NXPOMS-1719007347-3870

Site Security Target – NXP Shanghai Puxi

Revision	V1.4

Table of content

Table of Figures

1. SST Introduction

1 The chapters 1 to 8 of this document are based upon the Eurosmart Site Security Target Template [1] with adaptations such that it fits the site.

2 This Site Security Target is intended to be used by only one specific client, namely NXP Semiconductors. Therefore, the term 'client' in this document refers directly to NXP Semiconductors. Note that also the site of this Site Security Target as defined below belongs to NXP Semiconductors.

1.1 SST Reference

3 Company: NXP Semiconductors

4 Name of site: Shanghai Puxi

5 EAL: SARs taken from EAL6

1.2 Site Reference

6 The site is located at:

NXP (China) Management Ltd
BM InterContinental Business Centre
100 Yu Tong Road,
Shanghai 200070
P.R.C.

1.3 Site Description

1.3.1 Physical Scope

7 The following area of the site specified in section 1.2 is in the scope of the SST.

8 All areas in scope are classified as YELLOW[1] and RED[1] areas. These areas are comprised of three floors in a single building, namely 19-21.

The physical scope is only the development area located on floor 19 and the data center on floor 20.

9 A more detailed view of the layout is described in the Site Security Manual (SSM) for Shanghai Puxi.

10 Those locations contain security areas with restricted access under control of NXP where only authorized persons can enter.

11 Within those areas, only members of the development team are entitled to access sensitive information like source code, confidential development documentation and samples. To enforce such access restriction, a combination of physical, procedural, personnel and logical measurements have been installed. Note, that physical security objects have to be handled according to [2].

1.3.2 Logical Scope

12 The following life-cycle phases as defined in 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084) [3] are subject of the SST:

- Phase 1: Security IC Embedded Software Development,
- Phase 2: IC Development

13 To perform its activities the site uses Corporate IT infrastructures and services implemented in a stand-alone local Secure Data Center, only authorized IT engineers are allowed to maintain this infrastructure from security administration room remotely and locally. The site works according to CCC&S.

14 The following services and/or processes provided by NXP Shanghai Puxi are in the scope of the site evaluation process. Some processes are directly part of the phases presented before and others are supporting processes which can be involved at any phase of the development. The services are detailed in section 7.2 below.

1.3.2.1 Supporting service

- IT support;

[1] The terms YELLOW area and RED area are defined in the NXP internal document „NXPOMS-1719007347-2404 CCC&S Security Requirements Overview“

1.3.2.2 Shanghai Puxi Site Services related to [3] life cycle phases

- IC Embedded Software Development, Test Program Development, Verification and Validation (Phase 1) and/or IC Development, IC Dedicated Software Development, Verification and Validation (Phase 2)

2. Conformance Claim

15 This SST is conformant with Common Criteria Version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017, [4]
- Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017, [5]

16 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, [6]

17 This SST is CC Part 3 conformant.

18 The evaluation of the site comprises the following assurance components[2]:

19 ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1.

20 The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profile [3] and is therefore suitable for the evaluation of (software for) Security ICs.

21 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.

[2] The activities of the site are not directly related to production and shipping of secure products. Therefore, this site does not claim conformance to ALC_DEL. Since the used tools and techniques are defined upfront by the client (see A.Project-Setup), the site does not contribute to ALC_TAT and does not have any negative impact to it. Therefore, this site does not claim conformance to ALC_TAT.

3. Security Problem Definition

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

23 Where necessary the items in this section have been re-worked to fit the site.

3.1 Assets

24 The following section describes the assets handled at the site as per NXPOMS-1719007347-2401 “Security Objects Document”. They can be grouped within the following categories:

Physical Security objects: The site has physical security objects (samples, printed documents, etc.) in relation to developed TOEs. Both the integrity and the confidentiality of these must be protected.

Development data: The site has access to (and optionally copies thereof) electronic development data (specifications, guidance documentation, source code, etc.) in relation to developed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected.

Development tools: To perform its development activities the site uses tools (e.g. compiler) to transform source code (and potentially the libraries that come with these tools) into binaries. The integrity of these tools (running on local or remote development computers) must be protected.

3.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of assets: (1) physical security objects, (2) development data, (3) development tools. 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 attacker 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 possibly paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to

(1) development data with the intention to violate confidentiality and possibly integrity

(2) development computers with the intention to modify the development process.

T.Unauthorised-Staff: Employees or subcontractors not authorized to get access to assets violating the confidentiality and possibly the integrity of products.

