

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 1 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

NXPOMS-1719007347-4204

Site Security Target - NXP Semiconductors San Diego

Publication Summary

Reference Number (OMS-ID)	NXPOMS-1719007347-4204
Reference Title	Site Security Target - NXP Semiconductors San Diego
Publisher	CC Crypto & Security
Classification	PUBLIC
Author	Michael Sandu
Owner	Michael Sandu
Archive Numbers	See reference number

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 0 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

Revision History

Revision	Description	Author	Approval - Date
1.0	First Draft	Gordon Caffrey	03-27-2017
1.1	Serma Comments	Gordon Caffrey	04-20-2017
1.2	Rationale update	Gordon Caffrey	07-19-2017
2.0	Document reference changed from NXPOMS-1719007347-2778 (SST Full) and NXPOMS-1719007347-2778a (SST Lite) to NXPOMS-1719007347-4204 as this SST becomes a PUBLIC document with one version. Changed Publisher from BU ID to CC Crypto & Security SST reclassified from Company CONFIDENTIAL to PUBLIC Change of Author from NXP Security Gordon Caffrey to Michael Sandu Update of acceptance and approval flow Chapter 3 Conformance Claim; Update of Documentation to new releases. Chapter 5 Security Objectives, added O.Zero-Balance Chapter 9 Update of References Integrated 5.1.1 Mapping of Security Objectives, and improved text of rationales Separated Reference from 7.2.2 Security Requirements Rational and added 8.5 Mapping of the Evaluation Documentation Chapter 8.1 Preconditions required by the Site, added Assumptions mapping Chapter 9.1 Literature updated Chapter 9.2 Added Definition Client Chapter 9.3 Updated the List of Abbreviations	Michael Sandu	10-17-2019
2.1	Update of Evaluation Lab comments Update of Table 2 OSP – Security Objectives Rational (Update of Typos) Update of Table 1 Threats – Security Objectives Rational Added O.Physical-Access and O.LifeCycle-Doc to T.Computer-Net and T.Rugged-Theft Added OSP P.Zero-Balance and P.Scrap-Items and added the correct rationales. Added in 8.4 Objectives Rational the security objective O.Zero-Balance Added information that SARs operations are italic in 7.2 Security Requirements Rationales and updated the information	Michael Sandu	12-01-2019

Approvers

Sequence	Role	Name
Acceptance	Security Manager	Mark Buer
Approval	Head of Site Certification	Gordon Caffrey

Subscriber

Owner: Michael Sandu
Author: Michael Sandu

PUBLIC
© NXP Semiconductors N.V.
Uncontrolled copy if printed



NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 1 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

Role	Name	Notification	PDF-file
n.a.	N/A		

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 2 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 3 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

Table of Contents

1. Document Introduction	6
1.1 Reference	6
2. SST Introduction	7
2.1 SST Reference.....	7
2.2 Site Reference	7
2.3 Site Description	7
3. Conformance Claim.....	9
4. Security Problem Definition	10
4.1 Assets	10
4.2 Threats	10
4.3 Organizational Security Policies	11
4.4 Assumptions.....	12
5. Security Objectives	13
5.1 Security Objectives Rationale.....	15
5.1.1 Mapping of Security Objectives	15
6. Extended Assurance Components Definition.....	18
7. Security Assurance Requirements.....	19
7.1 Application Notes and Refinements	19
7.1.1 CM Capabilities (ALC_CMC.5).....	19
7.1.2 CM Scope (ALC_CMS.5).....	19
7.1.3 Development Security (ALC_DVS.2).....	19
7.1.4 Life-cycle Definition (ALC_LCD.1).....	19
7.2 Security Requirements Rationale.....	20
7.2.1 Security Requirements Rationale - Dependencies.....	20
7.2.2 Security Requirements Rationale – Mapping.....	21
8. Site Summary Specification	26
8.1 Preconditions required by the Site	26
8.2 Services of the Site	27
8.3 Security Assurance Rationale.....	27

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 4 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

