Site Security Target Lite LINXENS SINGAPORE CHANGI SITE

Author	Reviewer	Approver
Corentin Boe	Michael Tan	Chunleng Tan

Revision Control

Revision	Date	Description
0.1	10/08/2021	First document release
0.2	10/12/2021	Section 5.1.2 added
0.3	20/01/2023	Minor changes
0.4	10/10/2023	Update for extension
0.5	02/01/2024	Minor changes
0.6	26/05/2025	Add remote management possibility
0.7	24/10/2025	Added Packing room and R&D Cal lab in the Physical scope

Contents

1 Document Information

1.1 SST Reference

Title: Site Security Target Lite LINXENS SINGAPORE CHANGI SITE

Revision: 0.7

Date: 24/10/2025

Company: LINXENS SINGAPORE PTE LTD

Name of the site: LINXENS SINGAPORE CHANGI SITE

Product Type: Security IC

Evaluation Assurance Components: ALC_CMS.5, ALC_CMC.5, ALC_DVS.2 and ALC_LCD.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 (SST) refers to the following site:
LINXENS SINGAPORE CHANGI SITE
This site performs security chips packaging and testing activities, as well as initialization and pre-personalization activities for OS loading.
Initialization is a generic term and may include sub processes like OS Loading, Applet loading and Pre-Personalization. Due to the blur boundaries between those processes and due to the different nomenclature of the script providers, Linxens decided to summarize those processes into one process called “initialization”.

2.1 Identification of the Site

The LINXENS SINGAPORE CHANGI SITE (LXS) site is located at:

BLK 22, CHANGI NORTHWAY,
SINGAPORE
498810
SINGAPORE

2.2 Site Description

2.2.1 Physical Scope

The Linxens Changi Singapore site (LXS) is located on a fenced and guarded campus that is owned by Linxens Singapore Pte ltd and is not shared with other companies, which contains several buildings. CCTV controls the perimeter of the building in the scope of the evaluation and the access control to the building is by means of an employee badge (one-factor authentication). Tailgating is prevented by means of a turnstile on the building entrance. Several detections and stop mechanisms are implemented, such as physical access control mechanisms, CCTV (on the perimeter, entrance and corridors within the building) and alarms to guarantee the security of the LXS premises.
Relevant secure areas in the scope of the evaluation (concerning the production activities or guaranteeing the security of such activities), which are located on several mentioned buildings, are the following:

- Blk 24 building:
  - Workshop: Production, electrical testing, OS and Applet loading Area (level 1)
  - Wafer Storage Room (level 2)
  - Secure HSM Room (cryptographic key management area) (level 1)
  - Security IT Rooms (level 2).
  - Security systems (Access control + CCTV) room (level 2).
  - Packing room
  - R&D Cal lab

- Blk 22 building:
  - Security IT room for Firewall server (level 2)
- Security Guard house (located on the campus entrance)

Additional security mechanisms are implemented for the secure areas such as two-factor access control (by means of an employee badge and PIN) or two employee badges and PIN to enforce four-eyes principle, dedicated CCTV monitoring the activities conducted inside the secure areas and intrusion alarms. Only authorized employees can access the secure areas on a need-to-know principal basis.

2.2.2 Logical Scope

The following services and/or processes provided by Linxens Singapore Pte Ltd (LXS) are considered under the scope of this evaluation.

- Secure reception, identification, registration and storage of Smart Card wafers
- Assembly into Modules (Production includes the following steps: Die Bonding, Wire Bonding, Encapsulation, Inspection and Electrical Testing which does the functional testing of module to ensure is passed in Electrical testing)
- Secure delivery (internal shipment) of Smart Card wafers/modules.
- Cryptographic Key management (The key management is only performed in order to open a secure channel with the IC to load the initialization data.)
- Secure reception, storage, loading of the initialization data (COS and Applet) for Smart Card Products
- Secured storage of scraps and secured handling of offsite destruction.

All these services are performed in LXS site considering the proper level of physical and logical security measures to guarantee the confidentiality and integrity of the data generated and the manufactured physical assets.

To perform these activities the site uses the Linxens Mantes provided and managed the IT-infrastructure. Locally available IT equipment like workstations or VPN routers may be also provided and managed by Linxens Mantes.

It is assumed that product certifications, which will refer to this Site Security Target, will be related to a Target Of Evaluation that follows a TOE life-cycle. The LXS site covers:

- Phase 4: Security IC packaging, testing and pre-personalization
- Phase 5: Composite Product Integration

For more detailed information, refer to the ''Lifecycle Definition Document'' document (LXS-LCD).

