assembly, assembly, and electrical testing for both security and non-security products.

The security products are produced in Security Area. The Security Area is access controlled.

2.2.2 Logical Scope

The following high-level description of the services and/or processes provided by JCET Group JCAP and JSCC are in the scope of the site evaluation process.



Table 2.1 – Site logical scope of JCAP

Building	Services	Floor	Description
B2 Building	Pre-assembly	1 st Floor	Production Line: Wafer bumping Wafer Receiving Product Shipping CCTV & Security Center FA&RA Lab
B2 Building	Pre-assembly	2 nd Floor	Production Line: Wafer bumping
		3 rd floor	Wafer Bank Wafer Packaging Warehouse IT Datacenter
	Wafer Testing	2 nd Floor	Production Line: Wafer Probe
B2B Building	Assembly	1 st Floor	Production Line: Segment wafer to dice Finish Goods Storage Product Shipping CCTV & Security Center
	Wafer Testing	2 nd Floor	Production Line: Wafer Probe

Table 2.2 – Site logical scope of JSCC

Building	Services	Floor	Description
AB Building	Final Testing	1 st Floor	Production Line: Final Testing
		2 nd Floor	Production Line: Final Testing
	Assembly & Wafer Testing	3 rd floor	Production Line: Flip Chip FOL Production Line: Wafer Probe
DEFM Building	Final Testing	1 st Floor	Production Line: Final Testing Wafer/IC Receiving Test Bank Warehouse Finish Goods Storage FA&RA Lab Product Shipping CCTV & Security Center
	Assembly	2 nd Floor	Production Line: Wire Bonding Wafer Bank
	Assembly	3 rd Floor	Production Line: Flip Chip EOL Production Line: Wire Bonding Wafer Bank
	Office	4 th Floor	IT Datacenter

The complete logical flow of the Security IC at the site is covered by the SST. In addition, the management of the Security IC related processes and the site security are covered by the SST. The product flow of the Security IC on the site starts with the reception of wafers, dice, or packaged ICs up to the packing and handover for shipment of the processed product. Scrap is



returned to the client or destroyed as requested by the client.

The following life-cycle phases of the Security IC for Smart Card applications are subject of the SST (according to the protection profile [7]):

- Life cycle phase 3: IC Manufacturing
 - Security IC testing
 - Initialisation, and
 - Pre-personalisation if necessary

- Life cycle phase 4: IC Packaging
 - Security IC packaging (and testing)
 - Pre-personalisation if necessary



3 Conformance Claim

This SST is conformant to Common Criteria:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CC:2022, Revision 1, November 2022 ([1])
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CC:2022, Revision 1, November 2022 ([2])
- Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements; CC:2022, Revision 1, November 2022 ([3])
- Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, July 2024 ([9])

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation (CEM), Evaluation methodology; CEM:2022, Revision 1, November 2022 ([4])

Furthermore, the following guidance was considered:

- Supporting Document Guidance, Site Certification, CCDB-2007-11-001, Version 1.0, Revision 1, October 2007 ([5])
- Guidance for Site Certification, Bundesamt für Sicherheit in der Informationstechnik, Version 1.1, 2013-12-04 ([6])
- Site Security Target Template, Eurosmart, Version 2.0, 15.04.2021 ([8])

This SST is conformant to Common Criteria Part 3 and Part 5.

The chosen assurance components are those from the assurance class "Life-cycle Support" (ALC) according to the assurance level EAL6:

- ALC_CMC.5,
- ALC_CMS.5,
- ALC_DEL.1,
- ALC_DVS.2,
- ALC_TAT.3,
- ALC_LCD.1.

For the assessment of the security measures attackers with high attack potential are assumed. This allows for an evaluation of products according to AVA_VAN.5.

The assurance components chosen for the Site Security Target are compliant to the Protection Profiles [7] and therefore suitable for Security ICs.

Therefore, the scope of the evaluation is suitable to support product evaluations up to EAL6.



4 Security Problem Definition

The Security Problem Definition includes 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 TOE and the security management of the site. Goal is to achieve and hold a high security level to counter attacks with high attack potential at the site.

4.1 Assets

The following assets are handled at the site:

- wafers, dice & critical wafer
- test programs & data for wafer testing of the wafer
- documentation related to the wafer testing of the security products
- assembled products (packaged ICs & assembly ICs)
- product specifications necessary for assembly (e.g. information about pad location)
- test programs and data for final testing of assembled products
- documentation related to the final testing of the security products
- scrap & critical scrap, i.e. rejected wafers, dice, and IC packages
- FA&RA data for wafers, dice and packaged ICs

The site has internal documentation system and data that is relevant to maintain the confidentiality and integrity of an intended product. This comprises site security concepts and the associated security measures. These items are not explicitly listed in the list of assets above.

The integrity of any machine or tool used for production and testing is not considered as an asset. However, appropriate measures are defined for the site to ensure such integrity. These items consist of commercially available hardware and software which are programmed and customized by the site.

There can be further client specific assets like seals, special transport protection or similar items that support the security of the internal shipment to the client. They are handled in the same way as the other assets to prevent misuse, disclosure or loss of these sensitive items or information.

4.2 Threats

All threats endanger the integrity and confidentiality of the intended TOE and the representation of parts of the TOE. The intended TOE protects itself in life-cycle phase 7. However, during the development, production, test and assembly the TOE and the representation of parts of the TOE are vulnerable to such attacks.

The following threats are considered:

Table 4.1 – Threats addressed by the site

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



Threat	Description
T.Rugged-Theft	An experienced thief with specialized equipment for burglary, who may be paid to perform the attack tries to access sensitive areas and manipulate or steal sensitive assets.
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 production systems with the intention to modify the testing or production process thus violating integrity and possibly confidentiality.
T.Accident-Change	An employee, contractor or student trainee may exchange products of different production lots / different clients during production or changes tool configuration that have an impact on the intended TOE by accident.
T.Unauthorised-Staff	Unauthorised employees or subcontractors get access to assets or systems used for configuration management or production, so that the confidentiality and/or the integrity of the intended TOE is violated. This can apply to any production step and any asset related to the intended TOE or its configuration.
T.Staff-Collusion	An attacker tries to get access to assets handled at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.
T.Attack-Transport	An attacker might try to get data, specifications or products during the transport. The target is to compromise confidential information or violate the integrity of the products during the stated transport process to allow a modification, cloning or the retrieval of confidential information at later life cycle states. Confidential information comprises design information, test documentation and test data as far as classified as sensitive.

4.3 Organizational Security Policies

The following policies are introduced by the requirements of the assurance components of ALC for the assurance level EAL6. The chosen policies support the understanding of the production flow, and the security measures of the site. In addition, they allow an appropriate mapping to the Security Assurance Requirements (SAR).

