NXPOMS-1719007347-2677

Site Security Target - NXP Mougins

Publication Summary

Reference Number (OMS-ID)	NXPOMS-1719007347-2677
Reference Title	Site Security Target - NXP Mougins
Publisher	CCC&S (Competence Center Crypto & Security)
Classification	PUBLIC
Owner	Paul Brady
Author	Michael Sandu

Revision History

Revision	Description	Author	Approval - Date
0.1	Initial Draft	Paul Brady	2015-03-16
0.2	Update to Section 5.2 Threats and OSP - Security Objectives Rationale	Paul Brady	2015-03-23
0.3	Feedback from T-Systems – removal of all references to T.Attack-Transport as not applicable.	Paul Brady	2015-04-27
0.4	Corrected reference source errors. Added definition of security assets for scrap.	Paul Brady	2015-05-11
0.5	Modified Section 5.1 Security Objectives	Paul Brady	2015-05-26
0.6	Updated area definition and created light version	Paul Brady	2015-09-22
0.7	Feedback received and incorporated from review of 0.6	Paul Brady	2015-09-28
0.8	Updated Section 7.2.2 and section 8.5 to be in line with new certification approach. Added revision number for SSM.	Paul Brady	2015-12-03
0.9 (not released)	Updated version taking into account new test areas	Christophe Bouly	2017-10-10
0.91 (not released)	Updates after T-Systems comments and improvements, new template	Christophe Bouly	2017-12-14
0.92 (not released)	Update after T-Systems comments	Christophe Bouly	2017-12-15
0.93 (not released)	Update after T-Systems change	Christophe Bouly	2017-12-21
0.94 (not released)	Alignment with T-Systems	Christophe Bouly	2018-01-16
0.95 (not released)	Preparation for release	Christophe Bouly	2018-01-19
0.96 (not released)	Update with new Security Manual	Christophe Bouly	2018-02-15
1.0	Release to cover changes revision 0.9 – 0.96	Christophe Bouly	2018-02-16
2.0	Removed ALC_DEL.1, ALC_TAT.3, ALC_FLR.3 from scope Updated tables and references	Michael Sandu	2020-01-30
2.1	Chapter 2.1 Update from 2 physical RED areas to 3 Update from one physical YELLOW area to 2 areas Action points from BrightSight - Update Secure Shipment - Update Secure Scrap - Removed unnecessary Security Objectives in 5.1.1. T-Accident-Change - Update of Security Objectives mapping - Update phase (ii) validation	Michael Sandu	2020-02-24
2.2	Update Action points from BrightSight - Update CCC&S and NXP BLs - Update of NXPOMS Typo - Update Text of IC Development - Update Linking of Security Objectives	Michael Sandu	2020-03-02

2.3	Update Action points from BrightSight - Update Chapter 8.3 Security Objectives - Update Chapter 8.3 linking of Security Objectives	Michael Sandu	2020-03-11

Approvers

Sequence	Role	Name
Acceptance	Security Manager	Michael Sandu
Approval	Site Security Mougins	Paul Brady

Subscriber

Role	Name	Notification	PDF-file
n.a.	n.a		

Table of content

Table of Figures

1. Document Introduction

1.1 Reference

Title: Site Security Target - NXP Mougins

Version: 2.3

Date: 2020-03-11

Company: NXP Semiconductors France

Name of site: NXP Mougins

EAL: SARs taken from EAL6

2. SST Introduction

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

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

2.1 SST Reference

3 Title Site Security Target - NXP Mougins

4 Version 2.3

2.2 Site Reference

5 The site is leased by NXP and is located at:

NXP Semiconductors France
E Space Park, Building C
45 Allee des Ormes
06250 Mougins, FRANCE

2.3 Site Description

6 The following areas of the plant specified in section 2.2 is in the scope of the SST.

7 The development areas are located within the NXP Semiconductors. The development areas are secure areas with restricted access where only authorized persons can enter. They are in different wings and floors of the same building (Building C) as described hereafter:

- in the left wing on the first floor of the building, in a closed area and consists of one physical YELLOW area and 3 physical RED area contained within the YELLOW area[1].

- In the right wing on the ground floor of the building in a dedicated closed area consisting of 2 physical YELLOW areas.

