Site Security Target – NXP San Jose

Revision	v6.1

Table of Contents

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: NXP San Jose

5 EAL: SARs taken from EAL6

6 SST title: Site Security Target NXP San Jose

7 Ref, version, date: NXPOMS-1719007347-4559, v6.1, 03/25/2021

1.2 Site Reference

8 The site is located at:

NXP Semiconductors
411 East Plumeria Drive
San Jose, CA 95134
United States

1.3 Site Description

1.3.1 Physical Scope

9 The site is a single building location with two (2) floors occupied by NXP Semiconductors. The entire site is in-scope for this SST.

10 All areas in scope are classified as YELLOW[1] and RED[1] areas.

11 A more detailed view of the layout is described in the Site Security Manual (SSM) for San Jose.

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

13 Within those areas, only members of the IT department, development group and test team are entitled to access sensitive information like secure shipments, 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

14 The following life-cycle phases as defined in 'Security IC Platform Protection Profile' (PP-0035) [3] and 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084) [4] are subject of the SST:

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

15 To perform its development activities the site uses the NXP CCC&S provided and managed remote IT-infrastructure. Locally available IT equipment like workstations or VPN router is also provided and managed by NXP CCC&S directly. The site works as per NXP CCC&S processes.

16 The following services and/or processes provided by NXP San Jose 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] The terms YELLOW area and RED area are defined in the NXP internal document „NXPOMS-1719007347-2404 S&C Security Requirements"

2. Conformance Claim

17 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, [5]
- Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017, [6]

18 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, [7]

19 This SST is CC Part 3 conformant.

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

21 ALC_CMC.5, ALC_CMS.5, ALC_DVS.2 (The requirements are specifically aimed at an evaluation of EAL6 where the attacker has a high attack potential (AVA_VAN.5)), and ALC_LCD.1.

22 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.

23 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 potentially augmented 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.

3. Security Problem Definition

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

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

3.1 Assets

26 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:

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 computers: 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.

3.2 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 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.Config-Activities: The activities of the site shall be performed in accordance with the life cycle documentation (P.Config_IT-env) and helps to meet the objective of (O.Network-separation) using the IT-environment (O.Config-Activities).

P.Zero-Balance: The site ensures that all sensitive items (security relevant parts of the TOEs of different clients) are separated and traced on a device basis. For each handover, either an automated or an organizational “two-employees-acknowledgement” (four-eyes principle) is applied for functional and defect assets. As per the released production process the defect assets are either

destroyed at the site or sent back to NXP or customer and/or consumer (depending on the production-setup). The sent back procedures, whether to NXP or to the customer, are controlled through internal compliance policies and procedures.

P.Scrap-Items: Physical items that do not comply with the quality requirements are scrapped at the site in a way that the destructed items do not support any attacker.

3.4 Assumptions

27 The assumptions are outside the sphere of influence of NXP San Jose 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.Inherit-secure-IT: The local IT equipment (e.g. workstations) is connected to a secure remote IT-Infrastructure through a secure (encrypted) network connection. The local workstations, the remote secure IT-infrastructure and the secure connection to it satisfy all relevant ALC requirements and are provided and managed by the client. The workstations are configured such that any assets are contained within encrypted containers.

A.Shared-Docs: In case of necessary updates to the life cycle documentation[3] the site and the client cooperate.

A.Setup-Projects: To enable that the site participates in the development of products the client provides services to setup the necessary development computers (tools, user accounts, etc.) and configuration management systems (user accounts, repositories etc.).

A.Shipment: To enable the site to realize shipment such that assurance of integrity is assured throughout transport of physical security objects the client will adhere to the shipment method as described in the life cycle documentation.

A.Product-Setup: The site participates in the development of products. To define the participation of the site in the development while maintaining quality, for each product the site and the client agree on the activities to be

[3] Part of the life cycle documentation is written in corporation with the client where other parts are provided by the client.

performed by the site, the specifications of the input for the site and the acceptance of the results by the client.

