SONY®

Site Security Target
for SCO Operation Site

Version 1.00

Public Version

No. SCO-SSTP-E01-00

Introduction

The Site Security Target (hereinafter referred to as the "SST") describes the security features of a site.

This SST describes the site security of the development environment at the Sony City Osaki Operation Site of Sony Corporation (hereinafter referred to as the "SCO Operation Site").

The SCO Operation Site performs the design and development of the embedded software for security IC.

Contents

1 Introducing the Site Security Target

This document is the Site Security Target for CC evaluation of a site.

This Site Security Target is provided in accordance with "Common Criteria for Information Technology Security Evaluation" [CC].

For definitions of the terms and literary references used in this document, see Chapter 8, "Glossary and references".

1.1 SST and Site Identification

This section describes the location of the SCO Operation Site, and provides a general overview of the business operations and the confidential information handled there.

Table 1: SST identification

SST attribute	Value
Name	Site Security Target for SCO Operation Site
Version	1.00
Reference	SCO-SSTP-E01-00
Issue Date	June 2021

Table 2: Site identification

Site attribute	Value
Company	Sony Corporation
Name of the site	SCO Operation Site
Location	Sony City Osaki 24th floor, 2-10-1 Osaki, Shinagawa-ku, Tokyo, 141-8610 Japan

1.2 Site Description

1.2.1 Physical scope of the site

The site, as described in section 1.1, is located in 24th floor in the building, Sony City Osaki, which Sony fully occupies. The whole building is security-controlled by Sony. Only authorised persons including subcontractor are allowed to enter the development area. Development takes place at SCO Operation Site.

1.2.2 Logical scope of the site

The site is used by FeliCa Business Division to perform the development and testing of the embedded software for security IC. The development server, the dedicated network with the firewall and local IT equipment are located in the site. The developer can access the dedicated network remotely through VPN gateway server that FeliCa Business Division provides and manages.

The configuration management is provided by the configuration management tool in the development server. The activities in the site is Security IC Embedded Software Development (Phase 1) as defined in the Protection Profile (PP) [BSI-PP-0084].

2 Conformance Claims

2.1 CC Conformance Claim

The evaluation is based on the following:

- "Common Criteria for Information Technology Security Evaluation", Version 3.1 Release 5 (composed of Parts 1 and 3, [CC Part 1], and [CC Part 3])

This Site Security Target claims the following conformances:

- [CC Part 3] conformant

For the evaluation the following methodology will be used:

- "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1, Release 5 [CC CEM]
- “Supporting Document Guidance, Site Certification”, October 2007, Version 1.0, Revision 1 [CCDB-2007-11-001]

2.2 Package Claim

The chosen assurance components are:

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

2.3 Package Claim Rationale

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 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 at 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.

3.1 Assets

This section describes the assets handled at the site.

- Design documentations
- Source code
- Pre-personalisation data
- Guidance documentations
- Development tools and samples

3.2 Threats

T.Smart-Theft

An attacker tries to intrude into sensitive area for manipulation or theft of assets. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered. In addition, the attacker may be able to use specific working clothes of the site to camouflage the intention.

T.Rugged-Theft

An experienced thief with specialised equipment for burglary, who may be paid to perform the attack tries to intrude into sensitive area and manipulate or steal sensitive configuration items.

T.Computer-Net

A possibly paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to assets with the intention to violate the confidentiality and the integrity or computers with the intention to modify the development process.

T.Unauthorised-Staff

Employees or subcontractors without access authority to assets try to get access to violate the confidentiality and the integrity.

T.Staff-Collusion

An attacker tries to get access to assets by getting support from one employee through extortion or bribery.

T.Attack-Transport

An attacker tries to get assets during the internal and external delivery.

3.3 Organisational Security Policies

P.Config

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.

In addition, the services and/or processes provided by a site are controlled in the configuration management plan. This comprises tools used for the development and production of the product, the management of flaws and optimisations of the process flow as well as the documentation that describes the services and/or processes provided by a site.

P.LifeCycle-Doc

The site follows the life cycle documentation that describes: (1) description of configuration management systems and their usage; (2) a configuration items list; (3) site security; (4) the development process; (5) the development tools.

3.4 Assumptions

The SCO Operation Site has to rely on the information received from the platform site/client. This is reflected by the assumptions that must be defined for the interface.

