Site Security Target Lite

LINXENS TIANJIN SITE

Author	Reviewer	Approver
Lin SUN	Frank WU	Jungle Zheng

Revision Control

Revision	Date	Description
0.1	29/10/2021	Initial document
0.2	16/12/2021	Minor changes
0.3	25/01/2022	Refinement of security objectives according CB comments
0.4	22/02/2023	Updated to comply with SST for recertification
0.5	04/05/2024	Revised from SST file revision
0.6	05/06/2024	Minor Changes
0.7	12/07/2024	Revised from SST file revision
0.8	18/07/2024	Minor Changes

Contents

1 Document Information

1.1 Reference

Title: Site Security Target Lite LINXENS TIANJIN SITE

Revision: 0.8

Date: 2024/07/18

Company: Linxens Tianjin Co, Ltd.

Name of the site: LINXENS TIANJIN SITE

Product Type: Security IC

Evaluation Assurance Components: ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1 and ALC_FLR.1.

2 SST Introduction

This chapter is divided into the section 2.1 Identification of the Site and 2.2 Site Description.

This Site Security Target refers to the following site:

LINXENS TIANJIN SITE

This site is used for chips encapsulation production.

2.1 Identification of the Site

The site name is LINXENS TIANJIN SITE (hereinafter referred to as “LXT”), which is located at:

NO 68, Zhenxiang Road,

Binhai Maritime Hi-tech Area

300459 Tianjin China

This location is a campus, which belongs to Linxens Tianjin Co, Ltd.

This campus consists of several buildings and not all of them are within the physical scope of the site. Physical areas within the evaluation scope are listed below:

- Guardhouse room 1 (1st floor of guardhouse 1 building)
- Guardhouse room 2 (1st floor of guardhouse 2 building)
- Reception/Dispatching area (1st floor of plant building)
- Warehouse (1st floor of plant building)
- Wafer room (1st floor of plant building)
- Finished good room (1st floor of plant building)
- Packing area (1st floor of plant building)
- Module workshop (1st floor of plant building)
- IT server room (2nd floor of plant building)
- DCC room (2nd floor of plant building)
- Card making room (1st floor of plant building)
- Production office (1st floor of plant building)
- Laboratory (1st floor of plant building)

2.2 Site Description

All the areas within the scope are located inside a campus owned by Linxens Tianjin Co, Ltd. Not all areas within the campus are in the scope of this SST. The campus is surrounded by a fence that is guarded with CCTV surveillance and secured by 24/7 security guards. Additionally, guard services, access control, surveillance restrict and control the access to areas within the scope. The site includes guardhouse room, reception/dispatching area, warehouse, wafer room, finished good room, packing area, module workshop, IT server room, card making room, production office.

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

- Reception of secured product
- Registration of secured product for identification
- Storage of secured products including sawn wafer, unfinished module, finished module
- Assembly into Modules (Production includes following steps: Die Bonding, Wire Bonding, Encapsulation)
- Functional testing of finished modules (physical electrical testing)
- Quality control testing for incoming raw materials and production process
- Visual inspection of finished modules
- Warehousing and dispatch of finished modules
- Storage of wafer scrap and die chips rejected.
- Product security flaw collection, verification, correction and corrective action delivery

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 IC embedding processes and the site security are covered by the SST. The production flow of the security IC modules on the site starts with the receiving of parts of the product (raw materials) up to the packaging and shipment of the finished security IC modules or smart cards.

The following life-cycle phase of the Security IC modules can be subjected (but not restricted) as example to the PP0084 (PP-0084):

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

3 Conformance Claim

The evaluation is based on Common Criteria Version 3.1, Revision 5.

- Common Criteria for Information Technology Security Evaluation, Part1: Introduction and general model; Version 3.1, Revision 5, April 2017, (CC-PART1)
- Common Criteria for Information Technology Security Evaluation, Part3: Security assurance components; Version 3.1, Revision 5, April 2017, (CC-PART3)

For the evaluation, the methodology will be used:

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

This Site Security Target (SST) is CC Part 3 conformant, which consists of the following CC assurance components:

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

The assurance components chosen for the SST are taken from the definition of the EAL6 package defined in (CC-PART3), because EAL5+ and above are the levels usually applied for Smart Card and similar devices evaluations related with PP0084 (PP-0084).

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 claim ALC_TAT.3 since no development related activities of the TOE (or its parts) are carried out at the site.

The site does not claim ALC_DEL.1 since no delivery activities of the final TOE to the end user are carried out at the site.

4 Security Problem Definition

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

This Site Security Target is based on the life cycle defined in the Security IC Platform Protection Profile (PP-0084). The assets (Section 4.1), threats (Section 4.2) and Organizational Security Policies (OSP) defined in this document are derived from the life cycle defined in that PP (PP-0084).

The Security Problem Definition comprises two major so-called security problems. The first set of security problems comprises all kinds 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

The following section describes the assets handled at the site.

The site has internal documentation and data that is relevant to maintain the confidentiality and integrity of an intended TOE. This comprises site security concepts and the associated security measures as well as key and cryptographic tools for the encrypted change of data. These items are not explicitly listed in the list of assets below.

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 this important condition. These items consist of commercially available hardware and software, which are programmed and customised by LXT.

