Table of Contents

Table of Figures

Publication Summary

Reference Number (OMS-ID)	NXPOMS-
Reference Title	Site Security Target Lite Digital Reality
Publisher	NXP BLs
Classification	Public
Author	Antoinette Dickens
Owner	Monique Franssen

Objectives / Purpose

See Chapter 2

Scope

This document is applicable to the following organisation(s): Chandler; BL Microcontrollers; BL Secure Interface and Power; BL Secure Transactions and Identification; BL Radio Power Solutions

This page was left free intentionally!

1. Document Introduction

1.1 Reference

Title:	Site Security Target Lite Digital Reality
Version:	1.2
Date:	1/25/2019
Company:	Digital Reality
Name of site:	Digital Realty, 120 East Van Buren St, Phoenix, AZ 85004 United States
EAL:	SARs taken from EAL6

2. SST Introduction

1 The chapters 1 to 7 of this document is based upon the Eurosmart Site Security Target Template [1] with adaptions such that it fits the site (i.e. development site, testing of software, no production, no direct delivery to customers of the user of the site).

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

* Note that the site of this Site Security Target also belongs to NXP BU S&C.

2.1 SST Reference

2 Title Site Security Target Lite Digital Reality

3 Version 1.2

2.2 Site Reference

4 The site belongs to NXP Semiconductors and is located at:

Digital Realty, 120 East Van Buren St, Phoenix, AZ 85004 United States

2.3 Site Description

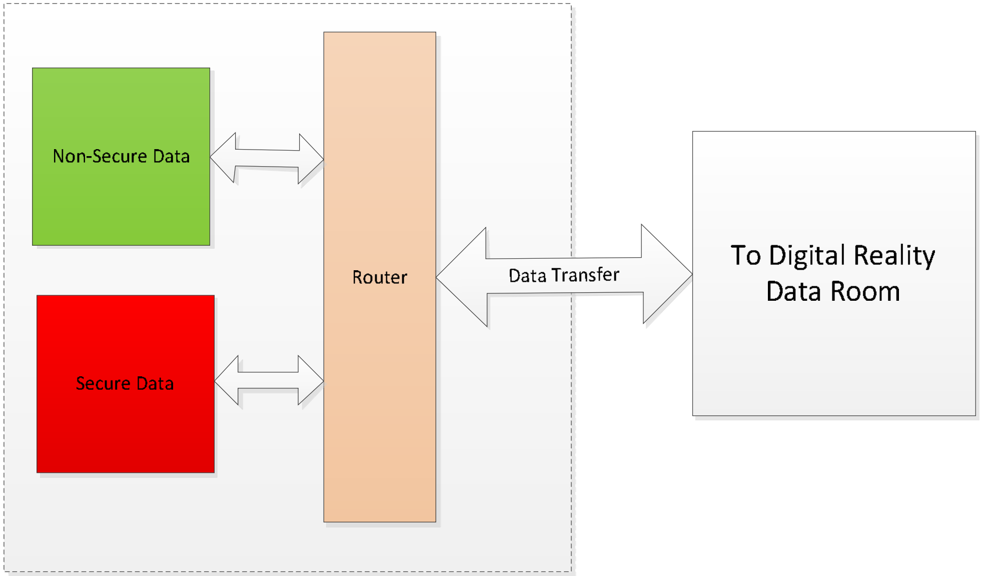
5 The entire Digital Reality building specified in Section 2.2 is in the scope of the SST. The surroundings of this building are not in the scope of the SST. Therefore, the walls of this building form the physical boundary of the site.

6 The Digital Reality building supports activities of many organisations, but only the NXP activities that take place in the NXP Cage are in the scope of this SST. Activities of other organisations are not in scope of this SST.

7 The NXP Secure Cage contains the following services:

Security-relevant services within scope: secured remote access to servers.

- Note that this server will be used (e.g. for data storage) in relation with designing, testing, producing, shipping etc. of security-related NXP products of a Business Unit of NXP. The secured remote access to servers is the subject of this certification.



8 The security-relevant system is only connected with other systems through VPN router provided by and remotely managed by the NXP Business Unit to whom the data belongs. The only connection to the outside world is protected through so that no unencrypted content is leaving the Security Relevant System. Only the NXP Business unit has the keys to encrypt/decrypt this is never performed on the Digital Reality Phoenix site.

9 The only activities that are actually physically performed in the cage are the installation, repair, removal and maintenance of the hardware constituting the systems and the backup of the security non-relevant system data on tapes. The backup of the security-relevant system data is done over the network by the NXP Business Unit.

10 All logical activities in the cage are performed remotely. Example: an NXP employee in e.g. Glasgow performs some design work on a security IC: the actual work is done in Glasgow, but logically and physically in the Cage.

11 The only personnel with physical access to the Cage is NXP personnel or authorized subcontractors. They perform only the physical activities listed earlier. This personnel is therefore not directly involved in designing, testing, producing, shipping etc. of NXP products.

12 However, as the site physically hosts electronic assets of NXP Business Units, confidentiality and integrity-related threats exist to these assets on this site. It is these threats that are the main subject of this Site Certification.

13 For smartcard products, the site activities can be related to Phases 1 to 6 of the Lifecycle Model in [7], depending on the roles that an NXP Business Unit that uses this Site has in these Phases.

14 The activities are: Security IC Embedded Software Development (Phase 1), IC Embedded Software and Testing (Phase 1), IC Design (Phase 2), IC Manufacturing (Phase 3), IC Packaging (Phase 4), Composite Product Integration (Phase 5), Personalisation (Phase 6), IC Dedicated Software and Testing (Phase 1) as defined in 'Security IC Platform Protection Profile' (PP-0035) and 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084)

15 The activities (and areas where they are performed) are:

Activity	Area
Data Centre	NXP Secure cage in Digital Reality - Phoenix DC

16 The typical Life Cycle model for Smart Cards usually comprises the following phases:

- Development,
- Production,
- Delivery,
- Preparation,
- Operation,

17 Whereas the site under evaluation supports only the life cycle phase

- Operation (IT Data Host)

3. Conformance Claim

18 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, 5, April 2017, [3]

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

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

- Minimum Site Security Requirement V2.1 December 2017 [6]

20 This SST is CC Part 3 conformant.

21 There are no extended components required for this SST for the Digital Reality Site.

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

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

23 The activities of the site are not directly related to designing, testing, producing, shipping etc. of secure products. Therefore, this site does not claim conformance to ALC_DEL, ALC_TAT and ALC_LCD

4. Security Problem Definition

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

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

4.1 Assets

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

- Electronic files on the security-relevant system in the Cage. Some of these files are relevant to secure products belonging to NXP Business Units and as such are protected.

4.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of assets (1) In this case development data with the intention to violate confidentiality and possibly integrity

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

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

T.Unauthorised-Staff: Employees or subcontractors not authorized to get access to assets by violating (1) In this case development data with the intention to violate confidentiality and possibly integrity

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 electronic files with the intention to violate confidentiality and possibly integrity

4.3 Organizational Security Policies

P.Config-Items: The configuration management system shall be able to uniquely identify configuration items. In this case the unique identification of items is solely the IT hardware used for these services

P.Config-Process: The processes provided by this site are controlled and documented. This describes the services and/or processes provided by a site.

4.4 Assumptions

A.Serv-Specification: The NXP Business Unit that is being managed must store data it wishes to keep secure on the Security-Relevant System in the Cage.

A.Secure_Conn NXP must arrange an encrypted network connection from the Security-Relevant System to its network.

The site is not intended for TOE development. Therefore the only configuration items are internal site security documents and procedures.

5. Security Objectives

27 The Security Objectives are related to physical IT infrastructure and organizational security measures.

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

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

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.Control-Scrap: The site will return any scrap to NXP; in this case the only possible scrap would be faulty hardware, but this is only handled by NXP or authorized subcontractors.

O.Staff-Engagement: All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job. All contractors and visitors must be escorted by a trained employee at all times.

O.Config-Items: NXP has a configuration management system that assigns a unique internal identification to each equipment installed in cage and their corresponding setting to each version of the internal procedures and guidance. This help ensure P.Config_Items and P.Config_Process

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

O.Exclusive-Access: The only way to access the Security-Relevant System from the NXP Business Unit network is through the encryption equipment provided by the NXP Business Unit[1] (and vice versa).

[1] See A.Secure_Conn

5.1 Security Objectives Rationale

28 The SST includes a Security Objective Rationale with two parts. The first part includes the tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part includes a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives (see column “Rationale” of table 1

Threat and OSP	Security Objective(s)	Rationale
T.Smart-Theft	O.Physical-Access O.Control-Scrap O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	O.Physical-Access ensures that the Secure Room is physically partitioned off, so that a burglar cannot just walk in. O.Control-Scrap ensures that scrap material cannot be accessed by an authorized party O.Security-Control ensures that an attacker will be detected when trying to reach the assets through the Secure Room O.Alarm-Response supports O.Physical_Access and O.Security_Control by ensuring that a response will be given to the alarm systems and that this response is quick enough to prevent access to the assets. O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T.Smart_Theft

T.Rugged-Theft	O.Physical-Access O.Control-Scrap O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	O.Physical-Access ensures that the Secure Room is physically partitioned off, so that a burglar cannot just walk in. O.Control-Scrap ensures that scrap material cannot be accessed by an authorized party O.Security-Control ensures that an attacker will be detected when trying to reach the assets through the Secure Room O.Alarm-Response supports O.Physical_Access and O.Security_Control by ensuring that a response will be given to the alarm systems and that this response is quick enough to prevent access to the assets. O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T.Rugged_Theft

T.Computer-Net	O.Exclusive-Access O.Logical-Operation O.Internal-Monitor O.Maintain-Security O.Control-Scrap O.Staff-Engagement O.Security-Control	O.Exclusive-Access ensures that all communication between the Secure Room and the Business Unit is done through encryption equipment (provided by the Business Unit). The attacker can therefore neither: • Listen in on or manipulate the network connection between the Secure Room and the Business Unit • Penetrate the Secure Room management stations through this connection The attacker also cannot use other networks that lead into the Secure Room as O.Exclusive-Access also ensures that all such connections are not connected to the encryption equipment. In addition, O.Logical-Operation ensures that all computer systems used to manage the Business Unit network are kept up to date (software updates, security patches, virus and spyware protection) O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. O.Control-Scrap ensures that scrap material cannot be accessed by an authorized party O.Staff-Engagement ensures that all staff is aware of its reponsibilities (signing NDAs, and being trained). O.Security-Control ensures that an attacker will be detected when trying to reach the assets through the Secure Room Together, these objectives will therefore counter T.Computer-Net.

T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Operation O.Internal-Monitor O.Maintain-Security O.Control-Scrap O.Staff-Engagement O.Config-Items	O.Security_Control ensures that all unauthorized people who have a legitimate need to visit the Secure Room are always accompanied. O.Physical-Access, O.Security-Control and O.Alarm-Response ensures that the unauthorized people cannot circumvent this (see the rationale for T.Smart-Theft for more details on this) In addition, O.Logical-Operation ensures that all computer systems used to manage the Business Unit network are kept up to date (software updates, security patches, virus and spyware protection O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. O.Control-Scrap ensures that scrap material cannot be accessed by an authorized party O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Config-Items assigns unique numbers to the internal procedures. As the site processes no other configuration items. Together, these objectives will therefore counter T.Unauthorised-Staff.
T.Staff-Collusion	O.Physical-Access O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Control-Scrap	O.Physical-Access, ensures that the unauthorized people cannot circumvent this (see the rationale for T.Smart-Theft for more details on this) O.Staff-Engagement ensures that all staff is aware of its reponsibilities (signing NDAs, and being trained). O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. O.Control-Scrap ensures that scrap material cannot be accessed by an authorized party. Together, these objectives will therefore counter T.Staff-Collusion.

P.Config-Items	O.Config-Items O.Physical-Access	The Security Objective directly enforces the OSP. O.Physical-Access ensures that unauthorized people cannot circumvent this (see the rationale for T.Smart-Theft for more details on this) O.Config-Items assigns unique numbers to the internal procedures. As the site processes no other configuration items, this is sufficient to meet P.Config-Items.
P.Config-Process	O.Config-Items O.Physical-Access	The Security Objective directly enforces the OSP. O.Physical-Access ensures that unauthorized people cannot circumvent this (see the rationale for T.Smart-Theft for more details on this) The services and processes provided by the site are described in the internal site procedures and guidance. O.Config-Items as are kept under CM (see the rationale above), this is sufficient to meet P.Config-Process.

Table 1 Threats and OSP - Security Objectives Rationale

6. Extended Assurance Components Definition

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

7. Security Assurance Requirements

30 Digital Reality using this Site Security Target requires a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profile [7].

31 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)

32 Because hierarchically higher components are used in this SST the Security Assurance Requirements listed above fulfil the requirements of:

- [6] ‘Minimum Site Security Requirements’

- [7] Eurosmart Protection Profile.

7.1 Application Notes and Refinements

33 The description of the site certification process 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)

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

35 As the scope of the configuration management system is rather limited (see section 7.1.2), the configuration management system only needs to keep a few documents under CM.

36 Items like wafers, dice, products, etc. are not in scope.

37 Items like source code and design information are considered electronic files therefore are in scope. The CM system is therefore relatively simple.

38 Due to the nature of the site, the refinements on ALC_CMC from [5] are not necessary, however the configuration management system of the Data Centre controlling activities will be in scope.

7.1.2 CM Scope (ALC_CMS.5)

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

40 The scope of the configuration management for a site certification process is limited to the documentation relevant for the SAR for the claimed life-cycle SAR and the configuration items handled at the site.

41 As this site is not directly involved with designing, testing, producing, storing or delivering the TOE, the only relevant configuration items are:

- This Site Security Target for this site
- The CM documentation for this site
- The Security documentation for this site

42 Due to the nature of the site, the refinements on ALC_CMS from [5] are not necessary, however the configuration management system of the Data Centre controlling activities will be in scope.

7.1.3 Development Security (ALC_DVS.2)

43 Refer to subsection ‘Application Notes for Site Certification’ in 5.4 ‘Application Notes for ALC_DVS’.

44 As ALC_DVS is relatively broad, and the security objectives are more specific, the following refinements are applied to ensure that ALC_DVS.2 will meet the objectives:

- 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.
- Assigned personnel of the site operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. This personnel are also responsible for registering and ensuring escort of visitors, unauthorised NXP employees, contractors and suppliers.
- 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 or guards is short enough to prevent a successful attack.

- 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.

- 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.

- The only way to access the Business Unit network is through management workstations connected to the encryption equipment provided by the Business Unit[2]. There is no internal network access to the encryption equipment.

- The computer systems in the Secure Room that are connected to the encryption equipment are kept up-to-date (software updates, security patches, virus protection, spyware protection).

- The Secure Room has measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive configuration items so that they do not support an attacker.

- 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.

7.1.4 Life-cycle Definition (ALC_LCD.1)

45 Refer to subsection ‘Application Notes for Site Certification’ in 5.6 ‘Application Notes for ALC_LCD’.

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

47 Not applicable

7.1.5 Tools and Techniques (ALC_TAT.3)

48 Refer to subsection ‘Application Notes for Site Certification’ in 5.7 ‘Application Notes for ALC_TAT’.

49 Not applicable

[2] See A.Secure_Conn.

7.2 Security Requirements Rationale

7.2.1 Security Requirements Rationale - Dependencies

50 The dependencies for the assurance requirements are as follows:

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

Assurance Family	Dependencies	Rationale
ALC_CMC.5	ALC_CMS.1 ALC_DVS.2 ALC_LCD.1	All included except ALC_LCD.1. ALC_LCD.1 is not included as it is related to development where this site is not involved in development.
ALC_CMS.5	No dependencies	N/a, no dependencies
ALC_DVS.2	No dependencies	N/a, no dependencies

As there is no processing on this site the Configuration Management of the TOE is controlled on other NXP sites. Data is never decrypted or worked on in the Digital Reality site.

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_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-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.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items

SAR	Security Objective	Rationale
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.6C: The CM system shall support the production of the product by automated means.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
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.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.8C: The CM system shall clearly identify the configuration items that comprise the TSF.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.10C: The CM system shall provide an automated means to	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in

SAR	Security Objective	Rationale
identify all other configuration items that are affected by the change of a given configuration item.		ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.16C: The evidence shall demonstrate that all configuration items have been and are	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet

SAR	Security Objective	Rationale
being maintained under the CM system.		O.Config-Items

Table 2 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMS.5.1C: The configuration list 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.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items

Table 3 Rationale for ALC_CMS.5

SAR	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall	O.Physical-Access O.Security-Control O.Alarm-Response	The security documentation (O.Physical-Access,

SAR	Security Objective	Rationale
describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	O.Internal-Monitor O.Maintain-Security O.Exclusive-Acccess O.Control-Scrap O.Staff-Engagement O.Logical-Operation	O.Security-Control, O.Logical-Operation, O.Alarm-Response), procedural (O.Internal-Monitor, O.Maintain-Security, O.Control-Scrap), personnel (O.Staff-Engagement), and technical (O.Exclusive-Access) enforce the security on site.
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Exclusive-Acccess O.Control-Scrap O.Staff-Engagement O.Logical-Operation	The security documentation (O.Physical-Access, O.Security-Control, O.Logical-Operation, O.Alarm-Response), procedural (O.Internal-Monitor, O.Maintain-Security, O.Control-Scrap), personnel (O.Staff-Engagement), and technical (O.Exclusive-Access) enforce the security on site
ALC_DVS.2.3C: The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Exclusive-Acccess O.Control-Scrap O.Staff-Engagement O.Logical-Operation	The security documentation (O.Physical-Access, O.Security-Control, O.Logical-Operation, O.Alarm-Response), procedural (O.Internal-Monitor, O.Maintain-Security, O.Control-Scrap), personnel (O.Staff-Engagement), and technical (O.Exclusive-Access) enforce the security on site

Table 4 Rationale for ALC_DVS.2

8. Site Summary Specification

8.1 Preconditions required by the Site

51 There are two preconditions that must be fulfilled in order to make use of the Site :

- The NXP Business Unit must store data on the Security-Relevant System in the cage. Backup of this data over the network connection (see below) must be arranged by the NXP Business Unit, as the Security-Relevant System does not provide this.
- The NXP Business Unit must arrange an encrypted network connection from the Security-Relevant System to its network. This includes the provisioning of robust network encryption equipment to the Cage, key management for this equipment etc.

8.2 Services of the Site

52 The Cage provides data storage and provision of remote access to data that may be related to designing, testing, producing, shipping etc. of security-related NXP products of a Business Unit of NXP, such as NXP BU S&C

8.2.1 Aspects of SARs

8.2.1.1 ALC_CMC.5 and ALC_CMS.5

53 As defined in [5], para 85-86: If the site does not provide configuration items to outside the site, nor accepts configuration items from outside the site, no information is to be provided in relation to TOEs.

8.2.1.2 ALC_DVS.2

54 All information provided to and from the Security-Relevant System towards any other NXP sites will be encrypted and provided by the NXP Business Unit requiring services from the site (see A.Secure_Conn for details). All other information is internal to the site, and does not need to be provided as defined in [5], (para 87).

- 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.
- Assigned personnel of the site operate the systems for access control and surveillance and respond to alarms. Technical security measures like video

control, motion sensors and similar kind of sensors support the enforcement of the access control. This personnel are also responsible for registering and ensuring escort of visitors, unauthorised NXP employees, contractors and suppliers.

- 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 or guards is short enough to prevent a successful attack.

- 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.

- 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.

- The Cage has measures in place to erase electronic media so that they do not support an attacker.

- 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.

8.3 Security Assurance Rationale

8.3.1 CM capabilities (ALC_CMC.5)

55 For full detail and evidences please view Section 7.2.2

8.3.2 CM scope (ALC_CMS.5)

56 For full detail and evidences please view Section 7.2.2

8.3.3 Development Security (ALC_DVS.2)

57 For full detail and evidences please view Section 7.2.2

8.4 Objectives Rationale

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

8.4.1 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, and 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.Staff-Collusion and T.Unauthorized-Staff is addressed. Also addresses the OSP P.Config_Items and P.Config_Process.

8.4.2 O.Security-Control

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

60 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 and T.Computer_Net are addressed.

8.4.3 O.Alarm-Response

61 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.

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

8.4.4 O.Internal-Monitor

63 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.

64 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.

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

8.4.5 O.Staff-Engagement

66 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 includes 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.

67 This addresses the threats T.Computer-Net, T.Staff-Collusion and T.Unauthorised-Staff

8.4.6 O.Control-Scrap

68 Scrap may exist in several forms on this site including redundant hardware and/or movable media. Hardware scrap is returned to the NXP head office for controlled secure destruction. Transport and actual destruction of security products is done under the 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 by NXP.

69 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

8.4.7 O.Maintain_Security

70 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

71 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

8.4.8 O.Exclusive-Access

72 Access to the secure cage from and to the outside is using encrypted links provided by the BUs.This addresses the threat T.Computer-Net.

8.4.9 O.Logical-Operation

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

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

8.4.10 O.Config_Items

75 All product configuration information is stored in the database on the NXP secure network. The information stored is encrypted data.

76 This is addressing the threat T.Unauthorised-Staff, and the OSP P.Config-Items and P.Config_Process.

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, Part3: Security Assurance Requirements; Version 3.1, Revision 5," April 2012.

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

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

[6] Minimum Site Security Requirement V2.1 December 2017

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

9.2 List of Abbreviations

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

9.3 Version History

Version	Date	Comment
V1.0	19 Jul 2016	first release
V1.1	23 Jan 2019	2019 Update
V1.2 (released)	25 Jan 2019	Conversion to New Template