Note: For better understanding, the term "key management" will be used along this document to refer to the cryptographic key related services provided by the site and considered under the scope of this evaluation.

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** and the following CC assurance components are covered:

ALC_CMC.5, ALC_CMS.5, ALC_DVS.2 and ALC_LCD.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) (Section 4.3) 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 (e.g., access control). These security problems are described in terms of Organizational Security Policies (OSPs).

4.1 Assets

The following section describes the assets handled at the site.

4.1.1 IC Assembly

Security is concerned with the protection of assets. Internal documentation and data at this site are relevant to maintain the confidentiality and integrity of an intended TOE, including 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 the correct operation of machines and tools based on regular maintenance and calibration. The assets are related to the production of security wafers as follows.

- Sawn wafer
- Unfinished Module
- Finished products as modules
- Scrap wafers and rejects

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

4.1.2 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.

This includes:

- The sensitive data generated during the key management processes (e.g., logs). The confidentiality and integrity of this asset must be protected.
- The non-sensitive data generated during the modules production (e.g., number of modules rejected). The integrity and availability of this asset must be protected.

4.1.4 Cryptographic keys

Cryptographic keys needed to authenticate the chips, which stored in encrypted form in HSM server, or the keys received from customer with encrypted PGP keys.

4.1.5 Pre-personalization/configuration/Initialization data

This includes the sensitive data used during pre-personalization/configuration/initialization (e.g., OS loading/patch scripts, Applet, Test software, etc). The confidentiality, authenticity and integrity of this asset must be protected.

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 (see PP-0084). However, during the production, test and assembly of 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 defective 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 large amount of time that can be spent by such the attacker to prepare the attack will impose a 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 (or its parts) during 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

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

Such accidental changes can include the modification of configurations for tools that may have an impact on the intended TOE, or misuse of the tools during production. Other examples could be

production machine failures or mixed products during production among operators that are responsible for products of different clients or different products of the same client. This also includes the disposal of sensitive products using the simple “trash” procedure and not the controlled secure handling of the defective sensitive products.

T.Unauthorized-Staff

Employees or subcontractors are not authorized to get access to products or systems used for production, or get access to products or affect production systems, so that the confidentiality and/or the integrity of the product could be impaired. This can apply to any intended TOE (or its parts) in production.

Also, other subcontractors like cleaning staff or maintenance staff for the building get limited access that may allow them to plan and conduct an attack. The secure handling of defective equipment and/or intended TOE (or its parts) 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 bribery.

T.Attack-Transport

An attacker might try to get information or products during the external delivery to client. 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 the intended TOE production.

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. All the OSPs described below shall be enforced by the Security Objectives of the site.

The evaluation of the security documentation of the site is maintained by the configuration management system. This comprises all site procedures and policies regarding the intended TOE production, quality inspection, tests, assembly control 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, modified or used at the site as well as the received, transferred and/or provided new 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 receiving, and

then each item is assigned with an internal unique identifier. 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 accessible by authorized personnel. Automated systems shall support the configuration management and ensure access control and 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 security documentation with the process descriptions and the security measures of the site are maintained by a version control system. Control measures are in place to ensure that the defined procedures for the documentation and production management are followed. 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 other 3rd party production data processing systems. This comprises also service levels and quality parameters.

P.Reception-Control

The inspection of incoming items (logical or physical) 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 specifications agreed with the client. The acceptance process is supported by automated means. Production records are generated during the acceptance process of the configuration items. Thereby, it is ensured that the properties of the product are ensured when the products are in the 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 defective assets are securely stored by this site.

The policy covers the packing and shipment of products at the site after the applied production flow. All finished products are returned to the clients that provided the items or sending the products to the specific locations requested by the clients. This is considered as an internal shipment to the client (not the end user).

P.Product-Transport

Technical and organizational measures shall ensure the correct labelling of the product. A controlled external delivery to client (not the end user) shall be applied. The transport supports traceability up to therecipient. In the case that the product needs to be moved within the building, this will be considered as internal transportation.

P.Organize-Product

The production process is applied as specified by the site's configuration management plan. If the production data includes sensitive items like cryptographic keys or configuration data, appropriate security measures must be applied. This includes the requirement that the knowledge of cryptographic keys shall be split to at least two different persons. Furthermore, technical measures like crypto-boxes, separation of network, split access permission and secure storage shall be implemented for this kind of sensitive production data.

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. This is reflected by the assumptions that must be defined for the site, even though the assumptions lay outside of the evaluation scope. Therefore, any assumptions made are considered to be satisfied (i.e., true) during the evaluation. Assumptions provide a basis for an appropriate production process setup to ensure secure handling and storage of all configuration items related to the intended TOE production.

