# Site Security Target – ICTK Seoul

## Lite version

*Version 2.0*

**January 10, 2025**

## Table of Contents

1. Document Information ..... 4
1.1. Reference ..... 4
1.2. Version History ..... 5
2. Introduction ..... 6
2.1. Identification of the Site ..... 6
2.2. Site Description ..... 6
2.2.1. Physical Scope ..... 6
Logical Scope ..... 6
2.2.2 ..... 6
3. Conformance Claim ..... 8
4. Security Problem Definition ..... 9
4.1. Assets ..... 9
4.1.1. Security IC Embedded Software Development ..... 9
4.1.2. IC Development ..... 9
4.1.3. Product Finishing Process ..... 9
4.1.4. Product Personalization ..... 10
4.1.5. Certification Data for Site ..... 10
4.1.6. Cryptographic Keys ..... 10
4.1.7. Development Tools: ..... 10
4.2. Threats ..... 10
4.3. Organizational Security Policies ..... 11
4.4. Assumptions ..... 13
5. Security Objectives ..... 14
5.1. Introduction ..... 17
5.2. Mapping of Security Objectives ..... 18
5.3. Security Objectives Rationale ..... 19
6. Extended Assurance Components Definition ..... 23
7. Security Assurance Requirements ..... 24
7.1. Application Notes and Refinements ..... 24
7.1.1. Overview and Refinements regarding CM Capabilities (ALC_CMC.5) ..... 24
7.1.2. Overview and Refinements regarding CM Scope (ALC_CMS.5) ..... 25
7.1.3. Overview and Refinements regarding Delivery Procedure (ALC_DEL.1) ..... 25
7.1.4. Overview and Refinements regarding Development Security (ALC_DVS.2) ..... 25
7.1.5. Overview and Refinements regarding Life-cycle Definition (ALC_LCD.1) ..... 26
7.1.6. Overview and Refinements regarding Tools and Techniques (ALC_TAT.3) ..... 26
7.2. Security Assurance Rationale ..... 26
8. Site Summary Specification ..... 36
8.1. Preconditions Required by the Site ..... 36
8.2. Services of the Site ..... 37
9. References ..... 40
9.1. Literature ..... 40
9.2. Definitions ..... 40
9.3. List of Abbreviations ..... 40
10. Contact Information ..... 41

## List of Tables

Table 1. Mapping of Security Objectives ..... 18
Table 2. Rationales, Aspects and References for ALC_CMC.4 ..... 27
Table 3. Rationales, Aspects and References for ALC_CMS.4 ..... 31
Table 4. Rationales, Aspects and References for ALC_DVS.2 ..... 32
Table 5. Rationales, Aspects and References for ALC_DEL.1 ..... 33
Table 6. Rationales, Aspects and References for ALC_LCD.1 ..... 33
Table 7. Rationales, Aspects and References for ALC_TAT.3 ..... 35
Table 8. Precondition of assumptions ..... 36
Table 9. Details of the services provided by the site ..... 37

# 1. Document Information

## 1.1. Reference

- Title: Site Security Target Lite – ICTK Seoul
- Version: 2.0
- Date: January 10, 2025
- Company: ICTK Co., Ltd.
- Name of the site: ICTK Seoul
- Address: 16, Gangnam-daero 84-gil, Gangnam-gu, Seoul, Republic of Korea
  (Jace Tower)
- Product type: Security IC
- Site type: Development and Provisioning Test, Documentation
- EAL-Level: The site allows the development of TOEs with an EAL level up to EAL 6

## 1.2. Version History

| Version | Date | Comment/Editor/Changes |
|---|---|---|
| 1.0 | December 13, 2024 | Initial version |
| 2.0 | January 10, 2025 | reviewed and corrected the discrepancies between the SST Lite and SST documents. |
| | | |

# 2. Introduction

This chapter is divided into the sections “Identification of the Site” and “Site Description”.

This document is based on the Eurosmart Site Security Target Template [6] with adaptations such that it fits the site (i.e. datacenter, no production).

This Site Security Target is intended to be used by ICTK.

## 2.1. Identification of the Site

The site ICTK Head Office is located at:

16, Gangnam-daero 84-gil, Gangnam-gu, Seoul, Republic of Korea (Jace Tower)

The building is also used by other companies. This site within the SoC Group provides SoC development and IP development, carries out provisioning and testing of security ICs that are produced externally and imported. The certification scope includes the development team(7F) and the Provisioning & Testing Room. (B1F)

## 2.2. Site Description

### 2.2.1. Physical Scope

The following areas of the plant specified in Section 2.1 are in the scope of the SST.

The surroundings of this building are not in the scope of the SST. Therefore, the walls of this building form the physical boundary of the site.

The following physical locations are in scope of the certification:

- The ICTK Development Area is located in the 7th floor.
  - R&D Unit
  - Server Room
- ICTK Provisioning and Testing Area is located in the Basement1.
  - Provisioning and Testing Room
  - Packing room
  - Locker room
  - Warehouse

The development, provisioning and testing areas are a security area with restricted access where only authorised persons are allowed to enter this area.

Within these areas, only members of the development, provisioning and test teams are entitled to access sensitive information like source code, confidential development documentation, emulators, simulators and samples. To enforce such access restriction, a combination of physical, procedural, personnel and logical measurements have been installed.

### 2.2.2. Logical Scope

The full scope of the site evaluation process, as defined in the 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084) is as follows:

- Phase1: Security IC Embedded Software Development
- Phase2: IC Development (IC design, IC Dedicated Software development)
- Phase3: IC Manufacturing and Testing
- Phase4: IC Packaging
- Phase5: Security IC Product Finishing (IC Test)
- Phase6: Security IC Personalization (Provisioning & delivery)
- Phase7: Security IC End-usage

Among these, the ICTK Seoul site supports only Phase1, Phase2, Phase5, and Phase6 of the entire 7 life cycle phases, as follows:

- Phase1: Security IC Embedded Software Development
- Phase2: IC Development (IC design, IC Dedicated Software development)
- Phase5: Security IC Product Finishing (IC Test)
- Phase6: Security IC Personalization (Provisioning & delivery)

The TOE Delivery is included in Phase 5 and Phase 6. Details about the delivery services provided by the site are described in Chapter 8.2.

# 3. Conformance Claim

This SST is conformant to 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, Revision 5, April 2017 [2]

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology [2]
- JIL-Minimum Site Security Requirements v3.1, December 2023 [2]

The evaluation of the site comprises the following assurance components:

- ALC_CMC.5
- ALC_CMS.5
- ALC_DEL.1
- ALC_DVS.2
- ALC_TAT.3
- ALC_LCD.1

This SST is Common Criteria Part 3 conformant.

The optional assurance family ALC_FLR is not part of the evaluation.

The assurance level chosen for the SST is compliant to the Protection Profile (PP) [4] and therefore suitable for the evaluation of (software for) Security ICs.

The chosen assurance components for the Site Security Target are taken from the definition of the EAL6 package defined in CC Part3, to support product evaluations up to EAL6 on this site. For the assessment of the security measures attackers with a high attack potential are assumed. Therefore, this site supports product evaluations up to EAL6.