8 Within the development area, only members of the development team are entitled to access sensitive information like source code, design material and confidential development documentation. To enforce such access restriction, a combination of physical, procedural,

[1] The terms GREEN / (NS), YELLOW / (RS) and RED / (HS) areas are defined in the NXP internal document „NXPOMS-1719007347-2404 S&C Security requirements.

personnel and logical measurements have been installed. Physical security objects (see Assets chapter) are handled as per the document [2] and [3].

9 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 2) as defined in 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084)

10 To perform its activities the site uses the NXP BU S&C provided and managed remote IT-infrastructure. Locally available IT equipment like workstations or VPN router is also provided and managed by NXP BU S&C IT authorized support directly or remotely. The site works according to NXP BU S&C processes.

11 The site performs secure shipment, which only refers to internal shipments and/or shipments between sites and not to shipment to customer or end user. Therefore ALC_DEL is not scope of the Site NXP Mougins.

12 The site performs secure scrap activities and has measures in place to either securely destruct assets (e.g. paper shredder) or return them to the client and/or to a certified site to perform higher scrap requirements.

[2] NXP Semiconductors - NXPOMS-1719007347-2401 Security Objects
[3] NXP Semiconductors - NXPOMS-1719007347-2404 BU S&C Security requirements

3. Conformance Claim

13 This SST is conformant with Common Criteria Version 3.1:

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

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

14 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 Requirements v2.2, April 2019 [5]

15 This SST is CC Part 3 conformant.

16 The evaluation of the site comprises the following assurance components[4]:

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

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

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

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

4. Security Problem Definition

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

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

4.1 Assets

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

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

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

Development tools: To perform its development activities the site uses tools (e.g. synthesis, layout and simulation tools) to transform design code, schematics and library elements into a design database. The integrity of these tools (running on local or remote development computers) 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) 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.

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.Accident-Change: An employee, contractor or student trainee may exchange products of different production lots or software of different clients during development/production by accident.

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

T.Staff-Collusion: An attacker tries to get access to assets by getting support from one employee through extortion or bribery.

T.Attack-Transport: An attacker tries to get access to shipped physical security objects when shipped in or out of the site with the intention to compromise confidentiality and/or integrity of the product design data, customer and/or consumer data like code and data (including personalisation data and/or keys) stored in the ROM and/or EEPROM or classified product documentation.

4.3 Organizational Security Policies

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

P.LifeCycle-Doc: The site follows the life cycle documentation that describes: (1) Description of configuration management systems and their usage; (2) A configuration items list; (3) Site security; (4) The development process; (5) The development tools.

P.Reception-Control: The inspection of incoming items done at the site ensures that the received configuration items comply with the properties stated by the client. Furthermore, it is verified that the items can be identified and assigned to a specific product.

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 the NXP BU. or customer and/or consumer (depending on the production-setup). The sent back

procedures, whether to the NXP BU 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.DevEnv-Provisioning: To enable that the site participates in the development of products the client provides services to setup and maintain the necessary development environment (e.g. workstations, tools) and configuration management systems (e.g. user accounts in project repositories) including a CM plan. The client also provides a secure connection between the IT equipment of the site and a secure remote IT infrastructure of the client.
These services are provided by the client in a secure way in order to properly protect the assets of the site. This includes the enforcement of a trustworthy access policy to the site equipment and data using the secure connection based on a “need-to-know” principle.

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

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

A.Internal-Shipment: The recipient (client) of the product is identified by the address of the client site. The address of the client is part of the product setup.

5. Security Objectives

22 The Security Objectives are related to physical, technical, and organizational security measures, the configuration management as well as the internal shipment.

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

O.LifeCycle-Doc: The site follows the life cycle documentation that describes: (1) Description of configuration management systems and their usage; (2) A configuration items list; (3) Site security; (4) The development process; (5) The development tools.

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organisational security measures allows a sufficient separation of employees to enforce the “need to know” principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorised people. The access control measures ensure that only registered employees can access restricted areas. Assets are handled in restricted areas only.

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

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

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

O.Maintain-Security: Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorised employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.

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

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

O.Control-Scrap: The site has measures in place to either securely destruct assets (e.g. paper shredder) 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.Reception-Control: Upon reception of TOE items an immediate incoming inspection is performed. The inspection comprises the received amount items and the identification and assignment of the product to a related internal production process

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.

5.1 Security Objectives Rationale

23 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).