8.3.1	CM capabilities (ALC_CMC.5)	27
8.3.2	CM scope (ALC_CMS.5)	27
8.3.3	Development Security (ALC_DVS.2)	27
8.3.4	Life-cycle definition (ALC_LCD.1)	27
8.4	Objectives Rationale	28
8.4.1	O.Config_IT-env	28
8.4.2	O.Physical-Access	28
8.4.3	O.Security-Control	28
8.4.4	O.Alarm-Response	28
8.4.5	O.Internal-Monitor	29
8.4.6	O.Logical-Operation	29
8.4.7	O.Staff-Engagement	29
8.4.8	O.Control-Scrap	30
8.4.9	O.Config_Activities	30
8.4.10	O.Network_Separation	30
8.4.11	O.Maintain_Security	30
8.4.12	O.LifeCycle_doc	31
8.4.13	O.Zero-Balance	31
8.5	Mapping of the Evaluation Documentation	31
9.	References	38
9.1	Literature	38
9.2	Definitions	38
9.3	List of Abbreviations	39

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 5 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

Table of Figures

Table 1 Threats - Security Objectives Rationale	16
Table 2 OSP - Security Objectives Rationale	17
Table 3 Rationale for ALC_CMC.5.....	23
Table 4 Rationale for ALC_CMS.5.....	24
Table 5 Rationale for ALC_DVS.2.....	25
Table 6 Rationale for ALC_LCD.1	25
Table 7 Mapping of the Evidence for the Configuration Management Capabilities.....	35
Table 8 Mapping of the Evidence for the Scope of the Configuration Management	35
Table 9 Mapping of the Evidence for the Development Security	36
Table 10 Mapping of the Evidence for the Developer defined Life-Cycle Model	37

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 6 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

1. Document Introduction

1.1 Reference

Title: Site Security Target - NXP Semiconductors San Diego

Version: 2.1

Date: 12/1/2019

Company: NXP Semiconductors

Name of site: NXP Semiconductors San Diego

EAL: SARs taken from EAL6

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 7 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

2. SST Introduction

- 1 This document is 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.

2.1 SST Reference

- 3 Title Site Security Target - NXP Semiconductors San Diego
- 4 Version 2.1

2.2 Site Reference

- 5 The site belongs to NXP Semiconductors and is located at:
- 6 NXP Semiconductors San Diego
15255 Innovation Drive
San Diego, California 92128
United States

2.3 Site Description

- 7 The San Diego facility is a two-story, multi-tenant facility in a mixed-use commercial and residential area. NXP's space will be on the first floor completely segregated from all other tenants. The NXP area will be segregated into RED¹, YELLOW¹, and GREEN¹ zones in accordance to NXP security policy.
- 8 This development area is a combination of YELLOW¹ and RED¹ physical zones. RS and HS networks will be deployed as per the certified NXP secure network infrastructure. These areas are exclusively occupied by NXP with restricted need to know access controlled by NXP for authorize personnel only.
- 9 The non-NXP controlled areas of this building are out with the scope of this site security target (SST).
- 10 This site is a dedicated R&D facility. The various engineering teams (Software, Hardware, Developmental Testing, and Quality Control) work in a cross-functional manner to develop parts for integration into NXP products.

¹ The terms GREEN, YELLOW and RED areas are defined in the NXP internal document „NXPOMS-1719007374-2404 BU S&C Security Requirements Overview “

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 8 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

- 11 Within the development area, only members of the development team are entitled to access sensitive information i.e. source code, confidential documentation, samples, etc.
- 12 The activities are: Security IC Embedded Software Development (Phase 1), IC Embedded Software and Testing (Phase 1), IC Design (Phase 2), IC Dedicated Software and Testing (Phase 1) as defined in 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084)
- 13 To perform these activities the site uses the NXP Semiconductors provided and managed remote IT-infrastructure. Locally available IT equipment like workstations or VPN routers are also provided and managed by NXP Semiconductors directly. The site works according to NXP Semiconductors processes.
- 14 The activities (and areas where they are performed) are:

Activity	Area
Development and testing* of software for secure integrated circuits.	NXP Secure Area
Also, development and testing of IC Hardware Design secure integrated circuits	NXP Secure Area
Engineering Test of Software development	NXP Secure Area

- 15 The typical Life Cycle model for Smart Cards usually comprises the following phases:
 - Development,
 - Production,
 - Delivery,
 - Preparation,
 - Operation,
- 16 Whereas the site under evaluation supports only the life cycle phase
 - Development
- 17 Development comprises of the generation of source code modules and the test of this code only.
- 18 Internal shipment of engineering samples to and from NXP Semiconductors Sites are performed at NXP San Diego.