# 4. Security Problem Definition

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

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

## 4.1. Assets

The following section describes the assets handled at the site.

### 4.1.1. Security IC Embedded Software Development

- Software specifications
- Source code in any form (ROM code or Flash,EEPROM code)
- Pre-personalization data
- Guidance documentation
- FPGAs containing netlists, (SmartCard Emulator),
- Un-fused secure element samples, (chips, cards),
- Physical prototype samples, (chips, cards),
- Development boards

### 4.1.2. IC Development

- Hardware and IC Dedicated Software specifications
- Source code for software and hardware (for software consider ROM code and/or Flash EEPROM code)
- Layout data for the hardware
- Pre-personalization data (optionally this data may include initialization data of the customer)
- initial communication key used when the chip is first connected
- Guidance documentation

### 4.1.3. Product Finishing Process

- modules or other packages
- finished products
- product specifications
- optionally initialization data
- test programs

- test vectors

### 4.1.4. Product Personalization

- finished products
- test program
- personalization data

### 4.1.5. Certification Data for Site

- Site Security Manual
- Document list

### 4.1.6. Cryptographic Keys

- Digital Keys, including secure boot private keys, secure boot symmetric keys, etc.

### 4.1.7. Development Tools:

- Development tools for hard and software development (e.g. compiler)

The assets that need to be protected should be clearly identified and managed based on their asset importance (confidentiality, integrity, and availability).

## 4.2. Threats

Threats damage the integrity and confidentiality of the intended TOE and the representation of parts of the TOE. The threats identified for the site imply the necessity of defining assets which are endangered by those threats, those assets are described in 4.1 Assets.

The threats at this site are considered as follows:

**T.Smart-Theft:** An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive assets. The attacker has enough time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered. In addition, the attacker may be able to use specific working clothes of the site to camouflage the intention.

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

**T.Computer-Net:** A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get access to development with the intention to modify the development process thus violating integrity and possibly confidentiality (*).

**T.Accident-Change:** An employee, contractor or student trainee may change tool configuration that have an impact on the intended TOE by accident.

**T.Unauthorised-Staff:** Unauthorised employees or subcontractors get access to assets or systems used for development, configuration management, so that the confidentiality and/or the integrity of the intended TOE is violated. This can apply to any development and any asset related to the intended TOE or its configuration.

| | |
|---|---|
| **T.Staff-Collusion:** | An attacker tries to get access to assets handled at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery. |
| **T.Attack-Transport:** | An attacker might try to get hold of any assets during the internal shipment and/or the external delivery. The target is to compromise confidential information or violate the integrity of the assets during the shipment/delivery process to allow a modification, cloning or the direct/indirect retrieval of confidential information. |

The threats identified for the site imply the necessity of defining objectives which are intended to minimise the following risks:

1. physical loss
2. intellectual loss
3. loss of reputation

Any physical or intellectual loss may lead to project realisation disturbance or may even cause a project to be discontinued.

Loss of reputation may cause the site to stop being considered trustworthy by the current and potential clients.

(*) whatever is applicable for this site according to chapter 1.1 (Reference – Site type) and 4.1 (Assets).

## 4.3. Organizational Security Policies

| | |
|---|---|
| **P.Config-IT_Env:** | In addition to the used software on development workstations and servers, the site uses configuration management systems for file versioning and problem tracking. For file versioning and problem tracking, the team members are assigned to project specific, centralized repositories to support proper management of multiple products and the site internal procedures. The team members are requested to use only project related IT equipment with the provided tools. |
| **P.LifeCycle-Doc:** | The site uses life-cycle documentation that describe:<br>1. Description of configuration management systems and their usage;<br>2. A configuration items list;<br>3. Site security;<br>4. The development process;<br>5. The development tools. |
| **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 or used at a site as well as the received and transferred and/or provided items. |
| **P.Config-Control:** | The procedures for setting up the development process for a new product as well as the procedure that allows changes of the initial setup for a product is only applied by authorised personnel. Automated systems 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 development process ensures that sufficient information is provided by the client. |

| | |
|---|---|
| **P.Config-Process:** | The services and/or processes provided by the site are controlled in the configuration management plan. This comprises incoming items, tools used for the development 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. A released development process is defined and under version control. |
| **P.Reception-Control:** | The inspection of incoming items done at the site ensures that the received assets comply with the properties stated by the client. If applicable this aspect includes the check that all required information and data is available to handle the incoming items. |
| **P.Accept-Product:** | The testing and quality control of the site ensures that the released intended TOE comply with the specification agreed with the client. The acceptance process is supported by automated measures. Records are generated for the acceptance process of the assets. Thereby, it is ensured that the properties of the intended TOE are ensured when internally shipped/externally delivered. |
| **P.Organise-Product:** | The development, configuration, pre-personalisation, initialization or personalisation process is applied as specified by the client/ICTK. If the data includes sensitive items like keys relevant for the life-cycle or configuration data that affect the security of the intended TOE, appropriate measures are in place. This includes the requirement that the knowledge of sensitive keys is split to at least two different persons. Furthermore, technical measures like crypto-boxes, separation of network, split access permission and secure storage is implemented for this kind of data. |
| **P.Product-Transport:** | Technical and organisational measures ensure the correct labelling of the intended TOE. A controlled internal shipment and/or the external delivery (*) is applied. The transport supports traceability up to the recipient. If applicable or required, this policy includes measures for packing to protect the product during transport. |
| **P.Data-Transfer:** | Any data in electronic form (e.g. keys, initialization data, design data, job deck, product specifications, test programs, test program specifications, 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, measures are used to control the integrity of the data after the transfer. |
| **P.Zero-Balance:** | Site ensures that all sensitive items (on the intended TOE from clients) are separated and traced by devices basis. Security products are traced and recorded to ensure traceability in the Inventory management system. As per the released production process the defect assets are either destroyed at the manufacturer or sent back to the ICTK. or customer and/or consumer (depending on the production-setup). The sent-back procedures, whether to the ICTK or to the customer, are controlled through internal compliance policies and procedures. |
| **P.Scrap-Items:** | Any item that is defect, end-of-life or that does not comply with the quality requirements is shipped back to the client for destruction or is scrapped at the site in a way that the destructed item does not support any attacker. |

## 4.4. Assumptions

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

| | |
|---|---|
| **A.Secure-IT-Provisioning:** | The local IT equipment (e.g. workstations, servers, HSMs) is connected to a secure IT-Infrastructure through a secure (encrypted) network connection. The local secure IT-infrastructure together with the secure IT-infrastructure and the secure connection between them will satisfy all relevant ALC requirements.<br><br>The main logical assets are stored on the NAS Server. The NAS allows access only to pre-approved accounts through ID-based authentication. Access permissions to the NAS is only granted for pre-approved IP addresses workstations. The scope of access can be configured to distinguish between entire employees, entire departments, specific individuals within a department, and specific individuals within the company. |
| **A.Prod-Specification:** | The client must provide appropriate information (e.g. specifications, definitions, process limits, process parameters, test requirements, test limits, bond plans, configuration, pre-personalization, initialization and personalization) to ensure an appropriate development process. The provided information includes the classification of the documents and product. |
| **A.Item-Identification:** | Each configuration item received by the site is appropriately labelled to ensure the identification of the configuration item. |
| **A.External-Delivery:** | The customer of the product is identified by his address. The address of the customer is part of the product setup in the ICTK system. |
| **A.Internal-Shipment:** | The recipient (client) of the product is identified by the address of the client site. The address of the client is part of the product setup. |
| **A.Init-Data:** | The scripts for the configuration and initialization process are created by ICTK of the product. |

# 5. Security Objectives

The Security Objectives are related to physical, technical and organizational security measures, the configuration management as well as the internal shipment and/or the external delivery.

