Reference	LXS-FR-P-CC-SST LITE Rev F	Document Type	CC Documentation
Secret Level	Public	Effective Date	28/10/2025

Site Security Target

LINXENS MANTES-LA-JOLIE

SITE

Author	Reviewer	Approver
Christian ZUNINO	Corentin BOE	Alek MELIS

Revision History

Revision	Date	Description
A	29/03/2022	First document release.
B	03/06/2022	Second document release.
C	17/02/2025	Update Actor Name and change of legal entity LINXENS FRANCE **SA** to LINXENS FRANCE **SAS**
D	21/03/2025	Add new service (IT management service for other Linxens sites)
E	26/05/2025	Update after certification audit comments
F	28/10/2025	Update after certification audit comments

Contents

Tables

1 Document Information

1.1 Reference

Title: Site Security Target LINXENS MANTES-LA-JOLIE SITE

Revision: F

Date: 28/10/2025

Company: LINXENS FRANCE SAS

Name of the site: LINXENS MANTES-LA-JOLIE

Product Type: Security IC

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

2 SST Introduction

This document describes the security features and services of Linxens Mantes-La-Jolie site (a.k.a. Linxens France SAS) and therefore defines the logical and physical scope of the site.

This section is composed by the sub-section “Identification of site” and “Site Description”.

2.1 Identification of Site

The Linxens Mantes-La-Jolie (LX-MLJ) site is located at:

Linxens France SAS

37 Rue des Closeaux,

78 200 Mantes-La-Jolie,

France

2.2 Site Description

2.2.1 Site Physical Scope

The Linxens Mantes-la-Jolie (LX-MLJ) site is located on a fenced and guarded campus that is owned by Linxens France SAS and is not shared with other companies, which contains several buildings. The perimeter of the building (Bâtiment Principal C) in the scope of the evaluation is controlled by CCTV 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 LX-MLJ) premises.

The relevant secure areas in the scope of the evaluation, which are located on the first floor of the mentioned building, are the following:

- Concerning the production activities (or guaranteeing the security of such activities):
    - Workshop: Production, electrical testing, OS and Applet loading Area. Within the workshop, the following areas (with additional access control measures) are defined:
        - Wafer Storage Room
    - Secure HSM Room (cryptographic key management area)
    - Security IT Room
    - Site Security Guard Post (located on the campus entrance)
    - Scrap destruction room
    - Security systems (Access control + CCTV) room (located on the second floor of the building mentioned)
- For IT management activities:
    - Security IT Room

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 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 Site Logical Scope

The following services and/or processes provided by Linxens Mantes-la-Jolie (LX-MLJ) are considered under the scope of this evaluation:

For production activities:

- 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)
- Secure delivery (internal shipment) of Smart Card wafers/modules.
- Cryptographic Key management (secure key generation, inventory and loading) for pre-personalization
- Secure reception, storage, loading of the initialization data (COS and Applet) for Smart Card Products
- Destruction of scraps with a scrapping machine which guarantees that wafers/ICs are unusable after scrapping process

For IT management activities:

- IT management service for other Linxens sites

All these services are performed in Linxens Mantes-la-Jolie (LX-MLJ) 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.

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 LX-MLJ site covers:

- For production activities:
    - 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-FR-R-CC-LCD).

- For IT management activities:
    - These activities could be related to any or all the six phases, depending on the roles that a managed sites has in these phases, limited to IT/infrastructure tasks

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, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017 (1).
- Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017 (2).

For the evaluation, the following methodology will be used:

- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017 (3).

This SST is CC Part 3 conformant.

The evaluation of the site comprises the following assurance components:

- ALC_CMC.5
- ALC_CMS.5
- ALC_DVS.2
- ALC_LCD.1

The assurance components chosen for the SST are taken from the definition of the EAL6 package defined in (2) and they are compliant with the Protection Profile (4) and therefore suitable for future product Security IC evaluations.

The chosen assurance components are derived from the assurance level EAL6 of the assurance class "Life-cycle Support".

For the assessment of the security measures attackers with a high attack potential (AVA_VAN.5) are assumed. Therefore, the site allows evaluations of products up to EAL6.

4 Security Problem Definition

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

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

4.1 Assets

The following section describes the assets handled at the site.