The processing at LXS 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 (products, specifications, guidance for assembly, initialization and/or COS/Applet upload, test requirements, bond plans, initialization data, upload packages, etc.) received by the site shall be appropriately labelled to ensure the correct identification of the configuration items received from the client.

A.Prod-Specification

The product developer must provide appropriate specification and guidance for the assembly and testing of the product. This comprises configuration management plan for an appropriate assembly process as well as test requirements and test parameters for the development of the functional tests or finished test programs appropriate for the final testing. If the initialization process and/or card operating system/applet upload is conducted by the site, further guidance for the initialization and/or COS/Applet upload and data must be provided by the client. 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 behavior of the chips based on insufficient operational condition or any command sequence generated by an attacker or by accident.

A.Init-Data

Devices that are initialized at Linxens must support the integrity control of the initialization data during the initialization process by itself. The client must provide the initialisation data, scripts and requirements in case they are not developed by Linxens.

A. Inherit-secure-IT

The local IT test equipment is connected to a secure remote IT Infrastructure through a secure (encrypted) network connection.

The test equipment, the remote secure IT-infrastructure and the secure connection to it will satisfy all relevant ALC requirements and are provided and managed by Linxens.

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 levels (level 1 to level 3) of physical access control rights, which are mapping to the controlled areas, security areas and high-security areas of the site. The access control measures ensure that only registered employees and vendors can access restricted areas. Sensitive products are handled in restricted areas only.

O.Security-Control

Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like video monitoring, motion sensors and similar kind of sensors support the enforcement of the physical 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 activated before an unauthorized person gets access to any sensitive configuration items (assets). After the alarm is triggered, the unauthorized person must be hold back by other security measures. The reaction time of the employees or guards must be short enough to prevent the 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 and uninterrupted 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 operation machines 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/hardware updates/upgrades, security patches and virus protection). The backup of sensitive data and security relevant logs is applied and protected according to the classification of the original data.

O.Config-Items

The site has configuration management systems that assign a unique internal identifier to each product/item to uniquely identify configuration items and allow their tracking and traceability. In addition, the internal security procedures and guidance are covered by the configuration management systems.

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 ships the outgoing configuration items that fulfil the specified properties. Parameter checks, functional and/or visual checks inspection, and quality tests as specified by the clients are performed to ensure the release product is compliant with the client specifications. The test results are logged to support tracing and the identification of the product failures.

O.Staff-Engagement

All employees who have access to intended TOE parts (or its parts), and who can move TOE (or its parts) out of the production areas are thoroughly checked for the security violations and must sign a non-disclosure agreement. Furthermore, all employees in the production areas 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 acknowledgement is applied during shipment of the functional chips. According to the agreed production flow, the defect chips will be handled as scrap. All the production stages of sensitive product are managed though 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/parts are under sufficient control.

O.Reception-Control

Upon reception of the incoming items (e.g. raw materials, guidance, OS image and related materials), 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 sender of a physical configuration item is identified by the assigned client address. The sender of an electronic configuration item (e.g. initialization data, response data) can be identified in different ways (e.g., certificates, public keys). The specific way is defined in the procedure of external delivery to/from a client (not the end user). The external delivery procedure is applied to all sensitive configuration data or items. The recipient of shipment can only be changed by a controlled process and authorization is required. The packaging (if any) is also part of the defined process and applied as agreed with the client. The approved couriers support the tracking of sensitive configuration data or items during external delivery. For every configuration data or item, the integrity and authenticity security measures are defined (if necessary) to protect the product against manipulation/alteration/forging.

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 authorized 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 authorized 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 security measures in place to destroy sensitive documentation/items/media and securely erase electronic data media, so that the data cannot be used in any meaningful way to impair confidentiality of the TOE. The defective and rejected products are stored securely until the secured destruction.

O.Organize-Product

For the configuration, pre-personalization or initialization process, it is ensured that the specified process is applied. The data integrity is controlled. Keys and other sensitive data can only be constructed by at least two employees. The operation is applied in crypto-boxes or similar devices. The specific measures are applied to protect the memory containing loaded OS in the product. After the release process changes are only applied based on the request of the client. The update is done according to a controlled process.