24 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 and OSP	Security Objective(s)	Rationale
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Control-Scrap	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat.
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Control-Scrap	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat.
T.Computer-Net	O.Network-separation O.Physical-Access O.Logical-Operation O.Internal-Monitor O.Maintain-Security	The development network is not connected to anything that an attacker could use to set up a remote connection.
T.Accident-Change	O.Logical-Operation O.Staff-Engagement O.Zero-Balance O.Control-Scrap O.Config_IT-env	Automated measures and control procedures allow preventing accidental changes on sensitive items.

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

Table 1 Threats and OSP - 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.Reception-Control	O.Reception-Control	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-Engagement) to enforce the OSP.
P.Scrap-Items	O.Control-Scrap	The Security Objective directly enforces the OSP.

Table 2 OSP - Security Objectives Rationale

6. Extended Assurance Components Definition

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

7. Security Assurance Requirements

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

27 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)

28 The Security Assurance Requirements listed above fulfill the requirements of [5] 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 [5]) are used in this Site Security Target.

7.1 Application Notes and Refinements

29 The description of the site certification process [5] 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)

30 Refer to subsection ‘Application Notes for Site Certification’ in [5] 5.1 ‘Application Notes for ALC_CMC’.

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

7.1.2 CM Scope (ALC_CMS.5)

32 Refer to subsection ‘Application Notes for Site Certification’ in [5] 5.2 ‘Application Notes for ALC_CMS’.

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

7.1.3 Development Security (ALC_DVS.2)

34 Refer to subsection ‘Application Notes for Site Certification’ in [5] 5.4 ‘Application Notes for ALC_DVS’.

7.1.4 Life-cycle Definition (ALC_LCD.1)

35 Refer to subsection 'Application Notes for Site Certification' in [5] 5.6 'Application Notes for ALC_LCD'.

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

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

7.2 Security Requirements Rationale

7.2.1 Security Requirements Rationale - Dependencies

38 The dependencies for the assurance requirements are as follows (see [3], appendix C):

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

39 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 [5] 5.1 'Application Notes for ALC_CMC'.
- ADV_IMP.1 is not fulfilled as there is no specific TOE. This is in-line with and further explained in [5] 5.7 'Application Notes for ALC_TAT'.

7.2.2 Security Requirements Rationale - Mapping

SAR	Security Objective	Rationale
ALC_CMC.5.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling.	O.Config_IT-env O.LifeCycle-Doc O.Reception-Control	Appropriate and consistent labeling is ensured through the application of the CM-Plan (O.LifeCycle-Doc) and the use of the configuration management systems (O.Config_IT-env). (O.Reception-Control) assures correct identification.
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	Unique identification of all CIs is realized by performing the CM activities in accordance with the CM-Plan (O.LifeCycle-Doc) using the Configuration management systems (O.Config_IT-env)
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config_IT-env O.LifeCycle-Doc	The configuration management systems (O.Config_IT-env) used according to the CM-Plan (O.LifeCycle-Doc) enforces automated measures such that only authorized changes are made to the configuration items
ALC_CMC.5.6C: The CM system shall support the production of the product by automated means.	O.Config_IT-env O.LifeCycle-Doc	The software on the development computers (O.Config_IT-env) supports automated production of products when used in accordance with the CM-Plan (O.LifeCycle-Doc)
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	O.LifeCycle-Doc	As described in the CM-Plan (O.LifeCycle-Doc) the activities performed are such that the person responsible for accepting a configuration item into CM is not the person who developed it.
ALC_CMC.5.8C: The CM system shall clearly identify the	O.Config_IT-env O.LifeCycle-Doc	The CM-Plan (O.LifeCycle-Doc) identifies the configuration items that

SAR	Security Objective	Rationale
configuration items that comprise the TSF.		comprise the TSF possibly supported by the configuration management system (O.Config_IT-env)
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the *intended* TOE by automated means, including the originator, date, and time in the audit trail.	O.Config_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configuration management systems (O.Config_IT-env) are configured such that an audit trail (showing originator, date and time) is automatically generated.
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O.Config_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configurations management system and software installed on the development workstations and servers (O.Config_IT-env) provide automated means to identify all other configuration items that are affected by the change of a given configuration item.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the *intended* TOE is generated.	O.Config_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configurations management system (O.Config_IT-env) identifies the version of the implementation representation from which the intended TOE is generated through baselines.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the *intended* TOE.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) describes how the CM system is used for the development of the product.

