	Shanghai Eternal Information Electronics Co., Ltd.	Document ID	EITSC11-2022
		Version	D/3
	Site Security Target Lite Eternal Packaging Centre Shanghai	Classification	Public
		Release date	2022.04.08

Site Security Target Lite

Eternal Packaging Centre Shanghai

Contents

1 Document Information

1.1 Reference

Title: Site Security Target Lite Eternal Packaging Centre Shanghai

Version: D/3

Date: 2022.04.08

Company: Shanghai Eternal Information Electronics Co., Ltd.

Name of the site: Eternal Packaging Centre Shanghai

Product Type: Security IC

EAL-Level: ALC_CMC.4, ALC_CMS.5, ALC_DVS.2 and ALC_LCD.1 (EAL5+)

2 SST Introduction

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

2 This Site Security Target refers to the following site:

Eternal Packaging Centre Shanghai

3 This site is used for chips encapsulation production.

2.1 Identification of the Site

4 The site Eternal Packaging Centre Shanghai (hereinafter referred to as “EPCS”) is located at;

No. 3576, Zhaolou Road,
Minhang District
Shanghai, 201112
People’s Republic of China

5 This location is a campus, which belongs to Shanghai Eternal Group Co., Ltd. (hereinafter referred as “Eternal Group”), Shanghai Eternal Information Electronics Co., Ltd. (hereinafter referred as “SEIE”) is subsidiary company of Eternal Group that is managing the site. This campus consists of seven buildings;

- **Office building:** This building is used for marketing, customer service, administrative management affairs and HR affairs.
- **EPCS building:** EPCS is managed by SEIE, only part of the 1st floor, the whole 2nd floor and part of the 3rd floor of this building are used for providing the chip assembly and test services for secure IC modules products, other parts of the building are rent by the other company, the physical construction isolation is deployed to separate.
- **Backup building:** The building is used as the backup workshop in the future or may be rent by the other companies which is out of the evaluation scope.
- **Canteen and dormitory:** A canteen and dormitory served for all the employees in this campus**.**
- **VIP lounge:** The building which is used for the VIP guest to have a rest in the campus.
- **Printing plant:** There are 2 buildings located in the campus of Eternal Group which are used for printing, and this printing plant is another subsidiary of Eternal Group.

2.2 Site Description

6 The whole EPCS site, which includes part of the 1st floor, the whole 2nd floor and part of the 3rd floor of the EPCS building are in the scope of this SST. The campus is surrounded by a fence that are guard with surveillance and secured by security guards, restrictions and access controlled from main gate. Additionally, guard services, access control system and surveillance restrict the access to EPCS production plant. The site includes security guard room, reception area, wastes area, loading/unloading area, logistics tunnel, engineering areas, security IC encapsulation production area, visitor corridor, equipment maintenance room, raw material temporary storage room, locker room, air shower room, testing room, central control room, finished product warehouse, lead frame warehouse, raw material warehouse, semifinished product warehouse, chip warehouse, cold warehouse, packing area, packing material area,

meeting room, office room, program editing room, printing room, documentation room, backup equipment room and a room used for the storage of sundries for the site.

7 The following service and/or processes provided by EPCS are in the scope of the evaluation process:

- Reception, identification, registration, and storage of sawn wafers
- Assembly into modules
- Functional testing of finished modules (physical- electrical testing)
- Warehousing and dispatch of finished modules
- Scrap and rejects handling

8 The complete flow of the security IC modules for smart card product at the site is covered by the SST. In addition, the management of the security IC modules for smart card related processes and the site security are covered by the SST. The production flow of the security IC modules for smart card on the site starts with the receipt of parts of the product (raw materials) up to the packing and handover for shipment of the finished security IC modules for smart card.

9 The following life-cycle phase of the Security IC modules for smart card application is subject of the SST according to protection profile (1).

- Life cycle phase 4: IC Packaging
  - ■ Security IC packaging (and testing)

3 Conformance Claims

10 The evaluation is based on Common Criteria (CC) Version 3.1, Revision 5.

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1, Revision 5, April 2017, (2)
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 5, April 2017, (3)

11 For the evaluation, the methodology will be used:

- Common Methodology for Information Technology Security Evaluation: Evaluation methodology. Version 3.1, Revision 5, April 2017, (4)

12 This Site Security Target (SST) is CC Part 3 conformant with following CC assurance components:

ALC_CMC.4, ALC_CMS.5, ALC_DVS.2 and ALC_LCD.1.

13 The assurance components chosen for the SST are taken from the definition of the EAL5 package defined in (3), because this is the level usually applied in Smart Card and similar devices evaluations. Since some protection profiles refer to EAL5 augmented by ALC_DVS.2 instead of ALC_DVS.1 as in the original package definition of EAL5, for this SST also ALC_DVS.2 has been selected instead of ALC_DVS.1.

14 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.

Note:

The site does not provide services that are covered by ALC_TAT.2 as no development activities are carried out in the site.

The site does not provide contributions to ALC_DEL.1 as no deliveries are done to the client.

The packaged modules, which are the final products produced by this site, will be mainly sent to the IC developer or ICC manufacture and this process will be treated as the internal shipment. The delivery of raw materials, semi-final, and final products between production sites identified in the life cycle of a security IC product is classified as internal shipment, the security of internal shipment is covered by ALC_DVS.2.

The clients for EPCS mentioned in this SST could be the IC developer who sends the sawn or unsawn wafer to EPCS and request chip packaging service from EPCS or ICC (smart card) developer who will embed the packaged modules into the card body.

4 Security Problem Definition

15 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. The configuration management covers the integrity of the products and the security management of the site.

16 This Site Security Target is based on the life cycle defined in the Security IC Platform Protection Profile (1). The assets (Section 4.1), threats (Section 4.2) and Organisational Security Policies (OSP) (Section 4.3) defined in this document are derived from the life cycle defined in that PP.