**O.Config-IT_Env:** In addition to the used software on development workstations/systems and servers, the site uses configuration management systems for file versioning and problem tracking. For file versioning unique repositories are used to support proper management of multiple products and the site internal procedures.

*This directly addresses the OSP P.Config-IT_Env.*

**O.LifeCycle-Doc:** Dedicated documents exist which define the use and the management of the configuration management systems, the site security, the development process and the development tools. The site follows the procedures and instructions of these documents.

*This directly addresses the OSP P.LifeCycle-Doc. The threat T.Attack-Transport can be prevented.*

**O.Physical-Access:** The combination of physical partitioning between the different access control levels together with technical and organizational security measures allows enough separation of employees to enforce the "need to know" principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorized people. The site enforces two or three levels of access control to sensitive areas of the site. The access control measures ensure that only registered employees and vendors can access restricted areas. Sensitive products and data are handled in restricted areas only. Network cabling is protected according to classification of the transferred data by avoiding routes through public areas or by usage of appropriate cryptographic measures.

*By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.*

**O.Security-Control:** Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers.

*By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.*

**O.Alarm-Response:** The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any sensitive configuration item (asset). After the alarm is triggered the unauthorized person still must overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack.

*By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.*

**O.Internal-Monitor:** The site performs security management meetings at least every year. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure enough protection.

*This helps to prevent the threat(s) T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff and T.Staff-Collusion.*

**O.Maintain-Security:** Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorized employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.

*This helps to prevent the threat(s) T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.*

**O.Logical-Access:** The site implements a firewall system to enforce a logical separation between the internal network and the internet. The firewall system ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into development networks, office and administration network. Specific networks for development and configuration/administration are further logically separated from other internal network to enforce access control. Access to the development network and related systems is restricted to authorised employees involved in the configuration tasks of the development systems. Every user of an IT system has its own user account and password. An authentication using a unique 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 applies a release procedure for the setup of the development 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

| | |
|---|---|
| | authorised personnel only. Automated systems support configuration management and development 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 development of the product, for the management of flaws and optimizations of the process flow as well as for the documentation that describes the services and/or processes provided by a site. |
| **O.Acceptance-Test:** | The site delivers assets that fulfil the specified properties. Parameter checks, functional and/or visual checks and tests are performed to ensure the compliance with the specification. The test results are logged to support tracing and the identification of systematic failures. |
| **O.Organise-Product:** | For the configuration, pre-personalization, initialization or personalization process it is ensured that the specified process is applied. The data integrity is controlled. Keys and other sensitive data can only be constructed by at least two employees. The operation is applied in crypto-boxes or similar devices. After the release process changes are only applied based on the request of the client/ICTK. The update is done according to a controlled process. |
| **O.Staff-Engagement:** | All employees who have access to sensitive assets and who can move parts of the product out of the defined development (*) flow are checked regarding security concerns and have to sign a nondisclosure agreement. Furthermore, all employees are trained and qualified for their job. |
| **O.Reception-Control.** | Upon reception of any product/ intended TOE (*) an immediate incoming inspection is performed. The inspection comprises the received amount, their identification and the assignment of the items to a related internal process. |
| **O.Internal-Shipment:** | 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 assets during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined. |
| **O.External-Delivery:** | The recipient of a physical configuration item is identified by the assigned consumer address. The external delivery procedure is applied to the sensitive configuration item. A delivery address is assigned to each product and subject of a controlled process. The packaging is also part of the defined process and applied as specified by the client. The forwarder supports the tracing of sensitive assets during external delivery. For every 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 authorized employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected. |

**O.Zero-Balance:** The site ensures that the status of security products is traced. Security products are traced and recorded to ensure traceability in the inventory management system.

**O.Control-Scrap:** The site has measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive assets so that they do not support an attacker.

(*) whatever is applicable for this site according to chapter 1.1 (Reference – Site type) and 4.1 (Assets).

## 5.1. Introduction

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

## 5.2. Mapping of Security Objectives

**Table 1. Mapping of Security Objectives**

| Security Objectives / Threats/OSPs | O.Config-IT_Env | O.LifeCycle-Doc | O.Physical-Access | O.Security-Control | O.Alarm-Response | O.Internal-Monitor | O.Maintain-Security | O.Logical-Access | O.Logical-Operation | O.Config-Items | O.Config-Control | O.Config-Process | O.Acceptance-Test | O.Organise-Product | O.Staff-Engagement | O.Reception-Control | O.Internal-Shipment | O.External-Delivery | O.Data-Transfer | O.Zero-Balance | O.Control-Scrap |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T.Smart-Theft | | | X | X | X | X | X | | | | | | | | | | | | | | |
| T.Rugged-Theft | | | X | X | X | X | X | | | | | | | | | | | | | | |
| T.Computer-Net | | | | | | | X | X | | | | | | | | | | | | | |
| T.Accident-Change | | | | | | | | X | X | X | X | X | X | | X | | | | | X | X |
| T.Unauthorised-Staff | | | X | X | X | X | X | | X | | | | | | X | | | | | X | X |
| T.Staff-Collusion | | | | | | X | X | | | | | | | | X | | | | | X | X |
| T.Attack-Transport | | X | | | | | | | | | | | | | | | X | X | | X | |
| P.Config-Items | | | | | | | | | | X | | | | | | X | | | | | |
| P.Config-Control | | | | | | | | X | | X | X | | | | | | | | | | |
| P.Config-Process | | | | | | | | | | | | X | | | | | | | | | |
| P.Reception-Control | | | | | | | | | | | | | | | | X | | | | | |
| P.Accept-Product | | | | | | | | | | | X | X | X | | | | | | | | |
| P.Organise-Product | | | | | | | | X | X | | X | X | | X | | | | | | | |
| P.Product-Transport | | | | | | | | | | | | X | | | | | X | X | X | | |
| P.LifeCycle-Doc | | X | | | | | | | | | | | | | | | | | | | |
| P.Config-IT_Env | X | | | | | | | | | | | | | | | | | | | | |
| P.Data-Transfer | | | | | | | | | | | | | | | | | | | X | | |
| P.Zero-Balance | | | | | | | | | | | | | | | | | | | | X | |
| P.Scrap-Item | | | | | | | | | | | | | | | | | | | | X | X |

Note that the assumptions of the SST cannot be used to cover any threat or OSP of the site. They are pre-conditions fulfilled either by the site providing the sensitive assets or by the site receiving the sensitive assets. Therefore, they do not contribute to the security of the site under evaluation.

