SONY

Sony Semiconductor Israel Site Security Target Lite

Document Classification:	Public
Document revision:	1.0
Author:	Tsion Shamay
Date:	May 11, 2022
File name:	Sony_Semiconductor_Israel_SST_Lite_v1.0

Revision History

Revision	Date	Description	Changed by
1.0	11/05/2022	First document release.	Tsion Shamay

Acronyms and Abbreviations

The following table contains a list of acronyms and other terms used in this document.

Acronym	Description
CC	Common Criteria
EAL	Evaluation Assurance Level
IC	Integrated Circuit
IS	Information Security
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SSI	Sony Semiconductors Israel
SST	Site Security Target
TOE	Target of Evaluation

Table of contents

List of Tables

1 SST Introduction

This document describes the security features and services of Sony Semiconductor Israel Secured Area site (a.k.a. SSI Secure Area) and therefore defines the logical and physical scope of the site.

This section is composed by the sub-section “SST Reference”, “Site Reference” and “Site Description”.

1.1 SST Reference

- SST name: Sony Semiconductor Israel Site Security Target Lite
- SST version and date: Version 1.0 - 11/05/2022
- Company: Sony Semiconductor Israel, Ltd.
- Site Name: Sony Semiconductor Israel Secured Area
- EAL: SARs taken from EAL6

1.2 Site Reference

The Sony Semiconductor Israel Secured Area site is located at:

Sony Semiconductor Israel

HaHarash St. 6,

Hod HaSharon,

Israel

1.3 Site Description

1.3.1 Site Physical Scope

Sony Semiconductor Israel site is located in a five buildings business park surrounded by a fence, cameras controlling the perimeter and 24/7 guards controlling the entrance to park. The entire park does not belong to Sony Semiconductor Israel Company but the 11th floor (Secure area) of building C is the exact location where Sony Semiconductor Israel performs the activities under the scope of this evaluation.

Building C has a 24/7 doorman, a controlled entry gate and cameras in the public areas and corridors to monitor the activities inside the building. The 11th floor is exclusively occupied by Sony Semiconductor Israel and implements some security detection and stop mechanisms such as physical access control mechanisms, CCTV (entrance and corridors) and alarms to guarantee the security of access to Sony Semiconductor Israel premises.

The Sony Semiconductor Israel Secured Area, which is the physical scope of this site certificate, is a dedicated space inside 11th floor that implements security mechanism in addition to the previous ones mentioned. These security mechanisms provide the secured area an additional detection and stop security layer such as a dedicated anti-tailgating gate with restricted access control under the control of Sony Semiconductor Israel, a dedicated CCTV monitoring the activities performed inside the secured area and intrusion alarm. Only authorized persons can access to Sony Semiconductor Israel Secure Area.

1.3.2 Site Logical Scope

The logical scope of SSI Secured Area site can be related with the following life-cycle phase defined in the “Security IC Platform Protection Profile with Augmentation packages” (1).

- Phase 3 (IC Manufacturing)

  The following services provided by Sony Semiconductor Israel Secured Area site are considered under the scope of this evaluation:

  - Key generation (for Pre-personalization/Provisioning process)
  - Key storage (for Pre-personalization/Provisioning process)
  - Key secured transmission (for Pre-personalization/Provisioning process)

  These services are part of the life-cycle phase mentioned before because the IC Pre-personalization/Provisioning process is performed during phase 3 (IC Manufacturing). For more detailed information please refer to section 1.2.3 TOE life cycle of (1) document.

  All these services are performed in Sony Semiconductor Israel Secured Area considering the proper level of physical and logical security measures set to guarantee the confidentiality and integrity of data generated.

  Note: For the sake of a better understanding, the term “key management” will be used throughout this document to refer to the three services provided by the site and considered under the scope of this evaluation.

2 Conformance Claim

The evaluation is based on Common Criteria Version 3.1, revision 5:

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

For the evaluation, the following methodology will be used:

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

This SST is CC Part 3 conformant.

The evaluation of the site comprises the following assurance components:

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

The assurance level chosen for the SST is compliant to the Protection Profile (1) and therefore suitable for Security ICs.

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 product evaluations up to EAL6.