The evaluation of the documentation of the site is under configuration management. That includes all procedures regarding the evaluated testing and assembly flows and the security measures that are in the scope of the evaluation.

Table 4.2 – OSP addressed by the site

Policy	Description
P.Config-Items	The configuration management system shall be able to uniquely identify all configuration items. This includes the unique identification of items that are created, generated, developed or used at a site as well as the received and transferred and/or provided 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 is only applied by authorised personnel. Automated systems support the configuration management and ensure access control or interactive acceptance measures for set up



Policy	Description
	and changes. The procedure for the initial set-up of a production process ensures that sufficient information is provided by the client.
P.Config-Process	The services and/or processes provided by the site are controlled in the configuration management plan. This comprises incoming items, tools used for the testing and production of the product, the management of flaws and optimizations of the process flow as well as the documentation that describes the services and/or processes provided by the site. A released production process is defined and under version control.
P.Reception-Control	The inspection of incoming items done at the site ensures that the received assets comply with the properties stated by the client. Furthermore, it is verified that the intended TOE can be identified, and a released production process is defined for the intended TOE. If applicable this aspect includes the check that all required information and data is available to handle the incoming items.
P.Accept-Product	The testing and quality control of the site ensures that the released intended TOE comply with the specification agreed with the client. The acceptance process is supported by automated measures. Records are generated for the acceptance process of the assets. Thereby, it is ensured that the properties of the intended TOE are ensured when internally shipped and externally delivered.
P.Zero-Balance	The site ensures that all sensitive items (security relevant parts of the intended TOEs of different clients) are separated and traced on a device basis. For each handover, either an automated or an organizational “two-employees-acknowledgement” (four-eyes principle) is applied for functional and defect assets. As per the released production process the defect assets are either destroyed at the site or sent back to the client.
P.Organise-Product	The pre-personalisation or initialization process is applied as specified by the client. If the data includes sensitive items like keys relevant for the life-cycle or configuration data that affect the security of the intended TOE, appropriate measures are in place. This includes the requirement that the knowledge of sensitive keys is split to at least two different persons. Furthermore, technical measures like crypto-boxes, separation of network, split access permission and secure storage is implemented for this kind of data.
P.Product-Transport	Technical and organisational measures ensure the correct labelling of the intended TOE. A controlled internal shipment and the external delivery is applied. The transport supports traceability up to the recipient. If applicable or required, this policy includes measures for packing to protect the product during transport.
P.Data-Transfer	High security level or sensitive data are encrypted and classified by the client to ensure its confidentiality; electronic form data e.g. test programs, product release information, test summary etc. and in addition a signature and/or password will be required to protect the data.

4.4 Assumptions

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



Table 4.3 – Assumption addressed by the site

Policy	Description
A.Prod-Specification	The client must provide appropriate information (e.g. specifications, definitions, process limits, process parameters, test requirements, test limits, bond plans) to ensure an appropriate development or production process. The provided information includes the classification of the documents and product.
A.Item-Identification	Each configuration item received by the site is appropriately labelled to ensure the identification of the configuration item.
A.External-Delivery	The recipient (consumer) of the product is identified by the address provided by the client. The address of the consumer is part of the product setup.
A.Internal-Shipment	The recipient (client) of the product is identified by the address of the client site. The address of the client is part of the product setup.
A.Init-Data	The scripts for the configuration and initialization process are provided by the client of the product. The client verifies the configuration and/or initialization process during the product introduction and the release process of the site.
A.Product-Integrity	The self-protecting features of the devices are fully operational, and it is not possible to influence the configuration and behaviour of the devices based on insufficient operational conditions or any command sequence generated by an attacker or by accident.
A.Destruct-Scrap	Scrap assets are also transferred, and they are destroyed at the receiving site so that they are useless for an attacker.



5 Security Objectives

5.1 Security Objectives

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

Table 5.1 – Security Objective addressed by the site

Objective	Description
O.Physical-Access	The combination of physical partitioning between the different access control levels together with technical and organizational security measures allows enough 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 unauthorized people. The site enforces two or three levels of access control to sensitive areas of the site. The access control measures ensure that only registered employees and vendors can access restricted areas. Sensitive products and data are handled in restricted areas only. Network cabling is protected according to classification of the transferred data by avoiding routes through public areas or by usage of appropriate cryptographic measures.
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 organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any sensitive configuration item (asset). After the alarm is triggered the unauthorized person still must 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 at least every six months. 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 every year to control the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure enough 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 authorized 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 implements a firewall system to enforce a logical separation between the internal network and the internet. The firewall system ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into



Objective	Description
	production networks, office and administration network. Production networks and configuration and/or administration are further logically separated from other internal network to enforce access control. Access to the production network and related systems is restricted to authorised employees involved in the configuration tasks of the production systems. Every user of an IT system has its own user account and password. An authentication using a unique user account and password is enforced by all computer systems.
O.Logical-Operation	All network segments and the computer systems are kept up-to-date (software updates, security patches, virus protection, spyware protection). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.
O.Config-Items	The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify configuration items and allow an assignment to the client. Also, the internal procedures and guidance are covered by the configuration management.
O.Config-Control	The site applies a release 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. Minor changes are handled by the site, major changes must be acknowledged by the client. A designated team is responsible for the release of new products and for the classification and release of changes. This team comprises specialists for all aspects of the services and/or processes. The services and/or processes can be changed by authorised personnel only. Automated systems support configuration management and production control.
O.Config-Process	The site controls its services and/or processes using a configuration management plan. The configuration management is controlled by tools and procedures for the development and production of the product, for the management of flaws and optimizations of the process flow as well as for the documentation that describes the services and/or processes provided by a site.
O.Acceptance-Test	The site delivers assets that fulfil the specified properties. Parameter checks, 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.
O.Organise-Product	For the pre-personalization, or initialization process it is ensured that the specified process is applied. The data integrity is controlled. Keys and other sensitive data can only be constructed by at least two employees. The operation is applied in crypto-boxes or similar devices. After the release process changes are only applied based on the request of the client. The update is done according to a controlled process.
O.Staff-Engagement	All employees who have access to sensitive assets and who can move parts of the product out of the defined production flow are checked regarding security concerns and have to sign a nondisclosure agreement. Furthermore, all employees are trained and qualified for their job.