## 5.3. Security Objectives Rationale

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

**O.Config-IT_Env:** The site uses only project related tools and IT equipment. To provide a separation between different projects, the site uses configuration file versioning and unique repositories as well as configuration management systems.

*This directly addresses the OSP P.Config-IT_Env.*

**O.LifeCycle-Doc:** Dedicated documents exist which define the use and the management of the configuration management systems, the site security, the development process and the development tools. The site follows the procedures and instructions of these documents.

*This directly addresses the OSP P.LifeCycle-Doc. The threat T.Attack-Transport can be prevented.*

**O.Physical-Access:** The site implements a “need to know” principle by separation measures using a combination of physical partitioning together with technical and organisational security measures. The access control measures support the enforcement of the separation and the “need to know” principle. The handling of assets is restricted to separate security areas.

*By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.*

**O.Security-Control:** The site is using dedicated, trained security personnel for guard services. These personnel are responsible for operation of the access control and alarm systems, performing patrol rounds, visitor registration, physical key management, the surveillance of the technical alarm sensors and the responses to incidents.

*By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.*

**O.Alarm-Response:** In case of an access attempt to an asset by an unauthorized person, the site has an alarm system in place. After the alarm is triggered the unauthorised person still must overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack.

*By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.*

**O.Internal-Monitor:** Regular meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This includes the assessment of security alarms and associated logs of the physical and logical protection. In addition, results of internal audits and assessments are reviewed.

| | |
|---|---|
| | *This helps to prevent the threat(s) T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff and T.Staff-Collusion.* |
| **O.Maintain-Security:** | The security related surveillance and alarm systems are maintained on a regular basis. The physical and logical access permission are reviewed and updated if needed. Logs of the associated systems are reviewed to support the work.<br><br>*This helps to prevent the threat(s) T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.* |
| **O.Logical-Access:** | The secure IT network is split in several segments according to different security level and purpose (development, administration, lab, manufacturing). The protection of network segments is implemented according to the classification of the processed data. The separation is enforced by firewalls and additional network components. Network services are limited to prevent the misuse and the access to network segments. User accounts are limited to the access rights required by the job task following a strict "need to know principle".<br><br>*This helps to address the OSP(s) P.Config-Control and P.Organise-Product. This helps to prevent the threat(s) T.Computer-Net and T.Accident-Change.* |
| **O.Logical-Operation:** | Virus protection and patch management for operating systems and applications ensure the secure operation of the computer systems and the defense against malfunctions provoked by malicious software. Furthermore, backup of the development control system and data processing tools is implemented and the classified data from the client is excluded from the backup.<br><br>*This directly addresses the OSP P.Organise-Product. This helps to prevent the threat(s) T.Unauthorised-Staff and T.Accident-Change.* |
| **O.Config-Items:** | The different items part of an "intended TOE" and the "intended TOE" itself is under configuration management. This configuration management system assigns unique identification numbers.<br><br>*This helps to address the OSP(s) P.Config-Items and P.Config-Control. This helps to prevent the threat T.Accident-Change.* |
| **O.Config-Control:** | "Intended TOE" development is performed by authorized people using configuration management plan and change management. Automated tools are used for configuration management and for development control.<br><br>*This helps to address the OSP(s) P.Organise-Product, P.Config-Control, P.Accept-Product . This helps to prevent the threat T.Accident-Change.* |
| **O.Config-Process:** | The control of the released development processes and the controlled introduction of changes ensure a reproducible and consistent development. Procedures for setting up the development process as well as changes to the released processes and documents are in place. Changes can only be done by authorised personnel. A team of specialists ensures that all aspects are covered for the introduction of |

| | |
|---|---|
| | new processes and for the assessment of changes. All documentation is under configuration management.<br><br>*This helps to address the OSP(s) P.Product-Transport, P.Organise-Product, P.Accept-Product and P.Config-Process. This helps to prevent the threat T.Accident-Change.* |
| **O.Acceptance-Test:** | After receiving the products from the subcontractor the data processing process includes verification steps. Several times the resulting data from the data processing is verified by ICTK and the results are verified against the design data and the requirement specification of ICTK.<br><br>*This directly addresses the OSP P.Accept-Product. This helps to prevent the threat(s) T.Accident-Change.* |
| **O.Organise-Product:** | Technical and organizational tools are used to ensure that the development and product finishing of the configuration items fulfill the specified process requirements. When receiving configuration, pre-personalization, initialization or personalization data, team in charge of these activities are trained to decipher the received package, to verify the origin of these data and to verify the integrity of received package.<br><br>*This directly addresses the OSP P.* Organise-Product. |
| **O.Staff-Engagement:** | The site has established personnel security measures. All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. This provides legal liability to protect the assets against disclosure. Furthermore, all employees are qualified for their job, are trained and had to pass a questionnaire to check the security awareness.<br><br>*This helps to prevent the threat(s) T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion.* |
| **O.Reception-Control.** | When design/test data is received, the integrity and completeness of the data is verified and assigned to the related client order. The link between data and client order ensures the unique identification. When receiving physical assets, an inspection of the items is performed in order to acknowledge the correct amount, their identification and the assignment. Received assets are registered within the tracking system.<br><br>*This helps to address the OSP(s) P.Reception-Control and P.Config-Items.* |
| **O.Internal-Shipment:** | Packing procedures including seal tape and the tracking of the transport support the identification of manipulations during the transport. The address of the client is part of the product setup and included in the requirements specification of the client.<br><br>*This directly addresses the OSP P.Product-Transport. The threat T.Attack-Transport can be prevented.* |

| | |
|---|---|
| **O.External-Delivery:** | The external delivery procedure is agreed with the every client. The procedure defines the recipient and the secure delivery procedures. Therefore this objective can support to prevent T.Attack-Transport.<br><br>*This directly addresses the OSP P.Product-Transport. The threat T.Attack-Transport can be prevented.* |
| **O.Data-Transfer:** | The integrity and confidentiality of the data transfer from/to the site is protected against modification and/or disclosure by cryptographic means during transfer. The selected cryptographic algorithms are appropriate to resist against high attack potential. Cryptographic keys and password used for secure communication are sufficiently protected against unauthorised access and disclosure.<br><br>*This helps to address the OSP P.Product-Transport and P.Data-Transfer.* |
| **O.Zero-Balance:** | Products are uniquely identified throughout the whole process. The amount of functional and non-functional dies on a wafer and for a production order is known. Scrap and rejects are following the good products thru the whole production process. At every process step the registration of good and rejected products is recorded and updated in the inventory management system.<br><br>*This helps to address the OSP(s) P.Zero-Balance and P.Scrap-Items. This helps to prevent the threat(s) T.Accident-Change,T.Attack-Transport, T.Unauthorised-Staff and T.Staff-Collusion.* |
| **O.Control-Scrap:** | The security of scrap handling is ensured by either securely destruct assets at the site (e.g. paper shredder) or return them to the client. Scrap material is stored, until destruction or shipment back to the client, in security environments. Procedures document the destruction process.<br><br>*This helps to address the OSP(s) P.Scrap-Items and P.Zero-balance. This helps to prevent the threat(s) T.Accident-Change, T.Unauthorised-Staff and T.Staff-Collusion.* |

# 6. Extended Assurance Components Definition

No extended components are currently defined in this SST template.