4. Security Objectives

28 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 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 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: The development network of the site exists within the secured areas of the site only. It is connected only to: (1) the VPN gateway that provides a secure connection to the remote secure network of the client; (2) the development workstations provided by the client; (3) Additional equipment (e.g. a printer) approved by the client.

O.Logical-Operation: Development workstations enforce that every user authenticates using a password and has a unique user ID.

O.Config-Activities: The activities of the site are performed in accordance with the life cycle documentation (O.Config_IT-env) using the IT-environment (O.LifeCycle-Doc).

O.Control-Scrap: The site has measures in place to either securely destruct assets (e.g. paper shredder) or send them to a certified scrap location.

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.Zero-Balance: The site ensures that all physical asset are separated and traced. Automated control and/or two employee's acknowledgements during hand over is applied for functional and defective material.

O.Control-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.

4.1 Security Objectives Rationale

29 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 2).

30 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.LifeCycle-Doc 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.Control-Scrap O.LifeCylce-Doc 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.Config_IT-env O.Network-separation O.LifeCycle-Doc O.Logical-Operation O.Physical-Access O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Config-Activities	The development network is not connected to anything that an attacker could use to set up a remote connection.

T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Config_IT-env O.Logical-Operation O.Control-Scrap O.Zero-Balance O.Config-Activities O.Network-separation O.Lifecycle-Doc O.Staff-Engagement	Physical and logical access control prohibits access to assets. Secure destruction of scrap limits the amount of assets
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Config_IT-env O.Control-Scrap O.Zero-Balance O.Config-Activities O.Lifecycle-Doc O.Physical-Access	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.Control-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.Config-Activities	O.Config-Activities O.Network-separation O.Security-Control O.Physical-Access	The Security Objective directly enforces the OSP.
P.Zero-Balance	O.Staff-Engagement	The Security Objective directly enforces the OSP.

	O.Zero-Balance O.Control-Scrap	
P.Scrap-Items	O.Control-Scrap	The Security Objective directly enforces the OSP.

Table 2 OSP - Security Objectives Rationale

5. Extended Assurance Components Definition

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

6. Security Assurance Requirements

32 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].

33 The Security Assurance Requirements are chosen from the class ALC (Life-cycle support) as defined in [6]:

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

34 The Security Assurance Requirements listed above fulfill the requirements of [8] 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 [8]) are used in this Site Security Target.

6.1 Application Notes and Refinements

35 The description of the site certification process [8] 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. Refinements introduced into the SAR are in *italic*

6.1.1 CM Capabilities (ALC_CMC.5)

36 Refer to subsection ‘Application Notes for Site Certification’ in [8] 5.1 ‘Application Notes for ALC_CMC’.

37 Note: Due to the Eurosmart PP [9] 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)

38 Refer to subsection ‘Application Notes for Site Certification’ in [8] 5.2 ‘Application Notes for ALC_CMS’.

6.1.3 Development Security (ALC_DVS.2)

39 Refer to subsection 'Application Notes for Site Certification' in [8] 5.4 'Application Notes for ALC_DVS'.

6.1.4 Life-cycle Definition (ALC_LCD.1)

40 Refer to subsection 'Application Notes for Site Certification' in [8] 5.6 'Application Notes for ALC_LCD'.

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

42 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

43 The dependencies for the assurance requirements are as follows:

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

44 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 [8] 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 labeling.	O.Config_IT-env O.LifeCycle-Doc O.Config-Activities	Appropriate and consistent labeling is ensured through the application (O.Config-Activities) of the CM-Plan (**O.LifeCycle-Doc**) and the use of the configuration management systems (**O.Config_IT-env**).