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 *intended* TOE.	O.LifeCycle-Doc	The acceptance procedures for modified or newly created configuration items are described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.LifeCycle-Doc	All configuration items are listed in the CI-list (O.LifeCycle-Doc)
ALC_CMC.5.16C: The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.	O.Config_IT-env O.LifeCycle-Doc	The CI-list (O.LifeCycle-Doc) is generated from the configuration management systems (O.Config_IT-env)

Table 3 Rationale for ALC_CMC.5

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

SAR	Security Objective	Rationale
		described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.	O.LifeCycle-Doc	The CI-List (O.LifeCycle-Doc) indicates the developer/subcontractor for each configuration items as described in the CM-Plan (O.LifeCycle-Doc).

Table 4 Rationale for ALC_CMS.5

SAR	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the *intended* TOE design and implementation in its development environment.	O.LifeCycle-Doc O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Network-separation O.Logical-Operation O.Internal-Shipment O.Control-Scrap O.Staff-Engagement	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, A.Internal-Shipment, O.Control-Scrap), personnel (O.Staff-Engagement), and other(O.Network-separation, O.Logical-Operation) security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment.
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *intended* TOE.	O.LifeCycle-Doc	The development security documentation (O.LifeCycle-Doc) justifies the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE.

Table 5 Rationale for ALC_DVS.2

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

Table 6 Rationale for ALC_LCD.1

8. Site Summary Specification

8.1 Preconditions required by the Site

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

41 To enable the site to participate in the development of products, the client needs to provide services to setup and maintain the necessary development environment (e.g. workstations, development tools) (A.DevEnv-Provisioning).

42 Further, the client needs to setup and maintain the used configuration management systems and provide a project specific CM plan. This includes the setup and maintenance of user accounts in the project repositories and other required configuration management tools (A.DevEnv-Provisioning). The client needs to agree about the configuration management methods and the usage of the configuration management tools (A.Project-Setup). The configuration management methods and tools by the client ensure the correct handling of the configuration items according to Common Criteria.

43 The client needs to setup and maintain a secure connection between the IT equipment of the site and a remote secure IT infrastructure of the client. The enforced access policy to the equipment and data of the site using this secure connection need to be restrictive and based on a “need-to-know” principle (A.DevEnv-Provisioning).

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

45 For each project setup, the client needs to agree on the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results from the site (A.Project-Setup).

46 For internal shipment, the client needs to specify the address to ship (A.Internal-Shipment). The shipment method is described in the shipment documentation.

47 Regarding a destruction of certain physical assets, the client needs to specify whether the scrap need to be destroyed by the site or need to be sent back to the client (A.Project-Setup). In the latter case the client is responsible for the secure destruction of the assets.

8.2 Services of the Site

48 The following services and/or processes provided by NXP Mougins are in the scope of the site evaluation process:

49 Security IC Embedded Software Development (Phase 1), IC Embedded Software and Testing (Phase 1), IC Design (Phase 2), IC Dedicated Software and Testing (Phase 2) as defined in 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084)

50 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.

Development comprises

- the generation of the GDSII layout of Smart Card ICs, the source code of embedded and IC dedicated software and the creation of development related documents.
- the verification and validation processes: verification comprises the simulation and emulation of hardware & software designs on dedicated test environments. The purpose of verification is the preparation of the design freeze and sample production. Validation comprises verification of the design with real samples. The purpose of validation is to release the product to the Operations organization that facilitates the volume ramp up.

8.3 Objectives Rationale

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

52 O.Config_IT-env: The site uses only project related tools and IT equipment. In order to provide a separation between different projects, the site uses configuration file versioning and unique repositories as well as configuration management systems. This helps to prevent the threat T.Accident-Change and directly addresses the OSP P.Config_IT-env.

53 O.LifeCycle-Doc: Dedicated documents exist for the site which define the use and the management of the configuration management systems, the configuration item list, the site security, the development process and the development tools. The site follows the procedures and instructions of these documents. This helps to prevent the threat T.Attack-Transport and directly addresses the OSP P.LifeCycle-Doc.

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

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

56 O.Alarm-Response: In case of an access attempt to an asset by an unauthorized person the site has an alarm system in place. After the alarm is triggered the unauthorised person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff.

57 O.Internal-Monitor: The established security measures of the site are regularly reviewed by security management meetings and internal audits. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff, T.Computer-Net and T.Staff-Collusion.

58 O.Maintain-Security: Technical security measures are maintained regularly. This ensures that the systems are working correctly and are configured as required to ensure the protection of the networks and computer systems. Hence, this helps to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff, T.Computer-Net and T.Staff-Collusion.