3 Security Problem Definition

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

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

3.1 Assets

The following section describes the assets handled at the site:

- **Production keys**: this includes the production keys generated during the key management process. The integrity and confidentiality of this asset must be protected.
- **Production data:** this includes the sensitive data generated during the key management processes (e.g. Blobs, logs). The integrity of this asset must be protected.
- **Documentation:** this includes all the internal documentation related to the key management process.
- **Physical security objects:** this includes all physical objects (e.g. PCs, IT infrastructure, etc.) used to perform the services defined as part of the logical scope.

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

3.2 Threats

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

Threat	Description
T.Smart-Theft	An attacker tries to access sensitive areas of the site for manipulation or theft of assets. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered.
T.Rugged-Theft	An experienced thief with specialized equipment for burglary, who may be paid to perform the attack tries to access sensitive areas and manipulate or steal assets.
T.Computer-Net	A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get sensitive data such as keys and logs generated during the key generation, key storage or key secures transmission processes.

Threat	Description
T.Unauthorized-Staff	Employees or subcontractors who are not authorized to access the assets or systems used for services obtain access to them, so that the confidentiality and/or the integrity of the assets or systems used are violated.
T.Staff-Collusion	An attacker tries to get access to assets processed at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.
T.Attack-Transmission	An attacker might try to get sensitive data (assets) during the shipment/transmission. The target is to compromise confidential information or violate the integrity of the sensitive data during the shipment/transmission process to allow a modification, cloning or the retrieval of confidential information after further steps.

Table 3.1 Threats

3.3 Organizational Security Policies

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

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

OSP	Description
P.Config-Items	The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of items that are created, generated, developed, or used at a site as well as the received and transferred and/or provided items.
P.Config-Control	The procedures for setting up the key generation process as well as the procedure that allows changes of the initial setup 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 key generation process ensures that sufficient information is provided by the developer.
P.Config-Process	The services and/or processes provided by a site are controlled in the configuration management plan. This comprises tools used for carrying out the services and/or processes and the documentation that describes the services and/or processes provided by a site.
P.Accept-Product	The testing and quality control of the site ensures that the key management process complies with the specification agreed with the client. The acceptance process is supported by automated measures. Records are generated for the acceptance process of the configuration items. Thereby, it is ensured that the properties of the product are ensured when they are shipped or transmitted.

OSP	Description
P.Organize-Product	The services provided by the site are applied as specified by the client. Appropriate measures must be in place due to the criticality of the generated data. Furthermore, technical measures like crypto-boxes, separation of network, split access permission and secured storage shall be implemented for this kind of data.
P.Product-Transmission	Technical and organizational measures shall ensure the correct labelling of sensitive data generated from the services provided by the site. A controlled internal/external shipment shall be applied. The transmission supports traceability up to the acceptor.

Table 3.2 Organizational Security Policies

3.4 Assumptions

Each site operating in a production 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.

The following assumptions are considered to be applicable to Sony Semiconductor Israel site:

Assumption	Description
A.Init-Data:	The data for the configuration and initialization of the service process are provided by the client. The client verifies the configuration and/or initialization process during the product introduction and the release process of the site.
A.Transfer-Data	After the transmission of sensitive data to the client, the client is responsible to maintain the confidentiality and integrity of sensitive data with the same level of security protection.

Table 3.3 Assumptions

4 Security Objectives

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

Security Objective	Description
O.Physical-Access	The combination of physical partitioning between the different access control levels together with technical and organizational security measures allows a sufficient separation of employees to enforce the “need to know” principle. The access control supports the limitation for the access to these areas including the identification and rejection of unauthorized people. The site enforces at least two levels of access control to sensitive areas of the site. The access control measures ensure that only registered employees and vendors can access restricted areas. Sensitive data/products are handled in restricted areas only.
O.Security-Control	Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering visitors, contractors and suppliers. The host is responsible to accompany the visitors during the entire stay at site premises.
O.Alarm-Response	The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any sensitive configuration item (asset). After the alarm is triggered the unauthorized person still has to overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack.
O.Internal-Monitor	The site performs security management meetings 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 at least every year to control the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure a sufficient protection.
O.Maintain-Security	Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorized employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.
O.Logical-Access	The site enforces a logical separation between the internal network and the internet by a firewall. The firewall ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into a production network and an office network. Additional specific networks for production and configuration are physically separated from any internal network to enforce access control. Access to the production network and related systems is restricted to authorized employees that work in the related area or that are involved in the configuration tasks or the production systems. Every user of an IT system has its own user account and password. An authentication using user account and password is enforced by all computer systems.