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 access to shipped physical security objects when shipped in or out of the site with the intention to compromise confidentiality and/or integrity of the product design data, customer and/or consumer data like code and data (including personalization data and/or keys) stored in the ROM and/or EEPROM or classified product documentation.

3.3 Organizational Security Policies

P.Config_IT-env: In addition to the used software on development workstations and servers, the site uses configuration management systems for file versioning and problem tracking. For file versioning, the team members are assigned to project specific, centralized repositories to support proper management of multiple products and the site internal procedures. The team members are requested to use only project related IT equipment with the provided tools.

P.LifeCycle-Doc: The site 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.

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

3.4 Assumptions

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

A.DevEnv-Provisioning: To enable that the site participates in the development of products the client provides services to setup and maintain the necessary development environment (e.g. workstations, tools, test samples) and configuration management systems (e.g. user accounts in project repositories) including a CM plan.

A.Project-Setup: The site participates in the development of products. For each product the site and the client agree on the following items:

- the activities to be performed by the site,
- the specifications of the input for the site including tools,
- the acceptance of the results by the client,
- the used configuration management methods and tools,
- the delivery and shipment details of any security relevant item,
- the handling of scrap configuration items: in case that scrap is not destroyed by the site, scrap configuration items are transferred back to the client.

The agreed methods and tools ensure the correct handling of the configuration items in terms of Common Criteria regarding the classes ALC_CMC and ALC_CMS.

4. Security Objectives

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

O.Config_IT-env: In addition to the used software on development workstations and servers, the site uses configuration management systems for file versioning and problem tracking. For file versioning, unique repositories are used to support proper management of multiple products and the site internal procedures. Only project related tools and IT equipment is used.

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.

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 shall support the limitation for the access to these areas including the identification and rejection of unauthorized people. The access control measures ensure that only registered employees can access restricted areas. Assets are handled in restricted areas only.

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

O.Alarm-Response: The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any asset. 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.

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

O.Maintain-Security:	Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only 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.Network-separation:	China Secure design is based on Split VPN concept where only secure traffic is tunneled through a VPN tunnel and all other traffic is directly sent to the NXP network. The logical network security is based on 2 security zones. The Normal Secure environment for the outside and the China security zone. These environments are separated by a Cisco Firewall. VPNs are set up between the secure rooms to ensure that data in China Secure is never sent over the NXP network unencrypted. The China Secure network zone is divided in certain subzones- Servers/Server Management/Admin/Clients/LAB.
O.Logical-Operation:	Development workstations enforce that every user authenticates using a password and has a unique user ID.
O.Control-Scrap:	The site has measures in place to either securely destruct paper-based secure objects, i.e. secure documents, or likewise secure CD/DVD media, by means of a secure cross-cutting shredder or return them to the client. Physical Security objects like samples are in any case sent back to the client. They are stored and collected in one of the high security rooms before sending.
O.Staff-Engagement:	All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.
O.Internal-Shipment:	The site has measures in place to provide assurance of integrity throughout transport of physical security objects. The recipient of a physical configuration item is identified by the assigned client address. The internal shipment procedure is applied to the configuration item. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of configuration items during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined.
O.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 authorized employees can extract the sensitive electronic configuration item. The keys

are exchanged based on secure measures and they are sufficiently protected.

4.1 Security Objectives Rationale

27 The SST includes a Security Objectives Rationale with two parts. The first part includes the 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 (see column “Rationale” of Table 1 and Table 2).

28 Note that the assumptions of the SST cannot be used to cover any threat or OSP of the site. They are pre-conditions fulfilled either by the site providing the sensitive 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

Threat	Security Objective(s)	Rationale
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat.
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat.
T.Computer-Net	O.Network-separation O.Maintain-Security O.Internal-Monitor	IT protections combined with security measures detect unauthorized access to logical assets.
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Operation O.Staff-Engagement O.Control-Scrap	Physical and logical access control prohibits access to assets. Secure destruction of scrap limits the number of assets.

Threat	Security Objective(s)	Rationale
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Control-Scrap	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees limits unauthorized access to assets.
T.Attack-Transport	O.Internal-Shipment O.LifeCycle-Doc	The shipment method and the organizational measures ensure that integrity changes of shipped objects are detected and appropriately responded upon.