The following assumptions are considered to be applicable to the SCO Operation Site.

A.Prod-Specification

The platform client must provide appropriate information (e.g. UGM, test tools) in order 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 platform client is appropriately labelled to ensure the identification of the configuration item.

4 Security Objectives

This chapter describes the security objectives for the site in response to the security needs identified in Chapter 3, "Security problem definition".

4.1 Security Objectives

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

O.Physical-Access

The combination of physical partitioning between the different access control levels together with technical and organisational security measures allows a sufficient separation of employees to enforce the “need to know” principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorised people. The access control measures ensure that only registered employees and vendors can access restricted areas. Sensitive products are handled in restricted areas only.

O.Alarm-Response

The technical and organisational security measures ensure that an alarm is generated before an unauthorised person gets access to any sensitive configuration item (asset). After the alarm is triggered the unauthorised 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 1 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 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 authorised 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 development network exists within the restricted area of the site and is logically separated from other networks by the firewall. The firewall allows the connection to VPN gateway that provides a secure connection to the remote secure network of the clients.

Access to the production network and related systems is restricted to authorised employees that work in the related area or that are involved in the configuration tasks or the production systems. Every user of an IT system has its own user account and password. An authentication using user account and password is enforced by all computer systems.

O.Logical-Operation

All network segments and the computer systems are kept up-to-date (software updates, security patches, virus protection, spyware protection). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.

O.Config

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 development member. Also, the internal procedures and guidance are covered by the configuration management.

In addition, 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 and production of the product, for the management of flaws and optimisations of the process flow as well as for the documentation that describes the services and/or processes provided by a site.

O.Staff-Engagement

All employees who have access to sensitive configuration items are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.

O.Internal-Shipment

The recipient of a 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. For every sensitive configuration item, the protection measures against manipulation are defined.

O.External-Delivery

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. For every configuration item, the protection measures against manipulation are defined.

O.Transfer-Data

Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorised employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected.

O.Control-Scrap

The site has measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive configuration items so that they do not support an attacker.

O.LifeCycle-Doc

The site follows the life cycle documentation that describes: (1) description of configuration management systems and their usage; (2) a configuration items list; (3) site security; (4) the development process; (5) the development tools.

4.2 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.

Note that the assumptions of the SST cannot be used to cover any threat or OSP of the site. They are seen as preconditions 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.

Table 3: Mapping of Security Objectives

Threat or OPS	Security Objective	Rationale
T.Smart-Theft	O.Physical-Access O.Alarm-Response O.Internal-Monitor O.Maintain-Security	O.Physical-Access and O.Alarm-Response detect unauthorized access, and O.Internal-Monitor and O.Maintain-Security control and maintain these security measures. Therefore, the threat is effectively addressed by these objectives.
T.Rugged-Theft	O.Physical-Access O.Alarm-Response O.Internal-Monitor O.Maintain-Security	O.Physical-Access and O.Alarm-Response detect unauthorized access, O.Internal-Monitor and O.Maintain-Security control and maintain these security measures. Therefore, the threat is effectively addressed by these objectives.
T.Computer-Net	O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement	O.Logical-Access, O.Logical-Operation and O.Staff-Engagement prevent unauthorized access from the internal and external network, and O.Internal-Monitor and O.Maintain-Security control and maintain these security measures. Therefore, the threat is effectively addressed by these objectives.
T.Unauthorised-Staff	O.Physical-Access O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Control-Scrap	O.Physical-Access, O.Alarm-Response, O.Logical-Access, O.LogicalOperationm, O.Staff-Engagement and O.Control-Scrap prevent unauthorised access to assets, and O.Internal-Monitor and O.Maintain-Security control and maintain these security measures. Therefore, the threat is effectively addressed by these objectives.
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement	O.Staff-Engagement ensures that all staff is aware of its responsibilities, and O.Internal-Monitor and O.Maintain-Security control and maintain these security measures. Therefore, the threat is effectively addressed by these objectives.

Threat or OPS	Security Objective	Rationale
T.Attack-Transport	O.Transfer-Data O.Internal-Shipment O.External-Delivery	O.Transfer-Data ensures that the sensitive item transferred to the external company are protected with the secure measures. O.Internal-Shipment and O.External-Delivery ensure that the internal and the external delivery procedure are applied to the sensitive item. Therefore, the threat is effectively addressed by these objectives.
P.Config	O.Config	O.Config directly enforces P.Config.
P.LifeCycle-Doc	O.LifeCycle-Doc	O.LifeCycle-Doc directly enforces P.LifeCycle-Doc.