Security Objective	Description
O.Logical-Operation	All network segments and the computer systems are kept up-to-date (software updates, security patches, virus protection, spyware protection). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.
O.Config-Items	The site has a configuration management system that assigns a unique internal identification to uniquely identify each configuration item.
O.Config-Control	The site applies a release procedure for each new production process on request of the client. In addition, the site has a process to classify and introduce changes for released products. A designated team is responsible for the release of new products and for the classification and release of changes. 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 product's production and the documentation that describes the services and/or processes provided by a site.
O.Acceptance-Test	The site delivers configuration items that fulfil the specified properties. Parameter checks 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.Organize-Product	For services provided by the site, it is ensured that the specified process is applied. The confidentiality and integrity of sensitive data is controlled. The operation is performed in an isolated network and applied in crypto-boxes or similar devices. After the release process changes are only applied based on the request of the client. The update is done according to a controlled process.
O.Staff-Engagement	All employees who have access to sensitive data and who can move parts of the product out of the defined production flow have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.
O.Transfer-Data	The transmission of sensitive data is protected with cryptographic algorithms to ensure confidentiality and integrity. Only authorized employees can transfer sensitive data according to the procedure defined.

Table 4.1 Security Objectives

4.1 Security Objectives Rationale

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

Please note that the assumptions of the SST are not used to cover any threat or OSP of the site. They are seen as pre-conditions fulfilled either by the site providing the sensitive configuration items or by the site receiving the sensitive configuration items. Therefore, they do not contribute to the security of the site under evaluation.

4.1.1 Mapping of Security Objectives

Thread and OSP	Security Objective	Note
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of these security objectives enables the detection of unauthorized access and provides an appropriate response to the threat. O.Physical-Access directly counters T.Smart-theft O.Security-Control directly counters T.Smart-theft O.Alarm-Response directly counters T.Smart-theft O.Internal-Monitor directly counters T.Smart-theft O.Maintain-Security directly counters T.Smart-theft
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of these security objectives enables the detection of unauthorized access and provides an appropriate response to the threat. O.Physical-Access directly counters T.Rugged Theft O.Security-Control directly counters T.Rugged-Theft O.Alarm-Response directly counters T.Rugged-Theft O.Internal-Monitor directly counters T.Rugged-Theft O.Maintain-Security directly counters T.Rugged-Theft
T.Computer-Net	O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement	The combination of these security objectives enables the detection of unauthorized access to the internal network and provides an appropriate response to the threat. O.Internal-Monitor directly counters T.Computer-Net O.Maintain-Security directly counters T.Computer-Net O.Logical-Access directly counters T.Computer-Net O.Logical-Operation directly counters T.Computer-Net O.Staff-Engagement directly counters T.Computer-Net
T.Unauthorized-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Config-Control O.Config-Process O.Staff-Engagement	The combination of these security objectives disables the access to sensitive data of unauthorized persons. O.Physical-Access directly counters T.Unauthorized-Staff O.Security-Control directly counters T.Unauthorized-Staff O.Alarm-Response directly counters T.Unauthorized-Staff O.Internal-Monitor directly counters T.Unauthorized-Staff O.Maintain-Security directly counters T.Unauthorized-Staff O.Logical-Access directly counters T.Unauthorized-Staff O.Logical-Operation directly counters T.Unauthorized-Staff O.Config-Control directly counters T.Unauthorized-Staff O.Config-Process directly counters T.Unauthorized-Staff O.Staff-Engagement directly counters T.Unauthorized-Staff
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Transfer-Data	The application of internal security measures, combined with the hiring policies that limits hiring to only trustworthy employees, prevents unauthorized access to sensitive data or items. O.Internal-Monitor directly counters T.Staff-Collusion O.Maintain-Security directly counters T.Staff-Collusion O.Staff-Engagement directly counters T.Staff-Collusion O.Transfer-Data directly counters T.Staff-Collusion