Table 1 Threats - Security Objectives Rationale

OSP	Security Objective(s)	Rationale
P.Config_IT-env	O.Config_IT-env	The Security Objective directly enforces the OSP.
P.LifeCycle-Doc	O.LifeCycle-Doc	The Security Objective directly enforces the OSP.
P.Transfer-Data	O.Transfer-Data	The Security Objective directly enforces the OSP.

Table 2 OSP - Security Objectives Rationale

5. Extended Assurance Components Definition

29 No extended components are defined in this Site Security Target.

6. Security Assurance Requirements

30 Clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profile [3].

31 The Security Assurance Requirements are chosen from the class ALC (Life-cycle support) as defined in [5]:

- CM capabilities (ALC_CMC.5)
- CM scope (ALC_CMS.5)
- Development Security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)

32 The Security Assurance Requirements listed above fulfill the requirements of [7] 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 [7]) are used in this Site Security Target.

6.1 Application Notes and Refinements

33 The description of the site certification process [7] includes specific application notes. The main item is that a product that is considered as intended TOE is not available during the evaluation. Since the term “TOE” is not applicable in the Site Security Target, the associated processes for the handling of products, or “intended TOEs” are in the scope of this Site Security Target and are described in this document. These processes are subject of the evaluation of the site.

6.1.1 CM Capabilities (ALC_CMC.5)

34 Refer to subsection ‘Application Notes for Site Certification’ in [7] 5.1 ‘Application Notes for ALC_CMC’.

35 Note: Due to the Eurosmart PP [3] refinements for ALC_CMS (see below) not being applicable those for ALC_CMC are also not applicable.

6.1.2 CM Scope (ALC_CMS.5)

36 Refer to subsection ‘Application Notes for Site Certification’ in [7] 5.2 ‘Application Notes for ALC_CMS’.

37 Note: Due to these application notes the refinements from the Eurosmart PP [3] (see section 6.2.1.3) are not applicable.

6.1.3 Development Security (ALC_DVS.2)

38 Refer to subsection ‘Application Notes for Site Certification’ in [7] 5.4 ‘Application Notes for ALC_DVS’.

6.1.4 Life-cycle Definition (ALC_LCD.1)

39 Refer to subsection 'Application Notes for Site Certification' in [7] 5.6 'Application Notes for ALC_LCD'.

40 Refer to '*Application Note 26'* in 6.2.1.2 'Refinements regarding Development Security (ALC_DVS)' in the Eurosmart PP [3] (application note 27).

41 Refer to subsection *'Refinement'* in 6.2.1.2 'Refinements regarding Development Security (ALC_DVS)' in the Eurosmart PP [3].

6.2 Security Requirements Rationale

6.2.1 Security Requirements Rationale - Dependencies

42 The dependencies for the assurance requirements are as follows (see [5], appendix C):

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

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

- ALC_LCD.1 is only partially fulfilled as the site does not represent the entire development environment. This is in-line with and further explained in [7] 5.1 'Application Notes for ALC_CMC'.

6.2.2 Security Requirements Rationale - Mapping

SAR	Security Objective	Rationale
ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*	O.Config_IT-env O.LifeCycle-Doc	Appropriate and consistent labeling is ensured through the application of the CM-Plan (O.LifeCycle-Doc) and the use of the configuration management systems (O.Config_IT-env).
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-Plan (O.LifeCycle-Doc).
ALC_CMC.5.3C: The CM documentation shall justify that the	O.LifeCycle-Doc	The adequate and appropriate acceptance procedures for configuration

SAR	Security Objective	Rationale
acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.		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_IT-env O.LifeCycle-Doc	Unique identification of all CIs is realized by performing the CM activities in accordance with the CM-Plan (O.LifeCycle-Doc) using the Configuration management systems (O.Config_IT-env)
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config_IT-env O.LifeCycle-Doc	The configuration management systems (O.Config_IT-env) used according to the CM-Plan (O.LifeCycle-Doc) enforces automated measures such that only authorized changes are made to the configuration items
ALC_CMC.5.6C: The CM system shall support the production of the product by automated means.	O.Config_IT-env O.LifeCycle-Doc	The software on the development computers (O.Config_IT-env) supports automated production of products when used in accordance with the CM-Plan (O.LifeCycle-Doc)
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 clearly identify the configuration items that comprise the TSF.	O.Config_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configuration management systems (O.Config_IT-env) are configured such that an audit trail (showing originator, date and time) is automatically generated.
ALC_CMC.5.9C: The CM system shall support the audit of all	O.Config_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configurations management