5 Extended Components Definition

No extended components are currently defined in this SST.

6 Security Requirements

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

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

The Security Assurance Requirements listed above fulfil the requirements of [CCDB-2007-11-001] because hierarchically higher components than the defined minimum site requirements (ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, see section 3.2.3 of [CCDB-2007-11-001]) are used in this Site Security Target.

6.1 Application Notes and Refinements

The description of the site certification process [CCDB-2007-11-001] 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 are in the focus and described in this SST.

These processes are subject of the evaluation of the site.

6.2 Overview and Refinements

6.2.1 CM Capabilities (ALC_CMC)

According to [CCDB-2007-11-001] the processes rather than a TOE are in the focus of the CMC examination. The configuration items for the considered product type are listed in section 3.1. The CM documentation of the site must be able to maintain the items listed for the relevant life-cycle step and the CM system must be able to track the configuration items.

A CM system has to be employed to guarantee the traceability and completeness of different configuration items. Appropriate administration procedures have to be provided in order to maintain the integrity and confidentiality of the configuration items.

6.2.2 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 configuration items handled at the site.

In the particular case of a Security IC development site the scope of the configuration management can include a number of configuration items. The configuration items already defined in section 3.1 that are considered as "TOE implementation representation" include:

- Design documentations
- Source code in any form
- Pre-personalisation data
- Guidance documentation
- Development tools and samples

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

6.2.3 Delivery Procedure (ALC_DEL)

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 customer or customer's site. 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 pre-personalisation data and/or configuration data may include supplements of the Security IC Embedded Software.

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

6.2.5 Life-Cycle Definition (ALC_LCD)

The site is not equal to the entire development environment. Therefore, the ALC_LCD criteria are interpreted in a way that only those life-cycle phases have to be evaluated which are in the scope of the site. The PP [BSI-PP-0084] 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 initialisation is performed at the site or not.

The PP [BSI-PP-0084] 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 1 “Security IC Embedded Software Development”.

6.2.6 Tools and Techniques (ALC_TAT)

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.1, “Well-defined development tools”, requires evidence for the suitability of the tools and techniques used for the development process of the TOE.

The site shall be identified 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.

6.3 Security Assurance Rationale

The dependencies for the assurance requirements are as follows;

- ALC_CMC.5: ALC_CMS.1, ALC_DVS.2 and ALC_LCD.1
- ALC_CMS.5: None
- ALC_DEL.1: None
- ALC_DVS.2: None
- ALC_LCD.1: None
- ALC_TAT.3: ADV_IMP.1

Table 4: Rationale for ALC_CMC.5

SAR	Objective	Rationale
ALC_CMC.5.1C: The TOE shall be labelled with its unique reference.	O.Config	The TOE is labelled with its unique reference by the configuration management system (O.Config).
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.LifeCycle-Doc	The method used to uniquely identify the configuration items is described in the CM documentation (O.LifeCycle-Doc).

SAR	Objective	Rationale
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.LifeCycle-Doc	The adequate and appropriate acceptance procedures for configuration items are described in the CM plan (O.LifeCycle-Doc).
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.Config	All configuration items are uniquely identified by the configuration management system (O.Config).
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	O.Config	The configuration system (O.Config) provided the automated measures such that only authorised change are made to the configuration items.
ALC_CMC.5.6C: The CM system shall support the production of the TOE by automated means.	O.Config	The building of the software and the testing are supported by the automated means of the configuration management system (O.Config).
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.LifeCycle-Doc	As described in the CM plan (O.LifeCycle-Doc) the activities performed are such that the person responsible for accepting a configuration item into CM is not the person who developed it.
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	O.Config	The configuration management system (O.Config) identifies the configuration items that comprise the TSF.
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.	O.LifeCycle-Doc O.Config	As described in the CM plan (O.LifeCycle-Doc) the configuration management system (O.Config) automatically generate all changes history, such as originator, date and time.
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O.LifeCycle-Doc O.Config	As described in the CM plan (O.LifeCycle-Doc) the configuration management system and software installed on the development servers (O.Config) provide automated means to identify all other configuration items that are affected by the change of a given configuration item.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.	O.LifeCycle-Doc O.Config	As described in the CM plan (O.LifeCycle-Doc) the configuration management system (O.Config) identifies the version of the implementation representation from which the intended TOE is generated.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.LifeCycle-Doc	The CM plan is described in the CM documentation (O.LifeCycle-Doc).
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE.	O.LifeCycle-Doc	The CM system usage is described in the CM documentation (O.LifeCycle-Doc).