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

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

61 O.Internal-Shipment: The site implements protection measures to provide assurance of integrity throughout transport of physical security objects. Hence, the threat T.Attack-Transport is prevented. This helps to address the OSP P.Product-Transport.

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

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

64 O.Zero-Balance: Products are uniquely identified throughout the whole process. Further on the number of masks and wafers is known. Handover and storage of security products is controlled by the 4-eyes principle and documented. Scrap and rejects are following the good products through the whole production process. At every process step the registration of good and scrapped/rejected products is updated. Before a production order is closed a zero-balance calculation is documenting the history of good and bad parts of this order. This addresses the threats T.Unauthorised-Staff, T.Staff-Collusion and T.Accident-Change and the OSP P.Zero-Balance.

65 O.Reception-Control: When received, an inspection of intended TOE items is performed to acknowledge the amount items, their identification and the assignment –which process for instance-. This addresses the OSP P.Reception-Control.

8.4 Assurance Measure Rationale

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

8.4.1 O.Config_IT-env

67 ALC_CMC.5.1C requires that the CM documentation show that a process is in place to ensure an appropriate and consistent labeling. ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items. ALC_CMC.5.6C requires that the CM system supports the production of the product by automated means. ALC_CMC.5.8C requires that the CM system clearly identifies the configuration items that comprise the TSF. ALC_CMC.5.9C requires that the CM system supports the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail. ALC_CMC.5.10C requires that the CM system provides an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.11C requires that the CM system is able to identify the version of the implementation representation from which the TOE is generated. ALC_CMC.5.16C requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system.

68 All these content elements of the SAR define required properties of the used configuration management system. Thereby this SAR is suitable to meet the security objective. Because the ALC_TAT requirement is not applicable for this site (see section 7.1.6 for the reason), the corresponding SAR content elements are not referenced.

8.4.2 O.LifeCycle-Doc

69 ALC_CMC.5.1C requires that the CM documentation show that a process is in place to ensure an appropriate and consistent labeling. ALC_CMC.5.2C requires that the CM documentation describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires that the CM documentation justifies that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items. ALC_CMC.5.6C requires that the CM system supports the production of the product by automated means. ALC_CMC.5.7C requires that the CM system ensures that the person responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.8C requires that the CM system clearly identifies the configuration items that comprise the TSF. ALC_CMC.5.9C requires that the CM system supports the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail. ALC_CMC.5.10C requires that the CM system provides an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.11C requires that the CM system is able to identify the version of the implementation representation from which the TOE is generated. ALC_CMC.5.12C requires that the CM documentation includes a CM plan. ALC_CMC.5.13C requires that the CM plan

describes how the CM system is used for the development of the TOE. ALC_CMC.5.14C requires that the CM plan describe the procedures used to accept modified or newly created configuration items as part of the TOE. ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system. ALC_CMS.5.1C requires that the CL includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan. ALC_CMS.5.2C requires that the CL uniquely identify the configuration items. ALC_CMS.5.3C requires that for each configuration item, the configuration list indicates the developer/subcontractor of the item.

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

71 ALC_DVS.2.2C requires that the development security documentation justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

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

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

74 All these content elements of the mentioned SARs require dedicated content of the CM documentation and the configuration list, properties of the SM system, content of the development security documentation and of the life-cycle documentation. Thereby these SARs are suitable to meet the security objective. Because the ALC_TAT requirement is not applicable for this site (see section 7.1.6 for the reason), the corresponding SAR content elements are not referenced.

8.4.3 O.Reception-Control

75 ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labeling of the products.

76 All these content elements of the mentioned SARs require dedicated content of the reception control operation. Thereby these SARs are suitable to meet the security objective.

8.4.4 O.Physical-Access

77 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

8.4.5 O.Security-Control

78 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

8.4.6 O.Alarm-Response

79 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

8.4.7 O.Internal-Monitor

80 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective..

8.4.8 O.Maintain-Security

81 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

8.4.9 O.Network-separation

82 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

8.4.10 O.Logical-Operation

83 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

8.4.11 O.Control-Scrap

84 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

8.4.12 O.Staff-Engagement

85 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

8.4.13 O.Zero-Balance

86 ALC_CMC.5.6C requires that the CM system supports the production of the product by automated means. ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

8.4.14 O.Internal-Shipment

87 ALC_DVS.2.1C requires that the development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment. Thereby this SAR is suitable to meet the security objective.

8.5 Mapping of the Evaluation Documentation

88 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 Mougins.