SAR	Security Objective	Rationale
changes to the *intended* TOE by automated means, including the originator, date, and time in the audit trail.		system and software installed on the development workstations and servers (O.Config_IT-env) provide automated means to identify all other configuration items that are affected by the change of a given configuration item.
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O.Config_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configurations management system (O.Config_IT-env) identifies the version of the implementation representation from which the intended TOE is generated through baselines.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the *intended* TOE is generated.	O.Config_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configurations management system (O.Config_IT-env) identifies the version of the implementation representation from which the intended TOE is generated through baselines.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the *intended* TOE.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) describes 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 *intended* TOE.	O.LifeCycle-Doc	The acceptance procedures for modified or newly created configuration items are described in the CM-Plan (O.LifeCycle-Doc).

SAR	Security Objective	Rationale
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.LifeCycle-Doc	All configuration items are listed in the CI-list (O.LifeCycle-Doc)
ALC_CMC.5.16C: The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.	O.Config_IT-env O.LifeCycle-Doc	The CI-list (O.LifeCycle-Doc) is generated from the configuration management systems (O.Config_IT-env)

Table 3 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMS.5.1C: The configuration list includes the following: the *intended* TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the *intended* TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan and a CI-List with the items required by ALC_CMS.5.1C
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.LifeCycle-Doc	The CI-List (O.LifeCycle-Doc) uniquely identifies the configurations items as described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.	O.LifeCycle-Doc	The CI-List (O.LifeCycle-Doc) indicates the developer/subcontractor for each configuration items as described in the CM-Plan (O.LifeCycle-Doc).

Table 4 Rationale for ALC_CMS.5

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

Table 5 Rationale for ALC_DVS.2

SAR	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the *intended* TOE.	O.LifeCycle-Doc	The model used to develop the intended TOE is described in the life cycle documentation (O.LifeCycle-Doc)
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and	O.LifeCycle-Doc	The life cycle model as described in the life cycle documentation (O.LifeCycle-Doc) provides for the necessary control over the development and

SAR	Security Objective	Rationale
maintenance of the *intended* TOE.		maintenance of the intended TOE.

Table 6 Rationale for ALC_LCD.1

7. Site Summary Specification

7.1 Preconditions required by the Site

44 The site performs development and test services for the construction of secure IC hardware and software. In order to perform these services in a secure way, the client of the site need to support the security processes of the site. The following paragraphs denote preconditions of the client that are required to ensure the security measures of the site in order to protect its assets. Please also refer to the site visit checklist requirements [16].

Precondition	Assumption
The client needs to setup and maintain the used configuration management systems and provide a project specific CM plan. This includes the setup and maintenance of user accounts in the project repositories and other required configuration management tools. The client needs to agree about the configuration management methods and the usage of the configuration management tools. The configuration management methods and tools by the client ensure the correct handling of the configuration items according to Common Criteria. For each project setup, the client needs to agree on the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results from the site. Regarding a destruction of certain physical assets, the client needs to specify whether the scrap needs to be destroyed by the site or needs to be sent back to the client. In case of physical shipment of security relevant items between the client and the site, the client needs to agree about the shipment details and procedures. In the latter case the client is responsible for the secure destruction of the assets. Paper-based secure objects, i.e. secure documents, or likewise secure CD/DVD media, are disposed of by means of a secure cross-cutting shredder. Physical Security objects, i.e. sample devices that are to be disposed are collected in one of the high security rooms. At the appropriate time they will	A.Project-Setup

Precondition	Assumption
be shipped in one to the client for secure scrapping and disposal.	
To enable the site to participate in the development of products, the client needs to provide services to setup and maintain the necessary development environment (e.g. workstations, development tools, test samples).	A.DevEnv-Provisioning

Table 7 Mapping of Preconditions to Assumptions

7.2 Services of the Site

45 The following services and/or processes provided by NXP Shanghai Puxi are in the scope of the site evaluation process:

IC Embedded Software Development and testing (Phase 1) and/or IC Dedicated Software Development and testing (Phase 2) as defined in 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084), as well as development and characterization/validation testing of secure smart card ICs.

The typical Life Cycle model for Smart Cards usually comprises the following phases: (i) Development, (ii) Validation, (iii) Production, (iv) Delivery, (v) Preparation, (vi) Operation whereas the site under evaluation supports only the life cycle phase (i) Development and (ii) Validation.