- **Sensitive products:** this includes:
  - Unfinished products such as wafers and modules
  - Finished products (packaged modules)
  - Defective or rejected products

  The confidentiality and integrity of this asset must be protected.
- **Cryptographic keys**: this includes the production keys generated during the key management process and used for pre-personalization and initialization.

  The integrity and confidentiality of this asset must be protected.
- **Production data:** 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 of this asset must be protected.
- **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 and integrity of this asset must be protected.
- **Documentation:** This includes all the internal documentation related to the key management and module assembly process (such as HSM documentation or Wafer Map files) and Linxens internal policies and procedures. The integrity (and confidentiality, depending on the document classification level) of this asset must be protected.
- **Physical security objects:** this includes all physical objects (e.g. PCs, IT infrastructure, HSM, etc.) used to perform the services defined as part of the logical scope. The confidentiality and integrity of this asset must be protected.

The integrity of any machine or tool used for a different purpose than the logical scope is not considered as an asset. However, appropriate measures must be defined for the site to ensure this important condition.

4.2 Threats

All threats endanger the integrity and confidentiality of the intended TOE related items. The intended TOE protects themselves after conclusion of the personalization phase. However, during the development and production of the intended TOE, related items are vulnerable to such attacks.

Table 4.1 Threats

Threat	Description
T.Smart-Theft	An attacker tries to access sensitive areas of the site for manipulation or theft of assets. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered. In addition, the attacker may be able to use specific working clothes of the site to camouflage the intention.
T.Rugged-Theft	An experienced thief with specialized equipment for burglary, who may be paid to perform the attack tries to access sensitive areas and manipulate or steal assets.
T.Computer-Net	A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get sensitive configuration data/items or modify security relevant processes.
T.Accident-Change	An employee, contractor or student trainee may exchange products of different production lots or different clients during production by accident.
T.Unauthorised-Staff	Employees or subcontractors not authorized to get access to assets or systems used for services provided by the site so that the confidentiality and/or the integrity of the assets or systems used are violated.
T.Staff-Collusion	An attacker tries to get access to assets processed at the site. The attacker tries to get support from one or more employees through an attempted extortion or an attempt at bribery.
T.Attack-Transport	An attacker might try to get sensitive data (assets) during the shipment/transmission. The target is to compromise confidential information or violate the integrity of the assets during the shipment/transmission process to allow a modification, cloning or the retrieval of confidential information after further steps.

4.3 Organizational Security Policies

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

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

Table 4.2 Organizational Security Policies

OSP	Description
P.Config-Items	The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of items that are created, generated, developed or used at a site as well as the received and transferred and/or provided items.
P.Config-Control	The procedures for setting up the production process as well as the procedure that allows changes of the initial setup for a product shall only be applied by authorized personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The procedure for the initial set up of a production process ensures that sufficient information is provided by the client.
P.Config-Process	The services and/or processes provided by a site are controlled in the configuration management plan. This comprises tools used to carry out the services and/or processes and the documentation that describes the services and/or processes provided by a site.
P.Reception-Control	The inspection of incoming items done at the site ensures that the received configuration items comply with the properties stated by the client.
P.Accept-Product	The testing and quality control of the site ensures that the released products comply with the specification agreed with the client. The acceptance process is supported by automated measures. Records are generated for the acceptance process of the configuration items. Thereby, it is ensured that the properties of the product are ensured when they are shipped or transmitted.
P.Zero-Balance	The site ensures that all sensitive items (security relevant parts of the intended TOEs of different clients) are separated and traced on a device basis. For each hand over, either an automated or an organizational “two-employees-acknowledgement” (four-eyes principle) is applied for functional and defect assets. According to the released production process the defect assets are destroyed at the site.
P.Organise-Product	The configuration, completion or initialisation process is applied as specified by the client. Performing the initialisation is an optional production step. If the data includes sensitive items like cryptographic keys relevant for the life-cycle or sensitive configuration data that affect the security of the product, appropriate measures must be in place. This includes the requirement that the knowledge of cryptographic keys shall be split to at least two different persons. Furthermore, technical measures like crypto-boxes, separation of network, split access permission and secure storage shall be implemented for this kind of sensitive configuration data.
P.Product-Transport	Technical and organizational measures shall ensure the correct labelling of the product. A controlled internal/external shipment shall be applied. The transport supports traceability up to the acceptor. If applicable or required, this policy shall include measures for packing if required to protect the product during transport.

4.4 Assumptions

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

The following assumptions are considered to be applicable to Linxens Mantes-la-Jolie (LX-MLJ).

Table 4.3 Assumptions

Assumption	Description
A.Prod-Specification	The client must provide appropriate information (e.g. specifications, definitions, process parameters, test requirements, bond plans) in order to ensure an appropriate production process. If the initialization process and/or card operating system/applet upload is conducted, further guidance for the initialization and/or COS/Applet upload and data are delivered. If module packaging is conducted, the wafers must be delivered with appropriate marking of goods and defect devices. The provided information includes the classification of the product, documents and data.
A.Prod-Release	The client is responsible for the release of the products to be produced.
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 in the site is appropriately labelled to ensure the identification and version management of the configuration item.
A.Internal-Shipment	The recipient (client) of the future TOE is identified by the address of the client site. The address of the client is part of the product setup.
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.Product-Integrity	The self-protecting features of the products in production are fully operational and it is not possible to influence the configuration and behaviour of the devices based on insufficient operational conditions or any command sequence generated by an attacker or by accident.
A.Destruct-Scrap	Scrap configuration items are collected at the site and stored securely. Non conform products are destroyed internally.
A.Serv-Specification	The Linxens site that is being managed must store data it wishes to keep secure on the Security-Relevant System in the site network.
A.Secure_Conn	Linxens must arrange an encrypted network connection from the Mantes site to its network. This includes provisioning of an additional encryption layer from Mantes site to the other Linxens site.

5 Security Objectives

The Security Objectives are related to physical, technical and organizational security measures, the configuration management as well as the shipment of sensitive data generated from the services provided by the site.

Table 5.1 Security Objectives

Security Objective	Description
O.Security-Documentation	The security of the site is maintained according to the site's security documentation covering all physical, logical and procedural 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 supports the limitation for the access to these areas including the identification and rejection of unauthorized people. The site enforces at least two levels of access control to sensitive areas of the site. The access control measures ensure that only registered employees and vendors can access restricted areas. Sensitive data/products are handled in restricted areas only.
O.Security-Control	Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers.
O.Alarm-Response	The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any sensitive configuration item (asset). After the alarm is triggered, the unauthorized person still has to overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack.
O.Internal-Monitor	The site performs security management meetings regularly. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed at least every year to control the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure a sufficient protection.
O.Maintain-Security	Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorized employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.
O.Logical-Access	The site enforces a logical separation between the internal network and the internet by a firewall. The firewall ensures that only defined services and

	defined connections are accepted. Furthermore, the internal network is separated into a production network and an office network. Additional specific networks for production and configuration are physically or logically separated from any internal network to enforce access control. Access to the production network and related systems is restricted to authorized 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. An 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 updates, security patches, virus protection, spyware protection). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.
O.Config-Items	The site has a configuration management system that assigns a unique internal identification to uniquely identify each configuration item (product, script, COS/Applet package, etc). Also, the internal procedures and guidance are covered by the configuration management.
O.Config-Control	The site applies a release procedure for the setup of the production process (including the initialisation/upload processes) for each new product. In addition, the site has a process to classify and introduce changes for services and/or processes of released products. The services/processes can be changed by authorised personnel only. Automated systems support configuration management and production control. 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 to produce the product and the documentation that describes the services and/or processes provided by a site.
O.Acceptance-Test	The site delivers configuration items that fulfil the specified properties. Parameter checks, functional and/or visual checks and tests are performed to ensure the compliance with the specification. The test results are logged to support tracing and the identification of systematic failures.
O.Organise-Product	For the configuration, completion, pre-personalization or initialization process it is ensured that the specified process is applied. Performing the initialisation is an optional production step. The data integrity is controlled. Keys and other sensitive data can only be constructed by at least two employees. The operation is applied in crypto-boxes or similar devices. After the release process changes are only applied based on the request of the client. The update is done according to a controlled process.
O.Staff-Engagement	All employees who have access to sensitive items/data and who can move parts of the product out of the defined production flow are checked regarding security concerns and must sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.
O.Zero-Balance	The site ensures that all sensitive products (intended TOE of different clients) are separated and traced on a device basis. Automated control and/or two employees acknowledgement during hand over of sensitive items is applied

	for functional and defective products. According to the agreed production flow the defect products are destroyed internally.
O.Reception-Control	Upon reception of a physical product an incoming inspection is performed. The inspection comprises the received number of products and the identification according to the documentation of the supplier. For electronic items that require authenticity, the authenticity is verified upon reception.
O.Internal-Shipment	The recipient of a physical configuration item is identified by the assigned client address. The internal shipment procedure is applied to all configuration items. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of configuration items during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined.
O.Transfer-Data	The transmission of sensitive items/data is protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys (asymmetric) must be assigned to individuals to ensure that only authorized employees are able to extract the sensitive electronic items/data according to the procedure defined. Alternatively, symmetric keys or password-based exchange methods might be used. The keys and/or passwords are exchanged based on secure measures, and they are sufficiently protected.
O.Control-Scrap	The site has measures in place to destroy sensitive documentation and erase electronic media. Scrap is stored securely until internal secure destruction. All these measures are implemented so that an attack is not supported.
O. Exclusive-access	The only way to access the Security-Relevant System from the Linxens site network is through the encryption equipment provided by the Linxens site[1] (and vice versa).

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 include a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives.

Note that the assumptions of the SST are not used to cover any threat or OSP of the site. They are seen as pre-conditions 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

Table 5.2 Security Objectives Rationale

Threat and OSP	Security Objective	Note
T.Smart-Theft	O.Security-Documentation O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threat.

[1] See A.Secure_Conn

T.Rugged-Theft	O.Security-Documentation O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threats.
T.Computer-Net	O.Security-Documentation O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Exclusive-Access	The combination of these security objectives allows to detect unauthorized access to the internal network and provide an appropriate response to the threat.
T.Accident-Change	O.Logical-Access O.Logical-Operation O.Config-Items O.Config-Process O.Acceptance-Test O.Staff-Engagement O.Physical-Access 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.Unauthorised-Staff	O.Security-Documentation O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Control-Scrap O.Zero-Balance	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.Internal-Shipment O.Transfer-Data	The combination of these security objectives avoids obtaining sensitive data and/or items during its shipment/transmission.
P.Config-Items	O.Config-Items O.Reception-Control	All relevant items are covered by the control.

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-Process	O.Config-Process	The scope of the configuration control comprises the production process.
P.Accept-Product	O.Config-Control O.Config-Process O.Acceptance-Test	On request of the client release tests are performed.
P.Organise-Product	O.Logical-Operation O.Logical-Access O.Config-Control O.Config-Process O.Organise-Product	The application of the production processes is ensured by O.Organise-Product supported by technical and organisational means.
P.Product-Transport	O.Config-Items O.Transfer-Data O.Internal-Shipment	The controlled shipment and delivery procedures ensure correct shipment and delivery of items.
P.Reception-Control	O.Reception-Control	The incoming control on physical items ensures that only authentic items of correct quantity are accepted. The incoming control on integrity and availability of items ensures that only authentic and qualified items are accepted.
P.Zero-Balance	O.Control-Scrap O.Internal-Monitor O.Staff-Engagement O.Zero-Balance	The handling of correct and defective items ensures that no unexpected missing items or left-over items occur.

5.1.2 Mapping of Security Objectives

T.Smart-Theft

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

The site is protected with the measures defined by O.Physical-Access preventing the intruder access to the facilities. Procedures and measures defined by O.Security-Control ensures the correct operation of mechanism supporting the physical security. O.Alarm-Response ensures that in the event of an intrusion, the intruder will not have time to complete the attack without triggering the response for mitigation of the attack.

O.Internal-Monitor defines the periodic review of suitability of the current protection mechanisms and its correct implementation and execution. The maintenance measures defined by O.Maintain-Security ensure that the required level of security to prevent unauthorised access attempts is established at all times.

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

T.Rugged-Theft

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

T.Computer-Net

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

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

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

O.Exclusive-Access ensures that all communication between the Mantes site and the other Linxens site is done with an additional encryption layer. An attacker can therefore neither:

- Listen in on or manipulate the network connection between the Mantes site and the other Linxens site
- Penetrate the IT room management stations through this connection

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

T.Accident-Change

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

O.Staff-Engagement ensures that staff interacting by any means with sensitive assets are well trained (O.Config-Process) and trustworthy, and by the objective of O.Zero-Balance is prevented that by mistake any asset could be leaked between clients. Before delivering the assets, O.Acceptance-Test guarantees that the delivery meets the required criteria imposed by the client.

Therefore the combination of O.Logical-Access, O.Logical-Operation, O.Physical-Access, O.Config-Items, O.Staff-Engagement, O.Config-Process, O.Zero-Balance and O.Acceptance-Test are sufficient to cover T.Accident-Change.

T.Unauthorised-Staff

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

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

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

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

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

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

The automated control and/or two employees acknowledgement during hand over of sensitive items defined by O.Zero-Balance ensure that not a single person has access to sensitive items.

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

T.Staff-Collusion

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

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

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

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

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

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

T.Attack-Transport

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

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

P.Config-Items

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

P.Config-Control

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

P.Config-Process

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

P.Reception-Control

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

P.Accept-Product

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

P.Organise-Product

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

P.Product-Transport

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

P.Zero-Balance

P.Zero-Balance is directly enforced by O.Zero-Balance and for the defective items it is enforced by O.Control-Scrap. O.Internal-Monitor and O.Staff-Engagement also contribute to enforce P.Zero-Balance.

6 Extended Assurance Component Definition

No extended components are defined in this Site Security Target.

7 Security Assurance Requirements

Client using this Site Security Target requires an evaluation against evaluation assurance level EAL6. This Security Assurance Requirement (SAR) is also included in the Security IC Platform Protection Profile (4).

The Security Assurance Requirements (SAR) are chosen from the class ALC (Lifecycle support) as defined in (2):

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

The Security Assurance Requirements listed above fulfill the requirements of (5) because hierarchically higher components are used in this Site Security Target compared to the Minimum Requirements in (5).

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 following dependency is partially fulfilled:

ALC_LCD.1 is part of this Site Security Target but it is only partially fulfilled as the site does not cover the entire life cycle of a specific TOE.

7.1 Application Notes and Refinements

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

Refinements regarding Security Assurance Requirements as defined in CC Part 3 (2) are written in italic. The term 'TOE' is replaced by 'product' or 'configuration item'.

7.1.1 Overview and Refinements regarding CM Capabilities (ALC_CMC)

The processes of the CM system are subject of examination in ALC_CMC.

For some requirements ALC_CMC cannot be applied the way it is written, as it assumes that a site handles a specific TOE. This is not necessarily the case because the Site Certification procedure by definition allows to certify sites independently to a TOE evaluation.

There is a dependency from ALC_CMC.5 to ALC_LCD.1. The reason for this dependency is to ensure that there is a CM system in place for the entire development environment of the future TOE. To assess this knowledge of all life cycle phases (and in terms of Site Certification knowledge of all sites) and confidence that different

life-cycle phases work together correctly is necessary. But this cannot be done for a single site if the site does not represent the entire development environment.

The analysis of the life-cycle is therefore part of the splicing procedure which will be performed later on. That means the dependency from ALC_CMC to ALC_LCD is covered during the future TOE evaluation (by applying the splicing procedure) in any case.

Please note that a site which claims ALC_LCD and does not represent the whole development environment of the future TOE does not completely fulfil this dependency.

7.1.2 Overview and Refinements regarding CM Scope (ALC_CMS)

The scope of the configuration management for a site certification process is limited to the documentation relevant for the SAR as well as the development tools used for production.

7.1.3 Overview and refinements regarding Development Security (ALC_DVS)

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

The TOE Manufacturer must ensure that the development and production of the future TOE is secure so that no information is unintentionally made available for the operational phase of the future TOE. The confidentiality and integrity of pre-personalization/initialization/configuration data must be guaranteed, access to any kind of Smart Card related products and related data and documentation must be restricted to authorised persons only.

Based on these requirements the physical security as well as the logical security of the site are in the focus of the evaluation. Beside the pure implementation of the security measures also the control and the maintenance of the security measures must be considered.

The transfer/shipment of configuration items between two sites involved in the production flow is included in the scope of this evaluation and covered by the evaluation of ALC_DVS.

7.1.4 Overview and Refinements 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 Requirements Rationale

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

The site has a process in place to ensure an appropriate and consistent identification of 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 (3) according to the application notes in the process description (5) are written in *italic*. The term “TOE” can be replaced by “product” or “configuration items”.

Table 7.1 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*	O.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. After integration into the CM system O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the item.
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	Upon reception of an item from another site 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 authorised 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 *product* 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 *configuration items* 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 other configuration items that are	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

affected by the change of a given configuration item**.**		items. O.Config-Process ensures that only controlled changes are applied.
ALC_CMC.5.11C The CM system shall be able to identify the version of *configuration items* from which the *product* is generated.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	O.Reception-Control comprises the control of the incoming configuration items. O.Config-Items and O.Config-Control cover the unique labelling and management of the client configuration items. O.Config-Process ensures that only controlled changes are applied.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.Config-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 *prodution* of the *product.*	O.Config-Control O.Config-Process O.Organise-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 *product*.	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 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 *all configuration items have been and are being maintained under the CM system.*	O.Config-Process O.Config-Control O.Zero-Balance	The operation of the CM system in accordance to the CM plan is ensured by O.Config-Process. 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 7.2 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 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 7.3 Rationale for ALC_DVS.2

SAR	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the *product* design and implementation in its development environment.	O.Security-Documentation O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Control-Scrap O.Internal-Shipment O.Transfer-Data O.Zero-Balance O.Exclusive-Access	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, O.Logical-Operation and O.Exclusive-Access. 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.Internal-Shipment. 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 *product*.	O.Security-Documentation O.Internal-Monitor O.Transfer-Data O.Acceptance-Test	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-Monitoring and O.Acceptance-Test. O.Transfer-Data support the confidentiality and integrity of sensitive data during its transmission.

Table 7.4 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 *product*.	O.Config-Control O.Organise-Product	The process followed for the production process is defined in the documentation related to O.Config-Control and O.Organise-Product.
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the *product*.	O.Acceptance-Test O.Config-Process O.Organise-Product	Control over the production process is maintained by O.Config-Process and O.Organise-Product, supported by the quality assurance measures defined by O.Acceptance-Test

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.

For production activities:

- 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. 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.
- Scrap parts are stored securely in the vault until they are securely destroyed on-site.

For IT management activities:

- The Linxens site that is being managed must provide appropriate information and means in order to allow the Mantes site to provide 2nd and 3rd level IT support to the Business Unit.
- The Linxens site must arrange an encrypted network connection from the Mantes site to its network. This includes the provisioning of robust network encryption layer to the Mantes site and key management for this equipment.

8.2 Services of the site

Linxens Mantes-la-Jolie (LX-MLJ)) provides the following services for production activities:

- 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)
- Secure delivery (internal shipment) of Smart Card wafers/modules.
- Cryptographic Key management (secure key generation, inventory and loading) for pre-personalization
- Secure reception, storage, loading of the initialization data (COS and Applet) for Smart Card Products
- Destruction of scraps with a scrapping machine which guarantees that wafers/ICs are unusable after scrapping process

And provides the following service for remote IT management activities:

- IT administration. This consists of activities such as:
    - Resolving problems and responding to incidents
    - Implementing approved IT Changes
    - Implementing approved Service Request

  For the services: =

    - • Client Systems and Workplace Services
    - • Infrastructure services
    - • Network Services
    - • Monitoring Services
    - • Collaboration Services
    - • Security Services
- 1st, 2nd and 3rd line IT support to the Linxens site. This consists of activities such as:
    - Ticket creation or 1st level telephone hotline
    - Remote support 2nd and 3rd level
    - Installation of Client Operating Systems
    - Remote installation of software upgrades and patches
    - Resolving problems and responding to incidents
    - Implementing approved IT Changes
    - Implementing approved Service Request

8.3 Objective Rationale

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

Table 8.1 Security Objectives Rationale

Security Objective	Rationale
O.Security-Documentation	The security of the site is maintained according to the site security documentation covering all physical, logical and procedural measures to ensure the security of the site. These security measures are necessary to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unautorised-Staff and T.Staff-Collusion.
O.Physical-Access	Physical access permissions will be assigned on a “need to know” basis. The persons will have physical access only to the minimal extent required for performing their duties. Physical access permissions will be managed using a computerized physical access control mechanism

	Access to areas that are defined as secure or sensitive will only be assigned to persons that must have them in order to perform their duties. The access privileges will be minimized to the bare necessity. By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft, T.Accident-Change and T.Unauthorised-Staff can be prevented.
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. By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.
O.Alarm-Response	Several alarm and detection sensors are installed to provide a warning system for entering the premises by T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff. Security staff will start to investigate any alarm immediately.
O.Internal-Monitor	The security manager performs meetings with all security staff on a regular basis. During this meeting security procedures are reviewed, and corrective actions are initiated (if necessary). In case security related incident occurred since the last security meeting, they will be addressed. In addition, internal audits are performed on a regular basis to ensure the application of the security measures. The monitoring and protection of the IT system (including network) is handled by the IT department under supervision of the security manager. These measures prevent T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion and promote the enforcement of P.Zero-Balance.
O.Maintain-Security	All security related alarm and detection systems are checked on a regular basis. Logs for building access or site access as well as access to especially secured areas are stored and checked on a regular basis. Network security is monitored permanently by the IT-department. These measures prevent T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.
O.Logical-Access	The IT network is logically separated from the outside world by a firewall which ensures that only authorised connections from and to the IT network are possible. The firewall secures the communication between external network with internal network and at the same time manages the internal communication by implementing logical network segmentation. Each user has an individual account. To access data on the company's network every user must 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.

	By the combination of these measures the threats T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff and the OSP P.Config-Control and P.Organise-Product can be prevented
O.Logical-Operation	Virus protection and patch management for operating systems and applications shall ensure the correct operation of the systems and prevent the systems from malfunction. They ensure that protective measures of the IT workplaces are up to date (virus definitions, security patches of operating system, security patches of programs, etc.). In addition, regular backups are applied to prevent loss of data. Backup media are securely stored protected against unauthorised modification and disclosure. These measures prevent T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff and support the OSP P.Organise-Product.
O.Config-Items	All configuration items are identified by a unique version number by the configuration management system. By these different products can be identified. By this the threat T.Accident-Change is countered and the OSPs P.Config-Items, P.Config-Control and P.Product-Transport are addressed.
O.Config-Control	The application of released procedures for the setup of the production process for each product and the controlled introduction of changes ensures a production according to clients' specifications. Procedures for setting up the production process as well as changes to the initial setup are done only by authorised personnel. The production process is supported by automated systems. By this the OSPs P.Organise-Product, P.Accept-Product and P.Config-Control are addressed.
O.Config-Process	Configuration items are stored in the configuration management system according to the site's configuration management plan. By this the OSPs P.Accept-Product, P.Config-Control, P.Config-Process, and P.Organise-Product are addressed. Because an authorized configuration process is defined, T.Accident-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.Accident-Change is countered and the OSP P.Accept-Product is addressed.
O.Organise-Product	The development processes are defined and applied according to the site's quality management system. By this the OSP P.Organise-Product is addressed.
O.Staff-Engagement	All employees working at the site and having access to sensitive information or data have to sign a non-disclosure agreement to provide legal liability to protect sensitive information against disclosure. In addition, all employees are trained regarding security to support the security awareness. All employees have to pass a security check before they are hired. These measures prevent T.Accident-Change, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion. Staff engagement can also facilitate the enforce of OSP P.Zero-Balance.
O.Zero-Balance	Automated means and/or the application of a 4-eye-principle ensures a continuous tracking of Smart Card Products during the whole production process. By this the OSP P.Zero-Balance is addressed and in addition, the threat T.Accident-Change and T.Unauthorised-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.Internal-Shipment	Security relevant physical items are internally shipped either by security transport (e.g. sealed boxes) or in person by company's internal staff. Security relevant electronic items are internally shipped using secure communication measures. This might be signed and/or encrypted emails or similar (e.g. SSL secured web portals) or shared network systems (e.g. shared configuration management system). This prevents T.Attack-Transport and covers also P.Product-Transport.
O.Transfer-Data	Sensitive electronic configuration items are protected against modification and/or disclosure by cryptographic means during transfer. Either symmetric means, asymmetric means or password protection are applied (as appropriate). Cryptographic keys and password used for secure communication are sufficiently protected against unauthorised access and disclosure. This prevents T.Staff-Collusion, T.Attack-Transport and covers also P.Product-Transport.
O.Control-Scrap	At this site sensitive documentation is destroyed and electronic media is erased. Scrap (Smart Card modules) are destroyed internally to avoid any material could be accessible from the personnel in the company. By this no employee could get uncontrolled access to scrap which might be helpful to support an attack. This prevents T.Unauthorised-Staff, T.Staff-Collusion and covers P.Zero-Balance.
O.Exclusive-Access	Access to the Mantes site, from and to the outside uses encrypted links provided by the other Linxens site. This addresses the threat T.Computer-Net.

8.4 Security Assurance Requirements Rationale

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

The content elements that are changed from the original CEM (3) according to the application notes in the process description (5) are written in *italic*. The term “TOE” can be replaced by “configuration items” or “product”.

8.4.1 ALC_CMC.5

The security assurance requirements of the assurance class "CM capabilities" listed above are suitable to support the production of intended TOE due to the formalized acceptance process and the automated

support. The identification of configuration items supports an automated production process. The requirement for authorized changes supports the integrity and confidentiality required for the intended TOE. Therefore, this assurance level meets the requirements for the configuration management.

8.4.2 ALC_CMS.5

The security assurance requirements of the assurance class "CM scope" listed above support the control of the production and test environment. This includes TOE related documentation and sensitive 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 assurance requirements are considered to be suitable.

8.4.3 ALC_DVS.2

The security assurance requirements of the assurance class "Development security" listed above are required since a high attack potential is assumed for potential attackers. The configuration items and information handled at the site during development, production, testing and pre-personalization/initialization/configuration of the intended TOE can be used by potential attackers for the development of attacks. Based on the assumed self-protection of the products the information is needed to apply an attack within considerable time and effort. The keys used during the initialization process also support the security during the shipment or delivery.

8.4.4 ALC_LCD.1

The security assurance requirements of the assurance class "Life-cycle definition" listed above are suitable to support the controlled production maintenance 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.Security-Documentation

  ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the product in its development environment. ALC_DVS2.2C requires the justification that the described measures are appropriate to provide the necessary level of protection. Thereby this objective contributes to meet the Security Assurance Requirement.

- O.Physical-Access

ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the product in its production environment. Thereby this objective contributes to meet the Security Assurance Requirement.

- O.Security-Control

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

- O.Alarm-Response

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

- O.Internal-Monitor

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

- O.Maintain-Security

  ALC_DVS.2.1C: The development security documentation shall describe the security measures that are necessary to protect the confidentiality and integrity of the product in its production environment. Thereby this objective contributes to meet the Security Assurance Requirement.

- O.Logical-Access

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

  ALC_CMC.5.5C requires automated measures such that only authorized changes are made to the configuration items. Therefore, the Security Assurance Requirements are suitable to meet the objective.

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

- O.Logical-Operation

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

- O.Config-Items

  ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. 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-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-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.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_LCD.1.2C requires control over the development and maintenance of the product.

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

- O.Organise-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.Staff-Engagement

  ALC_DVS.2.1C requires the description of personnel security measures that are necessary to protect the confidentiality and integrity of the product in its production environment. Thereby the objective fulfils this 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. Thereby the objective fulfils this combination of Security Assurance Requirements.

- 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.

- O.Internal-Shipment

  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. Thereby the objective fulfils this combination of Security Assurance Requirements.

- O.Transfer-Data

  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. Thereby the objective fulfils this combination of Security Assurance Requirements.

  ALC_DVS2.2C requires the justification that the described measures are appropriate to provide the necessary level of protection.

- O.Control-Scrap

  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. Thereby the objective fulfils this combination of Security Assurance Requirements.

- O.Exclusive-Access

  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.

8.6 Mapping of the Evaluation Documentation

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

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

9 Bibliography

1. Common Criteria. Common Criteria for Information Technology Security Evaluation; Part 1: introduction and general model; Version 3.1; Revision 5. April 2017.

2. —. Common Criteria for Information Technology Security Evaluation; Part:3 Security assurance components; Version 3.1; Revision 5. April 2017.

3. —. Common Methodology for Information Technology Security Evaluation; Evaluation methodology; Version 3.1; Revision 5. April 2017.

4. Eurosmart. Security IC Platform Protection Profile with Augmentation Packages; Version 1.0. BSI-CC-PP-0084-2014.

5. Common Critera. Common Criteria Supporting Document Guidance; Site Certification; Version 1.0; Revision 1. October 2007. CCDB-2007-11-001.

6. —. Configuration Management System Rev B

7. —. Configuration List Site Rev D

8. —. Development Security Policy Rev C

9. —. Lifecycle Definition Document Rev B

10. Library, Joint Interpretation. Minimum Site Security Requirements; version 3.1. December 2023.

11. Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Rev. 5, April 2017.