5.1 Security Objectives Rationale

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

Note that the assumptions defined in this SST 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	The combination of these security objectives allows to detect unauthorized access to the

	O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement	internal network and provide an appropriate response to the threat.
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 products related items and avoid accidental changes.
T.Unauthorized-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 O.Organize-Product	Physical, logical and organizational access control and policies limits the access to sensitive data and or products/product related items to authorised persons.
T.Staff-Collusion	O.Security-Documentation O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Transfer-Data O.Control-Scrap	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees prevent unauthorized access to the sensitive data or items.
T.Attack-Transport	O.External-Delivery O.Transfer-Data	The combination of these security objectives avoids obtaining sensitive data and/or items during its shipment/transmission.
P.Accept-Product	O.Acceptance-Test O.Config-Control O.Config-Process	On request of the client functional 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.Organize-Product	O.Logical-Operation O.Logical-Access O.Config-Control O.Config-Process O.Organize-Product	The application of the production processes is ensured and supported by technical and organizational 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 sensitive items loss occurring during production and shipment.

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.

SECURITY OBJECTIVE / THREAT, OSP	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.Organize-Product
P.Accept-Product	X		X		X														
P.Config-Control			X	X	X				X				X						
P.Config-Items				X									X						
P.Config-Process					X														
P.Organize-Product			X		X				X	X									X
P.Product-Transport				X			X										X		
P.Reception-Control													X						
P.Zero-Balance						X		X								X		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	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.Unauthorized-Staff		X				X		X	X	X	X	X		X	X	X		X	X

TABLE 2 MAPPING BETWEEN POLICIES/THREATS COVERING OBJECTIVES

5.1.2 Justification of Security Objectives mapping

T.Accidental-Change

Objectives O.Logical-Access and O.Physical-Access protect the sensitive items defined by O.Config-Items from an unauthorized physical and logical access.

O.Staff-Engagement ensures that staff with access to sensitive items are well trained and trustworthy and follow the CM plan defined by O.Config-Process.

O.Zero-Balance ensures correctness of shipment and traceability of the release products for each client.

Before shipment, O.Acceptance-Test guarantees that the release products meet 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 transportation. For electronic items, the threat is further countered 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 protect the assets of the site.

The logical security measures defined by O.Logical-Access prevent an attacker from unauthorized remote access to sensitive data. The measures defined by O.Logical-Operation ensure that the IT systems are kept up-to-date and ensure backups integrity, availability, and confidentiality.

O.Internal-Monitor ensures the periodic review of suitability/adequacy of the current protection mechanisms and their correct implementation and operation.

O.Maintain-Security requires the security checks to ensure the integrity and availability of the security mechanisms.

The measures defined by O.Staff-Engagement ensure that staff with access to sensitive items has the required skills to maintain the integrity and confidentiality of the TOE (or its parts) by the correct operation of the security measures/procedures 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 protect the assets of the site.

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

O.Internal-Monitor ensures the periodic review of suitability/adequacy of the current protection mechanisms and their correct implementation and operation. O.Maintain-Security requires the security checks to ensure the integrity and availability of the security mechanisms.

O.Alarm-Response ensures that in the event of an intrusion, the intruder will not have a sufficient amount of time to succeed the attack without being noticed by the security protection supporting forces. The facilities resistance time must exceed the reaction time of the security forces.

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 protect the assets of the site.

The measures defined by O.Staff-Engagement ensure that staff with access to sensitive items has the required skills to ensure integrity and confidentiality of the items, and to understand the risks and liabilities of supporting an external/internal attacker or acting as an attacker.

It is ensured that the required 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 the hiring process and security procedures for the terminated employees (e.g., deactivation of the user accounts, the user access rights revocation).

O.Transfer-Data ensures the integrity and confidentiality of sensitive data during transfer.

The security measures defined by O.Control-Scrap ensure that an attacker cannot get access to sensitive data from the scrap.

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, O.Physical-Access and O.Organize-Product, unauthorized staff cannot access any sensitive assets.

The threat is further countered by the additional physical and logical security measures defined by O.Security-Control, O.Logical-Operation and O.Internal-Monitor and O.Maintain-Security.

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

O.Alarm-Response ensures that in the event of an intrusion, the intruder will not have a sufficient amount of time to succeed the attack without being noticed by the security protection supporting forces. The facilities resistance time must exceed the reaction time of the security forces.

Staff attempting to deliberately or by mistake access the sensitive assets for which no authorization is granted, will be detected and prevented by the security measures defined by O.Internal-Monitor, and O.Zero-Balance. O.Staff-Engagement requires staff to be vigilant and repot any abnormal behaviors or situations.

Rejected assets will be collected before secure destruction, by measures defined in O.Control-Scrap.

P.Accept-Product

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

O.Config-Control and O.Config-Process contribute to the product quality acceptance framework necessary to enforce the policy.