Objective	Description
O.Zero-Balance	The site ensures that all sensitive products (intended TOE of different clients) are separated and traced on a device basis. Automated control and/or two employees acknowledgement during hand over is applied for functional and defective devices. According to the agreed production flow the defect devices are either destroyed at the site or sent to the client.
O.Reception-Control	Upon reception of any product an immediate incoming inspection is performed. The inspection comprises the received amount, their identification and the assignment of the items to a related internal process.
O.Internal-Shipment	The recipient of a physical configuration item is identified by the assigned client address. The internal shipment procedure is applied to the configuration item. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of assets during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined.
O.External-Delivery	The recipient of a physical configuration item is identified by the assigned consumer address. The external delivery procedure is applied to the sensitive configuration item. A delivery address is assigned to each product and subject of a controlled process. The packaging is also part of the defined process and applied as specified by the client. The forwarder supports the tracing of sensitive assets during external delivery. For every configuration item, the protection measures against manipulation are defined.
O.Transfer-Data	Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorized employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected.
O.Control-Scrap	The site has measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive assets so that they do not support an attacker.

5.2 Security Objectives Rationale

The SST includes a Security Objectives Rationale with two parts. The first part includes a tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part include a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives.

Note that the assumptions of the SST cannot be used to cover any threat or OSP of the site. They are pre-conditions fulfilled either by the site providing the sensitive assets or by the site receiving the sensitive assets. Therefore, they do not contribute to the security of the site under evaluation.



Table 5.2 – Mapping of Security Objectives

Security Objectives \ Threats/OSPs	O.Physical-Access	O.Security-Control	O.Alarm-Response	O.Internal-Monitor	O.Maintain-Security	O.Logical-Access	O.Logical-Operation	O.Config-Items	O.Config-Control	O.Config-Process	O.Acceptance-Test	O.Organise-Product	O.Staff-Engagement	O.Zero-Balance	O.Reception-Control	O.Internal-Shipment	O.External-Delivery	O.Transfer-Data	O.Control-Scrap
T.Smart-Theft	X	X	X	X	X														
T.Rugged-Theft	X	X	X	X	X														
T.Computer-Net				X	X	X	X						X						
T.Accident-Change						X	X	X	X	X	X		X	X					X
T.Unauthorised-Staff	X	X	X	X	X	X	X		X				X	X					X
T.Staff- Collusion				X	X								X	X					X
T.Attack-Transport																X	X	X	
P.Config-Items								X							X				
P.Config-Control						X		X	X										
P.Config-Process										X									
P.Reception-Control															X				
P.Accept-Product								X	X	X	X								
P.Zero-Balance													X	X					X
P.Organise-Product						X	X	X	X	X		X							
P.Product-Transport																X	X		
P.Data-Transfer																		X	



The following rationales provides a justification that shows that all threats and OSP are effectively addressed by the Security Objectives.

Table 5.3 – Justification of Security Objectives

Threat or OSP	Security Objective	Justification
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	O.Physical-Access and O.Security-Control protects the physical access of the site. O.Alarm-Response ensures in time detection of unauthorized access attempt. O.Internal-Monitor and O.Maintain-Security ensures procedural and technical measures operate correctly.
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	O.Physical-Access and O.Security-Control protects the physical access of the site. O.Alarm-Response ensures in time detection of unauthorized access attempt. O.Internal-Monitor and O.Maintain-Security ensures procedural and technical measures operate correctly.
T.Computer-Net	O.Maintain-Security O.Logical-Access O.Logical-Operation O.Internal-Monitor O.Staff-Engagement	O.Logical-Access and O.Logical-Operation protect internal network form remote attacks. O.Internal-Monitor and O.Maintain-Security ensures procedural and technical measures operate correctly. O.Staff-Engagement ensures well security awareness of the staff who can access sensitive data.
T.Accident-Change	O.Logical-Access O.Logical-Operation O.Config-Control O.Config-Items O.Config-Process O.Acceptance-Test O.Staff-Engagement O.Zero-Balance O.Control-Scrap	O.Logical-Access and O.Logical-Operation protect products from remote changes. O.Config-Control, O.Config-Items and O.Config-Process ensure appropriate configuration management and production control. O.Acceptance-Test ensures only compliant assets are delivered. O.Staff-Engagement ensures well security awareness of staff. O.Zero-Balance ensures segregation of sensitive products. O.Control-Scrap protects scraps are not disclosed.



Threat or OSP	Security Objective	Justification
T.Unauthorized-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Config-Control O.Zero-Balance O.Control-Scrap	O.Physical-Access and O.Security-Control protects the physical access of the site. O.Alarm-Response ensures in time detection of unauthorized access attempt. O.Internal-Monitor and O.Maintain-Security ensures procedural and technical measures operate correctly. O.Logical-Access and O.Logical-Operation protect assets form remote attacks. O.Staff-Engagement ensures well security awareness of staff. O.Zero-Balance ensures segregation of sensitive products. O.Control-Scrap protects scraps are not disclosed. O.Config-Control ensures changes of services are controlled.
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Zero-Balance O.Control-Scrap	O.Staff-Engagement ensures well security awareness of staff. O.Zero-Balance ensures segregation of sensitive products. O.Control-Scrap protects scraps are not disclosed. O.Internal-Monitor and O.Maintain-Security ensures procedural and technical measures operate correctly.
T.Attack-Transport	O.Internal-Shipment O.External-Delivery O.Transfer-Data	O.Internal-Shipment and O.External-Delivery ensure the correct and secure delivery of physical configuration items. O.Transfer-Data ensure the correct and secure delivery of electronic data.
P.Config-Items	O.Reception-Control O.Config-Items	O.Reception-Control ensures the secure reception of configuration items. O.Config-Items enforces the identification of configuration items.
P.Config-Control	O.Config-Items O.Config-Control O.Logical-Access	O.Config-Items enforces the identification of configuration items. O.Config-Control enforces the control of configuration items.



Threat or OSP	Security Objective	Justification
		O.Logical-Access ensures only authorized access to configuration items.
P.Config-Process	O.Config-Process	O.Config-Process directly enforces P.Config-Process as it is described.
P.Reception-Control	O.Reception-Control	O.Reception-Control directly enforces P.Reception-Control as it is described.
P.Accept-Product	O.Config-Control O.Config-Process O.Config-Items O.Acceptance-Test	O.Config-Items, O.Config-Control and O.Config-Process ensure the correct configuration management of assets of intended TOE. O.Acceptance-Test ensures and enforces the specification compliance testing of assets.
P.Zero-Balance	O.Staff-Engagement O.Zero-Balance O.Control-Scrap	O.Staff-Engagement ensures well security awareness of staff. O.Zero-Balance ensures segregation of sensitive products. O.Control-Scrap protects scraps are not disclosed.
P.Organise-Product	O.Config-Items O.Config-Process O.Config-Control O.Logical-Access O.Logical-Operation O.Organise-Product	O.Config-Items, O.Config-Control and O.Config-Process ensure the correct configuration management of assets of intended TOE. O.Logical-Access and O.Logical-Operation enforce technical measures on sensitive data. O.Organise-Product ensures specified process is applied and data integrity is controlled.
P.Product-Transport	O.Internal-Shipment O.External-Delivery O.Transfer-Data	O.Internal-Shipment and O.External-Delivery ensure the correct and secure delivery of physical product. O.Transfer-Data ensure the correct and secure delivery of electronic data.
P.Data-Transfer	O.Transfer-Data	O.Transfer-Data directly enforces P.Data-Transfer as it is described.