# 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 [5].

The Security Assurance Requirements (SAR) are:

**Class ALC:** Life-cycle support
CM capabilities (ALC_CMC.5)
CM scope (ALC_CMS.5)
Delivery (ALC_DEL.1)
Development security (ALC_DVS.2)
Life-cycle definition (ALC_LCD.1)
Tools and techniques (ALC_TAT.3)

The Security Assurance Requirements listed above fulfil the requirements of [4] because hierarchically higher components are used in this SST. In addition, the minimum set of SARs is extended by SAR of the assurance components for "Delivery" (ALC_DEL.1), "Life-cycle definition"(ALC_LCD.1) and "Tools and techniques" (ALC_TAT.3).

## 7.1. Application Notes and Refinements

The description of the site certification process [4] includes specific application notes. The main item is that a product that is considered as "intended TOE" is not available during the evaluation. Since the term "TOE" is not applicable in the SST the associated processes for the handling of products or "intended TOEs" are in the focus and described in this SST. These processes are subject of the evaluation of the site.

### 7.1.1. Overview and Refinements regarding CM Capabilities (ALC_CMC.5)

Configuration Management, as being the practice of handling all project changes systematically to maintain project integrity over time, is defined at the project starting phase.

According to [4] the processes rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below. Since the application notes in [4] are defined for ALC_CMC.5.

ICTK implements certain procedures, rules and uses tools that are required to manage and evaluate proposed changes, track the status of changes, and to maintain project.

Changes occurring within the project operation could be divided into groups:

1. **Changing project requirements** – change control management
2. **Software revision control changes** – practice that tracks and provides control over changes to source code
3. **Validation set-up configuration changes** – based on BKC (Best Known Configuration) provided by Client.

### 7.1.2. Overview and Refinements regarding 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.

As this site is not directly involved with producing, storing or delivering the TOE, the only relevant configuration items under CM scope are:

- This Site Security Target for this site,
- The Development Security documentation for this site (site security procedures),
- Life-cycle Support documentation,
- All documentation related to the inspection of the development process (client's audits confirmed with reports, internal audits confirmed with reports) and
- Test results.

### 7.1.3. Overview and Refinements regarding Delivery Procedure (ALC_DEL.1)

The CC assurance components of the family ALC_DEL (Delivery) refer to the external delivery of (i) the TOE or parts of it (ii) to the consumer or consumer's site (Composite TOE Manufacturer). The CC assurance component ALC_DEL.1 requires procedures and technical measures to maintain the confidentiality and integrity of the product. The means to detect modifications and prevent any compromise of the Initialization Data and/or Configuration Data may include supplements of the Security IC Embedded Software.

In the case of a Security IC more "material and information" than the TOE itself (which includes the necessary guidance) is exchanged with clients or consumers. Since the TOE can be externally delivered after different life-cycle phases (phases 6) the SST must consider the data that is exchanged by the sites either as part of the product or separate as input for further development steps.

As already outlined in the application notes of the PP [5] the external delivery of the TOE may require additional transfers between the product manufacturer and the client or consumer. These do not address the internal deliveries between sites involved in the life-cycle of the intended TOE. Since the assurance component ALC_DEL is only applicable to the external delivery to the consumer, the component cannot be used for internal shipment. Internal shipment is covered by ALC_DVS refer to the to the notes included in the Foreword and the Notes.

### 7.1.4. Overview and Refinements regarding 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 development of the TOE is secure so that no information is unintentionally made available for the operational phase of the TOE. The confidentiality and integrity of design information, test data, configuration data and pre-personalization data must be guaranteed, access to any kind of samples (customer specific samples or open samples) development tools and other material must be restricted to authorized persons only, scrap must be controlled and destroyed.

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

If the transfer of assets between two sites involved in the development 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 clearly distinguish to ensure the correct subject of the evaluation.

### 7.1.5. Overview and Refinements regarding 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 must be evaluated which are in the scope of the site. The PP [5] provides a life-cycle description their specific life-cycles steps can be assigned to the tasks at site. This may comprise a change of the life-cycle state if e.g. testing or initialization is performed at the site or not.

The PP [5] does not include any refinements for ALC_LCD. For a site under evaluation the dependencies to other sites must be explained if they are not covered by the obvious deliverables.

The life-cycle phase applicable for this site is Phase I “Security IC Embedded Software Development” and Phase II “IC Development”:

### 7.1.6. Overview and Refinements regarding Tools and Techniques (ALC_TAT.3)

The CC assurance components of family ALC_TAT refer to the tools that are used to develop, analyse and implement the TOE. The component ALC_TAT.3, “Compliance with implementation standards - all parts”, requires evidence for the suitability of the tools and techniques used for the development process of the TOE.

The site shall identify and clearly and completely described all tools and techniques used for the development, analysis and implementation of the TOE. This shall comprise all tools that have an impact on the behaviour of the TOE.

## 7.2. Security Assurance Rationale

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

The site has a process in place to ensure an appropriate and consistent identification of the products. If the site already receives assets, this process assumes that the received assets are appropriately labelled and identified, refer to **A.Item-Identification** defined in section 4.4.

Note: The content elements that are changed from the original CEM [3] according to the application notes in the process description [4] are written in italic. The term TOE can be replaced by configuration item or asset in most cases. In specific cases it is replaced by product or “intended TOE”.

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

**Some of the dependencies are not (completely) fulfilled:**

ADV_IMP.1 is not fulfilled as there is no specific TOE. This is in-line with and further explained in [4] 5.7 'Application Notes for ALC_TAT'.

**Table 2. Rationales, Aspects and References for ALC_CMC.4**

| SAR | Security Objective | Rationale |
|---|---|---|
| ALC_CMC.5.1C:<br>The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling. | O.Config-IT_Env | A CM-Plan which is mandatory for each project ensures appropriate and consistent labelling through its application. |
| | O.Reception-Control | Ensures the correct identification of the incoming items. |
| | O.LifeCycle-Doc | The provided tools include a configuration management system for versioning and bug tracking. |
| ALC_CMC.5.2C:<br>The CM documentation shall describe the method used to uniquely identify the configuration items. | O.Reception-Control | Incoming inspection according O.Reception-Control ensures product identification and the associated labeling. This labeling is mapped to the internal identification as defined by O.Config-Items. This ensures the unique identification of security products. |
| | O.Config-Control | 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 authorized staff. |
| | O.Config-Process | O.Config-Process provides a configured and controlled development process. |
| | O.LifeCycle-Doc | The method used to uniquely identify the configuration items is described in the CM-Plan. |
| ALC_CMC.5.3C:<br>The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items. | O.LifeCycle-Doc | The adequate and appropriate acceptance procedures for configuration items are described in the CM-Plan. |
| | O.Config-Control | Change acceptance is managed by authorized people only. Each product is setup according to O.Config-Control comprising all necessary items. |
| | O.Config-Items | O.Config-Item ensures that unique identification on security product. This comprises changes related to process flows, procedures and items of clients. |
| | O.Reception-Control | O.Reception-Control comprises the incoming labeling and the mapping to internal identifications. |

