Site Security Target Chandler

Revision	V1.6

Table of content

Table of Figures

1. SST Introduction

1 The chapters 1 to 7 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 Chandler

5 EAL: SARs taken from EAL6

6 SST reference: Site Security Target NXP Chandler, 7 May 2021, v1.6, NXPOMS-1719007347-4218

1.2 Site Reference

7 The site is located at:

NXP Semiconductors
1300 N. Alma School Rd. Chandler
AZ 28224
USA,
United States

1.3 Site Description

1.3.1 Physical Scope

8 The following areas of the plant specified in section 1.2 is in the scope of the SST.

9 All areas in scope are classified as YELLOW[1] and RED[1] areas. These areas will be within the following buildings.

- Building M: Shipping area (MDock)
- Building A: SIP area (SIP A2)
- Building G: Security Operation Center (SOC)

10 A more detailed view of the layout is described in the Site Security Manual (SSM) for Chandler.

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

12 Within those areas, only members of the development group and supporting functions such as IT 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

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

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

14 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.

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

1.3.2.1 Supporting service

- IT support;
- Warehousing and shipment;

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

1.3.2.2 NXP Chandler Site Services related to [3] life cycle phases

- IC and dedicated Development (Phase 1 and 2)

2. Conformance Claim

16 This SST is conformant with Common Criteria Version 3.1:

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

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

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

- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017, [6]

18 This SST is CC Part 3 conformant.

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

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

21 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.

22 The chosen assurance components are derived from the assurance level EAL6 of the assurance class "Life-cycle Support". For the assessment of the security measures attackers with a high attack potential are assumed. Therefore, this site supports product evaluations up to EAL6.

3. Security Problem Definition

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

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

3.1 Assets

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

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

Development data: The site has access to (and optionally copies thereof) electronic development data (specifications, evaluation Documents, Product Quality Engineering Documents, Product Documents, Software Development, and Test Software/Data/Documents, etc.) in relation to developed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected.

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

3.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of assets: (1) physical security objects, (2) development data, (3) development tools. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered.

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.

T.Computer-Net: A possibly paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to (1) development data with the intention to violate confidentiality and possibly integrity (2) development computers with the intention to modify the development process.

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

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: 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).

P.Product-Transport: Technical and organizational measures shall ensure the correct labeling of the product. A controlled internal shipment shall be applied. The transport supports traceability up to the acceptor. If applicable or required this policy shall include measures for packing if required to protect the product during transport.

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.

3.4 Assumptions

26 The assumptions are outside the sphere of influence of NXP Chandler 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 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.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.

A.Scrap: NXP is responsible for the secure disposal of scrap from Chandler.

4. Security Objectives

27 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; (6) CM_Plan
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 (plain-text) 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-Access:	The site enforces a logical separation between the internal network and the internet including a firewall. The security measures ensure that only defined services and defined connections are accepted on the internal network. The internal network is appropriately separated to prevent interference between the different environments (office, development and production environments). Additional specific networks for production and configuration are physically separated from any internal network to enforce access control. Access to the production network and associated systems is restricted to authorized employees working in the related area or involved in the configuration tasks of the production systems. Every user of an IT system has his/her own user account and password.
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 or return them to the client.
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.Internal-Shipment:	The site has measures in place to provide assurance of integrity throughout transport of physical security objects. The recipient of a physical configuration item is identified by the assigned client address. The internal shipment procedure is applied to the configuration item. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of configuration items during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined.

4.1 Security Objectives Rationale

28 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 Table 1 and Table 2).

29 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.Control-Scrap O.LifeCycle-Doc O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Config-Activities	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 O.Config-Activities	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat.
T.Computer-Net	O.LifeCycle-Doc 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.

Threat	Security Objective(s)	Rationale
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 number 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.Internal-Shipment O.LifeCycle-Doc	The shipment method and the organizational measures ensure that integrity changes of shipped objects are detected and appropriately responded upon.

Table 1 Threats - Security Objectives Rationale

OSP	Security Objective(s)	Rationale
P.Config_IT-env	O.Config_IT-env	The Security Objective directly enforces the OSP.
P.LifeCycle-Doc	O.LifeCycle-Doc	The Security Objective directly enforces the OSP.
P.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	All assets are traced internally until their possible destruction (O.Zero-Balance,O.Control-Scrap) by trained and authorized people (O.Staff-

OSP	Security Objective(s)	Rationale
		Engagement) to enforce the OSP.
P.Product-Transport	O.LifeCycle-Doc O.Internal-Shipment	Appropriate procedures for internal shipment ensure correct labelling and traceability until the recipient.