SAR	Security Objective	Rationale
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 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 O.Config-Activities	Unique identification of all CIs is realized by performing the CM activities (O.Config-Activities) in accordance with the CM-Plan (O.LifeCycle-Doc) using the Configuration management systems (C.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 O.Config-Activities	The configuration management systems (O.Config_IT-Env) used (O.Config-Activities) according to the CM-Plan (C.LifeCycleDoc) 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 O.Config-Activities O.Zero-Balance	The software on the development computers (O.Config_IT-env) supports automated production of products when used (O.Config-Activities) in accordance with the CM-Plan (O.LifeCycle-Doc). Zero-Balancing is performed at each step (O.Zero-Balance)

SAR	Security Objective	Rationale
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	O.LifeCycle-Doc O.Config-Activities	As described in the CM-Plan (O.LifeCycle-Doc) the activities performed (O.Config-Activities) 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 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	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

SAR	Security Objective	Rationale
which the *intended* TOE is generated.		*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).
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	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

SAR	Security Objective	Rationale
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: 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.Control-Shipment O.Control-Scrap O.Staff-Engagement O.Zero-Balance	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, O.Zero-Balance), 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

SAR	Security Objective	Rationale
		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 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 6 Rationale for ALC_LCD.1

7. Site Summary Specification

7.1 Preconditions required by the Site

45 The site activities are performed using an IT infrastructure consisting of development workstations, servers and configuration management systems. All of these are provided, configured and maintained by the client. **(A.Inherit-secure-IT)**

46 The IT infrastructure consists of local and remote equipment connected using an encrypted connection. NXP Hamburg (Master IT Site) provides, configures and maintains the local workstations and router (used for the encrypted connection) and all remote equipment such that they are secure. The workstations are configured such that any assets are contained within encrypted containers. **(A.Inherit-secure-IT)**

47 In case of necessary updates to the life cycle documentation[4] NXP will coordinate, communicate and deliver.**(A.Product-Setup)**

48 To enable that the site participates in the development of products the client provides services to setup the necessary development computers (tools, user accounts, etc.) and configuration management systems (user accounts, repositories etc.). (**A.Setup-Projects**)

49 To enable the site to realize internal shipment such that assurance of integrity is assured throughout transport of physical security objects the client will adhere to the shipment method. (**A.Setup-Projects**)

50 In case the site is unable to securely destruct certain physical assets the assets will be securely stored and shipped to an NXP certified site for destruction. (**A.Shipment**)

51 To define the participation of the site in the development while maintaining quality, for each product the site and the client agree on the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results by the client. (**A.Product-Setup**)

52 The site follows the development processes of the client. Applicable policies and processes are documented and available from the client to the site.

[4] Part of the life cycle documentation is written in corporation with the client where other parts are provided by the client.

7.2 Services of the Site

53 The site participates in the development and testing of software[5] for secure integrated circuits.

54 The site participates in the hardware development and testing of secure integrated circuits.

55 The site uses a shipment method such that assurance of integrity is assured throughout transport of physical security objects.

56 Supporting services:

The site is involved in the NXP datacenters[6] security supervision.

7.3 Objectives Rationale

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

58 **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. These measures address **T.Computer-Net**, **T.Staff-Collusion** and **T.Unauthorised-Staff** and also addresses the OSP **P.Config_IT-env**

59 **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 threats **T.Smart-Theft**, **T.Rugged-Theft**, **T.Attack-Transport**, **T.Computer-Net**, **T.Unauthorised-Staff** and **T.Staff-Collusion**.

60 **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**, **T.Computer-Net**,

[5] ‘Software’ means in this case: IC Embedded Software Development (Phase 1) and/or IC Dedicated Software Development (Phase 2) as defined in ‘Security IC Platform Protection Profile’ (PP-0035) [7] and ‘Security IC Platform Protection Profile with Augmentation Packages’ (PP-0084) [12].

[6] NXP datacenters : Colt Hamburg, Akquinet Hamburg, Digital Realty Data Center, Equinix SG1 Data Center.

T.Staff-Collusion and **T.Unauthorised-Staff** can be prevented. This also addresses the OSP **P.Config-Activities**

61 **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**. This also addresses the OSP **P.Config-Activities**.