46 The services as listed in section 1.3.1 and 1.3.2 are more detailed in the following.

- IC Development, IC embedded Software development and IC dedicated software which comprises:
    - The generation of the source code of embedded and IC dedicated software and the creation of development related documents. The development is done according to the BL C&S Product Creation described in NXPOMS-999116894-3989 - NPI 3.0 Handbook and associated procedures;
    - The generation of the analog and digital hardware designs, embedded and IC dedicated software and the creation of development related documents
    - The verification and validation process using or not simulation tools.

  The emulation devices are handled according to a packing and delivery procedure described in internal document NXPOMS-1719007347-2354. The purpose of verification is the preparation of developed software for implementation on the target device.
- IT environment including a local datacenter which provides
    - An appropriate physical environment for sensitive IT equipment provided for CS equipment.

7.3 Objectives Rationale

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

48 O.Config_IT-env: The site uses only project related tools and IT equipment. To provide a separation between different projects, the site uses configuration file versioning and unique repositories as well as configuration management systems. This directly addresses the OSP P.Config_IT-env.

49 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 OSP P.LifeCycle-Doc. Further, the threat T.Attack-Transport can be prevented.

50 O.Physical-Access: The site implements a “need to know” principle by separation measures using a combination of physical partitioning together with technical and organisational security measures. The access control measures support the enforcement of the separation and the “need to know” principle. The handling of assets is restricted to separates security areas. By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

51 O.Security-Control: The site is using dedicated personnel for guard services. These personnel are responsible for operation of the access control systems, for the enforcement of the access control, for the surveillance of the technical alarm sensors and the responses to incidents and for the escort of visitors. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff.

52 O.Alarm-Response: In case of an access attempt to an asset by an unauthorized person the site has an alarm system in place. After the alarm is triggered the unauthorised person still should 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.Unauthorised-Staff.

53 O.Transfer-Data: The protection of exchanged sensitive data is performed using crypto algorithms and key management is well done. This helps to address P.Transfer-Data.

54 O.Internal-Monitor: The established security measures of the site 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.Unauthorised-Staff and T.Staff-Collusion.

55 O.Maintain-Security: Technical security measures are maintained regularly. This ensures that the systems are working correctly and are configured as required to

ensure the protection of the networks and computer systems. Hence, this helps to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

56 O.Network-separation: The development network of the site is located in a dedicated secured area. This network is connected only to dedicated trustworthy systems. This prevents the threat T.Computer-Net.

57 O.Logical-Operation: The used workstations for development purposes are using authentication measures for the users of these systems. Hence the threats T.Unauthorised-Staff is prevented.

58 O.Internal-Shipment: The site implements protection measures to provide assurance of integrity throughout transport of physical security objects. Hence, the threat T.Attack-Transport is prevented.

59 O.Control-Scrap: The security of scrap handling is ensured by either securely destruct assets (e.g. paper shredder) or return them to the client. This helps to prevent the threats T.Unauthorised-Staff and T.Staff-Collusion.

60 O.Staff-Engagement: The site has established personnel security measures: All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job. This helps to prevent the threats T.Unauthorised-Staff and T.Staff-Collusion.

7.4 Assurance Measure Rationale

61 The following section provides a rationale for each security objective for the development environment (as defined in chapter 4), why each of the assigned SARs (as given in section 6.2.2) is suitable to meet the security objective.

62 The justification is given at the level of SAR content elements (see Table 3 to Table 6).

7.4.1 O.Config_IT-env

63 ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labeling of the products. ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items. ALC_CMC.5.6C requires that the CM system supports the production of the product by automated means. ALC_CMC.5.8C requires that the CM system clearly identifies the configuration items that comprise the TSF. ALC_CMC.5.9C requires that the CM system supports the audit of all changes to the intended TOE by automated means, including the originator, date, and time in the audit trail. ALC_CMC.5.10C requires that the CM system provides an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.11C requires that the CM system is able to identify the version of the implementation representation from which the intended TOE

is generated. ALC_CMC.5.16C requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system.

64 All these content elements of the SAR define required properties of the used configuration management system. Thereby this SAR is suitable to meet the security objective.