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

4.1 Assets

18 The following section describes the assets handled at the site.

4.1.1 IC Assembly

- Unfinished products as wafers and dice.
- Finished products as modules or other packages.
- Defective or rejected products (semi-finished product).
- Keys for blue film recycle bin lock.
- Mapping file.
- Keys for rejected modules recycle bin lock.
- Product Specification.
- BOM List.
- Bond Plan.
- Alarm system activation/deactivation code of central control room.
- Physical access control system.
- CCTV Monitor System.
- CCTV Record.
- DCC Administrator Account.
- DCC Server.
- ERP Server.
- Network Device.

- Alarm system activation/deactivation code of whole production plant.
- Personnel Security Profile.
- ISMS Documentation.
- Scrap and rejects (production waste).

19 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 lost.

4.2 Threats

20 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 production, test and assembly the TOE and the representation of parts of the TOE are vulnerable to such attacks.

21 The following threats are described in a general way. However, they are applicable to the site that provides services handling the items listed in Section 4.1 above. The explanation below the threats shall support the mapping to the Security Objectives of the site.

22 **T.Smart-Theft:**

An attacker tries to access sensitive areas of the site for manipulation or theft of TOE parts on production. The attacker has sufficient time to investigate the site out-side 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.

23 This attack already includes a variety of targets and aspects with respect to the various assets listed in the section above. It shall cover the range of individuals that try to get unregistered or defect devices that can be used to further investigate the functionality of the device and search for possible exploits. Such an attacker will have limited resources and a low financial budget to prepare the attack. However, the time that can be spent by such an attacker to prepare the attack and the flexibility of such an attacker will provide notable risk.

24 **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 TOE parts in production.

25 Although this attack is applicable for each site the risk may be different regarding the assets. These attackers may be prepared to take high risks for payment. They are sufficiently resourced to circumvent security measures and do not consider any damage of the affected company. The target of the attack may be products that can be sold or misused in an application context. This can comprise devices at a specific testing or personalisation state for cloning or introduction of forged devices. Those attackers are considered to have the highest attack potential.

26 Such attackers may not be completely defeated by the physical, technical and procedural security measures. Special measures like storage of items in safes or strong rooms or the splitting of sensitive data like keys provide additional support against such attacks. Also, the unique registration of the products can support the protection if they can be disabled or blocked.

27 **T.Accidental-Change:**

An employee, contractor or student trainee may exchange products of different production lots or different clients during production by accident.

28 Employees, contractors or student trainees that are not trained may take products or influence production systems without considering possible impacts or problems. This threat includes accidental changes e.g. due to working tasks of student trainees or maintenance tasks of contractors within the development, production or test area.

29 Such accidental changes can include the modification of configurations for tools that may have an impact on the TOE, the wrong assignment of tools for a dedicated process step. Further examples may be machine failure or misalignment between operators that are responsible for products of different clients or different products of the same client are mixed during production. This also includes the disposal of sensitive products using the standard flow and not the controlled destruction.

30 **T.Unauthorized-Staff:**

Employees or subcontractors not authorized to get access to products or systems used for production get access to products or affect production systems, so that the confidentiality and/or the integrity of the product is violated. This can apply to any TOE parts in production.

31 Also other subcontractors like cleaning staff or maintenance staff for the building get limited access that may allow them to start an attack. The disposal of defect equipment and/or TOE parts items must be considered.

32 **T.Staff-Collusion:**

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

33 **T.Attack-Transport:**

An attacker might try to get information or products during the internal shipment and/or the external delivery. The target is to compromise confidential information or violate the integrity of the products during the stated internal shipment and/or the external delivery process to allow a modification, cloning or the retrieval of confidential information after further production steps.

4.3 Organizational Security Policies

28 The following policies are introduced by the requirements of the assurance components of ALC_CMC.4, ALC_CMS.5, ALC_DVS.2 and ALC_LCD.1. 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). For each site it must be considered if all policies are required. This means that policies may be combined or may not be applicable based on the task of the site.

29 The evaluation of the documentation of the site is under configuration management. This comprises all procedures regarding the evaluated test and the security measures that are in the scope of the evaluation.

30 **P.Config-Items:**

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

31 The configuration management relies completely on the naming and identification of the received configuration items. The consistency with the expected identification is verified after receipt and each item is assigned to an internal unique identification. This holds also for test programs and other items that are provided to the site for local use. For configuration items that are created, generated or developed at the site the naming and identification must be specified.

32 **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 authorized 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 production process ensures that sufficient information is provided by the client.

33 The product setup includes the following information; (i) identification of the product, (ii) properties of the product when received at the site (iii) properties of the product when internally shipped, (iv) classification of the items (which are security relevant), (v) who (the client itself) is responsible for destruction of defect devices, (vi) how the product is tested after assembly, (vii) any configuration of the processed item as part of the services provided by the site, (viii) which address is used for the internal shipment.

34 **P.Config-Process:**

The services and/or processes provided by the site are controlled in the configuration management plan. This comprises tools used for the development 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.

35 The documentation with the process descriptions and the security measures of the site are under version control. Measure are in place to ensure that the evaluated status is ensured. In most cases tools are used to support the processes at the site. This comprises e.g. scripts or batch routines developed by the site and a commercial database system. This comprises also service levels and quality parameters.

36 **P.Reception-Control:**

The inspection of incoming items done at the site ensures that the received configuration items comply with the properties stated by the client. Furthermore, it is verified that the product can be identified, and a released production process is defined for the product. This aspect includes the check that all required information and data is available to process the items.

37 **P.Accept-Product:**

The testing and quality control of the site ensures that the released products comply with the specification agreed with the client. The acceptance process is supported by automated measures. Records are generated for acceptance process of the configuration items. Thereby, it is ensured that the properties of the product are ensured when internally shipped.

38 **P.Zero-Balance:**

The site ensures that all sensitive items (security relevant parts of the TOEs of different clients) are separated and traced on a device basis. For each hand over, either an automated or an organizational "two-employees-acknowledgement" (four-eye principle) is applied for functional and defect assets.

According to the released production process, the defect assets are securely stored within the site or sent back to the client (as per client request).

33 The following policy covers the packing and handover of products at the site after the applied production flow. All finished products are returned to the clients that provided the items. This is considered as internal shipment to the client.

39 **P.Transport-Prep:**

Technical and organisational measures ensure the correct labelling of the product. The products are packed as required by the client. A forwarder selected by the client is verified before the handover of security products. Measures to support traceability during the transport are supported by EPCS.