Thread and OSP	Security Objective	Note
T.Attack-Transmission	O.Logical-Access O.Logical-Operation O.Transfer-Data	The combination of these security objectives prevents the obtaining of sensitive data during its shipment/transmission. O.Logical-Access directly counters T.Attack-Transmission O.Logical-Operation directly counters T.Attack-Transmission O.Transfer-Data directly counters T.Attack-Transmission
P.Config-Items	O.Config-Items	O.Config-Items directly enforces P.Config-Items
P.Config-Control	O.Config-Items O.Config-Control O.Logical-Access	O.Config-Items directly enforces P.Config-Control O.Config-Control directly enforces P.Config-Control O.Logical-Access directly enforces P.Config-Control
P.Config-Process	O.Config-Process	O.Config-Process directly enforces P.Config-Process
P.Accept-Product	O.Config-Control O.Config-Process O.Acceptance-Test	O.Config-Control directly enforces P.Accept-Product O.Config-Process directly enforces P.Accept-Product O.Acceptance-Test directly enforces P.Accept-Product
P.Organize-Product	O.Logical-Operation O.Logical-Access O.Config-Control O.Config-Process O.Organize-Product	O.Logical-Operation directly enforces P.Organize-Product O.Logical-Access directly enforces P.Organize-Product O.Config-Control directly enforces P.Organize-Product O.Config-Process directly enforces P.Organize-Product O.Organize-Product directly enforces P.Organize-Product
P.Product-Transmission	O.Transfer-Data	O.Transfer-Data directly enforces P.Product-Transmission

Table 4.2 Security Objectives Rationale

5 Extended Assurance Component Definition

No extended components are defined in this Site Security Target.

6 Security Assurance Requirements

A client using this Site Security Target requires an evaluation against evaluation assurance level EAL6. This Security Assurance Requirement (SAR) is also included in the Security IC Platform Protection Profile (1).

The Security Assurance Requirements (SAR) are chosen from the class ALC (Lifecycle 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 fulfill the requirements of (5) because hierarchically higher components are used in this Site Security Target compared to the Minimum Requirements in (5). In addition, the minimum set of SAR is extended by SAR of the assurance component for "Life-cycle definition" (ALC_LCD.1).

The dependencies for the assurance requirements named above are as follows:

- ALC_CMC.5: ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
- ALC_CMS.5: None
- ALC_DVS.2: None
- ALC_LCD.1: None

The following dependency is partially fulfilled:

ALC_LCD.1 is part of this Site Security Target but it is only partially fulfilled as the site does not cover the entire life cycle of a specific TOE. This is in-line with the description provided in section 6.1.1 of this document .

6.1 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 the intended TOE, is not available during the evaluation. Since the term “TOE” is not applicable in the SST, the associated processes for the handling of products or intended TOE are in the scope of this SST and are described in this document. These processes are subject of the evaluation of the site.

6.1.1 Overview and Refinements regarding CM Capabilities (ALC_CMC)

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

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

There is a dependency from ALC_CMC.5 to ALC_LCD.1. The reason for this dependency is to ensure that there is a CM system in place for the entire development environment of the future TOE. To assess this knowledge of all life cycle phases (and in terms of Site Certification knowledge of all sites) and confidence that different life-cycle phases work together correctly is necessary. But this cannot be done for a single site if the site does not represent the entire development environment.

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

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

6.1.2 Overview and Refinements regarding CM Scope (ALC_CMS)

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

6.1.3 Overview and refinements regarding Development Security (ALC_DVS)

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

The TOE Manufacturer must ensure that the development and production of the future TOE is secured so that no information is unintentionally made available for the operational phase of the future TOE. The confidentiality and integrity of production keys used for the provisioning/pre-personalization process must be guaranteed and access to any kind of data related to this items must be restricted to authorized persons only.

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

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

6.1.4 Overview and Refinements regarding Life-cycle definition (ALC_LCD)

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

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

6.2 Security Assurance Requirements Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components of (3) to the Security Objectives defined in this SST.