7.4.2 O.LifeCycle-Doc

65 ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labeling of the products. ALC_CMC.5.2C requires that the CM documentation describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires that the CM documentation justifies that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items. ALC_CMC.5.6C requires that the CM system supports the production of the product by automated means. ALC_CMC.5.7C requires that the CM system ensures that the person responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.8C requires that the CM system clearly identifies the configuration items that comprise the TSF. ALC_CMC.5.9C requires that the CM system supports the audit of all changes to the intended TOE by automated means, including the originator, date, and time in the audit trail. ALC_CMC.5.10C requires that the CM system provides an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.11C requires that the CM system is able to identify the version of the implementation representation from which the intended TOE is generated. ALC_CMC.5.12C requires that the CM documentation includes a CM plan. ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development of the intended TOE. ALC_CMC.5.14C requires that the CM plan describe the procedures used to accept modified or newly created configuration items as part of the intended TOE. ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system. ALC_CMS.5.1C requires that the CL includes the following: the intended TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the intended TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan. ALC_CMS.5.2C requires that the CL uniquely identify the configuration items. ALC_CMS.5.3C requires that for each configuration item, the configuration list indicates the developer/subcontractor of the item.

66 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 intended TOE design and implementation in its development environment.

67 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 intended TOE.

68 ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the intended TOE.

69 ALC_LCD.1.2C requires that the life-cycle model provides for the necessary control over the development and maintenance of the intended TOE.

70 All these content elements of the mentioned SARs require dedicated content of the CM documentation and the configuration list, properties of the SM system, content of the development security documentation and of the life-cycle and tools documentation. Thereby these SARs are suitable to meet the security objective.

7.4.3 O.Physical-Access

71 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 intended TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.4 O.Security-Control

72 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 intended TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.5 O.Alarm-Response

73 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 intended TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.6 O.Internal-Monitor

74 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 intended TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.7 O.Maintain-Security

75 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 intended TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.8 O.Network-separation

76 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 intended TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.9 O.Logical-Operation

77 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 intended TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.10 O.Internal-Shipment

78 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 intended TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.11 O.Control-Scrap

79 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 intended TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.4.12 O.Staff-Engagement

80 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 intended TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

7.5 Mapping of the Evaluation Documentation

81 The scope of the evaluation as per 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 NXP Shanghai Puxi.

SAR	Aspects	Reference
ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure*	The sources are labeled in the version control system, which is owned by CCC&S. The	• NXPOMS-999116894-3989 - BL_CnS_BCaM_Handbook

SAR	Aspects	Reference
an appropriate and consistent labelling.	version control system is used as per O.Config_IT-env. Documents are labeled with a DOC-number, -title, -owner. Configuration Items are identified via the identifiers that are automatically provided by the system as well as the baseline labels that are given by the configuration manager.	• NXPOMS-999116894-3989 BL_CnS_BCaM_Handbook slide on Configuration management • Configuration Management References and Templates
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	All items can be uniquely identified by the version control system, which is owned by CCC&S. Documents can be uniquely identified using the labeling described above. Configuration Items are identified via the identifiers that are automatically provided by the system as well as the baseline labels that are given by the configuration manager.	• NXPOMS-999116894-3989 - BL_CnS_BCaM_Handbook, slide on Configuration management • Configuration Management References and Templates
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.	Review board is in place for every project. Steering is done by CCC&S.	• NXPOMS-999116894-3989 - BL_CnS_BCaM_Handbook, slide on Configuration management, Change Control Board - CCB & Change Control Process Outline • NXPOMS-999116894-3989 - BL_CnS_BCaM_Handbook, slide on NPI3.0 Key Review overview – NPI Lifecycle • Configuration Management References and Templates • NXPOMS-1719007347-2486 - Gate Checklist
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	All items can be uniquely identified by the version control system, which is owned by CCC&S.	• NXPOMS-999116894-3989 - BL_CnS_BCaM_Handbook, slide on Configuration management • Configuration Management References and Templates
ALC_CMC.5.5C: The CM system shall provide	Different CM tools like DesignSync, CollabNet as well	• NXPOMS-999116894-3989 - BL_CnS_BCaM_Handbook,