4.1.1 IC Assembly

The assets are related to the production of security wafers as follows.

- Sawn wafer
- Unfinished Module
- Module
- Scrap

There can be further client specific assets like seals, special transport protection or similar items that support the security of the external delivery to the client. They are handled in the same way as the other assets to prevent misuse, disclosure or lost.

4.1.2 Development Security Documentation

Development security documentation can be categorized into following parts:

- Internal documents where integrity is required (Most corporate policies, guidelines, and procedures with the exception of policies, guidelines and procedures related to physical or logical security)
- Restricted documents where integrity and availability are required (Physical and Logical Security policies, guidelines, and procedures without sensitive information)
- Confidential documents where confidentiality, integrity and availability are required (Documents containing sensitive information)

4.1.3 Production Data

Production data is the data generated during the production process. There is no confidentiality requirement for the production data. As long as the production will not be modified in an unauthorized way. Therefore, only integrity and availability of the production data are required to be protected. This asset is classified as Restricted.

4.2 Threats

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

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.

T.Smart-Theft:

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

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 chips that can be used to further investigate the functionality of the chip 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.

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 intended TOE parts in production.

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 chips at a specific testing or personalization state for cloning or introduction of forged chips. Those attackers are considered to have the highest attack potential.

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.

T.Computer-Net

A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get access to sensitive configuration data or items or modify security relevant production processes.

T.Accidental-Change

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

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.

Such accidental changes can include the modification of configurations for tools that may have an impact on the intended 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.

T.Unauthorised-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 intended TOE parts in production.

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 intended TOE parts items must be considered.

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.

T.Attack-Transport

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

4.3 Organizational Security Policies

The following policies are introduced by the requirements of the assurance components. 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).

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

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.

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.

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.

The product setup includes the following information: identification of the product, properties of the product when received at the site properties of the product when internally moved in the same building, how the product is tested after assembly, any configuration of the processed item as part of the services provided by the site, which address is used for the internal transportation.

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.

The documentation with the process descriptions and the security measures of the site are under revision 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, programs or batch routines developed by the site and some production data process system. This comprises also service levels and quality parameters.

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.

P.Accept-Product

The testing and quality control of the site ensures that the products released by the site 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 the products are in release phase.

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 the chip basis. 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).

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 or sending to the specific locations requested by the clients. This is considered as shipment to the final client.

P.Product-Transport

Technical and organisational measures shall ensure the correct labelling of the product. A controlled external delivery shall be applied. The transport supports traceability up to the acceptor. In the case the product needs to be moved within the building, this will be considered as internal transportation.

P.Organise-Product

The development process is applied as specified by the site’s quality management documentation. If the related data includes sensitive items appropriate measures must be in place.

P.Flaw-Remediation

A flaw remediation procedure must be in place to continually minimize potential flaw by tracking and handling reported security flaws across their life cycle.

4.4 Assumptions

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

The processing at LXT 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.

A.Item-Identification

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

A.Prod-Release

The client is responsible for the release of the products to be produced.

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.

A.External-Delivery

The recipient (Card issuer or Smart Card Production plant) of the product is identified by the address provided by the client. The address of the client is part of the product setup. Every recipient of the product is identified by the address provided by the client.

A.Product-Integrity

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

A.Destruct-Scrap

Scrap configuration items are collected at the site. If the clients request to send scraps back to them then scraps will be sent back to clients in a secure way. If the clients do not request to send scraps back to them, scraps will be stored securely within the site.

The assumptions are outside the scope of influence of LXT. 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

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

O.Security-Documentation

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

O.Physical-Access

The combination of physical partitioning between the different access control levels together with technical and 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 security levels concept for its physical areas, which are mapping to the normal areas, security areas and high-security areas of the site. The access control measures ensure that only registered employees, visitor and vendors can access normal areas. Sensitive products are handled in security areas and high security 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 annually. 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 are 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 and virus protection). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.

O.Config-Items

The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify 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 clients 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 intended 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 chip basis. Automated control and/or two employee's acknowledgements during hand over is applied for functional and defective chips. According to the agreed production flow, the defect

chips will be handled as scrap. All the production stages of sensitive product are managed through the configuration systems automatically, the quantity of the intended TOE and defective products are recorded in the configuration system and ensure that all the sensitive materials are under sufficient control.

O.Reception-Control

Upon reception of the incoming items (e.g. raw materials, maping files, etc.), an immediate incoming inspection is performed. The inspection of physical and logical items is done according to the internal requirements. It comprises the surface of raw materials, received number of items, the identification and assignment of the item to a related internal production process. For security checks, relevant integrity and authenticity of the incoming items are verified upon reception.

O.External-Delivery

The recipient of a physical configuration item is identified by the assigned client address. The recipient(s) of an electronic configuration item (e.g. initialisation data, response data) can be identified in different ways. The specific way is defined in the external delivery procedure. The external delivery procedure is applied to all sensitive configuration data or items. The recipient for shipment can only be changed by a controlled process. The packaging (if any) is also part of the defined process and applied as agreed with the client. The forwarder supports the tracing of sensitive configuration data or items during external delivery. For every configuration data or item, the protection measures against manipulation are defined (if necessary).