The site has a process in place to ensure an appropriate and consistent identification of the intended TOE

Refinement operations over SARs are written in italic. The term “TOE” can be replaced by “product” or “intended TOE”.

SAR	Security Objective	Rationale
ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*	O.Config-Items	O.Config-Items ensure appropriate and consistent labelling as well as unique identification of the configuration item.
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Config-Items O.Config-Control O.Config-Process	O.Config-Items ensure appropriate and consistent labelling as well as unique identification of the configuration item. In addition, configuration items are kept under configuration control by O.Config-Control. O.Config-Process provides a configured and controlled production process.
ALC_CMC.5.3C: The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	O.Config-Items O.Config-Control O.Config-Process	O.Config-Control and O.Config-Process ensures that the acceptance procedures are adequate and appropriate to review changes in the configuration items. O.Config-Items ensure appropriate and consistent labelling as well as unique identification of the configuration item.
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.Config-Items	O.Config-Items ensure appropriate and consistent labelling as well as unique identification of the item.
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	O.Config-Control O.Config-Process O.Logical-Access	Configuration items are kept under configuration control by O.Config-Control. O.Config-Process provides a configured and controlled production process. O.Logical-Access ensures that access to the production network and related systems is limited to only authorized employees that work in the related area or that are involved in the configuration tasks or the production systems.
ALC_CMC.5.6C: The CM system shall support the production of the *product* by automated means.	O.Config-Process O.Acceptance-Test	O.Config-Process provides a configured and controlled production process by automated means. In addition, O.Acceptance-Test provides an automated testing of the product and supports the tracing.

SAR	Security Objective	Rationale
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	O.Logical-Access O.Config-Control O.Config-Process	O.Config-Control and O.Config-Process ensures that the production process is configured and controlled following the CM plan. O.Logical-Access ensures that access to the production network and related systems is limited to only authorized employees that work in the related area or that are involved in the configuration tasks or the production systems.
ALC_CMC.5.8C: The CM system shall *clearly* identify the configuration items that comprise the TSF.	O.Config-Items O.Config-Control O.Config-Process	O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the item. O.Config-Control and O.Config-Process ensures that the production process is configured and controlled following the CM plan.
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the *product* by automated means, including the originator, date, and time in the audit trail.	O.Acceptance-Test O.Config-Control O.Config-Process	O.Acceptance-Test provides an automated testing of the product and supports the tracing. O.Config-Control and O.Config-Process ensures that the production process is configured and controlled following the CM plan.
ALC_CMC.5.10C: The CM system shall provide an automated means to identify other configuration items that are affected by the change of a given configuration item**.**	O.Config-Control O.Config-Process	O.Config-Control and O.Config-Process ensures that the production process is configured and controlled following the CM plan.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the *product* is generated.	O.Logical-Access O.Config-Control O.Config-Process	O.Config-Control and O.Config-Process ensures that the production process is configured and controlled following the CM plan. O.Logical-Access ensures that access to the production network and related systems is restricted to authorized employees that work in the related area or that are involved in the configuration tasks or the production systems.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.Config-Process	O.Config-Process ensures that services and/or processes are controlled using a CM plan.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the *product.*	O.Config-Control O.Config-Process O.Organize-Product	O.Organize-Product ensures that the services and/or processes provided by the site carried out following the defined procedure. O.Config-Control and O.Config-Process ensures that the production process is configured and controlled following the CM plan.

SAR	Security Objective	Rationale
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *product*.	O.Config-Items O.Config-Control O.Config-Process	O.Config-Control and O.Config-Process ensures that the production process is configured and controlled following the CM plan. In addition, O.Config-Items ensure appropriate and consistent labelling as well as unique identification of the configuration item.
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Config-Control O.Config-Items	Configuration items are kept under configuration control according to O.Config-Control. In addition, O.Config-Items ensure appropriate and consistent labelling as well as unique identification of the configuration item.
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.Config-Process	The operation of the CM system in accordance to the CM plan is ensured by O.Config-Process.