4.4 Assumptions

34 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.

35 The processing at EPCS relies on the following assumptions related to the products, the data, the documentation and the transfer information provided by the client or the product supplier.

36 **A.Item-Identification:**

Each configuration item received in the site, by the client, is appropriately labelled to ensure the identification of the configuration items.

37 **A.Prod-Specification:**

The product developer must provide appropriate specification and guidance for the assembly and testing of the product. This comprises bond plan for an appropriate assembly process as well as test requirements and test parameters for the development of the functional tests or a finished test program appropriate for the final testing. The provided information includes the classification of the delivered items, documents and data.

38 **A.Client-Delivery:**

The recipient of the product is defined by the client. The client provides the address and shipping information (select forwarder) via secure channel to EPCS. The client may define the requirements for packing of the security products in case the standard procedure of EPCS is not applicable.

39 **A.Product-Integrity:**

The self-protecting features of the device are fully operational and it is not possible to influence the configuration and behaviour of the devices based on insufficient operational condition or nay command sequence generated by an attacker or by accident.

EPCS assumes that the features used for testing of the dice at the end of the life-cycle phase 3 and 4 (according to (1)) are disabled. EPCS will be provided with the configuration of the product that will be the basis of the protection if the internal shipment.

36 The assumptions are outside the scope of influence of EPCS. They are needed to provide the basis for an appropriate production process, to assign the product to the released production process and to ensure the proper handling and storage of all configuration items related to the intended TOE.

5 Security Objectives

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

O.Physical-Access:

The combination of physical partitioning between the different access control levels together with technical and organizational 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 unauthorized people. The site enforces three levels (level 1 to level 3) 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 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 organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any sensitive configuration items (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 maybe controlled within a shorter period 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 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:

Access to the production machines operation and related systems (ERP) is restricted to authorize 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. Authentication using 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 up-dates, security patches, virus protection, and 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. In addition, 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. A designated team is responsible for integration of new products or changes 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 controlled by tools and procedures for the 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 the site.

O.Acceptance-Test:

The site delivers configuration items that fulfil the specified properties. Parameter checks, functional and/or visual checks and tests as specified by the client or customer are performed to ensure the compliance with the specification. The test results are logged to support tracing and the identification of systematic failures.

O.Staff-Engagement:

All employees who have access to TOE parts and who can move parts of the product out of the defined production flow are checked regarding security concerns and must sign a non-disclosure agreement.
Furthermore, all employees are trained and qualified for their job.

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 employee's acknowledgements during hand over is applied for functional and defective devices. According to the agreed production flow, the defect devices are securely stored within the site or sent back to the client (as per client request).

O.Reception-Control:

Upon reception of a product an immediate incoming inspection is performed. The inspection of physical products is done according to the documentation of the supplier. It comprises the received number of products and the identification and assignment of the product to a related internal production process. For security, relevant electronic item's authenticity and integrity is verified upon reception.

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 as specified by the client. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as specified by the client or supplier. The forwarder supports the tracing of configuration items during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined. Measures are in place to guarantee the internal shipments with equivalent measures compared to external deliveries.

O.Control-Scrap:

The site has measures in place to destruct sensitive documentation, erase, and destroy electronic media so that they do not support an attack. However, the scrap and rejects (production waste) are not destroyed within the site; they are collected and securely stored within the site or sent back to the client (as per client request).

5.1 Security Objectives Rationale

38 The SST includes a Security Objectives Rationale with a map, which shows how the threats and OSPs are covered by the Security Objectives.

39 Note that the assumptions defined in this Site Security Target cannot be used to cover any threat or OSP of the site. They are seen as preconditions fulfilled either by the site providing the sensitive configuration items or by the site receiving the sensitive configuration items. Therefore, they do not contribute to the security of the site under evaluation.

5.1.1 Mapping of Security Objectives

Threats and OSP	Security Objective	Note
T.Smart-Theft	O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Physical-Access O.Security-Control	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threat.
T.Rugged-Theft	O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Physical-Access O.Security-Control	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threats.
T.Accidental-Change	O.Acceptance-Test O.Config-Items O.Config-Process O.Logical-Access O.Physical-Access O.Staff-Engagement O.Zero-Balance	The automated measures and the control and verification procedures avoid accidental changes of sensitive items.

T.Unauthorized-Staff	O.Alarm-Response O.Control-Scrap O.Internal-Monitor O.Logical-Access O.Logical-Operation O.Maintain-Security O.Physical-Access O.Security-Control O.Staff-Engagement O.Zero-Balance	Physical and logical access control limits the access to sensitive data to authorized persons. In addition, organizational measures prevent uncontrolled access to products or product related items.
T.Staff-Collusion	O.Internal-Monitor O.Logical-Access O.Maintain-Security O.Physical-Access O.Staff-Engagement O.Zero-Balance	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees prevent unauthorized access to the sensitive data or items.
T.Attack-Transport	O.Internal-Monitor O.Internal-Shipment O.Physical-Access O.Logical-Access	The applied security measures on sensitive data during internal shipment and external delivery prevent modification or disclosure of any sensitive data during transport. The applied security measures on physical items during internal shipment and external delivery allow detection of attempted attacks.
P.Config-Items	O.Config-Items O.Reception-Control	All relevant items are covered by the control.
P.Config-Control	O.Config-Control O.Config-Items O.Logical-Access	The scope of the configuration control comprises the production process.
P.Config-Process	O.Config-Process O.Config-Control	The scope of the configuration control 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.Acceptance-Test O.Config-Control O.Config-Process	On request of the client release tests are performed.
P.Zero-Balance	O.Control-Scrap O.Internal-Monitor O.Staff-Engagement O.Zero-Balance	The handling of correct and defective items ensures that no unexpected missing items or leftover items occur.

P.Transport-Prep	O.Config-Process O.Internal-Shipment	Process configuration defines the process of the individual product and transfer correctly, product data are process configured to prevent data lost.

TABLE 5-1: SECURITY OBJECTIVE MAPING

The following is a table that demonstrates full coverage of Threats being countered and that all Organizational Security Policies are at least enforced by one or more Security Objective of the site.