6 Extended Assurance Components Definition

No extended components are currently defined in this SST.



7 Security Assurance Requirements

Clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Protection Profile [7].

The Security Assurance Requirements (SAR) are:

Class ALC:

- CM capabilities (ALC_CMC.5)
- CM scope (ALC_CMS.5)
- Delivery (ALC_DEL.1)
- Development security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)
- Tools and techniques (ALC_TAT.3)

The Security Assurance Requirements listed above fulfil the requirements of [5] because hierarchically higher components are used in this SST. In addition, the minimum set of SARs is extended by SAR of the assurance components for “Delivery” (ALC_DEL), “Life-cycle definition” (ALC_LCD.1) and “Tools and techniques” (ALC_TAT.3).

7.1 Application Notes and Refinements

The description of the site certification process [5] includes specific application notes. The main item is that a product that is considered as “intended TOE” is not available during the evaluation. Since the term “TOE” is not applicable in the SST the associated processes for the handling of products or “intended TOEs” are in the focus and described in this SST. These processes are subject of the evaluation of the site.

7.1.1 Overview and Refinements regarding CM Capabilities (ALC_CMC)

A production control system is employed to guarantee the traceability and completeness of different production charges or lots. The number of wafers, dies and packaged products (e.g. modules/inlays) is tracked by this system. Appropriate administration procedures are implemented for managing wafers, dies and packaged products, which are being removed from the production-process to verify and to control predefined quality standards and production parameters. It is ensured, that wafers, dies or assembled devices removed from the production stage (i) are returned to the production stage from where they were removed or (ii) are securely stored and destroyed.

According to [5] the processes rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below.

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

The life-cycle described in [7] is a complex production process. Only parts of this production process are normally provided at this site. In such a case the control of the product during such a production process must include enough verification steps to ensure the specified and expected result. Test procedures, verification procedures and the associated expected results must be under configuration management for these cases.

The assets for the considered product type are listed in section 4.1. The CM documentation of the site is able to maintain the items listed for the relevant life-cycle step and the CM system is able to track the configuration items.



A CM system is employed to guarantee the traceability and completeness of different production charges or lots. Appropriate administration procedures must be provided to maintain the integrity and confidentiality of the configuration items.

7.1.2 Overview and Refinements regarding CM Scope (ALC_CMS)

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

In addition, process control data, test data and related procedures and programs are in the scope of the configuration management.

7.1.3 Overview and Refinements regarding Delivery Procedure (ALC_DEL)

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

In the case of a Security IC more "material and information" than the TOE itself (which includes the necessary guidance) is exchanged with clients or consumers. Since the TOE can be externally delivered after different life-cycle phases (phases 4 or 5) the SST must consider the data that is exchanged by the sites either as part of the product or separate as input for further production steps.

As already outlined in the application notes of the PP [7] the external delivery of the TOE may require additional transfers between the product manufacturer and the client or consumer. These do not address the internal deliveries between sites involved in the life-cycle of the intended TOE. Since the assurance component ALC_DEL is only applicable to the external delivery to the consumer, the component cannot be used for internal shipment. Internal shipment is covered by ALC_DVS.

7.1.4 Overview and Refinements regarding Development Security (ALC_DVS)

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

The TOE Manufacturer must ensure that the development and production of the TOE is secure so that no information is unintentionally made available for the operational phase of the TOE. The confidentiality and integrity of design information, test data, configuration data and pre-personalization data must be guaranteed, access to any kind of samples (customer specific samples or open samples) development tools and other material must be restricted to authorized persons only, scrap must be shipped back to client or destroyed.

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.

If the transfer of assets between two sites involved in the production flow is included in the scope of the evaluation (life-cycle covered by the product evaluation) this is considered as internal



shipment. In general, the security requirements for confidentiality and integrity are the same but it must clearly distinguish to ensure the correct subject of the evaluation.

7.1.5 Overview and Refinements regarding Life-Cycle Definition (ALC_LCD)

The site is not equal to the entire development environment. Therefore, the ALC_LCD criteria are interpreted in a way that only those life-cycle phases must be evaluated which are in the scope of the site. The PP [7] provides a life-cycle description the specific life-cycles steps can be assigned to the tasks at site. This may comprise a change of the life-cycle state if e.g. testing or initialization is performed at the site or not.

The PP [7] does not include any refinements for ALC_LCD. The site under evaluation does not initiate a life cycle change of the intended TOE. The products are assembled, and the functional devices are delivered to the client. The defective devices are scrapped or also returned to the client.

7.1.6 Overview and Refinements regarding Tools and Techniques (ALC_TAT)

The CC assurance components of family ALC_TAT refer to the tools that are used to develop, analyses and implement the TOE. The component ALC_TAT.3, "Well-defined development tools", requires evidence for the suitability of the tools and techniques used for the development process of the TOE.

Since no TOE development and production in the sense of the Common Criteria is performed on the site, there are no development and production tools to be described. Especially, no compilation of products is performed. Therefore, there is no risk of mis-configurations due to not well-defined tools or ambiguous statements or comments that have to be addressed. However, the component is included here to support the reuse of the evaluation results and to enable the justification of the evaluator regarding ALC_TAT.3.

7.2 Security Assurance Requirements Rationale

This rationale addresses all content elements and thereby also implicitly all the developer action elements defined in [2]. Therefore the following Security Assurance Requirements rationale provides the justification for the selected Security Assurance Requirements. In general, the selected Security Assurance Requirements fulfil the needs derived from the Protection Profiles [7]. Because they are compliant with the Evaluation Assurance Level EAL6 all derived dependencies are fulfilled.

The Security Assurance Requirements (SARs) are:

Class ALC: Life-cycle support

- CM capabilities (ALC_CMC.5)
- CM scope (ALC_CMS.5)
- Delivery (ALC_DEL.1)
- Development security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)
- Tools and techniques (ALC_TAT.3)

7.2.1 ALC_CMC.5

The content and presentation elements for ALC_CMC.5:

ALC_CMC.5.1C The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.



