Table of content

Table of Figures

Publication Summary

Reference Number (OMS-ID)	NXPOMS-1719007347-3870
Reference Title	Site Security Target Lite NXP Shanghai
Publisher	NXP BLs
Classification	PUBLIC
Author	Tino Kaufmann
Owner	Echo Song
Archive Numbers (source file)	See reference number

1. Document Introduction

1.1 Reference

Title: Site Security Target Lite NXP Shanghai

Version: 0.8

Date: 3/12/2019

Company: NXP Semiconductors

Name of site: Development Center NXP Shanghai

EAL: SARs taken from EAL6

Based on: Site Security Target NXP Shanghai rev. 0.8

2. SST Introduction

1. This document is based upon the Eurosmart Site Security Target Template [1] with adaptations such that it fits the site (i.e. development site, testing of hardware and software, no production, no direct delivery to customers of the user of the site).

2. This Site Security Target is intended to be used by NXP Semiconductors Business Unit Security & Connectivity (BU S&C).

3. Therefore, the term 'client' in this document refers directly to NXP BU S&C. Note that also the site of this Site Security Target as defined below belongs to NXP BU S&C.

2.1 SST Reference

Title Site Security Target Lite NXP Shanghai

Version 0.8

2.2 Site Reference

The site belongs to NXP and is located at:

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

2.3 Site Description

2.3.1 Physical Scope

4. The following area of the site specified in section 2.2 is in the scope of the SST.

5. The NXP Shanghai site comprises of three floors of one building, named 19-21. The physical scope is only the development area located on floor 19 and the data center on floor 20. This is a closed area and consists of GREEN, YELLOW and RED areas[1].

6. The whole development area is a security area with restricted access where only authorized persons are allowed to enter this area.

7. Within the development area, only members of the development team are entitled to access sensitive information like source code, confidential development documentation

[1] The terms GREEN, YELLOW area and RED area are defined in the NXP internal document „NXPOMS-1719007347-2404 BU S&C Security requirements".

and samples. To enforce such access restriction, a combination of physical, procedural, personnel and logical measurements have been installed.

2.3.2 Logical Scope

8. The following services and/or processes provided by Development Center NXP Shanghai are in the scope of the site

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

9. The activities are: 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) as defined in 'Security IC Platform Protection Profile' (PP-0035) and 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084).

10. 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 NXP BU S&C processes.

11. Further description detailing the above listed services can be found in section 8.2.

3. Conformance Claim

12. This SST is conformant with Common Criteria Version 3.1:

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

    - Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017, [3]

13. For the evaluation, the following methodology will be used:

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

14. This SST is CC Part 3 conformant.

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

16. ALC_CMC.5, ALC_CMS.5, ALC_DVS.2 and ALC_LCD.1

17. The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profile [5], [6] and is therefore suitable for the evaluation of (software for) Security ICs.

18. 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.

4. Security Problem Definition

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

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

4.1 Assets

21. The following section describes the assets handled at the site.

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.

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.

4.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of assets. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered.

T.Rugged-Theft: An 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 or (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 during internal shipment with the intention to misuse samples and/or compromise confidentiality and/or integrity of the product design data or classified product documentation.

4.3 Organizational Security Policies

P.Config-IT-Env: In addition to the used software on development workstations and servers, the site uses configuration management systems for file versioning and problem tracking. For file versioning 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.

4.4 Assumptions

22. The assumptions are outside the sphere of influence of NXP Shanghai 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. The client also provides a secure connection between the IT equipment of the site and a secure remote IT infrastructure of the client.
These services are provided by the client in a secure way in order to properly protect the assets of the site. This includes the enforcement of a trustworthy access policy to the site equipment and data using the secure connection based on a “need-to-know” principle.

A.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.

5. Security Objectives

23. 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 organisational security measures allows a sufficient separation of employees to enforce the “need to know” principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorised people. The access control measures ensure that only registered employees can access restricted areas. Assets are handled in restricted areas only.

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

O.Alarm-Response: The technical and organisational security measures ensure that an alarm is generated before an unauthorised person gets access to any asset. After the alarm is triggered the unauthorised person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack.