SAR	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 TOE.	O.LifeCycle-Doc	The acceptance procedure for modified and newly created configuration items are described in the CM documentation (O.LifeCycle-Doc).
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.LifeCycle-Doc O.Config	The configuration items are listed in the CM documentation (O.LifeCycle-Doc). All electronic items are maintained under the configuration management system (O.Config).
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.LifeCycle-Doc O.Config	The configuration list (O.LifeCycle-Doc) is generated from the configuration management system (O.Config).

Table 5: Rationale for ALC_CMS.5

SAR	Objective	Rationale
ALC_CMS.5.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.	O.LifeCycle-Doc	The configuration list (O.LifeCycle-Doc) includes these items, and the configuration management plan manages the security flaw reports, resolution status and development tools and related information.
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config	The configuration list is generated from the configuration management system (O.Config).
ALC_CMS.5.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	O.Config	The configuration management system (O.Config) manages indicates the developer for each configuration items.

Table 6: Rationale for ALC_DEL.1

SAR	Objective	Rationale
ALC_DEL.1.1C: 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 O.Transfer-Data O.External-Delivery	The delivery documentation (O.LifeCycle-Doc) describes the procedural security measures that are necessary to protect the confidentiality and integrity (O.Transfer-Data and O.External-Delivery) of the electronic items delivered to the customer.

Table 7: Rationale for ALC_DVS.2

SAR	Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	O.Physical-Access O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Control-Scrap O.LifeCycle-Doc O.Transfer-Data O.Internal-Shipment	The development security documentation (O.LifeCycle-Doc) describes all the physical (O.Physical-Access, O.Alarm-Response), procedural (O.Internal-Monitor, O.MaintainSecurity, O.Control-Scrap), personnel (O.Staff-Engagement), internal shipment (O.Transfer-Data, O.Internal-Shipment) and other (O.Logical-Access, O.LogicalOperation) security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O.LifeCycle-Doc	The development security documentation (O.LifeCycle-Doc) justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

Table 8: Rationale for ALC_LCD.1

SAR	Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) describes the life cycle model used to develop and maintain the TOE.
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	O.LifeCycle-Doc	The life cycle model that is described by the life cycle documentation (O.LifeCycle-Doc) provides for the necessary control over the development and maintenance of the OE.

Table 9: Rationale for ALC_TAT.3

SAR	Objective	Rationale
ALC_TAT.3.1C: 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 defined.
ALC_TAT.3.2C: 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.

SAR	Objective	Rationale
ALC_TAT.3.3C: 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.

7 Site Summary Specification

7.1 Preconditions Required by the Site

The site performs the embedded software for security IC development and testing service. In order to perform these services in a secure way, the platform client need to support the security processes. The following denote preconditions of the platform client that are required to ensure the security measures of the site in order to its assets.

To enable the site to participate in the development and testing of products, the platform client needs to provide the necessary development environment (i.e., tools, samples) and information (i.e., specification, UGM). (**A.ProdSpecification**)

All provided items from the platform client are labelled to ensure the identification of the configuration items. (**A.Item-identification**)

7.2 Service of the Site

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

7.3 Objectives Rationale

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

O.Physical-Access

The physical, technical and organisational security measures ensure a separation of the site into four security levels. The access control ensures that only registered persons can access sensitive areas. Therefore this objective can support to prevent the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff.

O.Alarm-Response

During working hours the employees monitor the alarm system. If the alarm is sounded, the employees pay attention whether the suspicious person enter the area or not. During off-hours third party guard system supports the alarm system. The response time of the guard and the physical resistance match to provide an effective alarm response. Therefore this objective can support to prevent the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff.

O.Internal-Monitor

The established security measures of the site are regularly reviewed by security management meetings and internal audits. Therefore this objective can support to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

O.Maintain-Security

Technical security measures are maintained regularly and the logging of the server is checked regulary. This ensures that the systems are working correctly and unauthorised access is not occurred. Therefore this objective can support to prevent T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

O.Logical-Access

The development network is separated from the corporate network with a firewall. The firewall allows extremely limited applications. Each user is logging into the system with his/her personalised user ID and password. Therefore this objective can support to prevent T.Computer-Net and T.Unauthorised-Staff.