Table 6.1 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMS.5.1C: The configuration list shall include the following: the evaluation evidence required by the SARs; the parts that comprise the *product* and *documented procedures used for the production process.*	O.Config-Items O.Config-Control O.Config-Process	O.Config-Items ensure the unique identification of configuration items. O.Config-Control and O.Config-Process defines the configuration management for products, procedures and processes. *Note*: Since the process is subject of the evaluation no products are part of the configuration list.
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config-Items O.Config-Control O.Config-Process	O.Config-Items ensure the unique identification of configuration items. O.Config-Control and O.Config-Process define the configuration management for products, procedures and processes.
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer of the item.	O.Config-Items	Subcontractors are not involved in the production process. According to O.Config-Items all configuration items for secure products are identified.

Table 6.2 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 *product* design and implementation in its development environment.	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement 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.
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *product*.	O.Internal-Monitor O.Transfer-Data O.Acceptance-Test	The security measures which are 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 O.Internal-Monitoring and O.Acceptance-Test O.Transfer-Data support the confidentiality and integrity of sensitive data during its transmission.

Table 6.3 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 *product*.	O.Config-Control O.Organize-Product	The process followed for the production process is defined in the documentation related to O.Config-Control and O.Organize-Product
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the *product*.	O.Acceptance-Test O.Config-Process O.Organize-Product	Control over the production process is maintained by O.Config-Process and O.Organize-Product, supported by the quality assurance measures defined by O.Acceptance-Test

Table 6.4 Rationale for ALC_LCD.1

7 Site Summary Specification

7.1 Preconditions required by the site

This section provides a justification for the assumptions defined in section 3.4 of this document.

The site performs key management process which includes key generation, key storage and key secured transmission. To perform these services in a secured manner, the client of the site must support the security processes of the site. The following statements define the preconditions of the client that are required to ensure the security measures of the site in order to protect its assets.

The client must provide the data for configuration and initialization of the key management process. The configuration and/or initialization process during the product introduction and the release process of the site is verified by the client.

The client is responsible to maintain the confidentiality and integrity of sensitive data received by the site with the same level of security protection.

7.2 Services of the site

Sony Semiconductor Israel site provides the following services:

- Key generation

  Generation of package that includes keys, data, and configuration for each chip.

- Key storage

  In order to support ongoing and continued production, the per-chip packages are stored (encrypted and signed) on a local repository.

- Key secured transmission

  The per-chip packages are protected from the time of its generation, until it is programmed into the chip.

7.3 Objective Rationale

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

Security Objective	Rationale
O.Physical-Access	The site is located in a business park surrounded by a fence, cameras controlling the perimeter and 24/7 guards controlling the entrance to park. Building C has a 24/7 doorman, a controlled entry gate and cameras in the public areas and corridors to monitor the activities inside the building. The Sony Semiconductor Israel Secured Area is a dedicated space inside 11th floor of building C that implements security mechanisms in addition to the ones previous mentioned. These security mechanisms provide the secured area an additional detection and stop security layer such as a dedicated anti-bypass gate with restricted access control under the control of Sony Semiconductor Israel, a dedicated CCTV monitoring the activities performed inside the secured area and intrusion alarm. Only authorized persons can access to Sony Semiconductor Israel Secured Area. Physical access permissions will be assigned on a "need to know" basis. The persons will have physical access only to the minimal extent required for performing their duties. Physical access permissions will be managed using a computerized physical access control mechanism. Access to areas that are defined as secured or sensitive will only be assigned to persons that must have them in order to perform their duties. The access privileges will be minimized to the bare necessity. Certain assets (e.g. the ones in the Secured Area) require an additional identification means (such as a token, OTP or a biometric identifier). By the combination of these measures, the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorized-Staff can be prevented.
O.Security-Control	The IT Team together with the IS Team, will design the physical security controls according to the requirements and the sensitivity of the information that requires physical access restrictions. Once in 3 months, the IT team will ask the employees who employ outsourcing personnel to verify that these persons are still cleared to access Sony Semiconductor Israel's premises. By the combination of these measures, the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorized-Staff can be prevented.
O.Alarm-Response	An alarm system is in place to detect a case of an access attempt to an asset by an unauthorized person. After the alarm is triggered, the unauthorized 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. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorized-Staff.
O.Internal-Monitor	Physical and logical security measures are regularly reviewed by security management meetings and internal audits. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorized-Staff and T.Staff-Collusion.
O.Maintain-Security	Data owners will define the Users permitted to access the various information systems (based on roles, responsibilities and their rank) and define the level of access each will have. Using this definition, 'permission profiles' will be set for the users across the various systems. The permissions will be reviewed by the Information Security Steering Committee as control as needed. Data Owners together with the IS Team, will design the security requirements and the sensitive information that requires access restrictions. Every 12 months, the IT Team will send to the Information Assets Owners the persons permitted to access these assets (including systems / applications), and they will have to validate the names list. By the combination of these measures, the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorized-Staff and T.Staff-Collusion are addressed.