| SAR | Security Objective | Rationale |
|---|---|---|
| ALC_CMC.5.4C:<br>The CM system shall uniquely identify all configuration items. | O.Config-Control | O.Config-Control assigns the setup including processes and items for the development of each client. |
| | O.Config-Process | Unique identification of all configuration items is realized by performing the configuration management activities. |
| | O.Logical-Access | O.Logical-Access support the control by limiting the access and ensuring the correct operation for all tasks to authorized staff. |
| | O.Config-IT_Env | Provides the CM system. |
| | O.Config-Items | The configuration management system is ensuring uniqueness of the identification. |
| | O.LifeCycle-Doc | All actions are performed in accordance with the CM-Plan. |
| ALC_CMC.5.5C:<br>The CM system shall provide automated measures such that only authorised changes are made to the configuration items. | O.Config-IT_Env | Provides the CM system. |
| | O.Config-Items | Mandates a CM-Plan for each project. |
| | O.Config-Control | Ensures that only authorized changes are made to the configuration items. |
| | O.LifeCycle-Doc | Enforces the configuration management process. |
| | O.Config-Process | O.Config-Process comprises the control of the development processes. |
| ALC_CMC.5.6C:<br>The CM system shall support the production of the intended TOE by automated means. | O.Config-IT_Env | Provides the CM system. |
| | O.Config-Items | The CM system ensure unique identification. |
| | O.Config-Process | Mandates a CM-Plan for each project. |
| | O.LifeCycle-Doc | Enforces the configuration management process and the automated means. |
| | O.Zero-balance | CM system supports the production of the product by automated means. |
| ALC_CMC.5.7C:<br>The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it. | O.LifeCycle-Doc | Ensures, that activities performed are such that the person responsible for accepting a configuration item into CM is not the person who developed it. |
| | O.Config-Process | Mandates a CM-Plan for each project |
| | O.Logical-Access | O.Logical-Access supports the control by limiting the access and ensuring the correct operation for all tasks to authorized staff. |
| ALC_CMC.5.8C: | O.Config-IT_Env | Provides the CM system. |

| SAR | Security Objective | Rationale |
|---|---|---|
| The CM system shall identify the configuration items that comprise the TSF. | O.Config-Items | The CM system ensure unique identification. |
| | O.Config-Process | Mandates a CM-Plan for each project. |
| | O.LifeCycle-Doc | The CM-Plan identifies the configuration items that comprise the TSF supported by the configuration management system. |
| | O.Config-Control | O.Config-Items comprise the internal unique identification of all items that belong to a client part ID. |
| | O.Config-Process | According to O.Config-Process the CM plans describe the services provided by the site. |
| ALC_CMC.5.9C:<br>The CM system shall support the audit of all changes to the intended TOE by automated means, including the originator, date, and time in the audit trail. | O.Config-Items | The CM system ensure unique identification. |
| | O.Config-Process | Mandates a CM-Plan for each project. |
| | O.LifeCycle-Doc | As described in the CM-Plan the configuration management systems are configured such that an audit trail (showing originator, date and time) is automatically generated. |
| | O.Config-Control | O.Config-Control describes the management of the client part IDs at the site. |
| ALC_CMC.5.10C:<br>The CM system shall provide an automated means to identify all<br>other configuration items that are affected by the change of a given configuration item. | O.Config-IT_Env | Provides the CM system. |
| | O.Config-Items | The CM system ensure unique identification. |
| | O.Config-Process | Mandates a CM-Plan for each project. |
| | O.LifeCycle-Doc | As described in the CM-Plan the CM system and software installed on the development workstations and servers provide means to identify all other configuration items that are affected by the change of a given configuration item. |
| ALC_CMC.5.11C:<br>The CM system shall be able to identify the version of the Implementation representation from which the intended TOE is generated. | O.Config-IT_Env | Provides the CM system. |
| | O.Config-Items | The CM system ensure unique identification. |
| | O.Config-Process | Mandates a CM-Plan for each project. |
| | O.LifeCycle-Doc | The version of the implementation representation from which the “intended TOE” is generated can be determined through baselines. |

| SAR | Security Objective | Rationale |
|---|---|---|
| ALC_CMC.5.12C:<br>The CM documentation shall include a CM plan. | O.Config-Process | Mandates a CM-Plan for each project. |
| ALC_CMC.5.13C:<br>The CM plan shall describe how the CM system is used for the development of the intended TOE. | O.LifeCycle-Doc | The life-cycle documentation describes how the CM system is used for the development of the product. |
| | O.Config-Process | O.Config-Process the CM plans describe the services provided by the site. |
| ALC_CMC.5.14C:<br>The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the intended TOE. | O.LifeCycle-Doc | The acceptance procedures for modified or newly created configuration items are described in the CM-Plan. |
| | O.Config-Control | Mandates a CM-Plan for each project. |
| ALC_CMC.5.15C:<br>The evidence shall demonstrate that all configuration items are being maintained under the CM system. | O.LifeCycle-Doc | All configuration items are under configuration system and listed in the CI-list. |
| | O.Config-Process | Ensures, that all configuration items are under version control. |
| | O.Internal-Shipment | O.Internal-Shipment includes the packing requirements, the reports, logs and notifications including the required evidence. |
| | O.External-Delivery | O.External-Delivery include the packing requirements, the reports, logs and notifications including the required evidence. |
| ALC_CMC.5.16C:<br>The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan. | O.Config-IT_Env | Provides the CM system. |
| | O.Config-Process | Ensures, that all configuration items are under version control. |
| | O.LifeCycle-Doc | The CI-list is generated from the CM systems. |

The security assurance requirements of the assurance class “CM capabilities” listed above are suitable to support the development of complex products due to the formalized acceptance process and the automated support. The identification of all configuration items supports an automated and industrialized development process. The requirement for authorized changes supports the integrity and confidentiality required for the products. Therefore, this assurance level meets the requirements for the configuration management.

The scope of the evaluation according to the assurance class ALC_CMS comprises the security products, the complete documentation of the site provided for the evaluation and the configuration and initialization data as well as associated tools. The specifications and descriptions provided by the client are not part of the configuration management at the certified site.