O.Logical-Operation

Security patches and virus pattern files are automatically delivered from the Security Patch server in the development network to the development PC. The backup of the server is sufficiently protected and is only accessible for the administration. Therefore this objective can support to prevent T.Computer-Net and T.Unauthorised-Staff.

O.Config

All files related to the development are stored the development server. The server provides the configuration management system to maintain current and historical versions of files and to identify the TOE uniquely and the he configuration management plan is controlled by the configuration management tool installed in the development server. Therefore this object directly addresses P.Config.

O.Staff-Engagement

Each employee has the responsibility to maintain secrecy concerning company-confidential information. To enforce this, each employee must agree to and sign a non-disclosure agreement. All employees are trained and qualified for their job. Therefore this objective can support to prevent T.Computer-Net, T.UnauthorisedStaff and T.Staff-Collusion.

O.Internal-Shipment

The internal shipment 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.

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.

O.Transfer-Data

The confidentiality and integrity of the data transfer from/to the site is ensured by appropriate secure measures. The secure measures include using secure transfer protocol during transfer and encryption on sensitive information. Therefore this objective can support to prevent T.Attack-Transport.

O.Control-Scrap

The security of scrap handling is ensured by either securely destruct assets (e.g. paper shredder) or return them to the platform client. Therefore this objective can support to prevent T.Unauthorised-Staff and T.StaffCollusion.

O.LifeCycle-Doc

Dedicated documents exist for the site which define the use and the management of the configuration management systems, the configuration item list, the site security, the development process and the development tools. The site follows the procedures and instructions of these documents. This directly addresses the P.LifeCycle-Doc.

7.4 Security Assurance Requirements Rationale

The Security Assurance Rational is given in section 6.3. This rationale addresses all content elements and thereby also implicitly all the developer action elements defined in [CC Part 3]. Therefore, the Security Assurance Requirements rationale provides the justification for the selected Security Assurance Requirements. The selected Security Assurance Requirements fulfil the needs derived from the PP [BSI-PP-0084].

7.5 Assurance Measure Rationale

O.Physical-Access

ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore, this SAR is suitable to meet the security objective.

O.Alarm-Response

ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore, this SAR is suitable to meet the security objective.

O.Internal-Monitor

ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore, this SAR is suitable to meet the security objective.

O.Maintain-Security

ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore, this SAR is suitable to meet the security objective.

O.Logical-Access

ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore, this SAR is suitable to meet the security objective.

O.Logical-Operation

ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore, this SAR is suitable to meet the security objective.

O.Config

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. ALC_CMC.5.4C and ALC_CMS.5.2.C requires that the configuration management system uniquely identifies all configuration items. ALC_CMS.5.4C requires that for each configuration item, the configuration list indicates the developer/subcontractor of the item. ALC_CMC.5.5C requires that the configuration management system provides automated measures such that only authorized changes are made to the configuration items. ALC_CMC.5.6C requires that the configuration management system supports the production of the product by automated means. ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the configuration management system. ALC_CMC.5.16C requires that the evidence demonstrates that all configuration items have been and are being maintained under the configuration management system. All SARs define required properties of the configuration management system. Therefore, these SARs are suitable to meet the security objective.

O.Staff-Engagement

ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore, this SAR is suitable to meet the security objective.

O.Internal-Shipment

ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore, this SAR is suitable to meet the security objective.

O.External-Delivery

ALC_DEL.1.1C requires that the delivery documentation describes all procedures that are necessary to maintain security when distributing versions of the TOE to the customer. Therefore, this SAR is suitable to meet the security objective.

O.Transfer-Data

ALC_DEL.1.1C requires that the delivery documentation describes all procedures that are necessary to maintain security when distributing versions of the TOE to the customer. Therefore, this SAR is suitable to meet the security objective.

ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore, this SAR is suitable to meet the security objective.

O.Control-Scrap

ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore, this SAR is suitable to meet the security objective.