- 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 controls such that only authorized 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 clearly identify the configuration items that comprise the TSF.
- 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 chosen assurance level ALC_CMC.5 of the assurance family "CM capabilities" is suitable to support the production of high volumes due to the formalized acceptance process and the automated support. The identification of all configuration items supports an automated and industrialized production process. The requirement for authorized changes supports the integrity and confidentiality required for the products. Therefore, these security assurance requirements meet the requirements for the configuration management.

7.2.2 ALC_CMS.5

The content and presentation elements for ALC_CMS.5:

- ALC_CMS.5.1C** The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.
- ALC_CMS.5.2C** The configuration list shall uniquely identify the configuration items.
- ALC_CMS.5.3C** For each TSF relevant configuration item, the configuration list shall indicate the developer/subcontractor of the item.

The chosen assurance level ALC_CMS.5 of the assurance family "CM scope" supports the control of the production and test environment. This includes product related documentation and data as well as the documentation for the configuration management and the site security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE these security assurance requirements are considered to be suitable.



7.2.3 ALC_DVS.2

The content and presentation elements for ALC_DVS.2:

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

ALC_DVS.2.2C The development security documentation shall justify that the security controls provide the necessary level of protection to maintain the confidentiality and integrity of the product.

The chosen assurance level ALC_DVS.2 of the assurance family "Development Security" is required since a high attack potential is assumed for potential attackers. The configuration items and information handled at the site during production, assembly and testing of the product can be used by potential attackers for the development of attacks. Therefore, the handling and storage of these items must be sufficiently protected. Further on the Protection Profile [7] requires this protection for sites involved in the life-cycle of Security ICs development and production.

7.2.4 ALC_LCD.1

The content and presentation elements for ALC_LCD.1:

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

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

The chosen assurance level ALC_LCD.1 of the assurance family "Life-cycle definition" is suitable to support the controlled development and production process. This includes the documentation of these processes and the procedures for the configuration management. Because the site provides only a limited support of the described life-cycle for the production of Security ICs the focus is limited to this site. However, the assurance requirements are considered to be suitable to support the application of the site evaluation results for the evaluation of an intended TOE.

7.2.5 ALC_DEL.1

The content and presentation elements for ALC_DEL.1:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

The security assurance requirement of the assurance class "Delivery" listed above is suitable to define a controlled process for delivery product to the consumer. The confidentiality and integrity of the product during transport is addressed by this assurance class. Since the Protection Profile [7] requires the same assurance level, it is considered to be sufficient.

7.2.6 ALC_TAT.3

The content and presentation elements for ALC_TAT.3:

ALC_TAT.3.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.3.2C The documentation of each development tool shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.3.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

The assurance family "Tools and techniques" is not applicable because the tools used for the production process do not influence the behavior of the product. Therefore, they are not considered under ALC_TAT.



7.3 Security Assurance Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components of [2] to the Security Objectives defined in this SST. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of the products. If the site already receives assets, this process assumes that the received assets are appropriately labelled and identified, refer to **A.Item-Identification**.

The SAR Rationale does not explicitly address the developer action elements defined in [2] because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the preparation for the site visit. This includes the requirement that the procedures are applied as written and explained in the documentation.

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 TOE design and implementation in its development environment.

ALC_DVS.2.2C requires that 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. Thereby this Security Assurance Requirement contributes to meet the objective.

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 TOE design and implementation in its development and production environment.

ALC_DVS.2.2C requires that 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. Thereby this Security Assurance Requirement contributes to meet the objective.

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 TOE design and implementation in its development and production environment.

ALC_DVS.2.2C requires that 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. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Internal-Monitor

ALC_DVS.2.2C requires that 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. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Maintain-Security

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 TOE design, implementation and in its development and production environment.

ALC_DVS.2.2C requires that 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. Thereby this Security Assurance Requirement contributes to meet the objective.



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 TOE design, implementation and in its development and production environment.

ALC_DVS.2.2C requires that 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. Thereby this SAR is suitable to meet security objective.

ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. Thereby this Security Assurance Requirement contributes to meet the objective.

ALC_CMC.5.7C requires the CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it. Thereby this SAR is suitable to meet the security objective.

ALC_CMC.5.11C requires the CM system shall be able to identify the version of the implementation representation from which the TOE is generated. Thereby this SAR is suitable to meet the security objective.

O.Logical-Operation

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 TOE design, implementation and in its development and production environment.

ALC_DVS.2.2C requires that 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. Thereby this Security Assurance Requirement contributes to meet the objective.

ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Config-Items

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labeling of the products. A method used to uniquely identify the configuration items is required by ALC_CMC.5.2C.

ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items. In addition, ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items.

ALC_CMC.5.8C requires the CM system shall identify the configuration items that comprise the TSF.

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

ALC_CMC.5.14C requires that the CM plan describes the procedures used to accept modified or newly created configuration items as part of the TOE. The configuration list required by

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

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.

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

O.Config-Control

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.

ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items.

ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system.



ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items.

ALC_CMC.5.8C requires the CM system shall identify the configuration items that comprise the TSF.

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

ALC_CMC.5.10C requires 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 the CM system shall be able to identify the version of the implementation representation from which the TOE is generated.

ALC_CMC.5.12C requires a CM documentation that 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 TOE.

ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.5.15C requests evidence demonstrating that all configuration items are being maintained under the CM system.

ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. In addition,

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

O.Config-Process

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. The provision of automated measures such that only authorized changes is made to the configuration items as required by ALC_CMC.5.5C.

ALC_CMC.5.6C requires that the CM system supports the production by automated means.

ALC_CMC.5.8C requires the CM system shall identify the configuration items that comprise the TSF.

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

ALC_CMC.5.10C requires 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 the CM system shall be able to identify the version of the implementation representation from which the TOE is generated.

ALC_CMC.5.12C requires that the CM documentation includes a CM plan.

ALC_CMC.5.13C requires that the CM plan describe how the CM system is used for the development of the TOE.

ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.5.15C requests evidence showing that all configuration items are being maintained under the CM system.

ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.

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

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

O.Acceptance-Test

The testing of the products is considered as automated procedure as required by ALC_CMC.5.6C.

ALC_CMC.5.9C requires the CM system shall support the audit of all changes to the TOE by



automated means, including the originator, date, and time in the audit trail.

ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. In addition, ALC_LCD.1.2C requires control over the development and maintenance of the TOE. Thereby this Security Assurance Requirement contributes to meet the objective.

ALC_DVS.2.2C requires that 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. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Organise-Product

ALC_CMC.5.13C requires the CM plan to describe how the CM system is used to manufacture the product.

ALC_LCD.1.1C and ALC_LCD.1.2C require the life-cycle model to develop and maintain the TOE. Thereby this Security Assurance Requirement contributes to meet the objective.

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 TOE design and implementation in its development environment.