P.Config-Control

Objective O.Config-Control directly enforces the policy as all the production processes are explicitly tailored for each client. O.Config-Items, O.Config-Process, O.Reception-Control and O.Logical-Access define the additional security measures and procedures to enforce the policy.

P.Config-Items

Objective O.Config-Items directly enforces the policy as all the configuration items are explicitly tailored for each client. O.Reception-Control defines the additional security procedures to enforce the policy.

P.Config-Process

O.Config-Process directly enforces the policy as it defines all the security procedures and measures (CM plan) used during the production process.

P.Organize-Product

The Security Objective O.Organize-Product defines the security procedures to enforce P.Organize-Product.

O.Config-Process ensures that a configuration management plan is in place. O.Config-Control ensures the configuration management plan is applied and followed during the product process. The security objectives O.Logical-Access and O.Logical-Operation provide the necessary security measures to protect sensitive items from an unauthorized access or modifications.

P.Product-Transport

O.External-Delivery ensures a secure external transportation of the release products. O.Transfer-Data ensures secure transfer of sensitive electronic data items. O.Config-Items ensures the correct labelling of the product.

P.Reception-Control

O.Reception-Control ensures that the reception procedures for the secure products are applied and followed.

P.Zero-Balance

O.Zero-Balance and O.Control-Scrap ensure that no sensitive items loss occurring during production and shipment. Besides, O.Internal-Monitor and O.Staff-Engagement further contribute to the policy enforcement by defining additional security measures and procedures for the access control and staff awareness.

6 Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

7 Security Assurance Requirements

The Security Assurance Requirements (SARs) for this Site Security Target are derived from the ALC (Life-cycle support) assurance class as follows:

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

The assurance requirements listed above fulfil the Minimum Site Requirements (CC-MSSR).

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

The dependencies ALC_CMS.1 is satisfied by inclusion of the hierarchically higher assurance component ALC_CMS.5.

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

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
- be securely stored
- follow the secure process of destruction (service subcontracted to a third party provider under full supervision of LXS)

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 intended TOE Manufacturer must ensure that the development and production of the intended TOE is secure so that no information is unintentionally made available for the operational phase of the intended 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 securely stored before secure destruction.

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)

By definition, the life-cycle spans the entire development environment of a TOE, and a site may only cover part of the development environment. If the site is not equal to the entire development environment, the ALC_LCD criteria must be interpreted in a way that only those life-cycle phases have to be evaluated which are in the scope of the site.

ALC_LCD addresses the requirements to a specific TOE life-cycle. However, it is the intention of the Site Certification process to evaluate life-cycle models once and use them for a couple of TOE/products under the same life-cycle model. Therefore, the life-cycle models which are intended to be used should be examined independent from a specific TOE. For this the developer shall classify the types of TOEs he is going to develop and provide clear process instruction how to define/instantiate a TOE specific life-cycle model. The evaluator focuses his examination on the developers TOE classification and the LCD process instruction.

7.2 Security Assurance Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components of (CC-PART3) to the Security Objectives defined in this SST. The refinements described above are considered. The site has a process in place to ensure an appropriate and consistent identification of intended TOE. If the site already receives configuration items, this process is based on the assumption that the received configuration items are appropriately labelled and identified, refer to A.Item-Identification. The content elements that are changed from the original CEM (CC-CEM) according to the application notes in the process description (CC-SDG) are written in italic. The term “TOE” can be replaced by “product” or “configuration items”.

7.2.1 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMC.5.1C ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*	O.Reception-Control O.Config-Items	Upon reception of an item from another site, O.Reception-Control ensures that authenticity and labelling is verified for the shipped item. All products assembled at LXS get a unique production serial number generated by a database as defined by O.Config-Items, which is linked to the client part ID. The ID assignment for all configuration items is supported by automated tracking systems.
ALC_CMC.5.2C The CM documentation shall describe the	O.Reception-Control O.Config-Items	Upon reception of an item from another site