62 **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**.

63 **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**.

64 **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**.

65 **O.Network-separation**: The internal network is separated from the internet with a firewall. The internal network is further separated into subnetworks by internal firewalls. These firewalls allow only authorized information exchange between the internal subnetworks. Each user is logging into the system with his personalised user name and password. The objective is supported by **O.Internal-Monitor** based on the checks of the logging regarding security relevant events.

66 The individual accounts are addressing **T.Computer-Net**. All network configuration is stored in the database of the NXP secure network. Supported by **O.Config_IT-env** this addresses the threats **T.Unauthorised-Staff** and the OSP **P.Config-Activities**.

67 **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** and **T.Computer-Net** are prevented.

68 **O.Config-Activities**: All product configuration information is stored in the database on the NXP secure network. The information stored is covering process specifications, acceptance test instructions and specifications, and test programs. Products are identified by unique customer part IDs with are linked to the unique ID numbers of the associated configuration items.

69 This is addressing the threat **T.Computer-Net**, **T.Staff-Collusion**, **T.Unauthorised-Staff** and the OSP **P.Config-Activities**

70 **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.

71 **O.Control-Scrap**: The security of scrap handling is ensured by either securely destruct assets (e.g. paper shredder), use of certified scrapping or return them to the client. This helps to prevent the threats **T.Rugged-Theft, T.Unauthorised-Staff** and **T.Staff-Collusion** and addresses the OSP **P.Zero-Balance**, **P.Scrap-Items**.

72 **O.Staff-Engagement**: All employees are interviewed before hiring. They must sign an NDA and a code of conduct for the use of NXP equipment before they start working in the company. The formal training and qualification include security relevant subjects and the principles of handling and storage of security products. The security objectives **O.Physical-Access** and **O.Config-Items** support the engagement of the staff.

73 This addresses the threats **T.Computer-Net**, **T.Staff-Collusion** and **T.Unauthorised-Staff** and addresses the OSP **P.Zero-Balance**

74 **O.Zero-Balance**: The site ensures that all physical assets are separated and traced. Handover and storage of security assets is controlled by the 4-eyes principle and documented. Scrap and rejects are following the same process. At every process step the registration of good and scrapped/rejected products is updated.

75 This security objective is supported by O.Physical-Access and O.Staff-Engagement. This addresses the threats T.Unauthorised-Staff and T.Staff-Collusion and the OSP P.Zero-Balance.

7.4 Assurance Measure Rationale

76 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.

77 The justification is given at the level of SAR content elements (see Table 3 to Table 7).

7.4.1 O.Config_IT-env

78 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.

79 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

80 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.

81 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.

82 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.

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

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

85 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.Config-Activities

86 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.5.7C

requires that the CM system ensures that the person responsible for accepting a configuration item into CM is not the person who developed it.

7.4.4 O.Physical-Access

87 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.Security-Control

88 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.Alarm-Response

89 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.Internal-Monitor

90 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.Maintain-Security

91 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.Network-separation

92 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.Logical-Operation

93 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-Shipment

94 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.Control-Scrap

95 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.

7.4.13 O.Staff-Engagement

96 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.

7.4.14 O.Zero-Balance

97 ALC_CMC.5.6C requires that the CM system supports the production of the product by automated means. 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

98 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 San Jose.