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 9 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

3. Conformance Claim

19 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 Components; Version 3.1, Revision 5, April 2017, [3]

20 For the evaluation, the following methodology will be used:

- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017, [4]
- JIL - Minimum Site Security Requirement Version 2.2 April 2019 [8]

21 This SST is CC Part 3 conformant.

22 There are no extended components required for this SST for the NXP San Diego Site.

23 The evaluation of the site comprises the following assurance components:

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

24 The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profile [5] and is therefore suitable for the evaluation of software and Hardware design for Security ICs.

25 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.

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 10 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

4. Security Problem Definition

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

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

4.1 Assets

28 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 (printed documents, engineering samples, 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 (1) In this case development data with the intention to violate confidentiality and possibly integrity (2) Physical security objects in the form of printed documentation or engineering samples (3) Development Tools in the form of IT infrastructure hardware. 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 (1) In this case development data with the intention to violate confidentiality and possibly integrity (2) Physical security objects in the form of printed documentation or engineering samples (3) Development Tools in the form of IT infrastructure hardware.

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 11 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

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 by violating (1) In this case development data with the intention to violate confidentiality and possibly integrity (2) Physical security objects in the form of printed documentation or engineering samples (3) Development Tools in the form of IT infrastructure hardware.

T.Staff-Collusion: An attacker tries to get access to assets by getting support from one employee through extortion or bribery. (1) In this case development data with the intention to violate confidentiality and possibly integrity (2) Physical security objects in the form of printed documentation or engineering samples (3) Development Tools in the form of IT infrastructure hardware.

4.3 Organizational Security Policies

P.Config_IT-env: The site uses software on development workstations and servers in addition to configuration management systems for file versioning and problem tracking. For file versioning unique repositories shall be used to support proper management of multiple products and the site internal procedures and helps meet the objective of (O.Config_IT-env). The team members are instructed to use only project related IT equipment provided by NXP with the provided tools.

P.LifeCycle-Doc: The site uses 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.

These helps meet the objective of O.Lifecycle-Doc

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

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 12 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

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.

4.4 Assumptions

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 will satisfy all relevant ALC requirements and are provided and managed by NXP. The workstations are configured such that any assets are contained within encrypted containers.

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

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 NXP will manage the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results by NXP.

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

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 13 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

5. Security Objectives

29 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: The site uses software on development workstations and servers in addition to 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.

O.LifeCycle-Doc: The site uses 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.
- (6) CM_Plan

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.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 operate the systems for access control. Out of hour surveillance and respond to alarms is contracted to a 3rd party security company. Technical security measures like motion sensors and similar kind of sensors support the enforcement of the access control. NXP personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers.

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 14 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

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: The (plain-text) development network of the site exists within the secured areas of the site only. It is connected only to:

(1) The encryption equipment employs encrypted VPNs to the secure network provided by the NXP;

(2) The development workstations provided by the NXP;

(3) Additional equipment (e.g. a printer) approved by the NXP.

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

O.Control-Scrap: The site has measures in place to either securely destroy assets (e.g. paper shredder) or return them to the NXP Hamburg for destruction.

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.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. All contractors and visitors must be escorted by a trained employee at all times.

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 15 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

5.1 Security Objectives Rationale

- 30 The SST includes a Security Objective Rationale with two parts. The first part includes the tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part includes a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives (see column "Rationale" of Table 1 and Table 2)
- 31 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.

5.1.1 Mapping of Security Objectives

Threat	Security Objective(s)	Rationale
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat.
T.Rugged-Theft	O.Physical-Access O.Control-Scrap 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.

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 16 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

Threat	Security Objective(s)	Rationale
T.Computer-Net	O.Config_IT-env O.Network-separation O.Logical-Operation O.Physical-Access O.Internal-Monitor O.Maintain-Security O.Control-Scrap 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.Unauthorized-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.

Table 1 Threats - Security Objectives Rationale

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 17 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

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

Table 2 OSP - Security Objectives Rationale

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 18 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

6. Extended Assurance Components Definition

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

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 19 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

7. Security Assurance Requirements

- 33 Clients using this Site Security Target requires a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profile [5].
- 34 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)
- The Security Assurance Requirements listed above fulfill the requirements of [6] 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 [6]) are used in this Site Security Target.