**Table 3. Rationales, Aspects and References for ALC_CMS.4**

| SAR | Security Objective | Rationale |
|---|---|---|
| ALC_CMS.5.1C:<br>The configuration list includes the following: the intended TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the intended TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan. | O.LifeCycle-Doc | The life-cycle documentation includes a CI-List which contains all the items of this content element. |
| | O.Config-Control | O.Config-Control describes the release process. |
| | O.Config-Process | O.Config-Process defined the configuration control. |
| ALC_CMS.5.2C:<br>The configuration list shall uniquely identify the configuration items. | O.LifeCycle-Doc | The CI-List uniquely identifies the configurations items per project name, version, document ID, date, and configuration identification (CID). |
| | O.Config-Items | Items, products and processes are uniquely identified by the data base system according to O.Config-Items. |
| | O.Reception-Control | The identification of received products is defined by O.Reception-Control |
| | O.Internal-Shipment | The labeling and preparation for the transport is defined by O.Internal-Shipment |
| | O.External-Delivery | The labeling and preparation for the transport is defined by O.External-Delivery. |
| ALC_CMS.5.3C:<br>For each TSF relevant configuration item, the configuration list shall indicate the developer/ subcontractor of the item. | O.LifeCycle-Doc | The CI-List indicates the developer/subcontractor/ author for each configuration item. |
| | O.Config-Items | According to O.Config-Items all configuration items for secure products are identified. |

The security assurance requirements of the assurance class “CM scope” listed above support the control of the development 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 assurance requirements are suitable.

**Table 4. Rationales, Aspects and References for ALC_DVS.2**

| SAR | Security Objective | Rationale |
|---|---|---|
| ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment. | O.LifeCycle-Doc | This covers the overall development security documentation. |
| | O.Physical-Access | This covers the physical measures. |
| | O.Security-Control | This covers the organizational measures of the guard team. |
| | O.Alarm-Response | This covers the physical measures and their alarm follow up by the guard team. |
| | O.Internal-Monitor | This covers organizational measures by reviews and management attention. |
| | O.Maintain-Security | This covers organizational measures by maintenance. |
| | O.Staff-Engagement | The personnel security measures are provided by O.Staff-Engagement. |
| | O.Control-Scrap | Any scrap that may support an attacker is controlled according to O.Control-Scrap |
| | O.Logical-Operation | This covers logical measures and the user interaction with the security systems. |
| | O.Logical-Access | This covers logical measures in the area of firewall and virus protection as well at patch management. |
| | O.Internal-Shipment | This covers procedural measures of internal transport of security material. |
| | O.Control-Scrap | This covers procedural measures of secure destruction of security material. |
| | O.Staff-Engagement | This covers personnel measures. |
| | O.Data-Transfer | This covers logical measures related to cryptographic encryption and signature algorithms during electronic transfer of data. |
| ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE. | O.LifeCycle-Doc | The development security documentation justifies, that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the “intended TOE”. |
| | O.Internal-Monitor O.Logical-Operation O.Maintain-Security | The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous justification is subject of the objectives O.Internal-Monitor, O.Logical-Operation and O.Maintain-Security. |
| | O.Acceptance-Test | O.Acceptance-Test supports the integrity control by testing of the finished products. |
| ALC_DEL.1.1C: The delivery documentation shall | O.Internal-Shipment | The delivery to the client is protected by similar measures according to the requirements of the client based on O.Internal-Shipment. |

| SAR | Security Objective | Rationale |
|---|---|---|
| describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer. | O.External-Delivery | The delivery to the customer is protected by security measures according to the requirements of the client based on O.External-Delivery |

The security assurance requirements of the assurance class “Development security” listed above are required since a high attack potential is assumed for potential attackers. The assets and information handled at the site during development, testing and pre-personalization or personalization of the product can be used by potential attackers for the development of attacks. Any keys loaded into the intended TOE also support the security during the internal shipment or the external delivery. Therefore, the handling and storage of electronic keys must also be protected. Further on the Protection Profile [5] requires this protection for sites involved in the life-cycle of Security ICs development.

**Table 5. Rationales, Aspects and References for ALC_DEL.1**

| SAR | Security Objective | Rationale |
|---|---|---|
| ALC_DEL.1.1C:<br>The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer. | O.LifeCycle-Doc<br>O.Transfer-Data<br>O.External-Delivery | The processes for the secure shipment (external delivery) of secure products are defined according to O.External-Delivery. |

The security assurance requirement of the assurance class “Delivery” listed above is suitable to define a controlled process for delivery products to the consumer. The confidentiality and integrity of the product during transport is addressed by this assurance class. Since the Protection Profile [5] requires the same assurance level it is enough.

**Table 6. Rationales, Aspects and References for ALC_LCD.1**

| SAR | Security Objective | Rationale |
|---|---|---|
| ALC_LCD.1.1C:<br>The life-cycle definition documentation shall describe the model used to develop and maintain the intended TOE. | O.LifeCycle-Doc | The live-cycle documentation describes the model used to develop the “intended TOE”. |
| ALC_LCD.1.2C:<br>The life-cycle model shall provide for the necessary control over the development | O.LifeCycle-Doc | The life-cycle model as described in the life-cycle documentation ensures the necessary control over the development and maintenance of the “intended TOE”. |

| SAR | Security Objective | Rationale |
|---|---|---|
| and maintenance of the intended TOE. | O.Acceptance-Test<br>O.Config-Process<br>O.Organise-Product | The applied development-process is controlled according to O.Config-Process.<br>The finished client parts are tested according O.Acceptance-Test. |

The security assurance requirements of the assurance class “Life-cycle definition” listed above are suitable to support the controlled development process. This includes the documentation of these processes and the procedures for the configuration management. One site provides only a limited support of the described life-cycle for the development of Security ICs. However, the assurance requirements are suitable to support the application of the site evaluation results for the evaluation of an intended TOE.

**Table 7. Rationales, Aspects and References for ALC_TAT.3**

| SAR | Security Objective | Rationale |
|---|---|---|
| ALC_TAT.3.1C:<br>Each development tool used for implementation shall be well-defined. | O.LifeCycle-Doc | The tool documentation (O.LifeCycle-Doc) shows that the development tool used for implementation are well fefined. |
| ALC_TAT.3.2C:<br>The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation. | O.LifeCycle-Doc | The tool documentation (O.LifeCycle-Doc) unambiguously defines the meaning of all statements as well as all conventions and directives used in the implementation. |
| ALC_TAT.3.3C:<br>The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options. | O.LifeCycle-Doc | The tool documentation (O.LifeCycle-Doc) unambiguously define the meaning of all implementation-dependent options. |
| ALC_TAT.3.3D:<br>The developer shall describe and provide the implementation standards that are being applied by the developer and by any third-party providers for all parts of the TOE. | O.LifeCycle-Doc | The development documentation (O.LifeCycle-Doc) defines the development standards applied.. |

The security assurance requirements of the assurance class “Tools and Techniques” listed above shall support the secure development and optimization of the GDS file for of the mask data generation. The control, capabilities and configuration of the tools contribute to achieve reproducible and consistent development, production and test processes. Therefore, this Security assurance requirement is only partly suitable for this type of site.

# 8. Site Summary Specification

## 8.1. Preconditions Required by the Site

This section lists the preconditions required by the site to match the assumptions defined in this SST. These assumptions are relevant for the splicing process since they must be examined during the product evaluation. Especially aspects like the classification of items and the appropriate provision of specifications for the site must be verified by checking appropriate evidence (e.g. the set of specifications provided to the site with a site certificate) during the product evaluation.

The following table explains the preconditions of the client that are required to ensure the security measures of the site in order to protect its assets.