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

O.Maintain-Security: Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorised employees have access to sensitive areas as well as computer/network systems to ensure 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 send 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. VPN's are setup between the secure rooms to ensure that data in China Secure is never send 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-Shipment: The site has measures in place to provide assurance of integrity throughout transport of physical security objects.

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.

5.1 Security Objectives Rationale

24. The SST includes a Security Objectives Rationale in section 8.3.

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

6. Extended Assurance Components Definition

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

7. Security Assurance Requirements

27. Clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profile [5], [6].

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

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

29. 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.

7.1 Application Notes and Refinements

30. 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.

7.1.1 CM Capabilities (ALC_CMC.5)

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

32. Note: Due to the Eurosmart PP [5], [6] refinements for ALC_CMS (see below) not being applicable those for ALC_CMC are also not applicable.

7.1.2 CM Scope (ALC_CMS.5)

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

34. Note: Due to these application notes the refinements from the Eurosmart PP [5], [6] (see section 6.2.1.3) are not applicable.

7.1.3 Development Security (ALC_DVS.2)

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

7.1.4 Life-cycle Definition (ALC_LCD.1)

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

37. Refer to 'Application Note 26' in 6.2.1.2 'Refinements regarding Development Security (ALC_DVS)' in the Eurosmart PP [5] and [6] (application note 27).

38. Refer to subsection 'Refinement' in 6.2.1.2 'Refinements regarding Development Security (ALC_DVS)' in the Eurosmart PP [5] and [6].

7.2 Security Requirements Rationale

7.2.1 Security Requirements Rationale - Dependencies

39. The dependencies for the assurance requirements are as follows (see [3], 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

40. 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'.
- ADV_IMP.1 is not fulfilled as there is no specific TOE. This is in-line with and further explained in [7] 5.7

7.2.2 Security Requirements Rationale - Mapping

SAR	Security Objective	Rationale
ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling.*	O.Config-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).

SAR	Security 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-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	The CM-Plan (O.LifeCycle-Doc) identifies the configuration items that comprise the TSF possibly supported by the

SAR	Security Objective	Rationale
		configuration management system (O.Config-IT-Env)
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.	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.5.10C: 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 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.5.11C: 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	O.LifeCycle-Doc	The acceptance procedures for modified or newly created configuration items are

SAR	Security Objective	Rationale
accept modified or newly created configuration items as part of the *intended TOE*.		described in the CM-Plan (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	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 1 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	O.LifeCycle-Doc	The CI-List (O.LifeCycle-Doc) indicates the developer/subcontractor for

SAR	Security Objective	Rationale
shall indicate the developer/subcontractor of the item.		each configuration items as described in the CM-Plan (O.LifeCycle-Doc).

Table 2 Rationale for ALC_CMS.5

SAR	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the *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.Control-Shipment O.Control-Scrap O.Staff-Engagement	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.Control-Shipment, O.Control-Scrap), personnel (O.Staff-Engagement), and other(O.Network-separation, 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 3 Rationale for ALC_DVS.2

SAR	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model	O.LifeCycle-Doc	The model used to develop the intended TOE is described in the life cycle

SAR	Security Objective	Rationale
used to develop and maintain the *intended TOE*.		documentation (O.LifeCycle-Doc)
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the *intended TOE*.	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 maintenance of the intended TOE.

Table 4 Rationale for ALC_LCD.1

8. Site Summary Specification

8.1 Preconditions required by the Site

41. The site performs some development and test services for the construction of secure IC hardware and software.

42. In order to perform these services in a secure way, the client of the site (BU S&C) needs 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.

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 need to specify whether the scrap need to be destroyed by the site or need 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 be shipped in one to the client for secure scrapping and disposal.	A.Project-Setup

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). All provided services of the client need to respect the necessary measures to protect the assets of the site (see section 4.1)	A.DevEnv-Provisioning

8.2 Services of the Site

43. The following services and/or processes provided by Development Center NXP Shanghai are in the scope of the site evaluation process:

44. IC Embedded Software Development, Verification and Validation (Phase 1) and/or IC Development, IC Dedicated Software Development, Verification and Validation (Phase 2) as defined in 'Security IC Platform Protection Profile' (PP-0035) and 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084). 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. The services as listed in section 2.3.1 and 2.3.2 are 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 BU S&C Product Creation described in 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.