SAR	Aspects	Reference
ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*	The sources are labeled in the version control system, which is owned by CCC&S. The 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 - NPI3.0 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 - NPI3.0 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 - NPI3.0 Handbook, slide on Configuration management, Change Control Board - CCB & Change Control Process Outline • NXPOMS-999116894-3989 - NPI3.0 Handbook, slide on NPI3.0 Key Review overview – NPI Lifecycle • Configuration Management References and Templates • NXPOMS-1719007347-2486 - Gate Checklist

SAR	Aspects	Reference
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 - NPI3.0 Handbook, slide on Configuration management • Configuration Management References and Templates
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	Different CM tools like DesignSync, CollabNet as well 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	• NXPOMS-999116894-3989 - NPI3.0 Handbook, 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 - NPI3.0 Handbook, slide on Configuration management • Configuration Management References and Templates • NXPOMS-1719007347-2657 CM – Design Environment Maintenance • CollabNet 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-1719007347-1870 - NPI 3.0 Roles and Responsibilities
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	Per [7][7] there is no specific TOE in the focus, therefore this is only applicable to the CM documentation. The documentation can be	• Product/project specific CM plans and the CI list that is used for CC evaluation.

SAR	Aspects	Reference
	identified in the tool EnoviaNXP.	
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 all other configuration items that are affected by the change of a given configuration item.	In case a source file has been changed, the code is compiled again and all affected items are identified. Documents are checked for consistency.	• Tool documentation • 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 - NPI3.0 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 - NPI3.0 Handbook, slides referring to change control board, CCB process • Configuration Management Procedure

SAR	Aspects	Reference
		• 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 - NPI3.0 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 operated in accordance with the CM plan.	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 • Configuration Management Procedure

Table 7 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	Since no TOE is subject of the site evaluation the principles are defined. All configuration	• not applicable

SAR	Aspects	Reference
identify the configuration items.	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.	
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 8 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 measures that are necessary to protect the confidentiality and integrity of the *intended* TOE design and implementation in its development environment.	Access control to wing, surveillance, alarm system and on campus guard services to prevent access to the wing for unauthorized persons.	• NXPOMS-1719007347-2649 - Site Security Manual - NXP San Jose
	Visitors, external suppliers and cleaning personnel handling	• NXPOMS-1719007347-2649 - Site Security Manual - NXP San Jose
	Handling of physical objects, zero balancing, disposal of security products	• NXPOMS-1719007347-2649 - Site Security Manual - NXP San Jose
	Trustworthiness and training of staff	• NXPOMS-1719007347-2649 - Site Security Manual - NXP San Jose
	Physical security system: operation, emergency procedures, incident handling and reporting	• NXPOMS-1719007347-2649 - Site Security Manual - NXP San Jose
ALC_DVS.2.2C: The development security	The justification is provided in this security target because it	• Chapter 7 of this document

SAR	Aspects	Reference
documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *intended* TOE.	shows that all threats are addressed by the measures. In addition, the measures are monitored to control the effectiveness.	

Table 9 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 - NPI3.0 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 - NPI3.0 Handbook • NXPOMS-1719007347-2486 - Gate Checklist • NPI3.0 Intranet site

Table 10 Mapping of the Evidence for the Developer defined Life-Cycle Model

99 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.

7.6 Aspects of the SARs

7.6.1 CM capabilities (ALC_CMC.5)

100 Configuration Management is described in [10] and [11].

ALC_CMC.5.1C The TOE shall be labelled with its unique reference.

ALC_CMC.5.2C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.5.3C	The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.
ALC_CMC.5.4C	The CM system shall uniquely identify all configuration items.
ALC_CMC.5.5C	The CM system shall provide automated measures such that only authorized changes are made to the configuration items.
ALC_CMC.5.6C	The CM system shall support the production of the TOE by automated means.
ALC_CMC.5.7C	The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.
ALC_CMC.5.8C	The CM system shall identify the configuration items that comprise the TSF.
ALC_CMC.5.9C	The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.
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.
ALC_CMC.5.11C	The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.
ALC_CMC.5.12C	The CM documentation shall include a CM plan.
ALC_CMC.5.13C	The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.5.14C	The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ALC_CMC.5.15C	The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.5.16C	The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

7.6.2 CM scope (ALC_CMS.5)

101 Configuration Management is described in [10] and [11].

ALC_CMS.5.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.