7.1 Application Notes and Refinements

- 35 The description of the site certification process [6] 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)

- 36 Refer to subsection ‘Application Notes for Site Certification’ in [6] 5.1 ‘Application Notes for ALC_CMC’.

7.1.2 CM Scope (ALC_CMS.5)

- 37 Refer to subsection ‘Application Notes for Site Certification’ in [6] 5.2 ‘Application Notes for ALC_CMS’.

7.1.3 Development Security (ALC_DVS.2)

- 38 Refer to subsection ‘Application Notes for Site Certification’ in [6] 5.4 ‘Application Notes for ALC_DVS’.

7.1.4 Life-cycle Definition (ALC_LCD.1)

- 39 Refer to subsection ‘Application Notes for Site Certification’ in [6] 5.6 ‘Application Notes for ALC_LCD’.

- 40 Refer to ‘Application Note 26’ in 6.2.1.2 ‘Refinements regarding Development Security (ALC_DVS)’ in the Eurosmart PP [5].

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 20 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

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

42 Refer to subsection "C Excerpts from the Criteria in Security assurance components (chapter 7)" in [9] Security IC Platform Protection Profile (BSI-CC-PP-0084-2014), Version 1.0, Eurosmart, 2014.

7.2 Security Requirements Rationale

7.2.1 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 [6] 5.1 'Application Notes for ALC_CMC'.

45 Refinements introduced into the SAR are in *italic*.

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 21 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

7.2.2 Security Requirements Rationale – Mapping

SAR	Security Objective	Rationale
ALC_CMC.5.1C: <i>The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.</i>	O.Config_IT-env O.LifeCycle-Doc O.Config_Activities	Appropriate and consistent labelling 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).
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 (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 O.Config_Activities	The configuration management systems (O.Config_IT-Env) used (O.Config_Activities) 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 TOE by automated means.	O.Config_IT-env O.LifeCycle-Doc O.Config_Activities	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)
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a	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.

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 22 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

SAR	Security Objective	Rationale
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 <i>intended</i> 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 <i>intended</i> 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 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 <i>intended</i> TOE.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) describes how the CM system is used for the development of the product.

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 23 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

SAR	Security Objective	Rationale
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the <i>intended</i> 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

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 24 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

SAR	Security Objective	Rationale
ALC_CMS.5.1C: The configuration list includes the following: the <i>intended</i> TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the <i>intended</i> 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 <i>configuration item</i> , the configuration list shall indicate the developer/ <i>subcontractor</i> 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

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 25 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

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 <i>intended</i> 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-Scrap O.Zero-Balance 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-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 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 <i>intended</i> 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 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 <i>intended</i> TOE.	O.LifeCycle-Doc	The model used to develop the 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 <i>intended</i> 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 TOE.

Table 6 Rationale for ALC_LCD.1

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 26 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

8. Site Summary Specification

8.1 Preconditions required by the Site

- 46 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 NXP.
(A.Inherit-secure-IT)
- 47 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)**
- 48 In case of necessary updates to the life cycle documentation NXP will co-ordinate, communicate and deliver.**(A.Product-Setup)**
- 49 To enable that the site participates in the development of products NXP provides services to setup the necessary development computers (tools, user accounts, etc.) and configuration management systems (user accounts, repositories etc.) **(A.Setup-Projects)**
- 50 To enable the site to realize internal shipment, the shipment can only take place based on an order in SAP and to addresses defined in SAP. The shipment method is described in the shipment documentation.**(A.Shipment)**
- 51 In case the site is unable to securely destroy certain physical assets, the assets will be securely stored and shipped to an NXP certified site for destruction.
(A.Shipment)
- 52 To define the participation of the site in the development while maintaining quality, for each product NXP will manage the activities to be performed, the specifications of the input for the site and the acceptance of the results.
(A.Product-Setup)
- 53 The site follows the development processes of NXP. Applicable policies and processes are documented and available.

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 27 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

8.2 Services of the Site

54 The site participates in the design, development and engineering test of hardware and software for secure integrated circuits.

55 The site provides an appropriate physical environment for sensitive IT equipment provided by the client. This includes at least a RED area for RS/HS (network) equipment.