	O.Acceptance-Test	O.Alarm-Response	O.Config-Control	O.Config-Items	O.Config-Process	O.Control-Scrap	O.Internal-Monitor	O.Internal-Shipment	O.Logical-Access	O.Logical-Operation	O.Maintain-Security	O.Physical-Access	O.Reception-Control	O.Security-Control	O.Staff-Engagement	O.Zero-Balance
P.Accept-Product	X		X		X											
P.Config-Control			X	X					X							
P.Config-Items				X									X			
P.Config-Process			X		X											
P.Reception-Control													X			
P.Transport-Prep					X			X								
P.Zero-Balance						X	X								X	X
T.Accidental-Change	X			X	X				X			X			X	X
T.Attack-Transport							X	X	X			X				
T.Rugged-Theft		X					X				X	X		X		
T.Smart-Theft		X					X				X	X		X		
T.Staff-Collusion							X		X		X	X			X	X
T.Unauthorized-Staff		X				X	X		X	X	X	X		X	X	X

TABLE 5-2: SECURITY OBJECTIVE TRACING

5.1.2 Justification of Security Objectives Mapping

T.Accidental-Change

Objectives O.Logical-Access and O.Physical-Access contributes to a suitable environment where CM items management (defined by O.Config-Items) are protected against external or unauthorized interference.

O.Staff-Engagement ensures that staff interacting by any means with sensitive assets are well trained (O.Config-Process) and trustworthy, and by the objective of O.Zero-Balance is prevented that by mistake any asset could be leaked between clients.

Before delivering the assets, O.Acceptance-Test guarantees that the delivery meets the required criteria imposed by the client.

T.Attack-Transport

The attacker would require physical access to compromise the assets which is prevented by O.Physical-Access or logical access which is prevented with O.Logical-Access. The protections as well as the environment are monitored to guarantee the correct operation of the security measures as

defined by O.Internal-Monitor, where the internal transports takes place and shipments are processed.

The O.Internal-Shipment measures guarantees that the shipment or the data related to the shipment is protected against tamper.

T.Smart-Theft

The site is protected with the measures defined by O.Physical-Access preventing the intruder access to the facilities. Procedures and measures defined by O.Security-Control ensures the correct operation of mechanism supporting the physical security.

O.Internal-Monitor defines the periodic review of suitability of the current protection mechanisms and its correct implementation and execution and O.Maintain-Security defines the checks to ensure the integrity of the security mechanisms.

O.Alarm-Response ensures that in the event of an intrusion, the intruder will not have time to complete the attack without triggering the response for mitigation of the attack.

T.Rugged-Theft

The site is protected with the measures defined by O.Physical-Access preventing the intruder access to the facilities. Procedures and measures defined by O.Security-Control ensures the correct operation of mechanism supporting the physical security.

O.Internal-Monitor defines the periodic review of suitability of the current protection mechanisms and its correct implementation and execution and O.Maintain-Security defines the checks to ensure the integrity of the security mechanisms.

O.Alarm-Response ensures that in the event of an intrusion, the intruder will not have time to complete the attack without triggering the response for mitigation of the attack.

T.Staff-Collusion

Measures defined by O.Physical-Access and O.Logical-Access prevents non-authorized persons having access to the sensitive assets which implies that the target for a coercion is limited to the staff with access to the assets reducing the attack surface. By measures defined in O.Zero-Balance, the staff with access to a particular client assets is also reduced to a subset of the in principle authorized staff.

Measures on O.Staff-Engagement implies the staff being well trained and prepared for this kind of events.

Potentially coerced staff forced to act out of their authorized domain would be detected by measures implemented as part of O.Internal-Monitor and O.Maintain-Security.

T.Unauthorized-Staff

By measures defined by O.Logical-Access and O.Physical-Access, non-authorized staff can’t access any asset. Measures are kept operative by measures defined O.Security-Control, O.Logical-Operation and O.Internal-Monitor while its effectiveness is evaluated periodically by means of O.Maintain-Security.

Intruders attempting unauthorized access to any asset will be advertised by measures as defined in O.Alarm-Response.

Staff attempting (deliberately or by mistake) access to assets for which no authorization is granted will be detected before the access by O.Internal-Monitor, or prevented by measures defined in O.Zero-Balance. Cooperation of other staff members could be necessary and is enforced by O.Staff-Engagement.

Rejected assets are handled as defined in O.Control-Scrap.

P.Accept-Product

Objectives defined to accomplish with O.Acceptance-Test directly enforces the policy for which the products are released only when criteria defined by client is satisfied.

Both O.Config-Control and O.Config-Process contributes to the acceptance checks framework necessary to accomplish with the policy.

P.Config-Control

Objective O.Config-Control directly enforces the policy as all the processes are explicitly tailored on that purpose. The enforcement of P.Config-Control is supported by measures and procedures defined to satisfy with O.Config-Items and O.Logical-Access.

P.Config-Items

Objective O.Config-Items directly enforces the policy as all the processes are explicitly tailored on that purpose. The enforcement of P.Config-Items is supported by procedures defined to satisfy O.Reception-Control.

P.Config-Process

All services definition, procedures and internal relevant documentation are managed by a CM system and following a CM plan. This is part of the procedures and measures defined to satisfy O.Config-Process that directly enforces P.Config-Process. Objective O.Config-Control directly enforces the policy as all the processes are explicitly tailored on that purpose.

P.Reception-Control

Procedures defined to satisfy O.Reception-Control directly enforces the P.Reception-Control policy.

P.Transport-Prep

Measures of O.Internal-Shipment contributes to maintain the client identification of the items during internal shipments and to prepare the deliveries according to the indications of the client.

For keeping the trackability and unique identification of the items, all measures of O.Config-Process will contribute to never loss the identifications (both, internal and client's) of all assets delivered back to the client or to any forwarder specified by the client.

P.Zero-Balance

All production procedures are subject to periodic review (O.Internal-Monitor) to determine among other aspects that are suitable to implement steps or controls contributing to the policy of P.Zero-Balance.