O.Transfer-Data

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

O.Control-Scrap

The site has measures in place to destroy sensitive documentation and erase electronic media so that they do not support an attack. The defective and rejected products are not destroyed within the site; they are collected and returned back to the client. If the client does not request the scrapping material to be returned, these are securely stored within the site.

O.Flaw-Remediation

This site will define a written procedure and appoint responsible to collect, track and handle any reported security flaw to achieve a goal that reported security flaw being handled, potential security flaw being prevented and corrective actions being delivered to the intended TOE receiver.

5.1 Security Objectives Rationale

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

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.Security-Documentation O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threat.
T.Rugged-Theft	O.Security-Documentation O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threats.
T.Computer-Net	O.Security-Documentation O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement	The automated measures and the control and verification procedures avoid accidental changes of sensitive items.

T.Accidental-Change	O.Acceptance-Test O.Config-Items O.Config-Process O.Logical-Access O.Physical-Access 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.Unauthorised-Staff	O.Security-Documentation 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	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.Staff-Collusion	O.Security-Documentation O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Transfer-Data O.Control-Scrap	The applied security measures on sensitive data during internal transportation and external delivery prevent modification or disclosure of any sensitive data during transport. The applied security measures on physical items during internal transportation and external delivery allow detection of attempted attacks.
T.Attack-Transport	O.External-Delivery O.Transfer-Data	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threats.
P.Accept-Product	O.Acceptance-Test O.Config-Control O.Config-Process	On request of the client release tests are performed.
P.Config-Control	O.Config-Items O.Config-Control O.Logical-Access O.Reception-Control O.Config-Process	The scope of the configuration control comprises the production process.
P.Config-Items	O.Config-Items O.Reception-Control	All relevant items are covered by the control.
P.Config-Process	O.Config-Process	The scope of the configuration control comprises the production process.

P.Organise-Product	O.Logical-Operation O.Logical-Access O.Config-Control O.Config-Process	The application of the production processes is supported by technical and organisational means.
P.Product-Transport	O.Config-Items O.External-Delivery O.Transfer-Data	The controlled shipment and delivery procedures ensure correct shipment and delivery of items.
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 integrity and availability of items ensures that only authentic and qualified items are accepted.
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 left-over items occur.
P.Flaw-Remediation	O.Flaw-Remediation	Reported security flaw will be handled according to the written procedure of flaw remediation so that reported security flaw will be collected, tracked and handled in a concerted way.

TABLE 1 MAPPING OF SECURITY OBJECTIVES

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.External-Delivery	O.Internal-Monitor	O.Logical-Access	O.Logical-Operation	O.Maintain-Security	O.Physical-Access	O.Reception-Control	O.Security-Control	O.Security-Documentation	O.Staff-Engagement	O.Transfer-Data	O.Zero-Balance	O.Flaw-Remdediation
P.Accept-Product	X		X		X														
P.Config-Control			X	X	X				X				X						
P.Config-Items				X									X						
P.Config-Process					X														
P.Organise-Product			X		X				X	X									
P.Product-Transport				X			X										X		
P.Reception-Control													X						
P.Zero-Balance						X		X								X		X	
P.Flaw-Remediation																			X
T.Accidental-Change	X			X	X				X			X				X		X	
T.Attack-Transport							X										X		
T.Computer-Net								X	X	X	X				X	X			
T.Rugged-Theft		X						X			X	X		X	X				
T.Smart-Theft		X						X			X	X		X	X				
T.Staff-Collusion						X		X			X				X	X	X		
T.Unauthorised-Staff		X				X		X	X	X	X	X		X	X	X		X	

TABLE 2 MAPPING BETWEEN POLICIES/THREADS COVERING OBJECTIVES

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 security measures defined by O.External-Delivery ensure that an attacker cannot get access to sensitive physical or electronic data or items during internal or external delivery. For electronic items this is supported by the security measures defined by O.Transfer-Data.

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

T.Computer-Net

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

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

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

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

T.Smart-Theft and T.Rugged-Theft

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

The 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.

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

T.Staff-Collusion

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

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

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

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

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

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

T.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.

O.Security-Documentation can ensure from the policy aspect, the threat can not mitigated.

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 will be collected before leaving the facilities where the access is controlled and returned to the client, by measures 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, O.Config-Process, O.Reception-Control 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.

P.Organise-Product

This is supported by O.Config-Process, which ensures that a configuration management plan is in place, and by O.Config-Control, which ensures the application of the required procedures for the product release. The security objectives O.Logical-Access and O.Logical-Operation provide the necessary security measures to protect sensitive items.

P.Product-Transport

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

P.Reception-Control

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

P.Zero-Balance

P.Zero-Balance is enforced by O.Zero-Balance and O.Control-Scrap which ensures that no unexpected missing or left-over items occur. Besides, O.Internal-Monitor and O.Staff-Engagement also contribute to this policy.

P.Flaw-Remediation

P.Flaw-Remediation is achieved by O.Flaw-Remediation to ensure a formal security flaw handling procedure is in place.

6 Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

7 Security Assurance Requirements

The security assurance requirements for this Site Security Target are ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1 and ALC_FLR.1.