SAR	Aspects	Reference
automated measures such that only authorized changes are made to the configuration items.	as EnoviaNXP provides automated measures to only allow authorized changes to configuration items. Restricted access allows only authorized persons to do changes and the authorization for the change is approved by the Change Control Board using the change process	slide on Configuration management • Configuration Management References and Templates • CollabNet TeamForge – User Guide
ALC_CMC.5.6C: The CM system shall support the production of the *intended* TOE by automated means.	The above-mentioned tools support the development of the intended TOE by automated means.	• NXPOMS-999116894-3989 - BL_CnS_BCaM_Handbook, slide on Configuration management • Configuration Management References and Templates • NXPOMS-1719007347-2657 BL CS Design Environment MaintenanceCollabNet TeamForge – User Guide
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.	Specific roles in tools are defined in a way that the person responsible for accepting a configuration item into CM is not the person who developed it. The role Documentation Office publishes a document written by an author.	• NXPOMS-999116894-4839 - Project Setup in CollabNet instructions • Configuration Management Procedure • NXPOMS-999116894-14314 - BL CS – Project Role Descriptions
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	Per [7] there is no specific TOE in the focus, therefore this is only applicable to the CM documentation. The documentation can be identified in the tool EnoviaNXP.	• Product/project specific CM plans and the CI list that is used for CC evaluation.
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the *intended* TOE by automated means, including the originator, date, and time in the audit trail.	Different CM tools like DesignSync or CollabNet provide automated means to support the audit of all changes. Documents stored in EnoviaNXP are under version control.	• Enovia Synchronicity • DesignSync – System Administration Help • Technical Design - CollabNet service for CCC&S
ALC_CMC.5.10C: The CM system shall provide an automated means to identify	In case a source file has been changed, the code is compiled	• Tool documentation

SAR	Aspects	Reference
all other configuration items that are affected by the change of a given configuration item.	again and all affected items are identified. Documents are checked for consistency.	• Configuration Management Procedure • Requirements Engineering Procedure
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the *intended* TOE is generated.	Different CM tools like DesignSync or CollabNet provide means to tag a release version from which the intended TOE is generated. The version information of documents is stored in EnoviaNXP.	• Tool documentation • NXPOMS-999116894-3989 - BL_CnS_BCaM_Handbook, slides referring to Baselines • Configuration Management Procedure • Requirements Engineering Procedure
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	The development environment used is set up centrally as per the Release Manual and a project specific CM plan.	• Configuration Management Procedure • Product specific configuration management plan (CMP) available.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the *intended* TOE.	The development environment used is set up centrally as per the Release Manual and a project specific CM plan.	• Configuration Management Procedure • Product specific configuration management plan (CMP) available.
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *intended* TOE.	The development environment used is set up centrally as per the Release Manual and a project specific CM plan. Documents are handled centrally after creation by the Documentation Officer.	• NXPOMS-999116894-3989 - BL_CnS_BCaM_Handbook, slides referring to change control board, CCB process • Configuration Management Procedure • Product specific configuration management plan (CMP) available.
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	The development environment used is set up centrally as per the Release Manual and a project specific CM plan. Documents are stored in project vaults. Evidences can be provided during a site visit	• The development environment used is set up centrally and organized as per a project specific CM plan • NXPOMS-999116894-3989 - BL_CnS_BCaM_Handbook, slides referring to the configuration management • Product specific configuration management plan (CMP) available.
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being	The development environment used is set up centrally as per	• The development environment used is set up centrally and organized as

SAR	Aspects	Reference
operated in accordance with the CM plan.	the Release Manual and a project specific CM plan. Documents are stored in project vaults. Evidences can be provided during a site visit	per a project specific CM plan • Configuration Management Procedure

Table 8 Mapping of the Evidence for the Configuration Management Capabilities

SAR	Aspects	Reference
ALC_CMS.5.1C: The configuration list shall include the following: the *intended* TOE itself; the evaluation evidence required by the SARs; the parts that comprise the *intended* TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.	In terms of site certification on the one hand the configuration list is provided in form of the tables at hand. On the other hand, the configuration list is represented by the list of all applicable documents.	• SST • Document list/Bibliography
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	Since no TOE is subject of the site evaluation the principles are defined. All configuration items are maintained in the CM systems provided by CCC&S. Every document can be uniquely identified as stated above for ALC_CMC.5.1C.	• not applicable
ALC_CMS.5.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	The configuration list in case of site certification is the list of all applicable documents. In the document the author of each item is listed.	• Document list/Bibliography

Table 9 Mapping of the Evidence for the Scope of the Configuration Management

SAR	Aspects	Reference
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security	Access control to floors, surveillance, alarm system and on-site guard services to prevent access to the floors for unauthorized persons.	• NXPOMS-1719007347-4090, Site Security Manual Shanghai Puxi