8.3 Security Assurance Rationale

8.3.1 CM capabilities (ALC_CMC.5)

56 Configuration Management is described in ² ³ and ⁴

57 For full detail and evidences please view Section 7.2.2

8.3.2 CM scope (ALC_CMS.5)

58 Configuration Management is described in ² ³ and ⁴

59 For full detail and evidences please view Section 7.2.2

8.3.3 Development Security (ALC_DVS.2)

60 Development Security is described in ³.

61 For full detail and evidences please view Section 7.2.2

8.3.4 Life-cycle definition (ALC_LCD.1)

62 Life-cycle definition is described in ² and ³ [7].

63 For full detail and evidences please view Section 7.2.2

² NXPOMS-1719007347-2547 BU S&C ALC-CM - Common Criteria Documentation, Gordon Caffrey, NXP Semiconductors, 21. November 2017

³ NXPOMS-1719007347-4782 Site Security Manual - NXP Semiconductors San Diego, NXP Semiconductors, 17. October 2019

⁴ NXP Semiconductors San Diego Configuration List, Version 1.2, 17. October 2019

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 28 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

8.4 Objectives Rationale

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

8.4.1 O.Config_IT-env

65 The configuration of the IT environment is designed in such way to ensure segregation of duties and the need to know principals. These measures address T.Computer-Net, T.Staff-Collusion and T.Unauthorized-Staff. Also addresses the OSP P.Config-IT-env.

8.4.2 O.Physical-Access

The physical access is supported by O.Security-Control that includes the maintenance of the access control and the control of visitors. The physical security measures are supported by O.Alarm-Response providing an alarm system.

Thereby the threats T.Smart-Theft, T.Rugged-Theft can be prevented. The physical security measures together with the security measure provided by O.Security-Control enforce the recording of all actions. Thereby also T.Computer-Net, T.Staff-Collusion and T.Unauthorized-Staff is addressed. Also addresses the OSP P.Config-Activities.

8.4.3 O.Security-Control

66 During off hours the guard patrol the internal of the building and the alarm system is used to monitor the site with a dedicated off-site monitoring station. The CCTV system supports these measures because it is always enabled and monitored 24/7. The security control is further supported by O.Physical-Access requiring different level of access control for the access to security product during operation as well as during off-hours.

67 This addresses the threats T.Smart-Theft and T.Rugged-Theft. Supported by O.Maintain- Security and O.Physical-Access also an internal attacker triggers the security measures implemented by O.Security-Control. Therefore, also the Threat T.Unauthorized-Staff is addressed. This also addresses the OSP P.Config-Activities.

8.4.4 O.Alarm-Response

68 During working hours, the employees monitor the alarm system. The alarm system is connected to a control center that is manned 24 hours. During off-hours additional guard patrol supports the alarm system. O.Physical-Access requires certain time to overcome the different level of access control. The response time of the guard and the physical resistance match to provide an effective alarm response.

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 29 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

69 This addresses the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff

8.4.5 O.Internal-Monitor

70 Regular security management meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This comprises of all security events, security relevant systems, CCTV and access control. Major changes of security systems and security procedures are reviewed in general management systems review meetings (2x per year). Upon introduction of a new process a formal review and release for mass production is made before being generally introduced.

71 The security relevant systems enforcing or supporting O.Physical-Access, O.Security-Control and O.Logical-Access are checked and maintained regularly by the suppliers. In addition, the configuration is updated as required either by employees (for the access control system) of the supplier. Logging files are checked at least monthly for technical problems and specific maintenance requests.

72 This addresses T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion

8.4.6 O.Logical-Operation

73 All logical protection measures are maintained and updated as required, at least once a month. Critical items such as virus scanners are updated daily. The backup is sufficiently protected and is only accessible for the administration.

74 This addresses the threats T.Computer-Net and T.Unauthorised-Staff

8.4.7 O.Staff-Engagement

75 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, O.Logical- Access and O.Config-Items support the engagement of the staff.

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

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 30 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

8.4.8 O.Control-Scrap

- 77 Scarp may exist in several forms on this site printed secure objects, test samples or redundant hardware/movable media. Hardware and samples scrap are returned to an NXP certified site with controlled secure destruction. Transport and actual destruction of security products is done under supervision of a qualified employee in collaboration with the destructor. Sensitive information and information storage media are collected internally in a safe location and destroyed in a supervised and documented process. All documentation destroyed on site is by means of a Level 5 security shredder.
- 78 Supported by O.Physical-Access and O.Staff-engagement this addresses the threats T.Unauthorised-Staff, T.Computer-Net, T.Smart-Theft, T.Rugged-Theft and T.Staff-Collusion and addresses the OSP P.Zero-Balance and P.Scrap-Items.