Adequate staff training and preparation as defined in O.Staff-Engagement procedures, contributes to complement the procedures aimed to enforce the zero balance policy.

Scrap and rejects are handled as defined in O.Control-Scrap.

Finally, the measures and procedures to satisfy O.Zero-Balance directly enforces the P.Zero-Balance policy.

6 Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

7 Security Assurance Requirements

40 The security assurance requirements for this Site Security Target shall support an evaluation according to ALC_CMC.4, ALC_CMS.5, ALC_DVS.2 and ALC_LCD.1.

41 The Security Assurance Requirements (SARs) for the Class ALC (Life-cycle support) are:

- ALC_CMC.4 (CM Capabilities)
- ALC_CMS.5 (CM Scope)
- ALC_DVS.2 (Development Security)
- ALC_LCD.1 (Life-cycle Definition)

42 The dependencies for the SARs are:

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

43 All the dependencies for the SAR have been fulfilled.

7.1 Application Notes

44 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 are in the focus and described in this SST. These processes are subject of the evaluation of the site.

7.1.1 Overview Regarding CM Capabilities (ALC_CMC)

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

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

47 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.

48 The life-cycle described in (1) is a complex production process. Only parts of this production process are normally provided at a specific site. In such a case the control of the product during such a production process must include sufficient 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.

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

50 A CM system has to be employed to guarantee the traceability and completeness of different production charges or lots. Appropriate administration procedures have to be provided in order to maintain the integrity and confidentiality of the configuration items.

7.1.2 Overview Regarding CM Scope (ALC_CMS)

51 The scope of the configuration list 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.

52 Process control data, test data and related procedures and programs can be in the scope of the configuration management.

7.1.3 Overview Regarding Development Security (ALC_DVS)

53 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.

54 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, and scrap must be securely handled.

55 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.

56 If the transfer of configuration items 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 distinguished to ensure the correct subject of the evaluation.

7.1.4 Overview Regarding Life-Cycle Definition (ALC_LCD)

57 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 have to be evaluated which are in the scope of the site. The PP (1) provides a life-cycle description there 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.

58 The PP (1) 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 device are delivered to the client. The defective devices are securely stored within the site or sent back to the client (as per client request).

59 For this site the Life Cycle only the phase 'IC Packaging' is relevant.

7.2 Security Assurance Rationale

60 The Security Assurance Rationale maps the content elements of the selected assurance components of (2) to the Security Objectives defined in this SST. Refinements regarding Security Assurance Requirements as defined in CC Part 3 are written in *italic*.

61 Note: The content elements that are changed from the original (4) according to the application notes in the process description (5) are written in *italic*. The term “TOE” can be replaced by *configuration items* in most cases. In specific cases it is replaced by *product* (in the sense of “intended TOE”).

SAR	Security Objective	Rationale
ALC_CMC.4.1C *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*	O.Config-Items	All product assembled at EPCS get a unique customer part ID automatically generated by a database as defined by O.Config-Items.
ALC_CMC.4.2C 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 product identification that ensures associated labelling. Labelling 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 process.
ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.	O.Reception-Control O.Config-Items O.Config-Control	O.Reception-Control includes the incoming labelling and the mapping to internal identifications. O.Config-Items includes the internal unique identification of all items that belongs to a client part ID. Each product is setup according to O.Config-Control including all necessary items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config-Control O.Config-Process O.Logical-Access O.Logical-Operation	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 includes the control of the production processes. 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.
ALC_CMC.4.5C The CM system shall support the production of the *product* by automated means.	O.Config-Process O.Zero-Balance O.Acceptance-Test	O.Config-Process includes the automated management of the production processes. O.Zero-Balance ensures the control of all security products during production. O.Acceptance-Test provides an automated testing of the functionality and supports the tracing.
ALC_CMC.4.6C The CM documentation shall include a CM plan.	O.Config-Control O.Config-Process	According to O.Config-Control the setup of each client part ID includes an associated CM plan including the release. O.Config-Process ensures the reliability of the processes and tools based on dedicated CM plans.
ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the *product*.	O.Config-Control O.Config-Process	O.Config-Control describes the management of the client part IDs at the site. According to O.Config-Process, the CM plans describe the services provided by the site.
ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *product*.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	O.Reception-Control supports the identification of configuration items at EPCS. O.Config-Items ensures the unique identification of each product tested at EPCS by the client part ID. O.Config-Control ensures that each client part ID is releases based on a defined process. This includes modified or new items that are related to a client part ID. The configurations can only be done by authorized person. O.Config-Process ensures the automated control of released products.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Reception-Control O.Config-Control O.Config-Process O.Zero-Balance O.Internal-Shipment	The objectives O.Reception-Control, O.Config-Control, O.Config-Process ensure that only released client part IDs are produced. This is supported by O.Zero-Balance ensuring the tracing of all security products. O.Internal-Shipment includes the packing requirements, the reports, logs and notification including the required evidence.
ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.Config-Control O.Config-Process O.Acceptance-Test O.Internal-Shipment	O.Config-Control includes a release procedure as evidence. O.Config-Process ensures the compliance of the process. O.Acceptance-Test comprises the control that all finished parts ID. Since the finished products are returned to the client according to O.Internal-Shipment at least the labelling of controlled by the client.

TABLE 7-1 RATIONALE FOR ALC_CMC.4

SAR	Security Objective	Rationale
ALC_CMS.5.1C The configuration list shall include the following: the *product* itself; the evaluation evidence required by the SARs; the parts that comprise the *product*; the implementation representation; security flaw reports and resolution status; and development tools and related information.	O.Config-Items O.Config-Control O.Config-Process	Since the process is subject of the evaluation, no products are part of the configuration list. O.Config-Items ensure unique part IDs including a list of all items and processes for this part. O.Config-Control describes the release process for each client part ID. O.Config-Process defined the configuration control including part IDs. Procedures and processes.
ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.	O.Config-Items	Items, products and processes are uniquely identified by the data base system according to O.Config-Items. Within the production process the unique identification is supported by automated.
ALC_CMS.5.3C For each TSF relevant configuration item, the configuration list shall indicate the developer/*subcontractor* of the item.	O.Config-Items	EPCS does not involve subcontractors for the test of security products. According to O.Config-Items all configuration items for secure products are identified.

TABLE 7-2 RATIONALE FOR ALC_CMS.5

SAR	Security Objective	Rationale
ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the *product* design and implementation in its development environment.	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.Reception-Control O.Internal-Shipment	The physical protection is provided by O.Physical-Access, supported by O.Security-Control, O.Alarm-Response, and O.Maintain-Security. The logical protection of data and the configuration management is provided by O.Logical-Access and O.Logical-Operation. The personnel security measures are provided by O.Staff-Engagement. Any scrap that may support an aggressor is controlled according to O.Control-Scrap. The reception and incoming inspection supports the detection of attacks during the transport of the security products to EPCS according to O.Reception-Control. The delivery to the client is protected by similar measures according to the requirements of the client based on O.Internal-Shipment.
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*.	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Staff-Engagement O.Control-Scrap O.Internal-Monitor O.Zero-Balance O.Acceptance-Test O.Reception-Control O.Internal-Shipment	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 are subject of the objectives as there is not necessarily a TOE evaluation running the evidence needed may be taken previous TOE/product developments. The evaluator should get evidence that the security measures stated in the development documentation are followed can be achieved while performing a site visit which is handle by ALC_DVS.2.2E.

TABLE 7-3 RATIONALE FOR ALC_DVS.2

SAR	Security Objective	Rationale
ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the *product*.	O.Config-Control O.Config-Process	The process used for identification and manufacturing are covered by O.Config-Control and O.Config-Process.
ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the *product*.	O.Acceptance-Test O.Config-Process O.Zero-Balance	The site does not perform development tasks. The applied production process is controlled according to O.Config-Process, the finished client parts are tested according to O.Acceptance-Test and all security products are traced according to O.Zero-Balance.

TABLE 7-4 RATIONALE FOR ALC_LCD.1

62 SST references the PP (1); the life-cycle model used in this PP includes the processes provided by this site as well. Therefore, the life-cycle module described in the PP (1) is considered applicable for this site.

63 The performed production steps do not involve source code, designed tools, compilers or other tools used to build the security product (intended TOE).

64 The site always ships the finished security products to the client that provided the security products for the assembly. EPCS is always involved as subcontractor. There is no delivery if security products directly to the client regarding the next life cycle step. Therefore, the transport of security products is always considered as internal shipment.

8 Site Summary Specification

66 The Site summary specification describes aspects of how the Site meets the SARs.

8.1 Preconditions Required by the Site

67 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.

68 *A.Item-Identification*: The packing and the wafers must be labelled before delivery to EPCS to allow the product identification.

69 *A.Prod-Specification*: EPCS provides assembly services for smart cards. The sawn wafers are acceptable as input for the assembly lines. Defect dice on the wafer can be marked by inking. The devices delivered to EPCS are tested after the assembly using simple functional tests like the checking of the ATR as well as open and short measurements based on the test parameters provided by the client.

70 *A.Client-Delivery*: If specific requirements are needed for the transport of the finished products the related specifications and further items e.g. seal tape must be provided to EPCS.

71 *A.Product-Integrity*: EPCS assumes that the features used for testing of the dice at the end of the life-cycle phase 3 and 4 (according to (1)) are disabled. EPCS will be provided with the configuration of the product that will be the basis of the protection if the internal shipment.

8.2 Service of the Site

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

72 The processes for assembly, testing and acceptance are set up at EPCS according to the specification (e.g. bond plan, module specification, test specification and packing requirements if applicable) provided by the client. For the release a sample lot is produced at the site.

73 The complete product specific flow includes a functional test of each product as part of the acceptance process. Either the functional tests are developed by EPCS based on test specification and electrical parameters/limits provided by the client or the test program provided by the client is integrated in the test environment of EPCS. No sensitive information should be included in those test specifications.

74 EPCS 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 alerted if products are ready for transport because the transport must be organized by the client. Based on the alert the client provides information on the forwarder that is used for the verification of the forwarder before the handover of the products.

75 Defective and rejected products are securely stored within the site or sent back to the client (as pre client request). During the production setup, the rejects and defect devices on the wafer are also stored within the site or returned to the client (as per client request).

8.3 Security Objectives Rationale

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

8.3.1 O.Physical-Access

77 The EPCS site is surrounded by a fence and controlled by CCTV. The access to the building is only possible via access-controlled doors. For area within EPCS physical security surrounding zone, security cards are implemented that restrict the access to the authorized persons only. Intrusion detection system, access control system and CCTV system at controlled entrances and exits are installed at security areas. The access control system ensures that only authorized person can access sensitive area or related assets. This is supported by O.Security-Control that includes the maintenance of the access control and the control of visitors. The physical security are supported by O.Alarm-Response providing an alarm system.

78 Thereby the threats T.Smart-Theft and T.Rugged-Theft can be prevented. The physical security measures provided by O.Security-Control enforce the recording of all actions. Thereby also, T.Unauthorized-Staff is addressed.

79 By proper isolation among different internal areas, and additional access control mechanisms, its reduced the changes that mistakenly or under collusion, product or TOE parts are changed by staff working on different client products, which helps to mitigate the threats T.Accidental-Change, T.Staff-Collusion and T.Attack-Transport.

8.3.2 O.Security-Control

80 The security guards work 24 hours per day. The security guards in the security control centre monitor the site and surveillance system. When it is off-work, the alarm system is enable, any illegal infiltration detect by the alarm sensor triggers the alert in security control centre.

81 This addresses the threats T.Smart-Theft and T.Rugged-Theft. Supported by O.Maintain-Security and O.Physical-Access also an internal aggressor triggers the security measures implemented by O.Security-Control. Therefore also the threat T.Unauthorized-Staff is addressed.

8.3.3 O.Alarm-Response

82 O.Physical-Access requires certain time to overcome the different levels of access control.

83 The alarm system is connected to the security control centre that is manned 24 hours a day. Additional patrolling and observation of the CCTV system support the alarm response. The resulting response time of the guard and the physical resistance match to provide an effective alarm response.

84 This address the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorized-Staff.

8.3.4 O.Internal-Monitor

85 Regular security management meetings are organized to monitor security incidences as well as changes or updates of security relevant systems and processes. This comprises also logs and security events of security relevant systems like Firewall, Anti-Virus system and access control.

86 This address the threats T.Attack-Transport, T.Smart-Theft, T.Rugged-Theft, T.Unauthorized-Staff, T.Staff-Collusion and the OSP P.Zero-Balance.

8.3.5 O.Maintain-Security

87 The security relevant systems enforcing or supporting O.Physical-Access, O.Security-Control and O.Logical-Access are checked and maintained regularly by the security officer. In addition, the configuration is updated by the security Specialist requested by employees (for the access control system) as required. Logging files are checked at least monthly for technical problems and specific maintenance requests.

88 This addresses the threats T.Smart-Theft, T.Rugged-Theft, T.Unauthorized-Staff and T.Staff-Collusion.

8.3.6 O.Logical-Access

89 The internal network is separated from the internet with a firewall. The internal network is further separated into subnetworks by internal firewalls. These firewalls allow only authorized information exchange between the internal subnetworks. Each user is log in into the system with his/her assigned credentials. The objective is support by O.Internal-Monitor based on the checks of the access regarding security relevant events.

90 This objective is indirectly contributing to mitigation of the threats T.Accidental-Change as the users will not be able to alter any asset or configuration of production machines unless authorized, T.Attack-Transport, T.Staff-Collusion and T.Unauthorized-Staff as information delivered internally will be accessible only to authorized staff.

91 By restricting logical access to the resources of the site, the production machines can be configured per authorized staff which contributes with the OSP P.Config-Control.

8.3.7 O.Logical-Operation

92 All logical protection measures are maintained and updated as required, at least once a quarter. Critical items such as virus scanners are updated daily. This addresses the threat T.Unauthorized-Staff so escalation of privileges is prevented by keeping the software updated.

8.3.8 O.Config-Items

93 All product configuration information is stored in the database of the internal system. The information stored is covering used materials, process specifications, acceptance test instructions and specification, test programs and packing instructions. Products are identified by unique client part IDs with are linked to the unique ID numbers of the associated configuration items.

94 This is addressing the threat T.Accidental-Change and the OSPs P.Config-Items, P.Config-Control.

8.3.9 O.Config-Control

95 The released configuration information including production and acceptance specifications is automatically copied to every work order. The test program is manually loaded to the test machine according to the configuration information of the work order. 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 authorized personnel. The production process is supported by automated systems.

96 This addresses the OSPs P.Config-Control, P.Config-Process and P.Accept-Product.

8.3.10 O.Config-Process

97 The released configuration information including production and acceptance specifications is automatically copied to every work order. The test program is automatically loaded to the test machine according to the configuration information of the work order. Configuration items are stored in the configuration management system according to the site's configuration management plan. Because an authorized configuration process is defined, T.Accidental-Change is addressed in terms of less potential flaw caused by unauthorized operation process.

98 This also addresses the OSPs P.Config-Process, P.Accept-Product and P.Transport-Prep.

8.3.11 O.Acceptance-Test

99 Acceptance tests are introduced and released based on the client approval. The tools, specifications and procedures for these tests are controlled by means of O.Config-Items and O.Config-Control. Acceptance test result are logged and linked to a work order on EPCS internal system and T-card.

100 This addresses the threat T.Accidental-Change and the OSP P.Accept-Product.

8.3.12 O.Staff-Engagement

101 All employees are interviewed before hiring. They must sign an NDA and a code of conduct for the use of computers before they start working in the company. The formal training and qualification includes security relevant subjects and the principles of handling and storage of security products. The security objectives O.Physcial-Access, O.Logical-Access and O.Config-Items support the engagement of the staff.

102 This staff engagement contributes to prevent the threats T.Accidental-Change, T.Staff-Collusion, and T.Unauthorized-Staff since the staff is properly trained on the procedures and prevention mechanisms. The OSP P.Zero-Balance is also contributed with this objective by means of trainings and staff organization.

8.3.13 O.Zero-Balance

103 Products are uniquely identified throughout the whole process. Further on the amount of functional and non-functional dice on a wafer and for a production order is known. Handover and storage of security products is controlled by the 4-eyes principle and documented. Scrap and rejects are following the good products through the whole production process. At every process step the registration of good and scrapped/rejected products is updated. Before a production order is closed a zero-balance calculation is documenting the history of good and bad parts of this order. This security objective is supported by O.Physical-Access, O.Config-Items and O.Staff-Engagement.

104 This addresses the threats T.Accidental-Change, T.Unauthorized-Staff, T.Staff-Collusion and the OSP P.Zero-Balance.

8.3.14 O.Reception-Control

105 At reception each configuration item including security products are identified by the shipping documents, packaging labels and information in EPCS internal system based on shipment alerts from the client and supported by O.Config-Items. If a product cannot be identified, it is put on hold within a secure seal of these boxes if applicable. Thereby only correctly identified products are released for production.

106 The OSPs P.Config-Items and P.Reception-Control are addressed by the reception control.

8.3.15 O.Internal-Shipment

107 The recipient of a production lot is linked to the work order in the EPCS internal system and can only be modified by authorized users. Packing procedures are documented in the product configuration. This includes specific requirement from the client. This security objective is supported by O.Staff-Engagement and O.Config-Items.

108 The threat T.Attack-Transport and the OSP P.Transport-Prep are addressed by the internal transport procedures.

8.3.16 O.Control-Scrap

109 Scrap and rejects are securely stored within the site or sent back to the client (as per client request).

110 Supported by O.Physical-Access and O.Staff-engagement this addresses the threat T.Unauthorized-Staff and the OSP P.Zero-Balance.

8.4 SARs Rationale

111 The Security Assurance Rationale is given in section 7.2. This rationale addresses all content elements and thereby also implicitly all developer action elements defined in (3). Therefore, the following Security Assurance Requirements rationale provides the justification for the selected Security Assurance Requirements. In general, the selected Security Assurance Requirement fulfil the needs derived from the Protection Profile (1).

112 Because they are compliant with the Evaluation Assurance Level EAL5 augmented all derived dependencies are fulfilled.

8.4.1 ALC_CMC.4

113 The content and presentation elements for ALC_CMC.4:

ALC_CMC.4.1C	*The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*
ALC_CMC.4.2C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.4.3C	The CM system shall uniquely identify all configuration items.
ALC_CMC.4.4C	The CM system shall provide automated measures such that only authorized changes are made to the configuration items.
ALC_CMC.4.5C	The CM system shall support the production of the *product* by automated means.
ALC_CMC.4.6C	The CM documentation shall include a CM plan.
ALC_CMC.4.7C	The CM plan shall describe how the CM system is used for the development of the *product*.
ALC_CMC.4.8C	The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *product.*

ALC_CMC.4.9C	The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.4.10C	The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

114 The chosen assurance level ALC_CMC.4 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.

8.4.2 ALC_CMS.5

115 The content and presentation elements for ALC_CMS.5:

ALC_CMS.5.1C	The configuration list shall include the following: the *product* itself; the evaluation evidence required by the SARs; the parts that comprise the *product*; 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.

116 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.

8.4.3 ALC_DVS.2

117 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 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*.

118 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 handle

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 (1) requires this protection for sites involved in the life-cycle of Security ICs development and production.

8.4.4 ALC_LCD.1

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

120 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 development and 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.

8.5 Assurance Measure Rationale

8.5.1 O.Physical-Access

121 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 developer shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

8.5.2 O.Security-Control

122 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 developer shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

8.5.3 O.Alarm-Response

123 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 including the initialization in its development and production environment. ALC_DVS.2.2C requires that the developer shall justify that the security measures provide the necessary level of

protection to maintain the confidentiality and integrity of the TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

8.5.4 O.Internal-Monitor

124 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 TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

8.5.5 O.Maintain-Security

125 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. Thereby this objective contributes to meet the Security Assurance Requirement.

8.5.6 O.Logical-Access

126 ALC_CMC.4.4C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. 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 developer shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.

8.5.7 O.Logical-Operation

127 ALC_CMC.4.4C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. 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. Thereby this objective contributes to meet the Security Assurance Requirement.

8.5.8 O.Config-Items

128 ALC_CMC.4.1C requires a documented process ensuring an appropriate and consistent labelling of the products. A method used to uniquely identify the configuration items is required by ALC_CMC.4.2C. In addition, ALC_CMC.4.3C requires that the CM system uniquely identifies all configuration items. ALC_CMC.4.8C requires that the CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the product. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C requires that the configuration list shall uniquely identify the configuration items. ALC_CMS.5.3C requires that the developer of each TSF relevant configuration item is indicated in the configuration list. The objective meets the set of Security Assurance Requirements.

8.5.9 O.Config-Control

129 ALC_CMC.4.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.4.3C requires a unique identification of all configuration items by the CM system. ALC_CMC.4.4C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. ALC_CMC.4.6C requires a CM documentation that includes a CM plan. ALC_CMC.4.7C requires that the CM plan describes how the CM system is used for the development (setup of test process flow, correct pairing of wafers and customer data) of the TOE. ALC_CMC.4.8C requires that the CM plan describes the procedure used to accept modified or newly created configuration items of the TOE. ALC_CMC.4.9C requests evidence demonstrating that all configuration items are being maintained under the CM system. ALC_CMC.4.10C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. In addition, ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products. The objective meets the set of Security Assurance Requirements.

8.5.10 O.Config-Process

130 ALC_CMC.4.2C 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 are made to the configuration items as required by ALC_CMC.4.4C. ALC_CMC.4.5C requires that the CM system supports the production by automated means. ALC_CMC.4.6C requires that the CM documentation includes a CM plan. ALC_CMC.4.7C requires that the CM plan describe how the CM system is used for the development of the TOE. ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE. ALC_CMC.4.9C requests evidence showing that all configuration items are being maintained under the CM system. ALC_CMC.4.10C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_LCD.1.1C requires that the life-cycle definition documentation describe the model used to develop and maintain the products. ALC_LCD.1.2C requires control over the development and maintenance of the TOE. The objective meets the set of Security Assurance Requirements.

8.5.11 O.Acceptance-Test

131 The testing of the products is considered as automated procedure as required by ALC_CMC.4.5C. The operation of the CM system in accordance with the CM plan is required by ALC_CMC.4.10C. ALC_DVS.2.2C requires that the developer shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. In addition, ALC_LCD.1.2C requires control over the development and maintenance of the TOE. Thereby the objective fulfils this combination of Security Assurance Requirements.

8.5.12 O.Staff-Engagement

132 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 developer shall justify that the security measures provide the necessary

level of protection to maintain the confidentiality and integrity of the TOE. Thereby the objective fulfils this combination of Security Assurance Requirements.

8.5.13 O.Zero-Balance

133 ALC_CMC.4.5C requires that the CM system support the production of the TOE by automated means. ALC_CMC.4.9C requires evidence demonstrating that all configuration items are being maintained under the CM system. ALC_DVS.2.2C requires that the developer shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. ALC_LCD.1.2C requires control over the development and maintenance of the TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.

8.5.14 O.Reception-Control

134 ALC_CMC.4.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.4.3C requires a unique identification of all configuration items by the CM system. ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE. ALC_CMC.4.9C requests evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_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 developer shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.

8.5.15 O.Internal-Shipment

135 ALC_CMC.4.9C requests evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.4.10C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. ALC_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. This includes also the protection during the transport between production sides. ALC_DVS.2.2C requires that the developer shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

8.5.16 O.Control-Scrap

136 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 developer shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.

8.6 Mapping of the Evaluation Documentation

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

9 References

9.1 Literature

1. EUROSMART. Security IC Platform Protection Profile with Augmentation packages. Version 1.0, 2014.
2. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model. Version 3.1, Rev. 5, April 2017.
3. —. Part 3: Security Assurance Components. Version 3.1, Rev. 5, April 2017.
4. Common Methodology for Information Technology Security Evaluation. Evaluation methodology. Version 3.1, Rev.5, April 2017.
5. —. Supporting Document, Site Certification. Version 1.0, Rev.1, October 2007.

9.2 Terminology

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 List of Abbreviations

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