8.3 Objectives Rationale

45. Table 7 provides an overview for the correspondence between Security objectives as listed in chapter 5 to the threats and policies identified in chapter 4.2 and 4.3, and demonstrating that all threats and OSPs are mapped to at least one security objective. The following chapters provide a more detailed explanation of this mapping.

Security Objectives / Threats / OSPs	O.Config-IT-Env	O.LifeCycle-Doc	O.Physical-Access	O.Security-Control	O.Alarm-Response	O.Internal-Monitor	O.Maintain-Security	O.Network-separation	O.Logical-Operation	O.Control-Shipment	O.Control-Scrap	O.Staff-Engagement
T.Smart-Theft			X	X	X	X	X					
T.Rugged-Theft			X	X	X	X	X					
T.Computer-Net						X	X	X				
T.Unauthorised-Staff			X	X	X	X	X		X		X	X
T.Staff-Collusion						X	X				X	X
T.Attack-Transport		X								X		
P.Config-IT-Env	X											
P.LifeCycle-Doc		X										

Table 5 Mapping between security objectives, and threats / OSPs

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

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

O.LifeCycle-Doc: Dedicated documents exist 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.

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.

O.Security-Control: The site is using dedicated personnel for guard services. This personnel is 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.

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 has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff.

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.

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.

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.

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

O.Control-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.

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.

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.

8.4 Assurance Measure Rationale

47. The following section provides a rationale for each security objective for the development environment (as defined in chapter 5), why each of the assigned SARs (as given in section 7.2.2) is suitable to meet the security objective.

48. The justification is given at the level of SAR content elements (see Table 1 to Table 5).

8.4.1 O.Config-IT-Env

49. ALC_CMC.5.1C requires that the CM documentation show that a process is in place to ensure an appropriate and consistent labeling. 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 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 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.

50. 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.

8.4.2 O.LifeCycle-Doc

ALC_CMC.5.1C requires that the CM documentation show that a process is in place to ensure an appropriate and consistent labeling. 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 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 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 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 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 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 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.

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.

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.

51. 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 documentation. Thereby these SARs are suitable to meet the security objective.

8.4.3 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. Thereby this SAR is suitable to meet the security objective.

8.4.4 O.Security-Control

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. Thereby this SAR is suitable to meet the security objective.

8.4.5 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. Thereby this SAR is suitable to meet the security objective.

8.4.6 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. Thereby this SAR is suitable to meet the security objective..

8.4.7 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. Thereby this SAR is suitable to meet the security objective.

8.4.8 O.Network-separation

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. Thereby this SAR is suitable to meet the security objective.

8.4.9 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. Thereby this SAR is suitable to meet the security objective.

8.4.10 O.Control-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. Thereby this SAR is suitable to meet the security objective.

8.4.11 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. Thereby this SAR is suitable to meet the security objective.

8.4.12 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. Thereby this SAR is suitable to meet the security objective.

8.5 Mapping of the Evaluation Documentation

52. The mapping between the internal site documentation and the Security Assurance Requirements is only available within the full version of the Site Security Target.

8.6 Literature

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

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

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

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

[5] „Security IC Platform Protection Profile (BSI-PP-0035), Version 1.0,“ Eurosmart, 15.06.2007.

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

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

8.7 Definitions

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

8.8 List of Abbreviations

CC	Common Criteria
CS	China Secure – Development equipment and logical environment in NXP Shanghai
CI	Configuration Item
CL	Configuration List
CM	Configuration Management
EAL	Evaluation Assurance Level
IC	Integrated Circuit
IP	Intellectual Property
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation

8.9 Revision History

Revision	Description	Author	Approval - Date
0.8	Initial Version 0.8 based on NXP-OMS-1719007347-3869 rev.0.8	Tino Kaufmann	2019-03-12