O.LifeCycle_Doc

ALC_CMC.5.2C requires that the CM documentation describes the method used to uniquely identify the configuration items. ALC_CMC.5.12C requires that the CM documentation includes a configuration management plan. ALC_CMC.5.13C requires that the configuration management plan describes how the configuration management system is used for the development of the TOE. ALC_CMC.5.14C requires that the configuration management plan describe the procedures used to accept modified or newly created configuration items as part of the TOE. ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the configuration management system.

ALC_CMS.5.1C requires that the CL includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a configuration management plan.

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

ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the TOE. ALC_LCD.1.2C requires that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

ALC_TAT.3.1C requires that each development tool used for implementation is well-defined. ALC_TAT.3.2C requires that the documentation of each development tool unambiguously defines the meaning of all statements as well as all conventions and directives used in the implementation. ALC_TAT.3.3C requires that the documentation of each development tool unambiguously defines the meaning of all implementation dependent options.

All SARs require dedicated content of the CM documentation and the configuration list, properties of the configuration management system, content of the development security documentation, of the life-cycle documentation and of the used development tools. Therefore, these SARs are suitable to meet the security objective.

7.6 Mapping of the Evaluation Documentation

The scope of the evaluation according to the assurance class ALC comprises the processing and handling of security products and the complete documentation of the site provided for the evaluation. The specifications and descriptions provided by the client are not part of the configuration management at SCO Operation Site.

The mapping between the internal site documentation and the Security Assurance Requirements is described by the following tables.

Table 10: Mapping for ALC_CMC.5

SAR	References
ALC_CMC.5.1C: The TOE shall be labelled with its unique reference.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
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.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMC.5.6C: The CM system shall support the production of the TOE by automated means.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
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.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)

SAR	References
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)

Table 11: Mapping for ALC_CMS.5

SAR	References
ALC_CMS.5.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)
ALC_CMS.5.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	SCO Configuration Management Plan (SCO-CMP-E01-00) SCO Configuration List (SCO-CML-E01-00)

Table 12: Mapping for ALC_DEL.1

SAR	References
ALC_DEL.1.1C: The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.	SCO TOE Delivery Procedure (SCO-DEL-E01-00)

Table 13: Mapping for ALC_DVS.2

SAR	References
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	SCO Development Security (SCO-DVS-E01-00)

SAR	References
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	SCO Minimum Site Security Requirement Check List (SCO-MSSR-E01-00)

Table 14: Mapping for ALC_LCD.1

SAR	References
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	SCO Life Cycle Model (SCO-LCD-E01-00)
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	SCO Life Cycle Model (SCO-LCD-E01-00)

Table 15: Mapping for ALC_TAT.3

SAR	References
ALC_TAT.3.1C: Each development tool used for implementation shall be well-defined.	SCO Development Tool Definitions (SCO-TAT-E01-00)
ALC_TAT.3.2C: 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.	SCO Development Tool Definitions (SCO-TAT-E01-00) FeliCa OS Version 5.0 Coding Guidelines (OS5-IMP-Guide-E01-50)
ALC_TAT.3.3C: The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.	SCO Development Tool Definitions (SCO-TAT-E01-00)

8 Glossary and References

This chapter explains the terms, definitions and literary references (bibliography) used in this document. The list entries in this chapter are ordered alphabetically.

8.1 Terms and Definitions

The following list defines the product-specific terms used in this document:

Client

The term “client” is used in this SST to denote the platform developers or IC vendors.

Customer

The term “customer” is used in this SST to denote the customer of the IC vendors, which the finished and functionally tested ICs are delivered to and the entity responsible for pre-personalisation of the TOE.

Pre-personalisation Data

Any data supplied by the card manufacturer that is injected into the non-volatile memory by the IC manufacturer or the IC packaging manufacturer.

8.2 Bibliography

The following list defines the literature referenced in this document:

[BSI-PP-0084] EUROSMART, "Security IC Platform Protection Profile with Augmentation Packages, Version 1.0”, January 2014

[CC] "Common Criteria for Information Technology Security Evaluation", Version 3.1 (composed of Parts1 and Pars2, [CC Part 1] and [CC Part 3])

[CC Part 1] "Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model", Version 3.1, Revision 5, April 2017

[CC Part 3] "Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components", Version 3.1, Revision 5, April 2017

[CC CEM] "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1, Revision 5, April 2017

Site Security

Site Security Target for SCO Operation site
Version 1.00

June 2021 First Edition FeliCa Business Division

Sony Corporation

No. SCO-SSTP-E01-00

Printed in Japan