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

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

7.6.3 Development Security (ALC_DVS.2)

102 Development Security is described in [12]

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

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

7.6.4 Life-cycle definition (ALC_LCD.1)

103 Life-cycle definition is described in [10] and [11].

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

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

8. References

8.1 Literature

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

[2] P. v. Disseldorp, "Security Objects," NXP Semiconductors, NXPOMS-1719007347-2401, 14. March 2019.

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

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

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

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

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

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

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

[10] G. Caffrey, „BU S&C ALC-CM Common Criteria Documentation," NXP Semiconductors, NXPOMS-1719007347-2549.

[11] D. Do, „BU S&C ALC-CM San Jose - Common Criteria Documentation," NXP Semiconductors, NXPOMS-999116894-13440.

[12] D. Do, „Site Security Manual – San Jose," NXP Semiconductors, NXPOMS-1719007347-2649.

8.2 Definitions

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

8.3 List of Abbreviations

CC	Common Criteria
CCC&S	Competence Center Crypto & Security
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
SSM	Site Security Manual
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation

8.4 Revision History

Revision	Description	Author	Approval Date
6.1	Typo corrections	Christophe Bouly	2021-03-25
6.0	Corrections related to CCN comments	Christophe Bouly	2021-03-22
5.9	Change Author and add supporting service “data center supervision”	Christophe Bouly	2021-01-20
5.8	After internal discussion and alignment with evaluator Applus, remove ALC_TAT.3 from the scope of certification	Tino Kaufmann	2020-10-07
5.7	Updated logical scope, security objectives rationale, statement of security requirements, site summary specification and fixed minor typos	Tino Kaufmann	2020-06-04
5.6	- Changed BU name to Competence Center Crypto & Security (CCC&S) - Adapted to new template - Updated references	Dean Do	2020-04-22
5.5	SST Light -> SST. Original SST discontinued	Tino Kaufmann	2019-08-30
5.4	Changed approver to Tino Kaufmann. Merged SST Light and SST into a single SST Light	Tino Kaufmann	2019-08-21
5.3	− Final Release	Gordon Caffrey	2016-06-15
5.2	− Update to meet changes from other SST observations from Serma	Gordon Caffrey	2016-06-14
5.1	− Update to meet changes from other SST observations from Serma − DVS 2.3 added − Reference columns in tables 7.2.2 − Rationale added in 5.1 − Mapping adjusted between 5.1 and 8.4	Gordon Caffrey	2016-05-04
5.0 (not released)	Changed document owner to Dean Do. Changed BU Identity (BU ID) to BU Security & Connectivity (BU S&C). Updated Security Manger to Gordon Caffrey. Changed classification to “Company Confidential.” Updated section 2.3 Site Description with office locations where secure products are being developed and tested. Updated Bibliography [7][8][9].	Dean Do	
4.0	Removed Confidentiality statements, corrected references, unified formatting as requested by Certifier	Anno Hermanns	2014-08-12
3.0	Additional changes requested by Brightsight	Anno Hermanns	2014-07-01
2.0	Final version after additions changes from DL	Dirk Lützelberger	2014-04-08
1.0	Final version after additions by DL and AH	Anno Hermanns	2014-04-05
0.8	Due to internal Brightsight comments	Brightsight	2014-03-17
0.7	Update according to Brightsights requests	Anno Hermmans, Dirk Lützelberger	2014-02-27
0.6	Due to evaluator comments	Brightsight	
0.5	Adjusted Security Objectives based on auditor feedback	Riscure NA	2013-11-28

0.4	Removed references to hardware testing (audit concluded it is not presently in scope), replaced outdated, overly narrow reference to “secure microcontrollers” to “secure ICs”	Anno Hermanns	
0.3	Additional revisions following DLr comments & update security person	Joe Salvador	2013-08-14
0.2	Revision following DLr comments	Riscure NA	
0.1	Initial Draft	Riscure NA	

Approvers

Sequence	Role	Name
Acceptance	Security Manager	Christophe Bouly
Approval	Site Security San Jose	Dean Do