Table 2 OSP - Security Objectives Rationale

5. Extended Assurance Components Definition

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

6. Security Assurance Requirements

31 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].

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

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

33 The Security Assurance Requirements listed above fulfill the requirements of [7] because hierarchically higher components than the defined minimum site requirements (ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, see section 3.2.3 of [7]) are used in this Site Security Target.

6.1 Application Notes and Refinements

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

6.1.1 CM Capabilities (ALC_CMC.5)

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

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

6.1.2 CM Scope (ALC_CMS.5)

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

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

6.1.3 Development Security (ALC_DVS.2)

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

6.1.4 Life-cycle Definition (ALC_LCD.1)

40 Refer to subsection 'Application Notes for Site Certification' in [7] 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] (application note 27).

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 (see [5], appendix C):

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

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 [7] 5.1 'Application Notes for ALC_CMC'.

45 Refinements introduced into the SAR are in italic.

6.2.2 Security Requirements Rationale – Mapping

SAR	Security Objective	Rationale
ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*	O.Config_IT-env O.LifeCycle-Doc 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	O.LifeCycle-Doc	The method used to uniquely identify the configuration items is described in the CM-Plan (O.LifeCycle-Doc).

SAR	Security Objective	Rationale
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.	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 *configuration items* 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 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	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

SAR	Security Objective	Rationale
intended TOE by automated means, including the originator, date, and time in the audit trail.		audit trail (showing originator, date and time) is automatically generated.
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O.Config_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configurations management system and software installed on the development workstations and servers (O.Config_IT-env) provide automated means to identify all other configuration items that are affected by the change of a given configuration item.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the *intended* TOE is generated.	O.Config_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configurations management system (O.Config_IT-env) identifies the version of the implementation representation from which the 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)

SAR	Security Objective	Rationale
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 shall include 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 reports and resolution status; and development tools and related information..	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan and a CI-List with the items required by ALC_CMS.5.1C
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.LifeCycle-Doc	The CI-List (O.LifeCycle-Doc) uniquely identifies the configurations items as described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMS.5.3C: For each *configuration item*, the configuration list shall indicate the developer/*subcontractor* of the item*.*	O.LifeCycle-Doc	The CI-List 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	O.LifeCycle-Doc O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Network-separation	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,

SAR	Security Objective	Rationale
are necessary to protect the confidentiality and integrity of the *intended* TOE design and implementation in its development environment.	O.Logical-Operation O.Control-Scrap O.Zero-Balance O.Staff-Engagement	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 *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 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 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 TOE.

Table 6 Rationale for ALC_LCD.1

7. Site Summary Specification

7.1 Preconditions required by the Site

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

Precondition	Assumption
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. The IT infrastructure consists of local and remote equipment connected using an encrypted connection. NXP Hamburg (Master IT Site) provides, configures and maintains the 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
Internal 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
To perform secure scraping of physical assets, NXP will give details about the certified site to use.	A.Scrap

Table 7 **Mapping of Preconditions to Assumptions**

7.2 Services of the Site

47 The following services and/or processes provided by SST NXP Chandler are in the scope of the site evaluation process:

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

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

48 The services as listed in section 1.3 are more detailed in the following.

- Development of IC and dedicated software which comprises:
  - o the generation of the analog and digital hardware designs, embedded & IC dedicated software and the creation of development related documents;
  - o the verification process using or not simulations tools;
- IT support
  - o IT Help desk for development;
- Warehousing and Shipment
  - o this site provides the service of secure disposal, secure receipt, packing, storage and shipping of engineering samples.

7.3 Objectives Rationale

7.3.1 O.Config_IT-env

49 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.

7.3.2 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.

7.3.3 O.Security-Control

50 During off hours the guard patrol the internal of the building and the alarm system is used to monitor the site with dedicated 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.

51 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.

7.3.4 O.Alarm-Response

52 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.

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

7.3.5 O.Internal-Monitor

54 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.

55 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.

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

7.3.6 O.Logical-Operation

57 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.

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

7.3.7 O.Staff-Engagement

59 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.

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

7.3.8 O.Control-Scrap

61 Scrap 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.

62 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.

7.3.9 O.Config_Activities

63 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.

64 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.

7.3.10 O.Network_Separation

65 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.

7.3.11 O.Maintain_Security

67 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

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

7.3.12 O.LifeCycle_doc

69 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.