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

- ALC_CMC.5 (CM capabilities)
- ALC_CMS.5 (CM scope)
- ALC_DVS.2 (Development security)
- ALC_LCD.1 (Life-cycle definition)
- ALC_FLR.1 (Flaw remediation)

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

ALC_CMC.5: ALC_CMS.1, ALC_DVS.2, ALC_LCD.1

ALC_CMS.5: None

ALC_DVS.2: None

ALC_LCD.1: None

ALC_FLR.1: None

The dependency ALC_LCD.1 is partially fulfilled because the site does not cover the whole life cycle of the TOE development.

7.1 Application Notes and Refinements

The term "TOE" used for the product under evaluation is considered as "intended TOE" here because a specific product is not considered during the evaluation. Since the term “TOE” is not applicable in the SST the associated processes for the handling of products are in the focus and described in this SST. These processes are subject of the evaluation of the site.

Refinements regarding Security Assurance Requirements as defined in CC Part 3 (CC-PART3) are written in italic. The term 'TOE' is replaced by 'product' or 'configuration item'.

7.1.1 Overview regarding CM capabilities (ALC_CMC)

A production control system is employed to guarantee the traceability and completeness of different production charges or lots. The chip lots, production serial number, client part ID, production quantity, defective products quantity, operators, production progress, serial number of production machines, working time of operators, usage of raw materials, etc. 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 chip removed from the production stage that are not functional will be delivered to the client instead of destruction.

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 (PP-0084) 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.

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.

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)

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.

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)

The CC assurance components of family ALC_DVS refer to the “development environment”, 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 and configuration data must be guaranteed, access to any kind of samples (client’s specific samples or open samples) development tools and other material must be restricted to authorized persons only, and scrap must be controlled and returned.

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 configuration items between two lanes 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 transportation. 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.

7.1.4 Overview 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 have to be evaluated which are in the scope of the site. The PP (PP-0084) 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.

The PP (PP-0084) 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 delivered to the client. The defective products are also returned to the client.

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

7.1.5 Overview regarding Flaw Remediation (ALC_FLR)

Since this site is a production site and the finished good is not in a status that can be delivered to the final intended TOE user. Therefore, the flaw remediation procedure mentioned across this SST is focus on the service provided to the finished good receiver, normally it is the client who send the sawn wafer or wafer to this site. The intent of the flaw remediation procedure is to collect security flaw reported by client or reported internally and handle it with predefined way.

7.2 Security Assurance Rationale

The security assurance requirements rationale maps the content elements of the selected assurance components of (CC-PART3) to the security objectives defined in this Site Security Target. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of the products.

Note: The content elements that are changed from the original (CC-CEM) according to the application notes in the process description (CC-SDG) are written in italic. The term TOE can be replaced by configuration items or product.

7.2.1 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
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 LXT get a unique production serial number generated by a database as defined by O.Config-Items, which is linked to the client part ID.
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 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 released 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.5.3C The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	O.Config-Process O.Config-Control	O.Config-Process ensures that only authorised staff can apply changes. This comprises changes related to process flows, procedures and items of clients. Teams are defined to assess and release changes. O.Config-Control ensures that each client part ID is released 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.
ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	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. O.Config-Control ensures the assignment between all configuration items supported by automated tracking systems. O.Config-Process provides a configured and controlled production process.
ALC_CMC.5.5C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	O.Config-Control O.Config-Process O.Logical-Access O.Logical-Operation	According to O.Config-Control an automated system is in place to map the configuration items to a unique job number Changes can only be applied by authorised personal as described by O.Config-Process. 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.5.6C The CM system shall support the production of the *product* by automated means.	O.Config-Control O.Zero-Balance O.Acceptance-Test	O.Config-Control comprises an automated system that ensures the unique mapping between configuration items and the tracking of the different production steps. O.Zero-Balance ensures that the number of produces modules complies with the sum of the delivered modules and the scrap modules. O.Acceptance-Test provides an automated testing of the product and supports the tracing.
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.	O.Config-Process O.Reception-Control	The management of the production environment and the different steps is assigned to different teams as described by O.Config-Process. O.Reception-Control includes the incoming labelling and the mapping to internal identifications.
ALC_CMC.5.8C The CM system shall clearly identify the configuration items that comprise the TSF.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	Since there is no specific TOE in the main focus of the site certification. Evaluator should only select such kind of configuration items which are in the scope of the certified site like CM tools/documentation or development tools

		for example, which is nearly the same as ALC_CMC.5.4C. 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. O.Config-Control ensures the assignment between all configuration items supported by automated tracking systems. O.Config-Process provides a configured and controlled production process.
ALC_CMC.5.9C The CM system shall support the audit of all changes to the *configuration items* by automated means, including the originator, date, and time in the audit trail.	O.Config-Control O.Acceptance-Test	The automated production control covered by O.Config-Control comprises the logging of all production steps and thereby includes the required audit trail including the originator. O.Acceptance-Test provides an automated testing of the product and supports the tracing.
ALC_CMC.5.10C The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O.Config-Control O.Config-Items O.Config-Process O.Reception-Control	O.Reception-Control comprises the control of the incoming configuration items. O.Config-Items and O.Config-Control cover the unique labelling and management of the client configuration items. O.Config-Process ensures that only controlled changes are applied.
ALC_CMC.5.11C The CM system shall be able to identify *all the production related data* from which the *product* is generated.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	O.Reception-Control comprises the control of the incoming configuration items. O.Config-Items and O.Config-Control cover the unique labelling and management of the client configuration items. O.Config-Process ensures that only controlled changes are applied.
ALC_CMC.5.12C 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.5.13C The CM plan shall describe how the CM system is used for the *production* 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.5.14C 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-Process O.Acceptance-Test	O.Reception-Control supports the identification of configuration items at LXT. O.Config-Items ensures the unique identification of each product tested at LXT by the client part ID. O.Config-Process ensures the automated control of released products. O.Acceptance-Test ensures the released product meet the requirements imposed by client.
ALC_CMC.5.15C 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	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.
ALC_CMC.5.16C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.Config-Control O.Config-Process O.Zero-Balance	O.Config-Control includes a release procedure as evidence. O.Config-Process ensures the compliance of the process. O.Zero-Balance ensures that the number of produces modules complies with the sum of the delivered modules and the scrap modules.