method used to uniquely identify the configuration items.	O.Config-Control O.Config-Process	O.Reception-Control ensures that authenticity and labelling is verified for the shipped item. After integration into the CM system O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the item. In addition, configuration items are kept under configuration control by O.Config-Control. 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-Items O.Config-Control O.Config-Process	O.Config-Control and O.Config-Process ensures that the acceptance procedures are adequate and appropriate to review changes in the configuration items O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the configuration item.
ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.	O.Config-Items	O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the item.
ALC_CMC.5.5C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config-Control O.Config-Process O.Logical-Access	Configuration items are kept under configuration control by O.Config-Control. O.Config-Process provides a configured and controlled production process. O.Logical-Access ensures that access to the production network and related systems is restricted to authorized employees that work in the related area or that are involved in the configuration tasks or the production systems.
ALC_CMC.5.6C The CM system shall support the production of the TOE by automated means.	O.Config-Control O.Config-Process 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.Config-Process provides a configured and controlled production process by automated means. In addition, 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.Logical-Access O.Config-Control O.Config-Process	O.Config-Control and O.Config-Process ensures that the production process is configured and controlled following the CM plan. O.Logical-Access ensures that access to the production network and related systems is restricted to authorized employees that work in the related area or that are involved in the configuration tasks or the production systems.
ALC_CMC.5.8C The CM system shall *clearly* identify the configuration items that comprise the TSF.	O.Config-Items O.Config-Control O.Config-Process O.Reception-Control	O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the item. O.Config-Control and O.Config-Process ensures that the production process is configured and controlled following the CM plan. O.Reception-Control includes the incoming labelling and the mapping to internal identifications.
ALC_CMC.5.9C The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.	O.Config-Items O.Acceptance-Test O.Config-Control O.Config-Process	O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the item. O.Acceptance-Test provides an automated testing of the product and supports the tracing. O.Config-Control and O.Config-Process ensures that the production process is configured and controlled following the CM plan.
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 TOE 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-Process	O.Config-Process ensures that services and/or processes are controlled using a CM plan.
ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the TOE.	O.Config-Control O.Config-Process O.Organize-Product	O.Organise-Product ensures that the services and/or processes provided by the site are carried out following the procedure defined. O.Config-Control and O.Config-Process ensures that the production process is configured and controlled following the CM plan.
ALC_CMC.5.14C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.	O.Config-Items O.Config-Control O.Config-Process O.Reception-Control	O.Config-Control and O.Config-Process ensures that the production process is configured and controlled following the CM plan. In addition, O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the configuration item. O.Reception-Control ensures the correct acceptance of items when arrived to the site.
ALC_CMC.5.15C The evidence shall demonstrate that all configuration items *have been and* are being maintained under the CM system.	O.Config-Control O.Config-Items O.Reception-Control O.Zero-Balance	Configuration items are kept under configuration control according to O.Config-Control. In addition, O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the configuration item. O.Reception-Control ensures the correct acceptance of items when arrived to the site. O.Zero-Balance ensures the tracing of all security products.
ALC_CMC.5.16C The evidence shall demonstrate that the	O.Config-Process O.Config-Control	The operation of the CM system in accordance to the CM plan is ensured by O.Config-Process.

CM system is being operated in accordance with the CM plan.	O.Zero-Balance	O.Config-Control includes a release procedure as evidence. 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 The configuration list shall include the following*: the evaluation evidence required by the SARs;* and development tools and related information.	O.Config-Items O.Config-Control O.Config-Process	O.Config-Items ensures the unique identification of configuration items. O.Config-Control and O.Config-Process define the configuration management for products, procedures and processes. Note: Since the process is subject of the evaluation no products are part of the configuration list.
ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.	O.Config-Items O.Config-Control O.Config-Process	O.Config-Items ensures the unique identification of configuration items. O.Config-Control and O.Config-Process defines the configuration management for products, procedures and processes.
ALC_CMS.5.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	O.Config-Items	Subcontractors are not involved in the production process. 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	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation	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.

are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment *and provide evidence that these security measures are followed during the development and maintenance of the TOE*.	O.Staff-Engagement O.Maintain-Security O.Control-Scrap O.External-Delivery O.Security-Documentation O.Transfer-Data O.Zero-Balance	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. O.Zero-Balance ensure that no unauthorised access to products is possible for an attacker.
ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Control-Scrap O.External-Delivery O.Security-Documentation O.Transfer-Data O.Zero-Balance O.Internal-Monitor O.Acceptance-Test O.Reception-Control	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. O.Security-Documentation ensures that the security documentation is in agreement with the security measures implemented on site. The associated control and continuous justification is subject of the O.Internal-Monitor and O.Acceptance-Test. O.Transfer-Data support the confidentiality and integrity of sensitive data during its transmission. The identification of received products is defined by O.Reception-Control.

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 to develop and maintain the TOE.	O.Config-Control O.Organize-Product	The process used for identification and manufacturing are covered by O.Config-Control and O.Organize-Product.
ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	O.Acceptance-Test O.Config-Process O.Zero-Balance O.Organize-Product	The site does not perform development tasks. The applied production process is controlled according to O.Config-Process and O.Organize-Product, the finished products 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

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.