**Table 8. Precondition of assumptions**

| Assumption | Precondition |
|---|---|
| A.Secure-IT-Provisioning | To enable that the site participates in the development of products ICTK provides services to setup and maintain the necessary development environment (e.g. workstations, tools, test samples) and configuration management systems (e.g. user accounts in project repositories). ICTK also provides a secure connection between the IT equipment of the site and a secure IT infrastructure of the ICTK. These services are provided in a secure way in order to properly protect the assets of the site. This includes the enforcement of a trustworthy access policy to the site equipment and data using the secure connection based on a “need-to-know” principle. |
| A.Prod-Specification | All provided items from the platform client are labelled to ensure the identification of the configuration items. (A.Item-identification) |
| A.Item-Identification | Each configuration item received by the site is appropriately labelled to ensure the identification of the configuration item. |
| A.Internal-Shipment | Internal shipment can only take place based on an order and addresses defined in the shipment tools. The shipment method is described in the shipment and delivery documentation. The site had to be informed about correct shipment information. |
| A.External-Delivery | Every client of the product is identified by his address, which is part of the delivery process. The client provides the address and shipping information to ICTK. |
| A.Init-Data | The scripts for the configuration and initialization process are created by ICTK of the product. |

## 8.2. Services of the Site

Designed, Development and Provisioning & Testing of the embedded software for security IC are provided in the site. This site has configuration management system, the data storage and dedicated network system. The secure delivery method for protecting confidentiality and integrity is used for the data transfer.

**Table 9. Details of the services provided by the site**

| Service | Details |
|---|---|
| S.Internal_Shipment | The site uses a shipment method such that assurance of integrity is assured throughout transport of physical security objects. Internal shipment is covered under ALC_DVS.2.<br><br>Dependencies:<br>S.Secure_Area must be fulfilled to ensure physical security<br><br>Assumptions:<br>A.Item-Identification must be fulfilled<br>A.Internal-Shipment must be fulfilled |
| S.Development | IC Embedded Software Development and IC Development (Phase 1,2) and/or Security IC Product Finishing (Phase 5), Security IC Personalization (Phase6) as well as development and characterization and Personalization/validation testing of secure smart card ICs.<br><br>The typical Life Cycle model for Smart Cards usually comprises the following phases:<br>(i) Security IC Embedded Software Development<br>(ii) IC development,<br>(iii) IC Manufacturing and Testing,<br>(iv) IC Packaging,<br>(v) Security IC Product Finishing,<br>(vi) Security IC Personalization<br><br>whereas the site under evaluation supports the life cycle phase<br>(i) Security IC Embedded Software Development<br>(ii) IC development<br>(v) Security IC Product Finishing<br>(vi) Security IC Personalization and TOE Delivery.<br><br>Development of IC and dedicated software which comprises:<br>• The generation of the analog and digital hardware designs, including GDS Ⅱ layout, embedded & IC dedicated software and the creation of development related documents.<br>• The purpose of verification is the preparation of the design freeze and sample production.<br>• The purpose of validation is to release the product to the Operations organization that facilitates the volume ramp up. Samples can have a form of a wafer, a die, a module or package, a card or an inlay. |

| | |
|---|---|
| | • Debugging during development phase<br>• The sample creation (if applicable)<br><br>Dependencies:<br>**S.Secure_Area** must be fulfilled to ensure physical security<br><br>Assumptions:<br>**A.Secure-IT-Provisioning** must be fulfilled for secure networks<br>**A.Item-Identification** must be fulfilled |
| S.Secure_Area | The site provides a secure physical environment for classified IT infrastructure and equipment according to Common Criteria requirements.<br><br>Dependencies:<br>none<br><br>Assumptions:<br>none |
| S.Verification_And_ Validation | Verification comprises verification and simulation of embedded and IC dedicated software on emulation devices of Smart Card ICs.<br><br>The purpose of verification is the preparation of developed software for implementation on the target device. Validation comprises validation of embedded and IC dedicated software with real samples of Smart Card ICs, as well as validation of real SmartCard ICs without additional embedded software. The purpose of validation is to release the product to the Operations organization, that facilitates the volume ramp up.<br><br>Dependencies:<br>S.Secure_Area must be fulfilled to ensure physical security<br><br>Assumptions:<br>A.Secure-IT-Provisioning must be fulfilled for secure networks<br>A.Item-Identification must be fulfilled |
| S.Provisioning_And_Test | The processes for testing and acceptance are setup at the site according to the specifications (e.g. Bonding diagrams, modules / IC on inlay specification, test specification). For the release, a samples lot is produced at the site. The complete product specific development flow includes a functional test of each device as part of the acceptance process. The functional tests are developed by ICTK based on the test specifications and electrical parameters/ limits.<br><br>The provisioning of the products is done using scripts, data and keys provided by the ICTK/client. The items used for the pre-personalisation are treated as assets. ICTK provides a standardised environment for the processing of the scripts. The implemented setup ensures the correct assignment between |

| | |
|---|---|
| | products and associated scripts, data and keys during the provisioning process. Provisioning data supplied by the ICTK/client is injected into the non-volatile memory.<br><br>Dependencies:<br>none<br><br>Assumptions:<br>none |
| S.External_Delivery | The site uses a shipment method such that assurance of integrity is assured throughout transport of physical security objects. Thus, the site is compliant to ALC_DEL.1.<br><br>Dependencies:<br>S.Secure_Area must be fulfilled to ensure physical security<br><br>Assumptions:<br>A.Item-Identification must be fulfilled<br>A.External-Delivery must be fulfilled |
| S.Scrapping | Any item that is defect, end-of-life or that does not comply with the quality requirements is shipped back to the client for destruction or is scrapped at the site in a way that the destructed item does not support any attacker.<br><br>Dependencies:<br>S.Secure_Area must be fulfilled to ensure physical security<br><br>Assumptions:<br>none |

# 9. References

## 9.1. Literature


[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, Revision 5, April 2017

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

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

[5] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, January 13th, 2014, BSI-CC-PP-0084-2014

[6] Eurosmart. Site Security Target Template, Version 1.0, 21. June 2009.

[7] JIL, Minimum Site Security Requirements, Version 3.1, December 2023.


## 9.2. 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 words “customer” and “consumer” are only used here in the sense of CC. |
| Intended TOE | In the view of this site certification, there is no real product certified as the site certification is - per definition – product independent. Therefore, also no TOE does exist, and this SST is referring to the “intended TOE” only. |
| Product | A “product” would be the result of the development process. |

## 9.3. List of Abbreviations

| | |
|---|---|
| CC | Common Criteria |
| CI | Configuration Item |
| CL | Configuration List |
| CM | Configuration Management |
| EAL | Evaluation Assurance Level |
| IC | Integrated Circuit |
| 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 |

# 10. Contact Information

**Contact:**

**Headquarter**
**14F, JACE Tower, 16 Gangnam-daero 84-gil,**
**Gangnam-gu, Seoul, Korea**
**TEL: +82-2-569-0010**
**FAX: +82-2-569-0112**
**E-mail: puf@ictk.com**