TABLE 3 RATIONALE FOR ALC_CMC.5

7.2.2 Rationale for ALC_CMS.5

SAR	Security Objective	Rationale
ALC_CMS.5.1C	O.Config-Items O.Config-Control	Since the process is subject of the evaluation, no products are part of the configuration list. TOE itself, the parts

The configuration list shall include the following: *the evaluation evidence required by the SARs, the development tools and related information.*	O.Config-Process	comprise the TOE, the implementation representation and security flaws are not applicable for a site evaluation. 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 O.Config-Control O.Config-Process O.Reception-Control O.External-Delivery	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 tools according to O.Config-Control and O.Config-Process. The identification of received products is defined by O.Reception-Control. The labelling and preparation for the transport is defined by O.External-Delivery.
ALC_CMS.5.3C For each *product* relevant configuration item, the configuration list shall indicate the developer of the item.	O.Config-Items	LXT does not involve subcontractors for the test of security products. According to O.Config-Items all configuration items for secure products are identified.

TABLE 4 RATIONALE FOR ALC_CMS.5

7.2.3 Rationale for ALC_DVS.2

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	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement	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 confidentiality and integrity of the *product* design and implementation in its development environment.	O.Maintain-Security O.Control-Scrap O.External-Delivery O.Security-Documentation O.Transfer-Data O.Reception-Control	The personnel security measures are provided by O.Staff-Engagement. Any scrap that may support an aggressor is controlled according to O.Control-Scrap. Secure physical delivery between different sites is controlled by O.External-Delivery. O.Security-Documentation ensures the security related documentation control. O.Transfer-Data is intended to secure the data transmission. The reception and incoming inspection supports the detection of attacks during the transport of the security products to LXT according to O.Reception-Control.
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.Logical-Operation O.Staff-Engagement O.Control-Scrap O.Internal-Monitor O.Zero-Balance O.Acceptance-Test O.Reception-Control O.Maintain-Security O.Security-Documentation O.Transfer-Data	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. O.Zero-Balance ensure that no unauthorised access to products is possible for an attacker. The associated control and continuous justification is subject of the O.Internal-Monitor and O.Acceptance-Test.

TABLE 5 RATIONALE FOR ALC_DVS.2

7.2.4 Rationale for ALC_LCD.1

SAR	Security Objective	Rationale
ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used	O.Config-Control O.Config-Process	The process used for identification and manufacturing are covered by O.Config-Control and O.Config-Process.

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*.	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 6 RATIONALE FOR ALC_LCD.1

7.2.5 Rationale for ALC_FLR.1

SAR	Security Objective	Rationale
ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the *production lot*.	O.Flaw-Remediation	The procedures are established by O.Flaw-Remediation.
ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.	O.Flaw-Remediation	The description of the nature, effect of each security flaw, as well as the status of finding a correction to that flaw can be fulfilled by the establishment of O.Flaw-Remediation.
ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	O.Flaw-Remediation	Corrective actions can be identified by the establishment of O.Flaw-Remediation.
ALC_FLR.1.4C The flaw remediation procedures documentation shall	O.Flaw-Remediation	O.Flaw-Remediation established the procedures describing methods to provide flaw information, corrections and guidance.

describe the methods used to provide flaw information, corrections and guidance on corrective actions to *finished good receiver*.		

TABLE 7 RATIONALE FOR ALC_FLR.1

8 Site Summary Specification

8.1 Preconditions Required by the Site

This section provides a justification for the assumptions defined in section 4.4 of this document. The following statements define the preconditions of the client that are required to ensure the security measure of the site to protect its assets.

The main precondition of the design data preparation and the modules production is a released process technology between the wafer fab and the final client. This comprises the definition of the requirements specification as well as parameters and limits for the produced wafer. The requirement specification is independent of the product classification and fixed for a dedicated production process (to cover A.Prod-Release and .Prod-Specification).

The client provides a method of unique identification for all items shipped to the site (to cover A.Item-Identification).

The client provides appropriate information for the delivery of produced goods as well as electronic data to be delivered. This information shall at least comprise address data for physical items (to cover A.External-Delivery).

The self-protection features of the Smart Card modules to be produced are fully operational during production (to cover A.Product-Integrity).

Scrap parts are stored securely in the wafer room and may be send back if required by the client (to cover A.Destruct-Scrap).

8.2 Services of the Site

Reception, identification, registration and storage of secured products including sawn wafers, unfinished module and finished module: The chip of products received by LXT will be labelled with a unique client part ID (client parts). This part ID is linked with the chip that is assembled in the product.