The client must provide the data for pre-personalization/configuration/initialization and the product must support the integrity control of these data.

The client provides a method of unique identification for all items shipped to the site.

The client provides appropriate information for the delivery of produced goods as well as electronic data to be delivered. This information shall at least comprise address data for physical items.

The self-protection features of the Smart Card modules to be produced are fully operational during production.

The IT infrastructure consists of local and remote equipment connected using an encrypted connection. Linxens provides, configures and maintains the local workstations and firewalls/router (used for the encrypted connection) and all remote equipment such that they are secure.

8.2 Services of the Site

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

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

Functional testing and visual inspection of finished modules: The complete production specific flow includes a functional test of each product as part of the acceptance process. The functional testing program is developed by LXS based on test specifications and electrical parameters/limits provided by the client. The testing program is integrated in the test environment of LXS. No sensitive information or data should be included in those test specifications.

Warehousing and shipment of finished modules: LXS has a standard procedure for packing of finished products and preparation for shipment using protective materials. If special packing requirements are provided by the client, they are included in the process setup. The client is informed if products are ready for shipment because the transportation time and cost must be planned and covered by the client. The client will be provided the information such as the shipment details and express tracking number that are used for the shipment package identification and verification at the reception on the client side.

Cryptographic Key management (the key management is only performed in order to open a secure channel with the IC to load the OS.) for pre-personalization.

Secure reception, storage, loading of the initialization data (COS and Applet) for Smart Card Products.

Scrap and rejects storage, and their secure handling: Both the defective or rejected products and chips are securely destroyed (service subcontracted to a third-party provider under full supervision of LXS).

8.3 Objectives Rationale

The following rationale provides a justification that shows that all threats and organizational 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.Unauthorized-Staff
O.Config-Control	P.Config-Control, P.Organize-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.Organize-Product, T.Accidental-Change
O.Control-Scrap	P.Zero-Balance, T.Staff-Collusion, T.Unauthorized-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.Unauthorized-Staff
O.Logical-Access	P.Config-Control, P.Organize-Product, T.Accidental-Change, T.Computer-Net, T.Unauthorized-Staff
O.Logical-Operation	P.Organize-Product, T.Computer-Net, T.Unauthorized-Staff

O.Maintain-Security	T.Computer-Net, T.Rugged-Theft, T.Smart-Theft, T.Staff-Collusion, T.Unauthorized-Staff
O.Physical-Access	T.Accidental-Change, T.Rugged-Theft, T.Smart-Theft, T.Unauthorized-Staff
O.Reception-Control	P.Config-Control, P.Config-Items, P.Reception-Control
O.Security-Control	T.Rugged-Theft, T.Smart-Theft, T.Unauthorized-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.Unauthorized-Staff
O.Transfer-Data	P.Product-Transport, T.Attack-Transport, T.Staff-Collusion
O.Zero-Balance	P.Zero-Balance, T.Accidental-Change, T.Unauthorized-Staff
O.Organize-Product	P.Organize-Product, T.Unauthorized-Staff

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.Unauthorized-Staff and T.Staff-Collusion.

O.Physical-Access

The production site is operated by LXS. 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 (warehouse). The warehouse, which is the primary storage location, is inside 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 unauthorized person and therefore prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Unauthorized-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.Unauthorized-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.Unauthorized-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.Unauthorized-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.Unauthorized-Staff, T.Staff-Collusion.

O.Logical-Access

The IT network is logically separated from the outside world by a firewall which ensures that only authorized 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 LXS internal network.

These measures prevent T.Computer-Net, T.Accidental-Change and T.Unauthorized-Staff and support the OSPs P.Config-Control and P.Organize-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 unauthorized modification and disclosure.

These measures prevent T.Computer-Net and T.Unauthorized-Staff and support the OSP P.Organize-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 authorized personnel. The production process is supported by automated systems. By this the OSPs P.Organize-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.Organize-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.Unauthorized-Staff and T.Staff-Collusion. Staff engagement can also facilitate the enforcement 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.Unauthorized-Staff are covered.

O.Reception-Control

Upon reception of an electronic item relevant to security from a different site, authenticity of this item is verified (e.g., verification of a PGP signature when sent via email). Identification is performed if necessary (i.e., requested by the client; the client has to provide information how to identify the item). In case items are shared by a shared configuration management system between different sites or shared network drives, authenticity is implicitly assumed. By this the OSPs P.Config-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. 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 unauthorized 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.

Scraps (Smart Card modules) are destroyed 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.Unauthorized-Staff, T.Staff-Collusion and covers P.Zero-Balance.