ALC_DVS.2.2C requires that 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. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Zero-Balance

ALC_CMC.5.6C requires that the CM system supports the production of the TOE by automated means.

ALC_CMC.5.15C requires evidence demonstrating that all configuration items are being maintained under the CM system. Thereby this Security Assurance Requirement contributes to meet the objective.

ALC_DVS.2.2C requires that 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. Thereby this Security Assurance Requirement contributes to meet the objective.

ALC_LCD.1.2C requires control over the development and maintenance of the TOE. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Reception-Control

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.

ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items.

ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system.

ALC_CMC.5.7C requires 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.5.11C requires the CM system shall be able to identify the version of the implementation representation from which the TOE 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 TOE.

ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. Thereby this Security Assurance Requirement contributes to meet the objective.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. The configuration items shall be uniquely identified and listed with its developer in the configuration list according to



ALC_CMS.5.2C and ALC_CMS.5.3C.

ALC_DVS.2.2C requires that 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.

O.Internal-Shipment

ALC_DVS.2.2C requires that 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. This includes also the protection during the transport between production sites. Thereby this Security Assurance Requirement contributes to meet the objective.

ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system.

ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. Thereby this Security Assurance Requirement contributes to meet the objective.

ALC_CMS.5.2C requires the unique identification of the packing as configuration item. The configuration items shall be uniquely identified and listed with its developer in the configuration list according to ALC_CMS.5.2C and ALC_CMS.5.3C.

ALC_DVS.2.1C requires that physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the TOE during internal shipment.

O.External-Delivery

ALC_CMC.5.15C requires the configuration items to be maintained under CM system.

The configuration items shall be uniquely identified and listed with its developer in the configuration list according to ALC_CMS.5.2C and ALC_CMS.5.3C.

ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan.

ALC_DEL.1.1C requires the delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Transfer-Data

ALC_DVS.2.2C requires that 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. This includes also the protection during the transport between production sites. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Control-Scrap

ALC_DVS.2.1C requires that physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the TOE design and implementation.

ALC_DVS.2.2C requires that 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. Thereby this Security Assurance Requirement contributes to meet the objective.



8 Site Summary Specification

8.1 Preconditions Required by the Site

This section provides background information on the assumptions defined in section 4.4. These assumptions can be seen as guidance for the client regarding the information and deliverables which are needed to allow the production under conditions described in this Site Security Target.

The following deliverables are required to provide the services as described above according to the evaluated processes:

- wafers, dice & critical wafer
- test programs & data for wafer testing of the wafer
- documentation related to the wafer testing of the security products
- assembled products (packaged ICs & assembly ICs)
- product specifications necessary for assembly (e.g. information about pad location)
- test programs and data for final testing of assembled products
- documentation related to the final testing of the security products
- scrap & critical scrap, i.e. rejected wafers, dice, and IC packages
- FA&RA data for wafers, dice and packaged ICs

For the setup of the production process, the relevant specifications and product information is required by the site. In general, the release process can only be finished, if the required information is provided by the client and the samples are approved by the client. Based on the provided specifications also the tests are configured. The test environment allows functional tests to verify the operation after completion of the assembly. The production at the site is released after the client accepted the initial sample lot produced by the site. Therefore, each client is in charge for the verification of his products based on the sample lot provided by the site.

The site has procedures in place to protect and maintain classified products and properties of their clients. The protection is based on the classification agreed with the client or printed on the received item or document. This comprises data that is maintained as configuration item related to a product. For all classified items appropriate destruction procedures are in place. The scrap (i.e. rejected, defect or obsolete security products) is transferred back to the client or destroyed as requested by the client.

Table 8.1 – Precondition of assumptions

Assumption	Precondition
A.Prod-Specification	The client must provide appropriate information (e.g. specifications, definitions, process limits, process parameters, test requirements, test limits, bond plans) to ensure an appropriate wafer testing, pre-personalization, initialization or assembly process. The provided information must indicate the classification of the documents, testing programs and assets.
A.Item-Identification	Before sending item to this site, the previous site must label it uniquely.
A.External-Delivery	The client must provide the address and delivery requirements of the consumer of the product if they request this site to deliver finished



Assumption	Precondition
	product to the consumer.
A.Internal-Shipment	The client must provide the address and shipping requirements so that this site can send finished products back to them.
A.Init-Data	The scripts for the configuration and initialization process are provided by the client of the product. The client must verify the configuration and initialization process together with testing programs during the product introduction and the release process of the site. Only if the client confirms the correct verification, the product is released at this site.
A.Product-Integrity	The self-protection features of the wafers and dices are fully operational, or the client must ensure the integrity of the products by other measure during production.
A.Destruct-Scrap	If scrap is delivered back to the client depending on client's request, the client is responsible for secure destruction.

8.2 Services of the Site

Each product set up gets a unique client part ID (client parts). This part ID is linked with the security device that is assembled in the product.

The processes for pre-assembly, assembly, wafer testing and acceptance are set up according to the specifications provided by the client (e.g. IC specification, test specification for electrical testing and packing requirements if applicable). For the release a sample lot is produced at the site.

The complete product specific flow includes final test of each product as part of the acceptance process. The final tests are provided by the client or the test program provided by the client is integrated in the test environment. Test programs provided by the client must be dedicated for the test tools used at the site.

The site has a standard procedure for packing of finished products and preparation of shipment. If special packing requirements are provided by the client, they are included in the process setup. The client is notified if products are ready for transport because the transport must be organized by the client.

Defect devices on the wafer can be marked by inking or by electronic wafer map files. Broken wafers and ICs are collected completely and stored in secure cabinets. All scraps (i.e. the rejects and defect devices on the wafer) are either returned to the client or destroyed under control of the site.

Table 8.2 – Services provided by the site

Service	Details
S.Pre-Assembly	<ul style="list-style-type: none"> ● Bumping (Solder bump, Gold bump, Pillar bump, CuNiAu, Ni-Fe) ● Backside Metallization Packages
S.Assembly	<ul style="list-style-type: none"> ● Wafer Level Packaging (Fan-In WLP, Fan-Out WLP) ● Encapsulated Chip Package (ECP) ● Wafer Level Chip Scale Package (WLCSP) ● Flip Chip ICs, 2D/2.5D/3D ICs Integration