Security Objective	Rationale
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. In addition, the internal network is separated to a secured network and an office network. The secured network is not connected to the office network. The secured network is exclusively used for the key management process. Access to the secured network and related systems is restricted only to authorized employees that work in the related area or that are involved in the configuration tasks or the production systems. Every system requires identification of the user by a user account and a password. Each user will be assigned a unique user account that will enable to easily distinguish between users. Access permissions will be assigned to users' accounts on a 'need to know basis'. Access permissions will be managed using a computerized access control mechanism. Access permissions will be reviewed on a defined basis by Data Owners who were mapped by the IT Team. The IT Team will alert them to conduct the review. By the combination of these measures the threats T.Computer-Net, T.Attack-Transmission and T.Unauthorized-Staff and the OSP P.Config-Control and P.Organize-Product can be prevented
O.Logical-Operation	Updates for operating systems and applications ensure the correct operation of the systems and prevent the systems from malfunction. All logical protection measures are maintained and updated from time to time as required. Furthermore, regular backups are applied to the operating system, and they are sufficiently protected. By the combination of these measures, the threats T.Computer-Net, T.Attack-Transmission and T.Unauthorized-Staff and the OSP P.Organize-Product are addressed.
O.Config-Items	Configuration items are uniquely identified in the configuration management system. The CM system allows unique labelling of any set of configuration items in the configuration management system. By this measure, the OSP P.Config-Items and P.Config-Control are addressed.
O.Config-Control	Access to the configuration management system is controlled by a designated Team. The configuration management system covers the release and management of configuration items. Configuration items are uniquely identified and maintained by the CM system. In addition, automated procedures support the configuration management and production control of the product. By the combination of these measures the threat T.Unauthorized-Staff and Organizational Security Policies P.Config-Control, P.Accept-Product and P.Organize-Product are addressed.
O.Config-Process	Configuration items are stored in the configuration management system according to the configuration management plan. Tools and procedures support the key management process to guarantee that the process is performed according to the procedure established by the configuration management plan. By the combination of these measures the threat T.Unauthorized-Staff and the OSP P.Config-Process, P.Organize-Product and P.Accept-Product are addressed.
O.Acceptance-Test	Keys are generated fulfilling specific parameters checks and test to ensure that they are in compliance with the specification. Test results are logged to support tracing and identification of systematic failures. By the combination of these measures the threat the OSP P.Accept-Product are addressed.

Security Objective	Rationale
O.Organize-Product	Key management process is performed following the procedures defined. The confidentiality and integrity of sensitive data is guaranteed. Key generation is performed in an isolated network with a certified HSM. Changes are only applied based on client's request and following a controlled process. By the combination of these measures, the organizational security policy P.Organize-Product is addressed.
O.Staff-Engagement	All employees working at the site and having access to sensitive information or data have to sign a non-disclosure agreement to provide legal liability to protect sensitive information against disclosure. Moreover, all employees are trained regarding security to support the security awareness. By the combination of these measures the threats T.Computer-Net, T.Unauthorized-Staff, T.Staff-Collusion are addressed.
O.Transfer-Data	Key secured transmission is protected with strong cryptographic algorithms to ensure that confidentiality and integrity of the data transmitted is not compromised. Only authorized personnel are able to transmit sensitive data according to the procedure defined. By the combination of these measures the threats T.Staff-Collusion and T.Attack-Transmission and the OSP P.Product-Transmission are addressed.

Table 7.1 Security Objectives Rationale

7.4 Security Assurance Requirements Rationale

The SAR Rationale does not explicitly address the developer's action elements defined in (3) 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.