8.4.9 O.Config_Activities

- 79 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.
- 80 This is addressing the threat T.Rugged-Theft, T.Computer-Net, T.Staff-Collusion, T.Unauthorised-Staff, T.Smart-Theft and the OSP P.Config-Activities

8.4.10 O.Network_Separation

- 81 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.
- 82 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.

8.4.11 O.Maintain_Security

- 83 The 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

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 31 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

84 These security measures are necessary to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion

8.4.12 O.LifeCycle_doc

85 The security of the site is maintained according to the site security documentation covering all physical and logical measures to ensure the security of the site.

86 These security measures are necessary to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion. Also addressing the OSP P.Lifecycle-Doc

8.4.13 O.Zero-Balance

87 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.

88 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.

8.5 Mapping of the Evaluation Documentation

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

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

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 32 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

SAR	Aspects	Reference
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
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

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 33 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

SAR	Aspects	Reference
ALC_CMC.5.6C: The CM system shall support the production of the <i>intended</i> 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 “BU ID ALC-CM Common Criteria Documentation” there is no specific TOE in the focus, therefore this is only applicable to the CM documentation. The documentation can be identified in the tool EnoviaNXP.	• Product/project specific CM plans and the CI list that is used for CC evaluation.
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the <i>intended</i> 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	Different CM tools like DesignSync or CollabNet provide means to tag a	• Tool documentation

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 34 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

SAR	Aspects	Reference
implementation representation from which the <i>intended</i> TOE is generated.	release version from which the intended TOE is generated. The version information of documents is stored in EnoviaNXP.	• 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 <i>intended</i> 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 <i>intended</i> 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 • 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

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 35 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

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

Table 8 Mapping of the Evidence for the Scope of the Configuration Management

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 36 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

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 <i>intended</i> 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-1719007347-4782 - Site Security Manual - NXP Semiconductors San Diego
	Visitors, external suppliers and cleaning personnel handling	• NXPOMS-1719007347-4782 - Site Security Manual - NXP Semiconductors San Diego
	Handling of physical objects, zero balancing, disposal of security products	• NXPOMS-1719007347-4782 - Site Security Manual - NXP Semiconductors San Diego
	Trustworthiness and training of staff	• NXPOMS-1719007347-4782 - Site Security Manual - NXP Semiconductors San Diego
	Physical security system: operation, emergency procedures, incident handling and reporting	• NXPOMS-1719007347-4782 - Site Security Manual - NXP Semiconductors San Diego
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 <i>intended</i> TOE.	The justification is provided in this security target because it shows that all threats are addressed by the measures. In addition, the measures are monitored to control the effectiveness.	• Chapter 8 of this document

Table 9 Mapping of the Evidence for the Development Security

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 37 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

SAR	Aspects	Reference
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the <i>intended</i> TOE.	The intended TOE is developed and maintained as per NXP development process.	●NXPOMS-999116894-3989 - NPI3.0 Handbook ●NXPOMS-1719007347-2486 - BU S&C Gate Checklist
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the <i>intended</i> 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

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 38 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

9. References

9.1 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 Components; 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 Version 1.0," Eurosmart, 15.06.2007.
- [6] Common Criteria, "Supporting Document, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001," October 2007.
- [7] "NXPOMS-1719007347-2479 BU S&C ALC-CM Common Criteria Documentation" 21.11.2017.
- [8] JIL - Minimum Site Security Requirement Version 2.2, April 2019
- [9] Security IC Platform Protection Profile with Augmented Packages (BSI-CC-PP-0084-2014), Version 1.0, Eurosmart, 2014.

9.2 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.

NXP Semiconductors	Site Security Target NXP Semiconductors San Diego	Published
Product Creation		11/18/2019
NXP BLs		Page 39 of 41
Doc. Identifier: NXPOMS-1719007347-4204		Old System Identifier: N/A

9.3 List of Abbreviations

CC	Common Criteria
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