Service	Details
	<ul style="list-style-type: none"> ● Flip Chip Process ● Wire Bonding Process
S.Wafer-Testing	<ul style="list-style-type: none"> ● Wafer probing test ● Pre-personalization or initialization if such scripts are included in the testing program provided by the client
S.Final-Test	<ul style="list-style-type: none"> ● Assembly ICs Testing
S.Receiving	<ul style="list-style-type: none"> ● Wafer & ICs Receiving
S.Internal-Shipment	<ul style="list-style-type: none"> ● Assembled product shipped back to the client
S.External-Delivery	<ul style="list-style-type: none"> ● Assembled product delivered to the consumer following client's requirement
S.Scrap-Management	<ul style="list-style-type: none"> ● Scraps secure storage on site ● Scraps secure destruction under control of the site ● Scraps shipped back to the client
S.Identification-Traceability	<ul style="list-style-type: none"> ● Identification and traceability of client parts and product lots
S.Reliability-FA	<ul style="list-style-type: none"> ● Reliability and failure analysis in the lab

8.3 Security Assurance Requirement Aspects

Table 8.3 – Security Assurance Requirement aspects

SARs	Objectives	Aspects
ALC_CMC.5.1C The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	O.Config-Items	All products assembled at site are labeled with a unique client part ID automatically generated by a database as defined by O.Config-Items.
ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	Incoming inspection are based on O.Reception-Control's product identification that ensures associated labeling. Labeling is mapped to the internal identification as defined by O.Config-Items. This ensures the unique identification of security products. O.Config-Control ensures that each client part ID is releases based on a defined process. This includes changes that are related to a client part ID. The configurations can only be done by authorized person. O.Config-Process provides a configured and controlled production



SARs	Objectives	Aspects
		process.
<p>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.</p>	<p>O.Reception-Control O.Config-Items O.Config-Control</p>	<p>O.Reception-Control comprises the incoming labeling and the mapping to internal identifications.</p> <p>O.Config-Items comprise the internal unique identification of all items that belong to a client part ID.</p> <p>Each product is setup according to O.Config-Control comprising all necessary items.</p>
<p>ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.</p>	<p>O.Reception-Control O.Config-Items O.Config-Control O.Internal-Shipment</p>	<p>O.Reception-Control includes the incoming labeling and the mapping to internal identifications.</p> <p>O.Config-Items includes the internal unique identification of all items that belongs to a client part ID.</p> <p>Each product is setup according to O.Config-Control including all necessary items.</p> <p>O.Internal-Shipment ensures the configuration items are identified during internal shipment.</p>
<p>ALC_CMC.5.5C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.</p>	<p>O.Config-Control O.Config-Process O.Logical-Access O.Logical-Operation</p>	<p>O.Config-Control assigns the setup including processes and items for the production of each client part ID.</p> <p>O.Config-Process includes the control of the production processes.</p> <p>O.Logical-Access and O.Logical-Operation support the control by limiting the access and ensuring the correct operations for all tasks to the authorized staff.</p>
<p>ALC_CMC.5.6C The CM system shall support the production of the <i>product</i> by automated means.</p>	<p>O.Config-Process O.Zero-Balance O.Acceptance-Test</p>	<p>O.Config-Process includes the automated management of the production processes.</p> <p>O.Zero-Balance ensures the control of all security products during production.</p> <p>O.Acceptance-Test provides an automated testing of the functionality and supports the tracing.</p>



SARs	Objectives	Aspects
<p>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.</p>	<p>O.Reception-Control O.Logical-Access</p>	<p>O.Reception-Control comprises the incoming labeling and the mapping to internal identifications for all security products.</p> <p>O.Logical-Access supports the control by limiting the access and ensuring the correct operation for all tasks to authorised staff.</p>
<p>ALC_CMC.5.8C The CM system shall clearly identify the configuration items that comprise the TSF.</p>	<p>O.Config-Items O.Config-Control O.Config-Process</p>	<p>O.Config-Items comprises the internal unique identification of all items that belong to a client part ID.</p> <p>O.Config-Control describes the management of the client part IDs at the site.</p> <p>According to O.Config-Process the CM plans describe the services provided by the site.</p>
<p>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.</p>	<p>O.Config-Items O.Acceptance-Test O.Config-Control O.Config-Process</p>	<p>O.Config-Items comprises the internal unique identification of all items that belong to a client part ID.</p> <p>O.Config-Control describes the management of the client part IDs at the site.</p> <p>According to O.Config-Process the CM plans describe the services provided by the site.</p> <p>O.Acceptance-Test provides an automated testing of the functionality and supports the tracing.</p>
<p>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.</p>	<p>O.Config-Control O.Config-Process</p>	<p>O.Config-Control describes the management of the client part IDs at the site.</p> <p>According to O.Config-Process the CM plans describe the services provided by the site.</p>
<p>ALC_CMC.5.11C The CM system shall be able to identify the version of the implementation representation from which the product is generated.</p>	<p>O.Reception-Control O.Logical-Access O.Config-Control O.Config-Process</p>	<p>O.Reception-Control comprises the incoming labeling and the mapping to internal identifications.</p> <p>O.Logical-Access supports the control by limiting the access and ensuring the correct operation for all tasks to authorised staff.</p>



SARs	Objectives	Aspects
		<p>O.Config-Control describes the management of the client part IDs at the site.</p> <p>According to O.Config- Process the CM plans describe the services provided by the site.</p>
<p>ALC_CMC.5.12C The CM documentation shall include a CM plan.</p>	<p>O.Config-Control O.Config-Process</p>	<p>According to O.Config-Control the setup of each client part ID includes an associated CM plan including the release.</p> <p>O.Config-Process ensures the reliability of the processes and tools based on dedicated CM plans.</p>
<p>ALC_CMC.5.13C The CM plan shall describe howthe CM system is used for the development of the <i>product</i>.</p>	<p>O.Config-Control O.Config-Process O.Organise-Product</p>	<p>O.Config-Control describes the management of the client part IDs at thesite.</p> <p>According to O.Config-Process the CM plans describe the services provided by the site.</p> <p>The specified processes for configuration, pre-personalization and assembly are applied according to O.Organise-Product.</p>
<p>ALC_CMC.5.14C The CM plan shall describe the procedures used to accept modifiedor newly created configuration items (as part of the <i>product</i>).</p>	<p>O.Reception-Control O.Config-Items O.Config-Control O.Config-Process</p>	<p>O.Reception-Control supports the identification of configuration items on site.</p> <p>O.Config-Items ensures the unique identification of each product tested at site by the client part ID.</p> <p>O.Config-Control ensures a release foreach new or changed client part ID.</p> <p>O.Config-Process ensures the automated control of released products.</p>
<p>ALC_CMC.5.15C The evidence shall demonstrate that all configuration items are being maintained under the CM system.</p>	<p>O.Reception-Control O.Config-Control O.Config-Process O.Zero-Balance O.Internal-Shipment O.External-Delivery</p>	<p>The objectives O.Reception-Control, O.Config-Control, O.Config-Process ensure that only released client part IDsare produced.</p> <p>This is supported by O.Zero-Balance ensuring the tracing of all security products.</p> <p>O.Internal-Shipment and O.External-</p>