Assembly into modules: The processes for assembly, testing and acceptance are set up at LXT according to the specification (e.g. bond plan, module specification, test specification and packing requirements if applicable) provided by the client. Die bond and wire bound is performed in the production area. For the release a sample lot is produced at the site.

Quality control testing for the incoming raw materials and each production process: There is a quality control procedure be presented used to inspect the incoming materials and the product under production at each production process.

Functional testing and visual inspection of finished modules: The complete product specific flow includes a functional test of each product as part of the acceptance process. The functional testing program is developed by LXT based on test specification and electrical parameters/limits provided by

the client. The testing program is integrated in the test environment of LXT. No sensitive information should be included in those test specifications.

Warehousing and dispatch of finished modules: LXT 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 time cost must be organized by the client. Based on the alert the client will be provided the information such as the shipment details and express tracking number that is used for the verification while the reception of the products.

Scrap storage and its secure handling: Both the defective or rejected products and chips will be securely stored and disposed regularly by this site or sent back to the client (as per client request).

Product security flaw collection, verification, correction and corrective action delivery: Product security flaw will be reported, collected, verified, corrected and the correction action will be delivered to client.

8.3 Objectives Rationale

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

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

Security Objective	Threats and OSPs
O.Acceptance-Test	P.Accept-Product, T.Accidental-Change,
O.Alarm-Response	T.Rugged-Theft, T.Smart-Theft, T.Unauthorised-Staff
O.Config-Control	P.Config-Control, P.Organise-Product, P.Accept-Product
O.Config-Items	P.Config-Control, P.Config-Items, P.Product-Transport, T.Accidental-Change
O.Config-Process	P.Accept-Product, P.Config-Control, P.Config-Process, P.Organise-Product, T.Accidental-Change
O.Control-Scrap	P.Zero-Balance, T.Staff-Collusion, T.Unauthorised-Staff
O.External-Delivery	P.Product-Transport, T.Attack-Transport
O.Internal-Monitor	P.Zero-Balance, T.Computer-Net, T.Rugged-Theft, T.Smart-Theft, T.Staff-Collusion, T.Unauthorised-Staff
O.Logical-Access	P.Config-Control, P.Organise-Product, T.Accidental-Change, T.Computer-Net, T.Unauthorised-Staff

O.Logical-Operation	P.Organise-Product, T.Computer-Net, T.Unauthorised-Staff
O.Maintain-Security	T.Computer-Net, T.Rugged-Theft, T.Smart-Theft, T.Staff-Collusion, T.Unauthorised-Staff
O.Physical-Access	T.Accidental-Change, T.Rugged-Theft, T.Smart-Theft, T.Unauthorised-Staff
O.Reception-Control	P.Config-Control, P.Config-Items, P.Reception-Control
O.Security-Control	T.Rugged-Theft, T.Smart-Theft, T.Unauthorised-Staff
O.Security-Documentation	T.Computer-Net, T.Rugged-Theft, T.Smart-Theft, T.Staff-Collusion, T.Unautorised-Staff
O.Staff-Engagement	P.Zero-Balance, T.Accidental-Change, T.Computer-Net, T.Staff-Collusion, T.Unauthorised-Staff
O.Transfer-Data	P.Product-Transport, T.Attack-Transport, T.Staff-Collusion
O.Zero-Balance	P.Zero-Balance, T.Accidental-Change, T.Unauthorised-Staff
O.Flaw-Remediation	P.Flaw-Remediation

TABLE 7 OBJECTIVES RATIONALE

O.Security-Documentation

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

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

O.Physical-Access

The production site is operated by LXT. The site is separated into different security levels. The production site is monitored by security staff on duty and surveillance cameras at production times.

The building can only be entered presenting a company badge or visitor's badge to the card readers at the entrance. All employees and visitors have to wear their badges visible at any time.

The access to the production area is secured by full height turnstile with card readers. Access to the production area requires special permissions. It is ensured by policy that either no staff is present in the production area or at least two staff members are present in the production area. Since production area is 24/7, this area is never empty of personnel. For delivery of production material and goods into and from the production area special entrance systems are used which ensures that only material can get into the production area or out from the production area, but no persons can enter or exit the area via this system.

All access doors to high secure areas are monitored by surveillance cameras at all times. The outer area of the building is monitored by surveillance cameras. Emergency exits are also monitored by surveillance cameras.

All access attempts at any entrance at all locations named above will be recorded by the security staff.

Smart Card Products which are not in the process of production are stored in a specially secured area. The warehouse, which is the primary storage location, is beside the production area. Access to the warehouse is controlled by card readers and special permissions for this area. It is ensured by technical means that at least 2 people are present in the area or no one is present in this area.

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

O.Security-Control

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

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

O.Alarm-Response

Several alarm and detection sensors are installed to provide a warning system for entering the premises by T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff. Security staff will start to investigate any alarm immediately.

O.Internal-Monitor

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

The monitoring and protection of the IT system (including network) is handled by the IT department under supervision of the security manager.

These measures prevent T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion and promote the enforcement of P.Zero-Balance.