Refinement operations over SARs are written in *italic*. The term "TOE" can be replaced by "product" or "intended TOE".

7.4.1 ALC_CMC.5

ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling*.

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 *product* 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 *clearly* identify the configuration items that comprise the TSF.

ALC_CMC.5.9C: The CM system shall support the audit of all changes to the *product* 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 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 *product* 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 *product*.

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

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

7.4.2 ALC_CMS.5

ALC_CMS.5.1C: The configuration list shall include the following: the evaluation evidence required by the SARs; the parts that comprise the *product* and *documented procedures used for the production process.*

ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.

ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer of the item.

The security assurance requirements of the assurance class "CM scope" listed above supports the control of the development and test environment. This includes TOE related documentation and sensitive data as well as the documentation for the configuration management and the site security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE these assurance requirements are considered to be suitable.

7.4.3 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 *product* 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 *product*.

The security assurance requirements of the assurance class "Development security" listed above are required since a high attack potential is assumed for potential attackers. The configuration items and information handled at the site during development, production, testing and pre-personalization of the intended TOE can be used by potential attackers for the development of attacks. Any keys loaded into the intended TOE also support the security during the shipment. Therefore, the handling and storage of electronic keys must also be protected. Further on the Protection Profile (1) requires this protection for sites involved in the life-cycle of intended TOE development and production.

7.4.4 ALC_LCD.1

ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the *product*.

ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the *product*.

The security assurance requirements of the assurance class "Life-cycle definition" listed above are suitable to support the controlled development and production processes. 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 and production of the intended TOE. 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.

7.5 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 product 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 product in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

- O.Alarm-Response

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

- O.Internal-Monitor

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

- O.Maintain-Security

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

- O.Logical-Access

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

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

  ALC_CMC.5.7C requires that the CM system shall ensure that the person responsible for accepting a configuration item into the CM is not the person who developed it. Therefore, the Security Assurance Requirements are suitable to meet the objective.

  ALC_CMC.5.11C requires that the CM system shall be able to identify the version of the configuration items which the product is generated from. Therefore, the Security Assurance Requirements are suitable to meet the objective.

- O.Logical-Operation

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

- O.Config-Items

  ALC_CMC.5.1C requires a documented process for ensuring an appropriate and consistent labelling of the products. A method used to uniquely identify the configuration items is required by ALC_CMC.5.2C.

  ALC_CMC.5.3C requires that an adequate and appropriate review of changes to configuration items. In addition, ALC_CMC.5.4C requires that the CM system will uniquely identify all configuration items.

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

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

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

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

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

  ALC_CMS.5.3C requires that the developer of each configuration item is indicated in the configuration list. Therefore, the Security Assurance Requirements are suitable to meet the objective.

- O.Config-Control

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

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

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

ALC_CMC.5.7C requires that the CM system shall ensure that the person responsible for accepting a configuration item into the CM is not the person who developed it. Therefore, the Security Assurance Requirements are suitable to meet the objective.

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

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

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

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

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

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

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

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

ALC_CMS.5.2C requires that the configuration list shall uniquely identify the configuration items. In addition, ALC_LCD.1.1C requires that the life-cycle definition documentation shall describe the model used to develop and maintain the product.

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

- O.Config-Process

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

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

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

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

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

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

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

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

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

ALC_CMC.5.12C requires that the CM documentation will include a CM plan.

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

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

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

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

ALC_CMS.5.2C requires that the configuration list shall uniquely identify the configuration items. In addition, ALC_LCD.1.2C requires the necessary control over the development and maintenance of the product. Thereby the objective fulfils this combination of Security Assurance Requirements.

- O.Acceptance-Test

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

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

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

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

- O.Organize-Product

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

  ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the product. In addition, ALC_LCD.1.2C requires the necessary control over the development and maintenance of the product. Thereby the objective fulfils this combination of Security Assurance Requirements.

- O.Staff-Engagement

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

- O.Transfer-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 product. Thereby this objective contributes to meet the Security Assurance Requirement.

8 Bibliography

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

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

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

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

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

6. **Library, Joint Interpretation.** *Minimum Site Security Requirements; version 3.0.* February 2020.