70 These security measures are necessary to prevent the threats T.Smart-Theft, T.Rugged-Theft, T-Attack-Transport, T.Computer-Net, T.Unautorised-Staff and

T.Staff-Collusion. Also addressing the OSP P.Lifecycle-Doc and P.Product-Transport.

7.3.13 O.Zero-Balance

71 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.

72 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.

7.3.14 O.Internal-Shipment

73 The site implements protection measures to provide assurance of integrity throughout shipment of physical security objects. Hence, the threat T.Attack-Transport is prevented and the OSP P.Product-Transport addressed.

7.4 Mapping of the Evaluation Documentation

74 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 SST NXP Chandler.

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	• NXPOMS-999116894-3989 - NPI3.0 Handbook, slide on Configuration management • Configuration Management References and Templates

SAR	Aspects	Reference
	that are automatically provided by the system as well as the baseline labels that are given by the configuration manager.	
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
ALC_CMC.5.6C: The CM system shall support the production of the *configuration items* 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

SAR	Aspects	Reference
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 *clearly* 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 identified in the tool EnoviaNXP.	• Product/project specific CM plans and the CI list that is used for CC evaluation.
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the *intended* TOE by automated means, including the originator, date, and time in the audit trail.	Different CM tools like DesignSync or CollabNet provide automated means to support the audit of all changes. Documents stored in EnoviaNXP are under version control.	• Enovia Synchronicity • DesignSync – System Administration Help • Technical Design - CollabNet service for CCC&S
ALC_CMC.5.10C: The CM system shall provide an automated means to identify 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	The development environment used is set up centrally as per	• Configuration Management Procedure

SAR	Aspects	Reference
CM system is used for the development of the *intended* TOE.	the Release Manual and a project specific CM plan.	• 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 • 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 *all configuration items have been and 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 • Configuration Management Procedure

Table 8 **Mapping of the Evidence for the Configuration Management Capabilities**

SAR	Aspects	Reference
ALC_CMS.5.1C: The configuration list shall include the following: the *intended* TOE itself; the evaluation evidence required by the SARs; the parts that comprise the *intended* TOE; the implementation representation; security flaw reports and resolution status;	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

SAR	Aspects	Reference
and development tools and related information.		
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 *configuration item*, the configuration list shall indicate the developer/*subcontractor* of the item.	The configuration list in case of site certification is the list of all applicable documents. In the document the author of each item is listed.	• Document list/Bibliography

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

SAR	Aspects	Reference
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security 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-1719007347-4972 - Site Security Manual - NXP Chandler
	Visitors, external suppliers and cleaning personnel handling	• Site Security Manual - NXP Semiconductors Chandler
	Handling of physical objects, zero balancing, disposal of security products	• Site Security Manual - NXP Semiconductors Chandler
	Trustworthiness and training of staff	• Site Security Manual - NXP Semiconductors Chandler
	Physical security system: operation, emergency procedures, incident handling and reporting	• Site Security Manual - NXP Semiconductors Chandler
ALC_DVS.2.2C: The development security	The justification is provided in this security target because it	• Chapter 6. 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 10 **Mapping of the Evidence for the Development Security**

SAR	Aspects	Reference
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the *intended* TOE.	The intended TOE is developed and maintained as per NXP development process.	• NXPOMS-999116894-3989 - 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 11 **Mapping of the Evidence for the Developer defined Life-Cycle Model**

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, 14. March 2019.

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

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

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

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

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

[8] JIL - Minimum Site Security Requirement Version 3.0, Feb 2020

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

8.2 Definitions

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

8.3 List of Abbreviations

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

8.4 Revision History

Revision	Description	Author	Approval Date
1.0 (not released)	• First Draft	Gordon Caffrey	18 Mar 2017
1.1 (not released)	• Updated after TUV comments	Gordon Caffrey	22 Mar 2018
1.2 (not released)	• Update to Assumptions	Gordon Caffrey	29 Mar 2018
1.3	• Update with Serma comments	Gordon Caffrey	11 Sep 2018
1.4	• New OMS template, services scope change, creation of one PUBLIC SST to be used for certification, SST (NXPOMS-1719007347-4029) WITHDRAWN	Christopher Bouly	05 Oct 2020
1.5 (not released)	• Updated related to lab comments (CCENXP005-OR001-M0)	Christophe Bouly	30 March 2021
1.6	• Physical scope update • Service description alignment and update	Christophe Bouly	18 May 2021

Approvers

Sequence	Role	Name
Acceptance	Site Security Representative	Nick Meadows
Approval	Security Manager	Christophe Bouly