O.Maintain-Security

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

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

O.Logical-Access

The IT network is logically separated from the outside world by a firewall which ensures that only authorised connections from and to the IT network are possible. The firewall secures the communication between external network with internal network and at the same time manages the internal communication by implementing logical network segmentation.

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

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

The production network is additionally separated from the rest of LXT internal network.

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

O.Logical-Operation

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

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

O.Config-Items

All configuration items are identified by a unique revision number by the configuration management system. By this method, different products can be identified. By this the threat T.Accidental-Change is countered and the OSPs P.Config-Items, P.Config-Control and P.Product-Transport are addressed.

O.Config-Control

The application of released procedures for the setup of the production process for each product and the controlled introduction of changes ensures a production according to clients' specifications. Procedures for setting up the production process as well as changes to the initial setup are done only by authorised personnel. The production process is supported by automated systems. By this the OSPs P.Organise-Product, P.Accept-Product and P.Config-Control are addressed.

O.Config-Process

Configuration items are stored in the configuration management system according to the site's configuration management plan. By this the OSPs P.Accept-Product, P.Config-Control, P.Config-

Process and P.Organise-Product are addressed. Because an authorized configuration process is defined, T.Accidental-Change can be addressed in terms of less potential flaw caused by unauthorized operation process.

O.Acceptance-Test

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

O.Staff-Engagement

All employees working at the site and having access to sensitive information or data have to sign a non-disclosure agreement to provide legal liability to protect sensitive information against disclosure. In addition, all employees are trained regarding security to support the security awareness. All employees have to pass a security check before they are hired. These measures prevent T.Accidental-Change, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion. Staff engagement can also facilitate the enforce of OSP P.Zero-Balance.

O.Zero-Balance

Automated means and/or the application of a 4-eye-principle ensures a continuous tracking of Smart Card Products during the whole production process. By this the OSP P.Zero-Balance is addressed and in addition, the threat T.Accidental-Change and T.Unauthorised-Staff are covered.

O.Reception-Control

Upon reception of an item an immediate incoming inspection is performed. Identification is performed if necessary (i.e. requested by the client; the client has to provide information how to identify the item). In case items are shared by a shared configuration management system between different sites or shared network drives, authenticity is implicitly assumed.

Upon reception of an electronic item relevant to security from a different site, authenticity of this item is verified (e.g. verification of a PGP signature when sent via email).

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

O.External-Delivery

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

O.Transfer-Data

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

O.Control-Scrap

At this site sensitive documentation is destroyed and electronic media is erased.

Scrap (Smart Card modules) is securely sent back to the client or is stored and handled in a secure way in order to avoid any material could be accessible from the personnel in the company. By this no employee could get uncontrolled access to scrap which might be helpful to support an attack. This prevents T.Unauthorised-Staff, T.Staff-Collusion and covers P.Zero-Balance.

O.Flaw-Remediation

The written procedure and appointed responsible for collecting, tracking and handling any reported security flaw can ensure P.Flaw-Remediation is covered.

8.4 SAR Rationale

The Security Assurance Requirements rationale does not explicitly address the developer action elements defined in (CC-PART3) because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the preparation for the site visit. In addition, this includes that the procedures are applied as written and explained in the documentation.

8.4.1 ALC_CMC

The security assurance requirements of the assurance component "ALC_CMC.5" are suitable to support the production of complex products due to the formalized acceptance process and the automated production support. This comprises the identification of all configuration items and the automated control and tracking within an industrialized production process. The requirement for authorized changes and separate roles for operation and release support the integrity and confidentiality required for the products. Therefore, this assurance level meets the requirements for the configuration management.

8.4.2 ALC_CMS

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

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 PP-0084 (PP-0084) requires this protection for sites involved in the life-cycle of Security ICs development and production.

8.4.4 ALC_LCD

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.

8.4.5 ALC_FLR

The chosen assurance level ALC_FLR.1 of the assurance family “Flaw Remediation” is suitable to support the flaw remediation procedures. This comprises the reported security flaws can be collected, tracked and handled with a predefined written procedure. The defined written procedure and the appointed responsible can potentially support preservation of the integrity and confidentiality of the products. Therefore, this assurance level meets the requirements for flaw remediation.

8.5 Assurance Measure Rationale

O.Acceptance-Test

ALC_CMC.5.6C requires that the CM system shall support the production of the product by automated means. ALC_CMC.5.9C requires that the CM system shall support the audit of all changes to the configuration items by automated means, including the originator, date, and time in the audit trail.

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

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

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Alarm-Response

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation including the initialization in its development and production environment.

ALC_DVS.2.2C requires the justification of necessary level of protection is provided. Thereby this objective contributes to meet the Security Assurance Requirement.

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 that the CM system provides automated measures so that only authorized changes are made to the configuration items. ALC_CMC.5.4C and ALC_CMC.5.8C 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.5.6C requires the CM system to support the production of the intended TOE by automated means. ALC_CMC.5.9C requires the support of audit information for all changes to the intended TOE by automated means including the originator, date and time. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a change given to a configuration item. ALC_CMC.5.11C requires that all the production related data used to generate the modules can be identified. 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 intended TOE. ALC_CMC.5.15C requests evidence demonstrating that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires evidence of configuration items being operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, 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. The objective meats the set of Security Assurance Requirements listed here.

O.Config-Items

ALC_CMC.5.1C 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.5.2C. In addition, ALC_CMC.5.4C and ALC_CMC.5.8C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.10C requires an automated means is provided to identify affected configuration items by the change of a given configuration item. ALC_CMC.5.11C requires that all the production related data used to generate the intended TOE can be identified. ALC_CMC.5.14C requires a procedure is in place to accept modified or newly created configuration items. 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 addresses the same requirement as ALC_CMC.5.4C. ALC_CMS.5.3C requires that developer of each configuration item shall be indicated. The objective meets the set of Security Assurance Requirements.

O.Config-Process

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. ALC_CMC.5.4C requires configuration items shall be uniquely identified. 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.5.7C requires that the person or team accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.8C requires CM system shall identify configuration items comprising the TSF. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a change given to a configuration item. ALC_CMC.5.11C requires that all the production related data used at the site can be identified. ALC_CMC.5.12C requires a CM documentation that 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 intended TOE. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the intended TOE. ALC_CMC.5.15C requires evidence that configuration items being maintained under the CM system. ALC_CMC.5.16C requires that evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.

The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C and ALC_CMC.5.8C. 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 intended TOE. The objective meets the set of Security Assurance Requirements.

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 intended TOE design and implementation. ALC_DVS.2.2C justify the security measures are sufficient. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.External-Delivery

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

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.Internal-Monitor

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

O.Logical-Access

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design, implementation and in its development and production environment. ALC_DVS.2.2C justify the

security measures are sufficient. Thereby this objective is suitable to meet the Security Assurance Requirement. 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 objective contributes to meet the Security Assurance Requirement.

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 intended TOE design, implementation and in its development and production environment. Thereby this objective contributes to meet the Security Assurance Requirement. 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 intended TOE. Thereby this objective is suitable to meet the Security Assurance Requirement. 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 objective contributes to meet the Security Assurance Requirement.

O.Maintain-Security

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 intended TOE. 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 intended TOE design and implementation in its development and production environment. Thereby this objective contributes to meet the Security Assurance Requirement.

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 intended TOE design and implementation in its development environment. ALC_DVS.2.2C justify the security measures are sufficient. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Reception-Control

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.4C and ALC_CMC.5.8C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.7C requires that the person accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.10C requires an automated means is provided to identify affected configuration items by the change of a given configuration item. ALC_CMC.5.11C requires that all the production related data used to generate the modules can be identified. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the intended TOE. ALC_CMC.5.15C requires the evidence demonstrating that all configuration items are being maintained under the CM system.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_DVS.2.1C requires that the developer shall describe all security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation. ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the intended TOE during the transfer between sites. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Security-Control

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development and production environment. ALC_DVS.2.2C justify the security measures are sufficient. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Security-Documentation

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

O.Staff-Engagement

ALC_DVS.2.1C requires the description of personnel security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment. ALC_DVS.2.2C justify the security measures are sufficient. Thereby the objective fulfils this combination of Security Assurance Requirements.

O.Transfer-Data

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

O.Zero-Balance

ALC_CMC.5.6C requires that the CM system supports the production of the intended TOE by automated means. ALC_CMC.5.15C requires the evidence can demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires evidence demonstrating that the CM system is operated in accordance with the CM plan. ALC_DVS.2.2C requires security measures that are necessary to protect the confidentiality and integrity of the intended TOE. ALC_LCD.1.2C requires control over the development and maintenance of the intended TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Flaw-Remediation

ALC_FLR.1.1C requires procedures used to track all reported security flaws in each release of the production lot shall be provided. ALC_FLR.1.2C requires a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw. ALC_FLR.1.3C requires corrective actions be identified for each of the security flaws. ALC_FLR.1.4C requires the methods used to provide flaw information, corrections and guidance on corrective actions to finished good receiver. Therefore, this objective is suitable to meet the Security Assurance Requirement.

8.6 Mapping of the Evaluation Documentation

The scope of the evaluation according to the assurance class ALC comprises the processing and handling of security products and associated data as well as the complete documentation of the site provided for the evaluation.

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

9 Bibliography

CC-PART1 Common Criteria. Common Criteria for Information Technology Security Evaluation; Part 1: introduction and general model

Version 3.1; Revision 5. April 2017.

CC-PART3 Common Criteria for Information Technology Security Evaluation; Part:3 Security assurance components

Version 3.1; Revision 5. April 2017.

CC-CEM Common Methodology for Information Technology Security Evaluation; Evaluation methodology

Version 3.1; Revision 5. April 2017.

PP-0084 Eurosmart. Security IC Platform Protection Profile with Augmentation Packages

Version 1.0. BSI-CC-PP-0084-2014.

CC-SDG Common Criteria. Common Criteria Supporting Document Guidance; Site Certification

Version 1.0; Revision 1. October 2007. CCDB-2007-11-001.

LXT-CMC Configuration Management System Usage Procedure

Rev 0.15

LXT-CMS Configuration List Site Certification LXT

Rev 2.8

LXT-DVS Development Security Policy

Rev 0.20

LXT-LCD Lifecycle Definition Document

Rev 0.7

LXT-FLR Flaw Remediation Procedure Document

Rev 0.5

CC-MSSR Joint Interpretation Library. Minimum Site Security Requirements

version 3.1 December 2023.