SAR	Aspects	Reference
measures that are necessary to protect the confidentiality and integrity of the *intended TOE* design and implementation in its development environment.		
	Logical security concept	• NXPOMS-1719007347-4090, Site Security Manual Shanghai Puxi
	Protection of documents and code control	• NXPOMS-1719007347-4090, Site Security Manual Shanghai Puxi
	Backup	• NXPOMS-1719007347-4090, Site Security Manual Shanghai Puxi
	Visitors, external suppliers and cleaning personnel handling	• NXPOMS-1719007347-4090, Site Security Manual Shanghai Puxi
	Handling of physical objects, zero balancing, disposal of security products	• NXPOMS-1719007347-4090, Site Security Manual Shanghai Puxi
	Trustworthiness and training of staff	• NXPOMS-1719007347-4090, Site Security Manual Shanghai Puxi
	Handling of (security) incidents	• NXPOMS-1719007347-4090, Site Security Manual Shanghai Puxi
	Physical security system: operation, emergency procedures, incident handling and reporting	• NXPOMS-1719007347-4090, Site Security Manual Shanghai Puxi
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *intended* TOE.	The justification is provided in this security target because it shows that all threats are addressed by the measures. In addition, the measures are monitored to control the effectiveness.	• Chapter 7 of this document

Table 10 Mapping of the Evidence for the Development Security

SAR	Aspects	Reference
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the *intended* TOE.	The intended TOE is developed and maintained as per NXP development process.	● NXPOMS-999116894-3989 - BL_CnS_BCaM_Handbook ● NXPOMS-1719007347-2486 - Gate Checklist
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the *intended* TOE.	The development control of CCC&S provides the necessary control and compliance of the development environment in use.	● NXPOMS-999116894-3989 - BL_CnS_BCaM_Handbook ● NXPOMS-1719007347-2486 - Gate Checklist ● NPI3.0 Intranet site

Table 11 Mapping of the Evidence for the Developer defined Life-Cycle Model

82 The evidence in the tables above is mapped as per the main purpose and content of the referenced documents. Nevertheless, the procedures support each other. Especially the physical and technical security measures as well as the organizational security measures including maintenance of security measures supplement each other. Also, the control during development assures the configuration management and support the personal accountability and tracing of the sources. The table above shows that all aspects of the assurance components are covered by the implemented procedures.

8. References

Literature

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

[2] P. v. Disseldorp, "Security Objects," NXP Semiconductors, 14. March 2019.

[3] „Security IC Platform Protection Profile with Augmented Packages (BSI-CC-PP-0084-2014), Version 1.0,“ Eurosmart, 2014.

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

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

[6] Common Criteria, „Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5,“ April 2017.

[7] Common Criteria, „Supporting Document, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001,“ October 2007.

[8] jacky, title 1, NXP, 2020.

[9] „Check List for Site Visit NXP development site under site certification,“ 26. February 2020.

8.1 Definitions

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

8.2 List of Abbreviations

CC	Common Criteria
CCC&S	Competence Center Crypto & Security
CI	Configuration Item
CL	Configuration List
CM	Configuration Management
CTO	Chief Technology Organization
EAL	Evaluation Assurance Level
HH	Hamburg
HSM	High secure module
IC	Integrated Circuit
IP	Intellectual Property
IT	Information Technology
NPIT	New Product Introduction Team
OEF	Order Entry Form
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SNV	Static non-volatile
SSM	Site Security Manual
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation

8.3 Revision History

Revision	Description	Author	Date
0.8	Initial Version 0.8 based on NXP-OMS-1719007347-3869 rev.0.8	Tino Kaufmann	2019-03-12
0.9	• Updated Assumptions • Updated template	Tino Kaufmann	2020-10-13
1.0	• Changed 'Shanghai' site to 'Shanghai Puxi' site to make it more specific. • General update and replacement of BU S&C with BL C&S. • Added Security Objective O.Transfer-Data and rationale. • Updated Section 8.1 Literature and referenced documents. • Changed Approver from Tino Kaufmann to Christophe Bouly.	Echo Song	2020-12-10
1.1	• Updated version to answer evaluator comments (Action item lisl_v1.0)	Christophe Bouly	2021-01-14
1.2	• Updated version due to typo during conversion to pdf and corrections	Christophe Bouly	2021-02-11
1.3	• Update version due to the reference documents updates • Changed Approver from Christophe Bouly to Shu Gao.	Shu Gao	2022-03-17
1.4	• Updated version to answer evaluator's comments (updated ToC, corrected typo in Section 7.4.9, corrected reference typo for ALC_DVS.2.2C in Table 10, added reference [16] site visit checklist requirements in Section 7.1, 8.1).	Echo Song	2022-06-16

Approvers

Sequence	Role	Name
Acceptance	Site Security Representative	Echo Song
Approval	Security Manager	Shu Gao