Note: The scrap physical destruction is performed by a service subcontracted to a third-party provider under full supervision of LXS. The scraps are always accompanied and supervised by two LXS employees from storage room up to their destruction.

O.Organize-Product

The development processes are defined and applied according to the site's quality management system. By this the OSP P.Organize-Product and Threat T.Unauthorized-Staff are addressed.

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) 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.

8.5 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_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.

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

Thereby this objective contributes to meet the Security Assurance Requirements.

O.Alarm-Response

ALC_DVS.2.1C and ALC_DVS.2.2C require 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.

Thereby this objective contributes to meet the Security Assurance Requirement.

O.Config-Control

ALC_CMC.5.2C requires a method used to uniquely identify the configuration items.

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

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.5.7C requires the CM system to ensure a specific acceptance procedure for configuration items.

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

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

ALC_CMC.5.11C requires that the CM system shall be able to identify the version of configuration items from which the product is generated.

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

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

ALC_CMC.5.15C and ALC_CMC.5.16C request evidence demonstrating that all configuration items are being maintained under the CM system.

ALC_CMS.5.1C requires that specific configuration items shall be included in the configuration item list.

ALC_CMS.5.2C requires that the configuration list shall uniquely identify the configuration items.

In addition, ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the product.

Therefore, the Security Assurance Requirements are suitable to meet the objective.

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.

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

In addition, ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items.

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

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.5.10C requires an automated means to identify all other configuration items that are affected by the change of a given configuration item.

ALC_CMC.5.11C requires that all the production related data used to generate the intended TOE can be identified.

ALC_CMC.5.14C requires that the CM plan describes the procedures used to accept modified or newly created configuration items.

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

ALC_CMS.5.1C requires that specific configuration items shall be included in the configuration item list.

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

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

Therefore, the Security Assurance Requirements are suitable to meet the objective.

O.Config-Process

ALC_CMC.5.2C requires a method used to uniquely identify the configuration items.

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

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

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

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

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

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

ALC_CMC.5.11C requires that the CM system shall be able to identify the version of configuration items from which the product is generated.

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

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

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

ALC_CMC.5.16C requests evidence to demonstrate that the CM system is being operated in accordance with the CM plan.

ALC_CMS.5.1C requires that specific configuration items shall be included in the configuration item list.

ALC_CMS.5.2C requires that the configuration list shall uniquely identify the configuration items.

In addition, ALC_LCD.1.2C requires control over the development and maintenance of the product.

Thereby the objective fulfils this combination 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_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the product design and implementation in its development environment.

ALC_DVS.2.2C justify the security measures are sufficient.

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

O.Internal-Monitor

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE.

Thereby this objective contributes to meet the Security Assurance Requirement.

O.Logical-Access

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

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 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 justify the security measures are sufficient.

Thereby this objective contributes to meet the Security Assurance Requirement.

O.Maintain-Security

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

ALC_DVS.2.2C justify the security measures are sufficient.

Thereby this objective contributes to meet the Security Assurance Requirement.

O.Organize-Product

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

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

In addition, ALC_LCD.1.2C requires control over the development and maintenance of the product.

Thereby the objective fulfils this combination of Security Assurance Requirements.

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.5.1C 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.

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

ALC_CMC.5.10C requires an automated means to identify all other configuration items that are affected by the change of a given configuration item.

ALC_CMC.5.11C requires that 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 demonstration that all configuration items are being maintained under the CM system.

ALC_DVS.2.2C justify the security measures are sufficient.

Thereby the objective fulfils this combination of Security Assurance Requirements.

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.

ALC_DVS.2.2C justify the security measures are sufficient.

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_DVS.2.2C justify the security measures are sufficient.

Thereby this objective is suitable to meet the combination of Security Assurance Requirements.

O.Zero-Balance

ALC_CMC.5.15C requires the demonstration 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.2.1C requires the description of personnel security measures that are necessary to protect the confidentiality and integrity of the product in its production environment.

ALC_DVS.2.2C justify the security measures are sufficient.

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

Thereby the objective fulfils this combination of Security Assurance Requirements.

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.

LXS-CMC Linxens Singapore Pte Ltd. Configuration Management System Usage Procedure

Rev 0.12

LXS-CMS Configuration List Site Certification LXS

Rev 0.23

LXS-DVS Development Security Policy

Rev 0.15

LXS-LCD Linxens Singapore Pte ltd . Lifecycle Definition Document

Rev 0.10

CC-MSSR Joint Interpretation Library. Minimum Site Security Requirements

version 3.0. February 2020.