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 – NPI 3.0 Handbook, slide on Configuration management • Configuration Management References and Templates
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	All items can be uniquely identified by the version control system, which is owned by CCC&S. Documents can be uniquely identified using the labeling described above. Configuration Items are identified via the identifiers that are automatically provided by the system as well as the	• NXPOMS-999116894-3989 - NPI3.0 Handbook, slide on Configuration management • Configuration Management References and Templates

SAR	Aspects	Reference
	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 *intended* TOE by automated means.	The above-mentioned tools support the development of the intended TOE by automated means.	• NXPOMS-999116894-3989 - NPI3.0 Handbook, slide on Configuration management • Configuration Management References and Templates • NXPOMS-1719007347-2657 CM – Design Environment Maintenance • CollabNet TeamForge – User Guide

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 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 *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

SAR	Aspects	Reference
		• Product specific configuration management plan (CMP) available.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the *intended* TOE.	The development environment used is set up centrally as per the Release Manual and a project specific CM plan.	• Configuration Management Procedure • Product specific configuration management plan (CMP) available.
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *intended* TOE.	The development environment used is set up centrally as per the Release Manual and a project specific CM plan. Documents are handled centrally after creation by the Documentation Officer.	• NXPOMS-999116894-3989 - NPI3.0 Handbook, slides referring to change control board, CCB process • Configuration Management Procedure • Product specific configuration management plan (CMP) available.
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	The development environment used is set up centrally as per the Release Manual and a project specific CM plan. Documents are stored in project vaults. Evidences can be provided during a site visit	• The development environment used is set up centrally and organized as per a project specific CM plan • NXPOMS-999116894-3989 - NPI3.0 Handbook, slides referring to the configuration management • Product specific configuration management plan (CMP) available.
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	The development environment used is set up centrally as per the Release Manual and a project specific CM plan. Documents are stored in project vaults. Evidences can be provided during a site visit	• The development environment used is set up centrally and organized as per a project specific CM plan • Configuration Management Procedure

Table 7 Mapping of the Evidence for the Configuration Management Capabilities

SAR	Aspects	Reference
ALC_CMS.5.1C: The configuration list shall include the following: the *intended*	In terms of site certification on the one hand the configuration list is provided in form of the	• SST • Document list/Bibliography

SAR	Aspects	Reference
TOE itself; the evaluation evidence required by the SARs; the parts that comprise the *intended* TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.	tables at hand. On the other hand, the configuration list is represented by the list of all applicable documents.	
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

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 wings, surveillance, alarm system and on campus guard services to prevent access to the wings for unauthorized persons.	• NXPOMS-1719007347-639 Site Security Manual - NXP Semiconductors Mougins , chapter 4
	Visitors, external suppliers and cleaning personnel handling	• NXPOMS-1719007347-639 Site Security Manual - NXP Semiconductors Mougins , section 6.1

SAR	Aspects	Reference
	Handling of physical objects, zero balancing, disposal of security products	• NXPOMS-1719007347-639 Site Security Manual - NXP Semiconductors Mougins , section 6.2
	Trustworthiness and training of staff	• NXPOMS-1719007347-639 Site Security Manual - NXP Semiconductors Mougins , section 6.4
	Physical security system: operation, emergency procedures, incident handling and reporting	• NXPOMS-1719007347-639 Security Manual - NXP Semiconductors Mougins , section 7
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *intended* TOE.	The justification is provided in this security target because it shows that all threats are addressed by the measures. In addition the measures are monitored to control the effectiveness.	• Chapter 8 of this document

Table 9 Mapping of the Evidence for the Development Security

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

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

89 The evidence in the tables above is mapped according to the main purpose and content of the referenced documents. Nevertheless, the procedures support each other. Especially the physical and technical security measures as well as the organizational security measures including maintenance of security measures supplement each other. Also, the control during development assures the configuration management and support the personal accountability

and tracing of the sources. The table above shows that all aspects of the assurance components are covered by the implemented procedures.

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 Requirements; Version 3.1, Revision 5,“ April 2017.

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

[5] JIL, Minimum Site Security Requirements, Version 2.2, April 2019.

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

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

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. Note that in this special case the client is always NXP BU S&C, to which the site also belongs to.

9.3 List of Abbreviations

CC	Common Criteria
CI	Configuration Item
CL	Configuration List
CM	Configuration Management
EAL	Evaluation Assurance Level
IC	Integrated Circuit
IP	Intellectual Property
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation