INESA
上海仪电

# Site Security Target Lite INESA Shanghai

| | |
|---|---|
| 编号：YDZNCC-ZD-lite | 版本：1.6 版 |
| 页数：44 页 | 生效日期： 2023 年 8 月 3 日 |

| 更改史 – Revision History | | | | |
|---|---|---|---|---|
| 版本<br>Version | 生效日<br>Effective date | 起草人<br>Drafter | 批准人<br>Approver | 更改描述<br>Description |
| 1.3 | 2019-07-20 | 管晓敏 | 顾秋华 | Initial version 1.3 based on YDZNCC-ZD-001 Site Security Target INESA Shanghai v1.3 |
| 1.4 | 2019-08-02 | 管晓敏 | 顾秋华 | Update the chapter 2.3 regarding to the life cycle phase covered by the site |
| 1.5 | 2021-07-29 | 管晓敏 | 顾秋华 | Updated version 1.5 based on YDZNCC-ZD-001 Site Security Target INESA Shanghai v1.5 |
| 1.6 | 2023-08-03 | 梁洋洋 | 顾秋华 | Updated version 1.6 based on YDZNCC-ZD-001 Site Security Target INESA Shanghai v1.6 |

## Table of Contents

## Table of Figures

# 1. Document Introduction

## 1.1 Reference

Title: Site Security Target Lite INESA Shanghai

Version: 1.6

Date: 2023-8-3

Company: Shanghai INESA intelligent Electronics Co., Ltd

Name of site: INESA Shanghai

Based on: Site Security Target INESA Shanghai version 1.6

# 2. SST Introduction

This document is based upon the Eurosmart Site Security Target Template [1] with adaptions such that it fits the site (i.e. testing, no development site, no production).

## 2.1 SST Reference

Title: Site Security Target Lite INESA Shanghai

Version: 1.6

Reference: YDZNCC-ZD-lite

Issue date: 2023-8-3

Product type: Security IC

EAL-Level: EAL6

## 2.2 Site Reference

Company: Shanghai INESA intelligent Electronics Co., Ltd

Name of the site: INESA Shanghai

Location: No. 818, Jin Yu Road, Free Trading Zone, Shanghai, China P.R.

Site Description

The INESA Shanghai site performs secure production activities related to security ICs in accordance with client instructions. The activities at INESA Shanghai site are wafer testing, wafer sawing and back grinding, module packaging, module testing and pre-personalization secure physical shipment to the client. For details please refer to 8.2 'Services of the Site'.

### 2.2.1 Physical scope

This site is located at No.818, Jin Yu Road, Free Trading Zone, Shanghai, China P.R. built in 1994. The site is a closed area, surrounded by the fences, walls, electric fences and infrared alarms. There are only one people's entrance and one vehicle entrance side by side. Beside these two entrances, a 24h/7d running security guard room is located. There are two relevant buildings: Office/Wafer Manufacture building and Module Manufacturing building. Security relevant areas are:

Office/Wafer Manufacture building:
(the wafer manufacturing part: in total 4 floors)

- Raw material warehouse (1st floor)
- Die bank (1st floor)
- Wafer testing (2nd floor)

- Wafer sawing and back grinding (1st floor)
- Secure IT server room (2nd floor)
- Security guard room (2nd floor)
- Finished-good and scrap warehouse (2nd floor)

Note: The 3rd floor and 4th floor are not used.

(the office part: in total 5 floors)
- IT server room (3rd floor)
- HR management room (2nd floor)

Note: Other floors are office area

Module Manufacturing building (2 floors):
- Finished good warehouse (1st floor)
- Module packaging (1st floor)
- Module testing and pre-personalization (1st floor)
- Security guard room (1st floor)

Note: The 2nd floor has only a small clothing room.

*Note: The floors begin from the 1st floor.*

*In addition to the above security areas. The fences/walls of the campus, outer walls of the buildings, access control system and the CCTV systems are in the physical scope.*

### 2.2.2 Logical scope

The following services provided by INESA Shanghai are in scope of the site evaluation process.

- Wafer testing
- Wafer sawing and back grinding
- Module packaging
- Module testing (i.e. electrical characterization) and pre-personalization
- Warehousing
- Secure physical shipment to the client

In addition, the supporting IT-system located in the IT server rooms, the security guard rooms and the HR management room for operational control are in the evaluation scope.

The activities of the site cover the life cycle phase IC Manufacturing (Phase 3, only for IC testing and initialization) and the life cycle phase IC Packaging (Phase 4) as defined in the as defined in 'Security IC Platform Protection Profile' (PP-0035) and 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084).

# 3. Conformance Claim

This SST is conformant with Common Criteria Version 3.1:

- 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 Requirements; Version 3.1, 5, April 2017, [3]

and the following additional methodology:

- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1, 5, April 2017, [4]

- Supporting Document, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007, [5]

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 (at AVA_VAN.5 level), ALC_LCD.1[1] [2]

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 are assumed. Therefore, this site supports potentially augmented product evaluations up to and including EAL6.

[1] The site does not provide contributions to ALC_DEL.1. The security of transportation between the client and INESA is ensured by ALC_DVS.2.

[2] The site does not provide contributions to ALC_TAT.3.

# 4. Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site.

## 4.1 Assets

The following section describes types of the assets handled at the site.

Production data: The site has electronic testing programs in relation to processed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected.

Logical security objects: The site has documents in relation to processed products. Both the integrity and the confidentiality of these must be protected.

Physical security objects: The site has physical security objects in relation to processed products. Both the integrity and the confidentiality of these must be protected.

The detail assets are listed below:

### 4.1.1 Wafer testing

- Wafers
- Open Samples (optional. In case the wafers are open samples, the wafer test program must disable the test feature at the end of the wafer testing)
- Rejected dice
- Test programs (optional authentication data for testing) and instructions

### 4.1.2 Wafer sawing and back grinding

- Wafers and dice
- Sawing and back grinding specification

### 4.1.3 Module packaging

- Dice
- Modules
- Packaging specification

### 4.1.4 Module testing and pre-personalization

- Modules

- Rejected modules
- Pre-personalization program
- Test specification and instructions

### 4.1.5 Warehousing

- Wafers
- Diced wafers
- Modules
- Rejected dice and modules
- Secure seal

### 4.1.6 Secure physical shipment to the client

- Modules
- Rejected dice and modules
- Secure seal

## 4.2 Threats

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

The following threats are described in a general way. However, they are applicable to the site. The explanation below the threats shall support the mapping to the Security Objectives of the site.

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of 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.

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

It is expected that such an attacker can be defeated by state of the art physical, technical and procedural security measures like access control and surveillance. In general, an access control concept with two or three levels shall be implemented. If two levels are implemented, the more restrictive level of the access control shall prevent the simple access using a lost or stolen access token. Other restrictions may be the need for parallel access by two employees. The technical measures shall include automated measures to support the surveillance.

T.Rugged-Theft: An attacker with specialised equipment for burglary, who may be paid to perform the attack, tries to access sensitive areas and manipulate or steal assets.

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 considered to be sufficiently resourced to circumvent security measures and do not consider any damage of the affected company. The target of the attack may be products that can be sold or misused in an application context. This can comprise devices at a specific testing state for cloning or introduction of forged devices. Those attackers are considered to have the highest attack potential.

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

T.Computer-Net: A possibly paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to logical assets.

A logical attack against the network of the site provides the lowest risk for an attacker. The target of such an attack is to access the company network to get information that may allow to attack a product or manipulate a product or retrieve information to allow or change the configuration. In addition, a successful access to a company network leads to loss of reputation of the company processing the product or the company that produces the product.

Such attackers are considered to have high attack potential because the attacker may have appropriate technical equipment to perform such an attack. Furthermore, the attacker may have the resource to develop or buy software or hardware which can exploit known vulnerabilities within the tools and software used by the company.

Therefore, also for the company network a protective concept with more than one level is expected. This shall comprise a firewall to the external network, and further limitations of the network users and the network services for internal sub-networks. In addition, computer users shall have individual accounts which require authentication using e.g. a password. For specific tasks or processes standalone networks may be required. The protection must be supported by appropriate measures to update and maintain the computer and network systems and analyse logs that may provide indications for attack attempts.

T.Accident-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 production or test area.

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

T.Unauthorised-Staff: Employees or subcontractors not authorised to get access to products or systems used for production get access to products or affect production systems or configuration systems, so that the confidentiality and/or the integrity of the product is violated. This can apply to any production step and any configuration item of the final product as well as to the final product or its configuration.

Especially maintenance tasks of subcontractors may require the access to computer systems storing sensitive data. The implemented security measures may not work because a special dedicated access may be used to the network or specific tools may be used for this dedicated task. This comprises e.g. tools which process the layout data e.g. in the design centre, the mask shop and/or the wafer foundry as well as sensitive test and/or configuration data within the test centre.

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

The attack potential depends on the trustworthiness of the subcontracted company and the access required within the company. Related to this different measures are required.

T.Staff-Collusion: An attacker tries to get access to assets by getting support from one employee through extortion or bribery.

Personal accountability shall be traceable as far as possible. Handover procedures with dual control, enforcement of parallel access by two authorised employees and the split of sensitive knowledge can be implemented to prevent such an attack. The measures depend on the assets that must be protected at the site.

T.Attack-Transport: An attacker might try to get data, specifications or products during the internal shipment and/or the external delivery. The target is to compromise confidential information or violate the integrity of the

products during the stated internal shipment and/or the external delivery process to allow a modification, cloning or the retrieval of confidential information after further production steps. Confidential information comprises assets or part of them

The protection of the internal shipment is based on the configuration of the products that are provided to Shanghai INESA intelligent Electronics Co. Ltd. It is assumed that the features used for testing of the dice at the end of the life cycle phase 3 according to [6] are disabled, refer also to A.Product-Integrity.

## 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 shall support the understanding of the production flow and the security measures of the site. In addition, they shall allow an appropriate mapping to the Security Assurance Requirements (SAR). For each site it must be considered if all policies are required. This means that policies may be combined or may not be applicable based on the task of the site. The documentation of the site under evaluation is under configuration management. This comprises all procedures regarding the evaluated test and assembly flows and the security measures that are in the scope of the evaluation.

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

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

P.Config-Control: The procedures for setting up the production process for a new product as well as the procedure that allows changes of the initial setup for a product shall only be applied by authorized personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The procedure for the initial set up of a production process ensures that sufficient information is provided by the client.

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

P.Config-Process: The services and/or processes provided by a site are controlled in the

configuration management plan. This comprises tools used for the packaging and testing of the product and optimizations of the process flow as well as the documentation that describes the services and/or processes provided by a site.

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

P.Reception-control: The inspection of incoming items done at the site ensures that the received configuration items comply with the properties stated by the client. Furthermore, it is verified that the product can be identified and a released production process is defined for the product. If applicable 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 released products comply with the specification agreed with the client. The acceptance process is supported by automated measures and visual inspection. Records are generated for the acceptance process of the configuration items. Thereby, it is ensured that the properties of the product are ensured when internally shipped.

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, 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 sent back to the client.

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

P.Transport-Prep: Technical and organizational measures ensure the correct labelling of the product. The products are packed as required by the client products in case the standard procedure of Shanghai INESA intelligent Electronics Co., Ltd. Is not applicable. A forwarder selected by the client is verified before the handover of security products. Measures to support traceability during the transport are supported by the selected forwarder.

The following policy supports the electronic transfer of sensitive assets as specified in section 4.1.

P.Data-Transfer: Any data in electronic form (e.g. product specifications, test programs, release information etc.) that is classified as sensitive or higher security level by the client is encrypted to ensure confidentiality of the data. In addition, a signature is used to protect the integrity of the data if

required.

## 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 defined below for the interface with Shanghai INESA intelligent Electronics Co., Ltd.

A.Item-Identification: Each configuration item received by the site is appropriately labelled to ensure the identification of the configuration item.

A.Product-Spec: The client must provide appropriate production specifications and guidance for the assembly and testing of the product. This comprises bond plans for an appropriate assembly process as well as functional test programs or a finished test program appropriate for the final testing. All test programs are developed and provided by the client. The test program will disable test features at the end of the water testing. The provided information includes the classification of the delivered items, documents and data.

A.Internal-Shipment: The recipient (client) of the product is defined by the client. The client provides the address and shipping information (selected forwarder) via secure channel to Shanghai INESA intelligent Electronics Co., Ltd.. The client defines the requirements for packing of the security products in case the standard procedure of Shanghai INESA intelligent Electronics Co., Ltd is not applicable.

A.Product-Integrity: The self-protecting features of the devices are fully operational and it is not possible to influence the configuration and behavior of the devices based on insufficient operational conditions or any command sequence generated by an attacker or by accident.

A.Destruct-Scrap: Scrap are also transferred and they are destructed by the client so that they are useless for an attacker.

The assumptions are outside the sphere of influence of Shanghai INESA intelligent Electronics Co., Ltd . They are needed to provide the basis for an appropriate production process, to assign the product to the released production process and to ensure the proper handling, storage and destruction of all configuration items related to the intended TOE.

# 5. Security Objectives

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organisational security measures allows a sufficient separation of employees to enforce the “need to know” principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorised people. The access control measures ensure that only registered employees can access restricted areas. Assets 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 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 organisational security measures ensure that an alarm is generated before an unauthorised person gets access to any asset. After the alarm is triggered the unauthorised person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack.

O.Internal-Monitor: The site performs security management meetings at least every six months. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures.

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 authorised employees have access to sensitive areas as well as computer/network systems to ensure the protection of the networks and computer systems based on the appropriate configuration.

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 logically separated from any internal network to enforce access control. Access to the production network and related systems is restricted to authorised 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 each product to uniquely identify configuration items and allow an assignment to the client. Also the internal procedures and guidance are covered by the configuration management.

O.Config-Control: The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify configuration items and allow an assignment to the client. Also the internal procedures and guidance are covered by the configuration management. The site applies a release procedure for the setup of the production process for each new product. In addition, the site has a process to classify and introduce changes for services and/or processes of released products. Minor changes are handled by the site; major changes must be acknowledged by the client. A designated team is responsible for the release of new products and for the classification and release of changes. This team comprises specialists for all aspects of the services and/or processes. The services and/or processes can be changed by authorized personnel only. Automated systems support configuration management and production control.

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 protection of test programs and the assembly of the products, for the management of flaws and optimizations of the process flow as well as for the documentation that describes the services and/or processes provided by a site.

O.Acceptance-Test: The site delivers configuration items that fulfil the specified properties. Parameter checks, functional and 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.Zero-Balance: The site ensures that all security products (intended TOE of different clients) are separated and traced on a device basis. Automated control and/or two employees' acknowledgement during hand over is applied for functional and defective devices. All devices are tracked until they are shipped.

O.Reception-control: Upon reception of products an immediate incoming inspection is performed. The inspection comprises the received amount of products and the identification and assignment of the product to a related internal production process.

O.Internal-Transport: The recipient of a physical configuration item is identified by the assigned client address. The internal shipment procedure is applied to the configuration item. 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.Data-Transfer: Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorised employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected.

O.Staff-Engagement: All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.

## 5.1 Security Objectives Rationale

The Site Security Target 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. In chapter 5.1.1 the column 'Note' gives a brief explanation. The detailed rationale can be found in chapter 8.3.

Note that the assumptions defined in this Site Security Target cannot be used to cover any threat or OSP of the site. They are seen as 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

| **Threat** | **Security Objective(s)** | **Note** |
|---|---|---|
| T.Smart-Theft | O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security | The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat. |
| T.Rugged-Theft | O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security | The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat. |

| | | |
|---|---|---|
| T.Computer-Net | O.Internal-Monitor<br>O.Maintain-Security<br>O.Logical-Access<br>O.Logical-Operation<br>O.Staff-Engagement | The technical and organisational measures prevent unauthorised access to internal network. |
| T.Accident-Change | O.Logical-Access<br>O.Config-Control<br>O.Config-Items<br>O.Config-Process<br>O.Acceptance-Test<br>O.Staff-Engagement<br>O.Zero-Balance<br>O.Logical-Operation | The logical access control and configuration management together with organisational measures detect the accident change to the TOE and allow for appropriate response on the threat. |
| T.Unauthorised-Staff | O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security<br>O.Logical-Access<br>O.Logical-Operation<br>O.Staff-Engagement<br>O.Config-Control<br>O.Zero-Balance | Physical and logical access control prohibits access to assets. Both scraps and normal products are under control. |
| T.Staff-Collusion | O.Internal-Monitor<br>O.Maintain-Security<br>O.Staff-Engagement<br>O.Zero-Balance<br>O.Data-Transfer | The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees limits unauthorized access to assets. |
| T.Attack-Transport | O.Internal-Transport<br>O.Data-Transfer | The shipment method and the organizational measures ensure that integrity changes of shipped objects are detected and appropriately responded upon. |

Table 1 Threats - Security Objectives mapping

| OSP | Security Objective(s) | Note |
|---|---|---|
| P.Config-Items | O.Reception-Control<br>O.Config-Items | The Security Objective directly enforces the OSP. |
| P.Config-Control | O.Config-Items<br>O.Config-Control<br>O.Logical-Access | The Security Objective directly enforces the OSP. |
| P.Config-Process | O.Config-Process | The Security Objective directly enforces the OSP. |
| P.Reception-Control | O.Reception-Control | The Security Objective directly enforces the OSP. |

| | | |
|---|---|---|
| P.Accept-Product | O.Config-Control<br>O.Config-Process<br>O.Acceptance-Test | The Security Objective directly enforces the OSP. |
| P.Zero-Balancing | O.Internal-Monitor<br>O.Staff-Engagement<br>O.Zero-Balance | The Security Objective directly enforces the OSP. |
| P.Transport-Prep | O.Config-Process<br>O.Internal-Transport<br>O.Data-Transfer<br>O.Config-Items | The Security Objective directly enforces the OSP. |
| P.Data-Transfer | O.Data-Transfer | The Security Objective directly enforces the OSP. |

**Table 2 OSP - Security Objectives mapping**

# 6. Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

# 7. Security Assurance Requirements

Clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profile [6].

The Security Assurance Requirements are chosen from the class ALC (Life-cycle support) as defined in [3]:

- 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 fulfil the requirements of [5] because hierarchically higher components are used in this Site Security Target. In addition, the minimum set of SAR is extended by SAR of the assurance components for "Life-cycle definition" (ALC_LCD.1).

## 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 Site Security Target, the associated processes for the handling of products, or “intended TOEs” are in the scope of this Site Security Target and are described in this document. These processes are subject of the evaluation of the site.

### 7.1.1 CM Capabilities (ALC_CMC.5)

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

According to [5] the processes rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below.

The configuration control and a defined change process for the procedures and descriptions of the site under evaluation are mandatory. The control process must include all procedures that have an impact on the evaluated production processes as well as on the site security measures.

The life-cycle described in [6] is a complex production process. Only part of this production process is normally provided at a specific site. In such a case the control of the product during such a production process must include sufficient verification steps to ensure the specified and expected result. Test procedures, verification procedures and the associated expected results must be under configuration management for these cases.

The configuration items for the considered product type are listed in section 4.1. The CM documentation of the site is able to maintain the items listed for the relevant lifecycle step and the CM system is able to track the configuration items.

A CM system is employed to guarantee the traceability and completeness of different production charges or lots. Appropriate administration procedures are in place to maintain the integrity and confidentiality of the configuration items.

### 7.1.2 CM Scope (ALC_CMS.5)

The scope of the configuration management for a site certification process is limited to the documentation relevant for the SAR for the claimed life-cycle SAR and the configuration items handled at the site.

In addition, process control data, test data and related procedures and programs can be in the scope of the configuration management.

### 7.1.3 Development Security (ALC_DVS.2)

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 production of the TOE is secure so that no information is unintentionally made available for the operational phase of the TOE. The confidentiality and integrity of test data and configuration data must be guaranteed, access to any kind of samples (client specific samples or open samples) and other material must be restricted to authorised persons only, scrap must be controlled and refunded to the client.

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

If the transfer of configuration items between two sites involved in the production flow is included in the scope of the evaluation (life-cycle covered by the product evaluation) this is considered as internal shipment. In general, the security requirements for confidentiality and integrity are the same but it must be clearly distinguished to ensure the correct subject of the evaluation.

### 7.1.4 Life-cycle Definition (ALC_LCD.1)

The site is not equal to the entire development environment. Therefore, the ALC_LCD criteria are interpreted in a way that only those life-cycle phases have to be evaluated which are in the scope of the site. The PP [6] provide a life-cycle description where specific life-cycles steps can be assigned to the tasks at site. This may comprise a change of the life-cycle state if e.g. testing or initialisation is performed at the site or not.

The PP [6] does not include any refinements for ALC_LCD. The site under evaluation does not initiate a life cycle change of the intended TOE. The products are assembled and the functional devices are delivered to the client. The defective devices are returned to the client.

## 7.2 Security Requirements Rationale

### 7.2.1 Security Requirements Rationale - Dependencies

The dependencies for the assurance requirements 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

Some of the dependencies are not (completely) fulfilled:

- ALC_LCD.1 is only partially fulfilled as the site does not represent the entire development and production environment. This is in-line with and further explained in [5] 5.1 'Application Notes for ALC_CMC'.
- ALC_DEL.1 and ALC_TAT.3 are not applicable therefore no dependency and rationale is required.

### 7.2.2 Security Requirements Rationale – Mapping

| 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 labeling. | O.Config-Items | All products assembled at INESA get a unique client part ID automatically generated by a data base as defined by O.Config-Items. |
| ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items. | O.Reception-Control<br>O.Config-Items<br>O.Config-Control<br>O.Config-Process | Incoming inspection according to O.Reception-Control ensures product identification and the associated labelling. This labelling is mapped to the internal identification as defined by O.Config-Items. This ensures the unique identification of security products.<br>O.Config-Control ensures that each client part ID is setup and released based on a defined process. This comprises also changes related to a client part ID. The configurations can only be done by authorised staff.<br>O.Config-Process provides a configured and controlled production process. |
| ALC_CMC.5.3C: The CM documentation shall justify that the acceptance procedures | O.Reception-Control<br>O.Config-Items<br>O.Config-Control | O.Reception-Control ensures the incoming changed configuration items from the client can be recognized and labelled correctly. |

| SAR | Security Objective | Rationale |
|---|---|---|
| provide for an adequate and appropriate review of changes to all configuration items. | O.Config-Process | O.Config-Items and O.Config-Control ensures the changes to both the internal and external configuration items are recorded and reviewed.<br>O.Config-Process ensures that only authorised staff can apply changes. This comprises changes related to process flows, procedures and items of clients. Teams are defined to assess and release changes. |
| ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items. | O.Reception-Control<br>O.Config-Items<br>O.Config-Control | O.Reception-Control comprises the incoming labelling and the mapping to internal identifications.<br>O.Config-Items comprises the internal unique identification of all items that belong to a client part ID.<br>Each product is setup according to O.Config-Control comprising all necessary items. |
| ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items. | O.Config-Control<br>O.Config-Process<br>O.Logical-Access<br>O.Logical-Operation | O.Config-Control assigns the setup including processes and items for the production of each client part ID.<br>O.Config-Process comprises the control of the production processes.<br>O.Logical-Access and O.Logical-Operation support the control by limiting the access and ensuring the correct operation for all tasks to authorised staff. |
| ALC_CMC.5.6C: The CM system shall support the production of the product by automated means. | O.Config-Process<br>O.Zero-Balance<br>O.Acceptance-Test | O.Config-Process comprises the automated management of the production processes.<br>O.Zero-Balance ensures the control of all security products during production.<br>O.Acceptance-Test provides an automated testing of the functionality 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.Reception-Control<br>O.Acceptance-Test<br>O.Config-Process<br>O.Logical-Access | O.Reception-Control ensures the reception procedure of the physical configuration item. Since the site is only receiving physical configuration item from the client, the person responsible for accepting the physical configuration item cannot be the developer.<br>O.Acceptance-Test ensures the test results are recorded in the CM.<br>O.Config-Process ensures the procedure of the CM plan. It is required in the procedure that the CM manager is not the |

| SAR | Security Objective | Rationale |
|---|---|---|
| | | CM developer.<br>O.Logical-Access ensures the configuration item developer cannot accept the configuration items in the CM system. |
| ALC_CMC.5.8C: The CM system shall clearly identify the configuration items that comprise the TSF. | not applicable | The site receives an implementation representation that does not allow to separate or to identify any parts that comprise TSF. |
| ALC_CMC.5.9C: The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail. | O.Config-Control<br>O.Config-Process<br>O.Config-items<br>O.Acceptance-Test | The automated production control covered by O.Config-Control comprises the logging of all production steps and thereby includes the required audit trail including the originator.<br>O.Config-items ensures the changes of the configuration items are recorded.<br>O.Config-Process ensures that the changes from the production steps are recorded automatically by the CM system.<br>O.Acceptance-Test ensures the changes from the acceptance test are recorded automatically. |
| ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item. | O.Config-Control<br>O.Config-Process | O.Config-Control describes the management of the configuration items received from the client and delivered to the client. According to O.Config-Process the CM plans covers the general dependencies of the production process. |
| ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the TOE is generated. | O.Reception-Control<br>O.Config-Items<br>O.Config-Control<br>O.Config-Process | O.Reception-Control comprises the control of the incoming configuration items.<br>O.Config-Items and O.Config-Control cover the unique labelling and management of the client configuration items.<br>O.Config-Process ensures that only controlled changes are applied. |
| ALC_CMC.5.12C: The CM documentation shall include a CM plan. | O.Config-Control<br>O.Config-Process | According to O.Config-Control the setup of each client part ID includes an associated CM plan including the release.<br>O.Config-Process ensures the reliability of the processes and tools based on dedicated CM plans. |

| SAR | Security Objective | Rationale |
|---|---|---|
| ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE. | O.Config-Control<br>O.Config-Process | O.Config-Control describes the management of the client part IDs at the site.<br>According to O.Config-Process the CM plans describe the services provided by the site. |
| ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE | O.Reception-Control<br>O.Config-Items<br>O.Config-Control<br>O.Config-Process | O.Reception-Control supports the identification of configuration items at INESA.<br>O.Config-Items ensures the unique identification of each product produces at INESA by the client part ID.<br>O.Config-Control ensure a release for each new or changed client part ID.<br>O.Config-Process ensures the automated control of released products |
| ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system. | O.Reception-Control<br>O.Config-Control<br>O.Config-Process<br>O.Zero-Balance<br>O.Internal-Transport | The objectives O.Reception-Control, O.Config-Control, O.Config-Process ensure that only released client part IDs are produced.<br>This is supported by O.Zero- Balance ensuring the tracing of all security products.<br>O.Internal-Transport include the packing requirements, the reports, logs and notifications including the required evidence. |
| ALC_CMC.5.16C: The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system. | O.Config-Control<br>O.Config-Process<br>O.Acceptance-Test<br>O.Internal-Transport | O.Config-Control comprises a release procedure as evidence.<br>O.Config-Process ensures the compliance of the process.<br>O.Acceptance-Test comprises the control that all finished parts based on the test assigned to this part ID.<br>The finished products are returned to the client according to O.Internal-Transport. |

Table 3 Rationale for ALC_CMC.5

| SAR | Security Objective | Rationale |
|---|---|---|
| ALC_CMS.5.1C: The configuration list includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the TOE; the | O.Config-Items<br>O.Config-Control<br>O.Config-Process | Since the process is subject of the evaluation no products are part of the configuration list.<br>O.Config-Items ensures unique part IDs including a list of all items and processes for this part.<br>O.Config-Control describes the release process for each client part ID. |

| SAR | Security Objective | Rationale |
|---|---|---|
| implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan. | | O.Config-Process defined the configuration control including part IDs, procedures and processes. |
| ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items. | O.Config-Items<br>O.Config-Control<br>O.Config-Process<br>O.Reception-Control<br>O.Internal-Transport | Items, products and processes are uniquely identified by the database system according to O.Config-Items.<br>Within the production process the unique identification is supported by automated tools according to O.Config-Control and O.Config-Process. The identification of received products is defined by O.Reception-Control. The labelling and preparation for the transport is defined by O.Internal-Transport. |
| ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item. | O.Config-Items | INESA does not involve subcontractors for the assembly of security products. According to O.Config-Items all configuration items for secure products are identified. |

Table 4 Rationale for ALC_CMS.5

| SAR | Security Objective | Rationale |
|---|---|---|
| ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. | O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Logical-Access<br>O.Logical-Operation<br>O.Staff-Engagement<br>O.Maintain-Security | The physical protection is provided by O.Physical-Access, supported by O.Security- Control, O.Alarm-Response, and O.Maintain-Security. The logical protection of data and the configuration management is provided by O.Logical-Access and O.Logical-Operation. The personnel security measures are provided by O.Staff-Engagement. The scraps are securely stored in the warehouse and returned to the client. A.Destruct-Scrap. |
| ALC_DVS.2.2C: The development security documentation shall justify that the security | O.Internal-Monitor<br>O.Logical-Operation<br>O.Maintain-Security<br>O.Zero-Balance | The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly |

| SAR | Security Objective | Rationale |
|---|---|---|
| measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. | O.Acceptance-Test | implemented and enforced. The associated control and continuous justification is subject of the objectives O.Internal-Monitoring, O.Logical-Operation and O.Maintain-Security. All devices including functional and non-functional are traced according to O.Zero-Balance. O.Acceptance-Test supports the integrity control by functional testing of the finished products. |
| ALC_DVS.2.3C: Confidentiality and integrity of the product during internal shipment. | O.Reception-Control<br>O.Internal-Transport<br>O.Data-Transfer | The reception and incoming inspection supports the detection of attacks during the transport of the security products to INESA according to O.Reception-Control.<br>The delivery to the client is protected by similar measures according to the requirements of the client based on O.Internal-Transport. Sensitive data received by INESA as well as sensitive data sent by INESA is encrypted according O.Data-Transfer to ensure access by authorised recipients only. |

Table 5 Rationale for ALC_DVS.2

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

Table 6 Rationale for ALC_LCD.1

The site always returns the security products back to the client that provided the security products for the assembly. Shanghai INESA intelligent Electronics Co.Ltd. is always involved as subcontractor. There is no delivery of security products directly to the customer regarding the next life cycle step. Therefore, the transport of security products is always considered as internal transport between INESA and the client (ALC_DVS.2).

# 8. Site Summary Specification

## 8.1 Preconditions required by the Site

This site provides wafer sawing and back grinding, module assembly and pre-personalization services for security ICs and similar devices. Wafers or sawn wafers are expected as input for the production lines. Defect devices on the wafer can be marked by inking and/or by electronic wafer map files. The packing and the wafers must be labelled to allow the product identification.

When the wafers are received by INESA as the input for production, the test features of the samples are enabled (i.e. open samples). On the other hand, the test features of the sawn wafers must be disabled (i.e. closed samples) before shipping them to INESA. The wafers delivered to this site are tested before (wafer testing) and after (module functional testing) the assembly using the wafer test program and the module functional test program provided by the client. To protect the samples, the wafer test program must lock the sample after the wafer testing. Because the samples are already locked, the configuration data and/or identification data stored on the samples cannot be changed by the module functional testing in the test environment of this site. Therefore, the final modules are no longer open samples. Since the test features of the sawn wafers are disabled, the sawn wafers are only tested by the module functional test program after assembly.

The production at this site is released after the client accepted the initial sample lot produced by INESA. Therefore each client is in charge for the verification of his products based on the sample lot provided by INESA.

If specific requirements are needed for the transport of the finished products the related specifications and further items e.g. seal tape must be provided to this INESA.

The client is responsible for delivery and transfer of the products. This comprises the selection of the forwarder and the provision of data for the verification of the transport order. The selected forwarder is responsible for the traceability during the transportation.

Secure physical destruction and scrap handling are supported by the client. The site does not provide a secure physical destruction process as a service. All scraps are securely shipped to the client.

All the digital assets delivered between INESA and the client shall be secured by PGP keys.

## 8.2 Services of the Site

The INESA Shanghai site can perform the following secure production activities related to security ICs in accordance with client instructions:

- Wafer testing

  Digital & analogue testing are done on open samples. Optional authentication data is embedded in the wafer test programs for enabling the test mode. After wafer testing, the test features are blocked by the test program. All test programs are provided by the client. Scrap dice may be identified during wafer testing. The scrap dice are first kept in the warehouse then securely shipped back to the client.

- Wafer sawing and back grinding

  Wafer sawing and back grinding according to the production specification and produce dice.

- Module packaging

  The dice are picked, wire bounded and packaged into modules according to the production specification.

- Module testing and pre-personalization

  Module testing: Functional testing on the produced modules without any key involved. Scrap modules may be identified during module testing. The scraps are first kept in the warehouse then securely shipped back to the client. Mainly test the connectivity and basic characteristics of the module.

  Pre-personalization: After the IC module packaging and electrical performance test is completed, the tester pre-loads the personalized data (via the pre-personalization program) of the industry application required by the application issuer into the module. This process is the prerequisite to personalize the IC card terminal industry application.

- Secure physical shipment to the client

  The finished modules and scrap modules/dice are securely shipped back to the client with secure seal. INESA has a standard secure procedure for packing of finished products and preparation of shipment. If special packing requirements are provided by the client they are included in the process setup. The client is alerted if products are ready for transport because the transport must be organized by the client. Therefore only the secure packaging for the shipment is in the certification scope. The shipping method is out of the certification scope. Based on the alert the client provides information on the forwarder that is used for the verification of the forwarder before the handover of the products.

Note: There is no explicit digital key (from the client or the customer) handled in this site. Instead, the authentication data are keys embedded in the test programs provided by the client for wafer testing.

## 8.3 Objectives Rationale

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

O.Physical-Access

The site is a closed area, surrounded by the fence, electric fence and infrared alarms. The access to the building is only possible via access controlled doors. The enabling of the alarm system and the additional external control are graduated according to the running operation at the site. This considers the manpower per shift as well as the operational needs regarding receipt and delivery of goods. The physical, technical and organizational security measures ensure a separation of the site into three security levels. The access

control ensures that only registered persons can access sensitive areas. This is supported by O.Security-Control that includes the maintenance of the access control and the control of visitors. The physical security measures are supported by O.Alarm-Response providing an alarm system.

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

O.Security-Control

The guard service monitors the site and surveillance systems continuously. The CCTV system supports these measures because it is always enabled. Further on the security control is supported by O.Physical-Access requiring different level of access control for the access to security product during operation as well as during off-hours.

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

O.Alarm-Response

The guard service is monitoring the alarm system continuously. The guard is also maintaining and alarm log for review and audit purposes. O.Physical-Access requires certain time to overcome the different level of access control. The response time of the guard and the physical resistance match to provide an effective alarm response.

This addresses the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff

O.Internal-Monitor

Regular security management meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This comprises also logs and security events of security relevant systems like Firewall, Virus protection and access control. Major changes of security systems and security procedures are reviewed. Upon introduction of a new process a formal review and release for mass production is made before being generally introduced.

This addresses T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance

O.Maintain-Security

The security relevant systems enforcing or supporting O.Physical-Access, O.Securitycontrol and O.Logical-Access are checked and maintained regularly by the suppliers. In addition the configuration is updated as required either by employees (for the access control system) of the supplier. Logging files are checked regularly for technical problems and specific maintenance requests.

This addresses T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion

O.Logical-Access

The internal network is separated from the internet. The internal network is further separated into subnetworks by internal firewalls. These firewalls allow only authorized information exchange between the internal subnetworks. Each user is logging into the system with his personalised user name and password. The objective is supported by O.Internal-Monitor based on the checks of the logging regarding security relevant events. The individual accounts are addressing T.Computer-Net. All configuration is stored in the databse of the ERP system. Supported by O.Config-Items this addresses the threats T.Accident-Change and T.Unauthorised-Staff and the OSP P.Config-Control. O.Logical-Operation All logical protection measures are maintained and updated as required, at least once a month. Critical items such as virus scanners are updated regularly. The backup is sufficiently protected and is only accessible for the administration.

This addresses the threats T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff

O.Logical-Operation

All logical protection measures are maintained and updated as required. The gate firewall is evaluated by the third party security company every three months. The backup is sufficiently protected and is only accessible for the administration.

This is addressing the threats T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff

O.Config-Items

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

This is addressing the threat T.Accident-Change and the OSP P.Config-Items, P.Config-Control and P.Transport-Prep.

O.Config-Control

Procedures arrange for a formal release of specifications and test programs by the client based on an engineering run. The information is also stored in the configuration database. The ERP requires personalised access controlled by passwords. Each user has access rights limited to the needs of his function. Thereby only authorised changes are possible.

Supported by O.Config-Items this addresses the threats T.Unauthorised-Staff, T.Accident-Change and the OSP P.Config-Control, P.Accept-Product

O.Config-Process

The released configuration information by the client including production and acceptance specifications is copied to every work order by the authorised personnel. The test program is loaded to the test machine according to the configuration information of the work order.

This addresses the threat T.Accident-Change and the OSP P.Config-Process, P.Accept-Product and P.Transport-Prep.

O.Acceptance-Test

Acceptance tests are introduced and released based on the client's approval. The tools, specifications and procedures for these tests are controlled by the means of O.config-Items and O.Config-Control. Acceptance test results are logged and linked to a work order in the ERP system.

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

O.Staff-Engagement

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

This addresses the threats T.Computer-Net, T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance

O.Zero-Balance

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

This addresses the threats T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance.

O.Reception-Control

At reception each configuration item including security products are identified by the shipping documents, packaging labels and information in the ERP system based on shipment alerts from the clients and supported by O.Config-Items. If a product cannot be identified it is put on hold in a secure storage. Inspection at reception is counting the amount of boxes and checking the integrity of security seals of these boxes if applicable. Thereby only correctly identified products are released for production.

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

O.Internal-Transport

The recipient of a production lot is linked to the work order in the ERP system and can only be modified by authorized users. Packing procedures are documented in the product

configuration. This includes specific requirement of the client. This security objective is supported by O.Staff-Engagement and O.Config-Items.

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

O.Data-Transfer

Sensitive electronic information is stored and transferred encrypted using PGP procedures.

Supported by O.Logical-Acces and O.Staff-engagement this addresses the threats T.Staff-Collusion and T.Attack-Transport as well as the OSP P.Transport-Prep and P.Data-Transfer.

## 8.4 Security Assurance Requirements Rationale

### 8.4.1 CM capabilities (ALC_CMC.5)

ALC_CMC.5.1C The TOE shall be labelled with its unique reference.

ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

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.

ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.

ALC_CMC.5.5C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.5.6C The CM system shall support the production of the TOE by automated means.

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.

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

ALC_CMC.5.9C The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.

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

ALC_CMC.5.11C The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.

ALC_CMC.5.12C The CM documentation shall include a CM plan.

ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.5.14C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

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

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

The chosen assurance level ALC_CMC.5 of the assurance family "CM capabilities" is suitable to support the production of high volumes due to the formalized acceptance process and the automated support. The identification of all configuration items supports an automated and industrialised production process. The requirement for authorized changes support the integrity and confidentiality required for the products. Therefore these security assurance requirements meet the requirements for the configuration management.

### 8.4.2 CM scope (ALC_CMS.5)

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.

The chosen assurance level ALC_CMS.5 of the assurance family "CM scope" supports the control of the production and test environment. This includes product related documentation and data as well as the documentation for the configuration management and the site security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE these security assurance requirements are considered to be suitable.

### 8.4.3 Development Security (ALC_DVS.2)

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

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

The chosen assurance level ALC_DVS.2 of the assurance family "Development security" is required since a high attack potential is assumed for potential attackers. The configuration items and information handled at the site during production, testing of the product can be used by potential attackers for the development of attacks. Therefore the handling and storage of these

items must be sufficiently protected. Further on, the Protection Profile [6] requires this protection for sites involved in the life-cycle of security ICs development and production.

### 8.4.4 Life-cycle definition (ALC_LCD.1)

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.

The chosen assurance level ALC_LCD.1 of the assurance family "Life-cycle definition" is suitable to support the controlled development and production process. This includes the documentation of these processes and the procedures for the configuration management. Because the site provides only a limited support of the described life-cycle for the development and production of security ICs the focus is limited to this site. However the assurance requirements are considered to be suitable to support the application of the site evaluation results for the evaluation of an intended TOE.

## 8.5 Assurance Measure Rationale

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

O.Maintain-Security

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

O.Logical-Access

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design, implementation and in its development and production environment. Thereby this objective is suitable to meet the Security Assurance Requirement. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items. Thereby this objective contributes to meet the Security Assurance Requirement. ALC_CMC.5.7C requires that CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.

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 TOE design, implementation and in its development and production environment. Thereby this objective contributes to meet the Security Assurance Requirement. ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective is suitable to meet the Security Assurance Requirement. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items. 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. ALC_CMC.5.2C requires to describe the method used to uniquely identify the configuration items. The acceptance procedures provide for an adequate review of changes to the CIs is required by ALC_CMC.5.3C. In addition ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.9C requires the CM system shall support the audit of changes to TOE by automated means. ALC_CMC.5.14C requires that the CM plan describes the procedures used to accept modified or newly created configuration items as part of the TOE. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_CMS.5.2C requires that the developer of each TSF relevant configuration item is indicated in the configuration list. The objective meets the set of Security Assurance Requirements.

O.Config-Control

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items. ALC_CMC.5.6C requires the CM system to support the production of the intended TOE by automated means. ALC_CMC.5.9C requires the support of audit information for all changes to the TOE by automated means including the originator, date and time. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a change given to a configuration item. ALC_CMC.5.11C requires that the version of test programs and the production processes used for production can be identified. ALC_CMC.5.12C requires a CM documentation that includes a CM plan. ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development (production) of the TOE. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. In addition ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products. The objective meets the set of Security Assurance Requirements.

O.Config-Process

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. The provision of automated measures such that only authorized changes are made to the configuration items as required by ALC_CMC.5.5C. ALC_CMC.5.6C requires that the CM system supports the production by automated means. ALC_CMC.5.7C requires that the person or team accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.9C requires the CM system shall support the audit of changes to TOE by automated means. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a change given to a configuration item. ALC_CMC.5.11C requires that the version of test programs, internal procedures and processes used at the site can be identified. 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 TOE. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_LCD.1.1C requires that the lifecycle definition documentation describes the model used to develop and maintain the products. ALC_LCD.1.2C requires control over the development and maintenance of the TOE. The objective meets the set of Security Assurance Requirements.

O.Acceptance-Test

The testing of the products is considered as automated procedure as required by ALC_CMC.5.6C. ALC_CMC.5.7C requires that the CM system ensures that the person responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.9C requires the CM system shall support the audit of changes to TOE by automated means. ALC_CMC.5.13C requires that the CM plan describe how the CM system is used to accept finished configuration items. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items. The operation of the CM system in accordance with the CM plan is required by ALC_CMC.5.16C. In addition ALC_LCD.1.2C requires control over the development and maintenance of the TOE. ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the TOE during production. 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 TOE design and implementation in its development environment. Thereby the objective fulfils this combination of Security Assurance Requirements.

O.Zero-Balance

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

O.Reception-Control

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.7C requires that the person accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.11C requires that the version of design data used to generate the test scripts can be identified. ALC_CMC.5.14C requires that the version of test programs and the production processes used for production can be identified. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the TOE during internal transport. Thereby this objective is suitable to meet the Security Assurance Requirement

O.Internal-Transport

ALC_DVS.2.2C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE. This includes also the protection during internal transport. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. ALC_CMS.5.2C according the unique identification of the packing as configuration item. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Data-Transfer

ALC_DVS.2.2C: 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. This includes also the protection during the transport between production sides. Thereby this objective is suitable to meet the Security Assurance Requirement.

## 8.6 Mapping of the Evaluation Documentation

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. References


[1] "Site Security Target Template, Version 1.0, published by Eurosmart," Eurosmart, 21.06.2009.

[2] "Common Criteria for Information Technology Security Evaluations, Part 1: Introduction and General Model; Version 3.1, Revision 5," April 2017.

[3] "Common Criteria for Information Technology Security Evaluation, Part3: Security Assurance Requirements; Version 3.1, Revision 5," April 2017.

[4] "Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5," April 2017.

[5] "Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001," October 2007.

[6] "Security IC Platform Protection Profile with Augmentation Packages, Version 1.0," Eurosmart, 13.01.2014.


## 9.1 Definitions

Client The site providing the Site Security Target may operate as a subcontractor of the TOE manufacturer. The term “client” is used here to define this business connection. It is used instead of customer since the terms “customer” and “consumer” are reserved in CC. In this document, the terms “customer” and “consumer” are only used in the sense of the CC.

## 9.2 List of Abbreviations

CC Common Criteria

EAL Evaluation Assurance Level

IC Integrated Circuit

IP Intellectual Property

IT Information Technology

OSP Organizational Security Policy

PP Protection Profile

SAR Security Assurance Requirement

SST Site Security Target

ST Security Target

**TOE Target of Evaluation**