SARs	Objectives	Aspects
		<p>Delivery include the packing requirements, the reports, logs and notifications including the required evidence.</p>
<p>ALC_CMC.5.16C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.</p>	<p>O.Config-Control O.Config-Process O.Acceptance-Test O.Internal- Shipment O.External-Delivery</p>	<p>O.Config-Control includes a release procedure as evidence.</p> <p>O.Config-Process ensures the compliance of the process.</p> <p>O.Acceptance-Test comprises the test logs as evidence.</p> <p>Since the finished products are returned to the client or delivered to the consumer according to O.Internal-Shipment and O.External-Delivery respectively, the labeling is controlled as evidence.</p>
<p>ALC_CMS.5.1C The configuration list includes the following: <i>clear instructions how to consider these items in the list</i>;the evaluation evidence required by the SARs of the <i>life-cycle</i>; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include aCM plan.</p>	<p>O.Config-Items O.Config-Control O.Config-Process</p>	<p>Since the process is subject of the evaluation, no products are part of the configuration list.</p> <p>O.Config-Items ensure unique part IDs including a list of all items and processes for this part.</p> <p>O.Config-Control describes the release process for each client part ID.</p> <p>O.Config-Process defined the configuration control including part IDs. Procedures and processes.</p>
<p>ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.</p>	<p>O.Config-Items O.Config-Control O.Config-Process O.Reception-Control O.Internal-Shipment O.External-Delivery</p>	<p>Items, products and processes are uniquely identified by the data base system according to O.Config-Items.</p> <p>Within the production process, the unique identification is supported by automated tools according to O.Config-Control andO.Config-Process.</p> <p>The identification of received products is defined by O.Reception-Control.</p> <p>The labeling and preparation for the transport is defined by O.Internal-</p>



SARs	Objectives	Aspects
		Shipment and O.External-Delivery.
<p>ALC_CMS.5.3C <i>For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.</i></p>	<p>O.Reception-Control O.Internal-Shipment O.External-Delivery O.Config-Items</p>	<p>Since no development is done at the site, the source of each configuration item at delivery is documented.</p> <p>Internal shipments and external deliveries are tracked by technical and organizational measures.</p> <p>The developer of configuration item is listed in the asset inventory.</p>
<p>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 TOE design and implementation in its development environment.</p>	<p>O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Control-Scrap O.Internal-Shipment</p>	<p>The physical protection is provided by O.Physical-Access, supported by O.Security-Control, O.Alarm-Response, and O.Maintain-Security.</p> <p>The logical protection of data and the configuration management is provided by O.Logical-Access and O.Logical-Operation.</p> <p>The personnel security measures are provided by O.Staff-Engagement.</p> <p>Any scrap that may support an aggressor is controlled according to O.Control-Scrap.</p> <p>Internal shipment is protected by technical and procedural measures.</p>
<p>ALC_DVS.2.2C The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the <i>product</i>.</p>	<p>O.Internal-Monitor O.Logical-Operation O.Maintain-Security O.Zero-Balance O.Acceptance-Test O.Reception-Control O.Internal-Shipment O.Transfer-Data O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Staff-Engagement O.Control-Scrap</p>	<p>The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous justification is subject of the objectives O.Internal-Monitor, O.Logical-Operation and O.Maintain-Security.</p> <p>All devices including functional and non-functional are traced according to O.Zero-Balance.</p>



SARs	Objectives	Aspects
		<p>O.Acceptance-Test supports the integrity control by testing of the finished products.</p> <p>The reception and incoming inspection supports the detection of attacks during the transport of the security products to the site according to O.Reception-Control.</p> <p>The delivery to the client is protected by similar measures according to the requirements of the client based on O.Internal-Shipment.</p> <p>Sensitive data received by the site as well as sensitive data sent by the site is protected according to O.Transfer-Data to ensure access by authorised recipients only.</p> <p>Physical security measures are implemented according to O.Physical-Access, O.Security-Control, and O.Alarm-Response.</p> <p>Logical security access is controlled by O.Logica-Access.</p> <p>Personal security is achieved by O.Staff-Engagement.</p> <p>Scraps treated on site is managed by O.Control-Scrap.</p>
<p>ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.</p>	<p>O.External-Delivery</p>	<p>All external deliveries to consumers are done secured according to O.External-Delivery.</p>
<p>ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.</p>	<p>O.Config-Control O.Config-Process O.Organise-Product</p>	<p>At the site no development related to the TOE takes place.</p> <p>The site covers only life-cycle phases to manufacture the products. This is done under O.Organise-Product, O.Config-Control and O.Config-Process.</p>



SARs	Objectives	Aspects
<p>ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.</p>	<p>O.Acceptance-Test O.Zero-Balance O.Config-Process O.Organise-Product</p>	<p>At the site no development related to the TOE takes place.</p> <p>The site covers only life-cycle phases to manufacture the products. This is done under O.Organise-Product, O.Zero-Balance and O.Config-Process in order to ensure conformance to the product specifications.</p> <p>On behalf of the client, O.Acceptance-Test is done as specified.</p>

Since this SST references the PP [7], the life-cycle module used in this PP includes also the processes provided by this site. Therefore, the life-cycle module described in the PP is considered to be applicable for this site.

The performed production steps do not involve source code, design tools, compilers or other tools used to build the security product (intended TOE). Therefore, the site does not use or maintain tools according to the definition of ALC_TAT.3. However, the component included here to support the reuse of the evaluation results and to enable the justification of the evaluators regarding ALC_TAT.3.



9 References

9.1 Literature

- [1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CC:2022, Revision 1, November 2022
- [2] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CC:2022, Revision 1, November 2022
- [3] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements; CC:2022, Revision 1, November 2022
- [4] Common Methodology for Information Technology Security Evaluation (CEM): Evaluation methodology; CEM:2022, Revision 1, November 2022
- [5] Supporting Document, Site Certification, October 2007, Version 1.0, Revision 1, CCDB- 2007-11-001
- [6] Guidance for Site Certification, Bundesamt für Sicherheit in der Informationstechnik, Version 1.1, 2013-12-04
- [7] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, January 13th, 2014, BSI-CC-PP-0084-2014
- [8] Site Security Target Template, Eurosmart, Version 2.0, 15.04.2021
- [9] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, 2024-07-22

9.2 Definitions

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

intended TOE

In the view of this site certification, there is no real product certified as the site certification is - per definition – product independent. Therefore, also no TOE does exist, and this SST is referring to the “intended TOE” only.

product A “product” would be the result of the development and production process.



9.3 List of Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
IC	Integrated Circuit
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SSTL	Site Security Target Lite
ST	Security Target
TOE	Target of Evaluation

