Site Security Target Lite

Shanlv Production Centre Zibo

Contents

1 SST Introduction

This Site Security Target (SST) refers to the following site:

Shanlv Production Centre Zibo

This site performs security chips packaging activities.

1.1 SST Reference

Title: Site Security Target Lite Shanlv Production Centre Zibo

Version: 0.6

Date: 2025.10.27

Company: ShanDong Shanlv Electronic Technology Co, Ltd.

Name of the site: Shanlv Production Centre Zibo

Product Type: Security IC

Assurance Requirements: ALC_CMC.4, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1

1.2 Site Reference

The site name is Shanlv Production Centre Zibo (hereinafter referred to as “SPCZ”), which is located at:

No.10 Taimei Road,

Zibo High-new Technology Development Zone,

Zibo, Shandong, 255088, People’s Republic of China.

This location is a campus consisting of several buildings and only one building belongs to ShanDong Shanlv Electronic Technology Co, Ltd. (hereinafter referred to as “SSE”). This building has three floors, the staff have their offices on the 2nd and 3rd floors, the production and warehouse areas are located on the 1st floor (ground level).

The security areas within the evaluation scope are located on the 1st floor of this building:

- Guardhouse room (24/7)
- Main material storeroom
- Raw material storeroom
- Finished goods storeroom
- Delivery/Loading area
- Main server room

- Backup server room
- External packaging area
- Encapsulation production area (including the production workshop and internal packaging area)

1.3 Site Description

Physical Scope

All the security areas within the evaluation scope are located on the 1st floor (ground level) of a building owned by SSE. The outer sides of the building are all monitored by the CCTV system and secured by 24/7 security guards. Additionally, access control of the entrances, irremovable metal bars and mesh grids on the windows and intrusion detection system restrict the access to the security areas laying within the evaluation scope. The site includes the high security areas: production workshop, guardhouse room, main material storeroom, finished goods storeroom, main server room, and backup server room. The site also includes the restricted areas: raw material storeroom, delivery/loading area and external packaging area.

Logical Scope

The following services and/or processes performed at SPCZ are in the scope of the evaluation process:

- Reception of secured products
- Registration of secured products for identification
- Storage of secured products including sawn wafers, unfinished modules, finished modules
- Assembly into modules (Production includes the following steps: Die Bonding, Wire Bonding, Encapsulation or Molding, Electronic Testing and Inspection)
- Quality control for incoming raw materials and each production process
- Electronic testing and visual inspection of the finished modules
- Warehousing and shipment of the finished modules
- Scrap and rejects storage, and their secure handling

The complete IC packaging flow of the security IC modules for the smart card products at the site is covered by this SST. In addition, the management of the security IC modules for the smart card related processes and the site security are covered by this SST. The production flow of the security IC modules for smart cards starts from the delivery of parts for the product (incoming raw materials) up to the packaging phase, and then shipping the finished security IC modules for smart cards to the next production phase (external parties: clients). The clients of SSE, e.g., an IC developer, or ICC (smart card) developer, send the sawn wafer to SPCZ for the chips packaging. Next, the packaged finished modules, which are the final products of this site, will be sent back to the clients.

The site life-cycle phase for the Security IC modules can be subjected (but not limited to) to the Protection Profile (1) Phase 4:

- Life cycle Phase 4: IC Packaging
    - Security IC packaging and testing

2 Conformance Claims

The evaluation of this site is based on Common Criteria (CC):

- *Common Criteria for Information Technology Security Evaluation*, Part 1: Introduction and general model; November 2022, CC:2022 Revision 1. (2)
- *Common Criteria for Information Technology Security Evaluation*, Part3: Security assurance components; November 2022, CC:2022 Revision 1. (3)
- Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities; November 2022, CC:2022 Revision 1. (4)

For the evaluation, the following methodology is used:

- *Common Methodology for Information Technology Security Evaluation*: Evaluation methodology; November 2022, CEM:2022 Revision 1. (5)

This SST is ***CC Part 3 conformant*** (see (3)). This SST claims to the following assurance components:

- ***ALC_CMC.4***
- ***ALC_CMS.5***
- ***ALC_DVS.2***
- ***ALC_LCD.1***

The assurance components chosen for the SST are derived from the EAL5 package, because EAL5 is commonly applied for the Smart Cards and Similar Devices evaluations which are related to Protection Profile (1).

This SST claims the high attack potential level which is commensurate with the assurance component ***AVA_VAN.5*** of the final TOE (see (6)).

This SST does not claim ***ALC_TAT.2*** since there are no development related activities of the TOE (or its parts) are carried out at the site.

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

3 Security Problem Definition

The Security Problem Definition comprises security problems derived from the threats of the assets handled at the site and security problems derived from the configuration management. The configuration management covers the integrity and confidentiality 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 (1). The assets (Section 3.1), threats (Section 3.2) and Organizational Security Policies (OSP) (Section 3.3) are derived from the life cycle defined in the Protection Profile (1).

The Security Problem Definition comprises two major so-called security problems. The first set of security problems comprises all types of attacks related to 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 by the Organizational Security Policies (OSPs).

3.1 Assets

The following sections describe the assets handled at the site, SPCZ.

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

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

IC Assembly

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

- Sawn wafer and 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.

Development Security Documentation

The development security documentation containing sensitive information is regarded as a sensitive asset in terms of its integrity and confidentiality, which is classified as “Confidential” or “Strictly Confidential”. However, the development security documentation with the absence of sensitive information is classified as “Internal”.

Production Data

Production data is the data being generated during the production process. It is considered as a sensitive information asset requiring the protection in accordance with the confidentiality and integrity of the intended TOE. Therefore, the production data is classified as “Confidential”.

3.2 Threats

All threats endanger the integrity and confidentiality of the intended TOE and the representation of its parts. The intended TOE protects itself in the life-cycle Phase 7 (see (1)). However, during the production, testing and assembly of the intended TOE and the representation of parts of the intended TOE are vulnerable to the integrity and confidentiality attacks.

The following threats are described in a general way. However, they are applicable to the site that handles the assets listed in Section 3.1. All the threats described below shall be countered by the Security Objectives of the site.

T.SMART_THEFT

An attacker tries to access security areas of the site for manipulation or theft of intended TOE (or its parts) during production. The attacker has sufficient time to investigate the site outside 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 hide 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 for further investigation of the functionality of the chips 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 security 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 security measures like storage of items in safes or secured rooms provide additional defense 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 access the critical network segments remotely to get access to sensitive configuration data or items or modify security relevant production processes.

T.ACCIDENTAL_CHANGE

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

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

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.UNAUTHORISED_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 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 the confidential information after the intended TOE production.

3.3 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 documentation 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 evaluation.

P.CONFIG_ITEMS

The configuration management system shall be able to uniquely identify all configuration items. This includes the unique identification of items that are created, generated, developed, 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 the authorized personnel. Automated systems shall support the configuration management and ensure access control and interactive acceptance measures for setup and changes. The procedure for the initial setup 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 stated in the configuration management plan. This plan 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 processes 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 performed 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 produced 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 sent back to the client, if requested, or securely stored at the site.

This policy covers the packaging and shipment of the products at the site after the applied production flow. All finished products are sent back 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 the recipient. In case the product needs to be moved within the site, this will be considered as internal transportation.

P.ORGANISE_PRODUCT

The production process is applied as specified by the site's configuration management plan. If the production data includes sensitive items, appropriate security measures must be applied.

3.4 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 from the previous site. This is reflected by the assumptions that might be defined for the site, even though the assumptions lay outside of the evaluation scope. Therefore, any assumptions made are considered to be satisfied (ie, 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 activities at SPCZ rely on the assumptions related to the products, the data, the documentation and the transfer information/items provided by the client or the product supplier.

A.ITEM_IDENTIFICATION

Each configuration item 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 specifications 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 electronic tests or finished test programs appropriate for the final testing. The provided information includes the classification of the delivered items, documents and data.

A.CLIENT_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 or behavior of the chips based on insufficient operational condition or any commands sequences generated by an attacker or by accident. The developer assumes that the features used for testing of the chip (die) at the end of the life-cycle Phase 3 and Phase 4 (according to (1)) are disabled. The developer will be provided with the configuration of the product that will be used as the basis for the integrity protection during the internal transportation.

4 Security Objectives

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

4.1 Security Objectives for the Site

O.SECURITY_DOCUMENTATION

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

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 for the development areas. The access control system shall limit the access to these areas including the identification and rejection of unauthorized people. The site enforces three levels (from level 1 to level 3) of the physical access control, which correspond to the controlled/restricted areas (level 1), security areas (level 2) and high-security areas (level 3) of the site. The access control measures ensure that only authorized employees and vendors can access such the areas. Sensitive products are only handled in the development areas.

O.SECURITY_CONTROL

Assigned personnel of the site or security guards operate the systems for the access control and surveillance and they respond to alarms. Technical security measures like video monitoring, motion sensors support the enforcement of the physical access control. These personnel are also responsible for registration and escorting visitors, contractors and suppliers.

O.ALARM_RESPONSE

The technical and organizational security measures ensure that an alarm is activated (detection layer) before an unauthorized person gets access to any sensitive configuration items (assets). After the alarm has been triggered, the unauthorized person must be hold back by other security measures (stop layer). The reaction time of the employees or security 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 the security measures are correctly configured, 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 the sufficient level of protection.

O.MAINTAIN_SECURITY

Technical security measures are maintained regularly to ensure correct and uninterrupted operation. The logging information of the 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 developer network and computer systems.

O.LOGICAL_ACCESS

Access to the production operation machines and related production systems are restricted to authorized employees that work in the related areas or that are involved in the configuration tasks or the production operations. Every user of an IT system has its own user account and password. Authentication of the users is enforced on 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 an their trackability and traceability. In addition, the internal security procedures and guidance documentation 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 to the services and/or processes of the released products. A designated team/employee is responsible for the 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 production 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. Parameters checks, electronic and/or visual checks and 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 the intended TOE (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. The defective chips will be sent back to the client, if requested, or securely stored at the site. All the production stages of sensitive products are automatically managed though the configuration systems, the quantity of the intended TOE and defective products are recorded in the configuration system to ensure that all the sensitive materials/parts are under control.

O.RECEPTION_CONTROL

Upon reception of the incoming products (raw materials), an immediate inspection is performed. The inspection of the physical products is done according to the internal requirements. It comprises the surface checks of raw materials, quantity of products checks, the identification and assignment of the product to a related internal production process. For security checks, the integrity and authenticity of the incoming products are verified upon reception.

O.EXTERNAL_DELIVERY

The sender of a physical configuration item is identified by the assigned client address on the shipment form. 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 to/from client (not the end user). 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, the symmetric key or password-based exchanges methods might be used (e.g., symmetric key encrypted files, password protected archives). In the latter case, it has to be ensured that only authorized users have access to the symmetric cryptographic keys or passwords. The cryptographic keys and/or passwords are exchanged/stored based on the defined security 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 (scraps) are collected and returned back to the client (if requested), or securely stored at the site.

4.2 Security Objectives Rationale

Table 1 provides the tracing from the Security Objectives to the Threats and/or Organizational Security Policies (OSPs).

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
P.ACCEPT_PRODUCT	X		X		X													
P.CONFIG_CONTROL			X	X	X				X				X					
P.CONFIG_ITEMS				X									X					
P.CONFIG_PROCESS					X													
P.ORGANISE_PRODUCT			X		X				X	X								
P.PRODUCT_TRANSPORT				X			X										X	
P.RECEPTION_CONTROL													X					
P.ZERO_BALANCE						X		X								X		X
T.ACCIDENTAL_CHANGE	X			X	X				X			X				X		X
T.ATTACK_TRANSPORT							X										X	
T.COMPUTER_NET								X	X	X	X				X	X		
T.RUGGED_THEFT		X						X			X	X		X	X			
T.SMART_THEFT		X						X			X	X		X	X			
T.STAFF_COLLUSION						X		X			X				X	X	X	
T.UNAUTHORISED_STAFF		X				X		X	X	X	X	X		X	X	X		X

TABLE 1 SECURITY OBJECTIVES: TRACING

Table 2 provides the rationale for the Security Objectives tracing showing that all the Threats and/or OSPs are effectively addressed by the Security Objectives.

Threat, OSP	Security Objective	Rationale
T.SMART_THEFT	O.SECURITY_DOCUMENTATION O.PHYSICAL_ACCESS O.SECURITY_CONTROL O.ALARM_RESPONSE O.INTERNAL_MONITOR 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.PHYSICAL_ACCESS prevents an unauthorized access to the developer facilities. O.SECURITY_CONTROL ensures the correct operation of the access control mechanisms supporting the physical security. 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. 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.
T.RUGGED_THEFT	O.SECURITY_DOCUMENTATION O.PHYSICAL_ACCESS O.SECURITY_CONTROL O.ALARM_RESPONSE O.INTERNAL_MONITOR 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.PHYSICAL_ACCESS prevents an unauthorized access to the developer facilities. O.SECURITY_CONTROL ensures the correct operation of the access control mechanisms supporting the physical security. 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. 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.

T.COMPUTER_NET	O.SECURITY_DOCUMENTATION O.LOGICAL_ACCESS O.LOGICAL_OPERATION O.INTERNAL_MONITOR O.MAINTAIN_SECURITY O.STAFF_ENGAGEMENT	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.LOGICAL_ACCESS prevents an attacker from unauthorized remote access to sensitive data. O.LOGICAL_OPERATION ensures that the IT systems are kept up-to-date, and ensures 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. O.STAFF_ENGAGEMENT ensures that staff with access to the sensitive items have 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.
T.ACCIDENTAL_CHANGE	O.LOGICAL_ACCESS O.PHYSICAL_ACCESS O.CONFIG_ITEMS O.STAFF_ENGAGEMENT O.CONFIG_PROCESS O.ZERO_BALANCE O.ACCEPTANCE_TEST	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 the 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. O.ACCEPTANCE_TEST guarantees that before shipment, the release products meet the required criteria imposed by the client.
T.UNAUTHORISED_STAFF	O.LOGICAL_ACCESS O.PHYSICAL_ACCESS O.SECURITY_CONTROL O.LOGICAL_OPERATION O.INTERNAL_MONITOR O.MAINTAIN_SECURITY O.SECURITY_DOCUMENTATION O.ALARM_RESPONSE O.ZERO_BALANCE O.STAFF_ENGAGEMENT O.CONTROL_SCRAP	O.LOGICAL_ACCESS and O.PHYSICAL_ACCESS ensure that 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,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. O.CONTROL_SCRAP ensures that the rejected assets (scraps) will be securely collected and returned to the client, or securely stored at the site.
T.STAFF_COLLUSION	O.SECURITY_DOCUMENTATION O.STAFF_ENGAGEMENT O.INTERNAL_MONITOR O.MAINTAIN_SECURITY O.TRANSFER_DATA O.CONTROL_SCRAP	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.STAFF_ENGAGEMENT ensures that staff with access to the 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 the sensitive data during transfer. O.CONTROL_SCRAP ensures that an attacker cannot get access to sensitive data from the scrap.
T.ATTACK_TRANSPORT	O.EXTERNAL_DELIVERY O.TRANSFER_DATA	O.EXTERNAL_DELIVERY ensures that an attacker cannot get access to sensitive physical or electronic data or items during internal or external transportation. For the electronic items, the threat is further countered by the security measures defined by O.TRANSFER_DATA.
P.ACCEPT_PRODUCT	O.ACCEPTANCE_TEST O.CONFIG_CONTROL O.CONFIG_PROCESS	O.ACCEPTANCE_TEST directly enforces the policy for which the products are released only when the quality criteria defined by the client are satisfied. O.CONFIG_CONTROL and O.CONFIG_PROCESS contribute to the product quality acceptance framework necessary to enforce the policy.
P.CONFIG_CONTROL	O.CONFIG_CONTROL O.CONFIG_ITEMS O.CONFIG_PROCESS O.RECEPTION_CONTROL O.LOGICAL_ACCESS	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	O.CONFIG_ITEMS O.RECEPTION_CONTROL	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	O.CONFIG_PROCESS directly enforces the policy as it defines all the security procedures and measures (CM plan) used during the production process.
P.ORGANISE_PRODUCT	O.CONFIG_PROCESS O.CONFIG_CONTROL O.LOGICAL_ACCESS O.LOGICAL_OPERATION	O.CONFIG_PROCESS ensures that a configuration management plan is in place. O.CONFIG_CONTROL ensures that the configuration management plan is applied and followed during the product process. 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 O.TRANSFER_DATA O.CONFIG_ITEMS	O.EXTERNAL_DELIVERY ensures a secure external transportation of the release products. O.TRANSFER_DATA ensures secure transfer of the sensitive electronic data items. O.CONFIG_ITEMS ensures the correct labelling of the product.
P.RECEPTION_CONTROL	O.RECEPTION_CONTROL	O.RECEPTION_CONTROL ensures that the reception procedures for the secure products are applied and followed.
P.ZERO_BALANCE	O.ZERO_BALANCE O.CONTROL_SCRAP O.INTERNAL_MONITOR O.STAFF_ENGAGEMENT	O.ZERO_BALANCE and O.CONTROL_SCRAP ensure that no sensitive items loss occurring during production and shipment. 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.

TABLE 2 SECURITY OBJECTIVES: RATIONALE

5 Extended Components Definition

No extended components are defined in this Site Security Target.

6 Security Requirements

6.1 Security Assurance Requirements for the Site

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

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

The ALC_DVS.2 listed above fulfil Minimum Site Requirements (6).

Application Note for ALC requirements in terms of Site Certification:[1]

1. In the scope of Site Certification, the term "TOE" shall be understood as an "intermediate product", "incomplete product", or "non-final TOE" since the TOE itself is not the subject of evaluation. The term "product" can be used interchangeably with the term "TOE" depending on the context relevance.
2. Since the TOE is not directly in the focus of Site Certification, certain TOE requirements (SARs) cannot be applied to the site in the way they are written. Therefore, such SARs will be refined in this document as follows:
   a. ~~exclusion of some parts of the requirement which are not applicable to site~~,[2]
   b. *inclusion of some parts into the requirement which are applicable to site*,[3] and
   c. <u>new requirement which is applicable to site</u>.[4]

ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies:

ALC_CMS.1 TOE CM coverage

ALC_DVS.1 Identification of security measures

ALC_LCD.1 Developer defined life-cycle processes

The dependencies ALC_CMS.1 and ALC_DVS.1 are satisfied by inclusion of the hierarchically higher assurance components ALC_CMS.5 and ALC_DVS.2.

The dependency ALC_LCD.1 is partially fulfilled because the site does not cover the whole life cycle of the TOE development. For this site, only the Phase 4 (IC Packaging) (1) is relevant.

Objectives:

[1] Application Note shall be applied to the whole document, whenever suitable in the specified context.
[2] ~~Strikethrough~~
[3] *Italic*
[4] <u>Underline</u>

This requirement aims to determine whether the developer has clearly identified the product and its associated configuration items with unique reference, and whether the ability to modify these items is properly controlled by automated tools, thus making the CM system less susceptible to human error or negligence.

The acceptance procedure is to ensure that the parts of the product are of adequate quality and to confirm that any creation or modification of configuration items is authorized.

Production support procedures help to ensure that the generation of the product from a managed set of configuration items is correctly performed in an authorized manner, particularly in the case when different developers are involved, and integration processes have to be carried out.

SAR	Description
ALC_CMC.4.1C	The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.
ALC_CMC.4.2C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.4.3C	The CM system shall uniquely identify all configuration items.
ALC_CMC.4.4C	The CM system shall provide automated measures such that only authorised changes are made to the configuration items.
ALC_CMC.4.5C	The CM system shall support the production of the TOE by automated means.
ALC_CMC.4.6C	The CM documentation shall include a CM plan.
ALC_CMC.4.7C	The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.4.8C	The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ALC_CMC.4.9C	The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.4.10C	The evidence shall demonstrate the CM system is being operated in accordance with the CM plan.

ALC_CMS.5 Development tools CM coverage

Dependencies:

None

Objectives:

This requirement aims to determine whether the configuration list includes all the configuration items that have been placed under CM. Placing the evaluation evidence, production tools and related information under CM provides assurance that they have been modified in a controlled manner with proper authorizations.

Production tools play an important role in ensuring the production of a quality version of the product. Therefore, it is important to control modifications to these tools.

SAR	Description

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

ALC_DVS.2 Sufficiency of security controls

Dependencies: None

Objectives:

This requirement aims to determine whether the developer's security controls on the production environment are adequate to provide the confidentiality and integrity of the product design and implementation that is necessary to ensure that secure operation of the product is not compromised.

Development security is concerned with physical, procedural, personnel, and other security measures that may be used in the production environment to protect the product and its parts. It includes the physical security of the production location and any procedures used to select production staff.

SAR	Description
ALC_DVS.2.1C	The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment *and provide evidence that these security measures are followed during the development and maintenance of the TOE*.
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.

ALC_LCD.1 Developer defined life-cycle processes

Dependencies: None

Objectives:

This requirement aims to determine whether the developer has used a documented model of the TOE life cycle. A life-cycle model encompasses the procedures, tools and techniques used to develop and maintain the product.

SAR	Description
ALC_LCD.1.1C	The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.
ALC_LCD.1.2C	The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

6.2 Security Requirements Rationale

Table 3 provides the tracing from the SARs to the Security Objectives.

SAR / SECURITY OBJECTIVE	ALC_CMC.4.1C	ALC_CMC.4.2C	ALC_CMC.4.3C	ALC_CMC.4.4C	ALC_CMC.4.5C	ALC_CMC.4.6C	ALC_CMC.4.7C	ALC_CMC.4.8C	ALC_CMC.4.9C	ALC_CMC.4.10C	ALC_CMS.5.1C	ALC_CMS.5.2C	ALC_CMS.5.3C	ALC_DVS.2.1C	ALC_DVS.2.2C	ALC_LCD.1.1C	ALC_LCD.1.2C
O.ACCEPTANCE_TEST		X	X					X		X					X		X
O.ALARM_RESPONSE														X	X		
O.CONFIG_CONTROL		X	X	X	X	X	X		X	X	X	X				X	
O.CONFIG_ITEMS	X	X	X					X			X	X	X				
O.CONFIG_PROCESS		X	X	X		X	X	X	X	X	X	X				X	X
O.CONTROL_SCRAP														X	X		
O.EXTERNAL_DELIVERY										X		X		X			
O.INTERNAL_MONITOR															X		
O.LOGICAL_ACCESS				X										X	X		
O.LOGICAL_OPERATION				X										X	X		
O.MAINTAIN_SECURITY														X	X		
O.PHYSICAL_ACCESS														X	X		
O.RECEPTION_CONTROL		X	X					X	X			X			X		
O.SECURITY_CONTROL														X	X		
O.SECURITY_DOCUMENTATION														X	X		
O.STAFF_ENGAGEMENT														X	X		
O.TRANSFER_DATA														X	X		
O.ZERO_BALANCE					X				X	X					X		X

TABLE 3 SARS: TRACING

Table 4 provides the rationale for the SARs tracing showing that all the Security Objectives are effectively addressed by the SARs.

Security Objective	SAR	Rationale
O.ACCEPTANCE_TEST	ALC_CMC.4.2C ALC_CMC.4.3C ALC_CMC.4.8C ALC_CMC.4.10C ALC_DVS.2.2C ALC_LCD.1.2C	ALC_CMC.4.2C requires the description of the method used to uniquely identify the configuration items. ALC_CMC.4.3C requires a unique identification of all configuration items used by the CM system. ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items as part of the intended TOE. ALC_CMC.4.10C requires the CM system to be operated as intended. ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.

		ALC_LCD.1.2C requires the defined life-cycle model to provide for the necessary control over the development and maintenance of the intended TOE.
O.ALARM_RESPONSE	ALC_DVS.2.1C ALC_DVS.2.2C	ALC_DVS.2.1C requires the description all the 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 environment and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.
O.CONFIG_CONTROL	ALC_CMC.4.2C ALC_CMC.4.3C ALC_CMC.4.4C ALC_CMC.4.5C ALC_CMC.4.6C ALC_CMC.4.7C ALC_CMC.4.9C ALC_CMC.4.10C ALC_CMS.5.1C ALC_CMS.5.2C ALC_LCD.1.1C	ALC_CMC.4.2C requires the description of the method used to uniquely identify the configuration items. ALC_CMC.4.3C requires a unique identification of all configuration items used by the CM system. ALC_CMC.4.4C requires the CM system to provide automated measures such that only authorized changes are made to the configuration items. ALC_CMC.4.5C requires the CM system to support the production of the intended TOE by automated means. ALC_CMC.4.6C requires a CM plan to be implemented. ALC_CMC.4.7C requires the CM plan to describe how the CM system is used for the development of the intended TOE. ALC_CMC.4.9C requires the evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.4.10C requires the CM system to be operated as intended. ALC_CMS.5.1C requires the configuration list to include the following: the TOE itself, the evaluation evidence required by the SARs and development tools and related information. ALC_CMS.5.2C requires the configuration list to uniquely identify the configuration items. ALC_LCD.1.1C requires the description of the life-cycle model used to develop and maintain the intended TOE.
O.CONFIG_ITEMS	ALC_CMC.4.1C ALC_CMC.4.2C ALC_CMC.4.3C ALC_CMC.4.8C ALC_CMS.5.1C ALC_CMS.5.2C ALC_CMS.5.3C	ALC_CMC.4.1C requires a documented process ensuring an appropriate and consistent labelling of the products. ALC_CMC.4.2C requires the description of the method used to uniquely identify the configuration items. ALC_CMC.4.3C requires a unique identification of all configuration items used by the CM system. ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items as part of the intended TOE.

		ALC_CMS.5.1C requires the configuration list to include the following: the TOE itself, the evaluation evidence required by the SARs and development tools and related information. ALC_CMS.5.2C requires the configuration list to uniquely identify the configuration items. ALC_CMS.5.3C requires that developer of each configuration item shall be indicated.
O.CONFIG_PROCESS	ALC_CMC.4.2C ALC_CMC.4.3C ALC_CMC.4.4C ALC_CMC.4.6C ALC_CMC.4.7C ALC_CMC.4.8C ALC_CMC.4.9C ALC_CMC.4.10C ALC_CMS.5.1C ALC_CMS.5.2C ALC_LCD.1.1C ALC_LCD.1.2C	ALC_CMC.4.2C requires the description of the method used to uniquely identify the configuration items. ALC_CMC.4.3C requires a unique identification of all configuration items used by the CM system. ALC_CMC.4.4C requires the CM system to provide automated measures such that only authorized changes are made to the configuration items. ALC_CMC.4.6C requires a CM plan to be implemented. ALC_CMC.4.7C requires the CM plan to describe how the CM system is used for the development of the intended TOE. ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items as part of the intended TOE. ALC_CMC.4.9C requires the evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.4.10C requires the CM system to be operated as intended. ALC_CMS.5.1C requires the configuration list to include the following: the TOE itself, the evaluation evidence required by the SARs and development tools and related information. ALC_CMS.5.2C requires the configuration list to uniquely identify the configuration items. ALC_LCD.1.1C requires the description of the life-cycle model used to develop and maintain the intended TOE. ALC_LCD.1.2C requires the defined life-cycle model to provide for the necessary control over the development and maintenance of the intended TOE.
O.CONTROL_SCRAP	ALC_DVS.2.1C ALC_DVS.2.2C	ALC_DVS.2.1C requires the description all the 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 environment and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.
O.EXTERNAL_DELIVERY	ALC_CMC.4.10C ALC_CMS.5.2C	ALC_CMC.4.10C requires the CM system to be operated as intended.

	ALC_DVS.2.1C	ALC_CMS.5.2C requires the configuration list to uniquely identify the configuration items. ALC_DVS.2.1C requires the description all the 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 environment and provide evidence that these security measures are followed during the development and maintenance of the TOE.
O.INTERNAL_MONITOR	ALC_DVS.2.2C	ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.
O.LOGICAL_ACCESS	ALC_CMC.4.4C ALC_DVS.2.1C ALC_DVS.2.2C	ALC_CMC.4.4C requires the CM system to provide automated measures such that only authorized changes are made to the configuration items. ALC_DVS.2.1C requires the description all the 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 environment and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.
O.LOGICAL_OPERATION	ALC_CMC.4.4C ALC_DVS.2.1C ALC_DVS.2.2C	ALC_CMC.4.4C requires the CM system to provide automated measures such that only authorized changes are made to the configuration items. ALC_DVS.2.1C requires the description all the 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 environment and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.
O.MAINTAIN_SECURITY	ALC_DVS.2.1C ALC_DVS.2.2C	ALC_DVS.2.1C requires the description all the 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 environment and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.
O.PHYSICAL_ACCESS	ALC_DVS.2.1C ALC_DVS.2.2C	ALC_DVS.2.1C requires the description all the 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 environment and provide evidence that these security measures are followed during the development and maintenance of the TOE.

		ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.
O.RECEPTION_CONTROL	ALC_CMC.4.2C ALC_CMC.4.3C ALC_CMC.4.8C ALC_CMC.4.9C ALC_CMS.5.2C ALC_DVS.2.2C	ALC_CMC.4.2C requires the description of the method used to uniquely identify the configuration items. ALC_CMC.4.3C requires a unique identification of all configuration items used by the CM system. ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items as part of the intended TOE. ALC_CMC.4.9C requires the evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMS.5.2C requires the configuration list to uniquely identify the configuration items. ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.
O.SECURITY_CONTROL	ALC_DVS.2.1C ALC_DVS.2.2C	ALC_DVS.2.1C requires the description all the 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 environment and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.
O.SECURITY_DOCUMENTATION	ALC_DVS.2.1C ALC_DVS.2.2C	ALC_DVS.2.1C requires the description all the 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 environment and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.
O.STAFF_ENGAGEMENT	ALC_DVS.2.1C ALC_DVS.2.2C	ALC_DVS.2.1C requires the description all the 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 environment and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.
O.TRANSFER_DATA	ALC_DVS.2.1C ALC_DVS.2.2C	ALC_DVS.2.1C requires the description all the 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 environment

		and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE.
O.ZERO_BALANCE	ALC_CMC.4.5C ALC_CMC.4.9C ALC_CMC.4.10C ALC_DVS.2.2C ALC_LCD.1.2C	ALC_CMC.4.5C requires the CM system to support the production of the intended TOE by automated means. ALC_CMC.4.9C requires the evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.4.10C requires the CM system to be operated as intended. ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE. ALC_LCD.1.2C requires the defined life-cycle model to provide for the necessary control over the development and maintenance of the intended TOE.

TABLE 4 SARS: RATIONALE

7 Site Summary Specification

7.1 External Behaviour of the Site

The main precondition for the design specifications, data preparation and the modules production, is a release process technology between the wafer fab and the final client. This comprises the definition of the design specifications as well as parameters and limits for the wafer fabrication. The design specifications are used for the product classification and production process setup.

This section provides background information on the assumptions. These assumptions impose the additional requirements on the clients and SPCZ regarding the production process, information and deliverables which are needed to enable the correct product production and delivery under the conditions described in this Site Security Target.

A.ITEM_IDENTIFICATION: The production configuration items must be properly labelled before delivery to SPCZ to allow the correct identification of the received items.

A.PROD_SPECIFICATION: SPCZ provides assembly (wafer fabrication), testing and packaging services for the smartcard ICs. The wafers, sawn wafers and lead frames are acceptable as input for the assembly lines. Defective dies on the wafer will be marked by inking or wafer mapping. The finished products (IC packages) shall be labelled before delivery to the client to allow the correct products identification.

A.CLIENT_DELIVERY: If specific requirements are needed for the shipment of the final products, the related instructions and cargo/security items, e.g., anti-tampering labels/tapes/boxes, shall be provided by the client.

A.PRODUCT_INTEGRITY: SPCZ will conduct the finished modules testing after the assembly, using electronic tests as well as open and short measurements based on the test parameters, and design specifications provided by the client.

7.2 Internal Behaviour of the Site

Reception, identification, registration and storage of the materials: It includes wafers, sawn wafers, unfinished modules and finished modules. The materials received by SPCZ will be labelled with a unique client part ID (client parts). This part ID is linked to the chips that are assembled in the modules.

Assembly into modules: The processes for assembly, testing and acceptance are setup at SPCZ according to the specifications (e.g., bond plan, module specification, test specification and packaging requirements) 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.

Quality control: There is a quality control procedure used to inspect the incoming materials and the modules under production at each step of the production process.

Electronic testing and visual inspection of the finished modules: The complete production specific flow includes an electronic testing of each product as a part of the acceptance process. The electronic testing is performed by SPCZ following the test specifications and electrical parameters provided by the client. The testing program is integrated in the development environment of SPCZ. No sensitive information or data should be included in the tests.

Warehousing and shipment of the finished products: SPCZ has a standard procedure for packaging of the finished modules and preparation for shipment using protective materials. If special packaging 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 with the information such as shipment details and the express tracking number that are used for the shipment package identification and verification at the reception on the client side.

Scrap storage and its secure handling: Both, the defective or rejected products and chips, are returned to the client, if requested. Otherwise, scraps will be security stored at the site.

7.3 Description of the Site Requirements

ALC_CMC.4 Production support, acceptance procedures and automation

SAR	Site Aspect
ALC_CMC.4.1C	All products assembled at the site get a unique production serial number generated by a database, which is linked to the client part ID. The ID assignment for all configuration items is supported by automated tracking systems.
ALC_CMC.4.2C	Incoming inspections are based on product identification that ensures associated labelling. Incoming labelling is mapped to the internal identification that ensures the unique identification of security products.
ALC_CMC.4.3C	The internal unique identification of all items belongs to a client part ID. Each client part ID is released based on the defined process.
ALC_CMC.4.4C	The changes can only be done by the authorized personnel. The logical access is limited and controlled for all tasks to ensure that the critical operations and changes are only performed by the authorized personnel.
ALC_CMC.4.5C	An automated system ensures the unique mapping between configuration items and the tracking of the different production steps. A configured and controlled automated production process is implemented. An automated system is in place to map the configuration items to a unique job number. Automated electronic testing of finished modules ensures that the released products meet the requirements imposed by a client.
ALC_CMC.4.6C	The setup of each client part ID includes the associated CM plan for the product release. The reliability and correctness of the processes and tools used are ensured by the associated CM plan.

ALC_CMC.4.7C	The CM plan provides the production release procedure to manage the client part IDs at the site. The CM plan describes the production steps performed at the site.
ALC_CMC.4.8C	The automated control of released products is supported.
ALC_CMC.4.9C	The identification of configuration items is supported by the production process. The unique identification of each product is ensured by the client part ID. The tracing of all security products is supported.
ALC_CMC.4.10C	The production release process is defined according to the CM plan. Only released client part IDs are produced. The compliance of the production process is ensured by physical/logical security measures. The number of produced modules corresponds to the sum of the delivered modules and the scrap modules.

ALC_CMS.5 Development tools CM coverage

SAR	Site Aspect
ALC_CMS.5.1C	Since the process is the subject of evaluation, no product parts are in the configuration list. The TOE itself, the parts that comprise the product, the implementation representation, security flaw reports and resolution status are not applicable for a site evaluation. Configuration items are stored in the configuration management system and identified by a unique number. The release process for each client part ID is defined. The configuration control for part IDs, procedures and processes is defined.
ALC_CMS.5.2C	Items, products and processes are uniquely identified by the database system. Within the production process the unique identification is supported by automated tools. The authenticity verification and identification of received products is defined.
ALC_CMS.5.3C	The site does not involve subcontractors for the test of security products. The labelling and preparation process for the shipment is defined. All configuration items for secure products are identified in the system.

ALC_DVS.2 Sufficiency of security controls

SAR	Site Aspect
ALC_DVS.2.1C	The physical protection is provided and supported by security systems including access control, alarm and intrusion detection to prevent unauthorized access. Procedures are defined to ensure the correct operation of security systems. The logical protection of data/network, physical access control, intrusion detection, monitoring and the configuration management are provided. Evidence is provided showing that all the security measures are followed during the development and maintenance of the product. The personnel security measures are provided. Any scrap that may support an attacker is physically controlled in high security areas.

	Secure physical delivery between different sites is controlled. The security related documentation control is ensured. The production data transmission is secured.
ALC_DVS.2.2C	The security of the site is maintained according to the site's security documentation covering all physical, logical, procedural and personnel measures to ensure the security of the site, and the necessary level of the integrity and confidentiality protection for the TOE. Internal audits and improvements are performed on a regular basis to ensure the correct implementation and application, and adequacy of the security measures employed at the site.

ALC_LCD.1 Developer defined life-cycle processes

SAR	Site Aspect
ALC_LCD.1.1C	The processes used for identification, manufacturing and configuration management are covered.
ALC_LCD.1.2C	The site does not perform development tasks. The applied production process is controlled by the automated means. The finished products are tested, and all security products are traced by automated means and/or the four-eye principle (where applicable) is applied. Configuration items are stored in the configuration management system according to the site's configuration management plan.

8 References

1. **EUROSMART.** *Security IC Platform Protection Profile with Augmentation packages.* Version 1.0, 2014.

2. **Common Criteria for Information Technology Security Evaluation.** *Part 1: Introduction and general model.* CC:2022 Revision 1, November 2022.

3. —. *Part 3: Security assurance components.* CC:2022 Revision 1, November 2022.

4. —. *Part 4: Framework for the specification of evaluation methods and activities.* CC:2022 Revision 1, November 2022.

5. **Common Methodology for Information Technology Security Evaluation.** *Evaluation methodology.* CEM:2022 Revision 1, November 2022.

6. **Joint Interpretation Library.** *Minimum Site Security Requirements.* Version 3.1, December 2023.

7. **Common Criteria.** *Supporting Document Guidance, Site Certification.* Version 1.0, Rev. 1, October 2007.