HCL Gothenburg for NXP Site Security Target Lite

Version 1.0

13.12.2017

Table of Contents

1 Document Information

1.1 Reference

Title:	HCL Gothenburg for NXP Site Security Target Lite
SST Reference	HCL Gothenburg SST Lite ref 1.0_131217
Version:	Version 1.0
Date:	13.12.2017
Company:	HCL
Name of the site:	HCL for NXP
Product type:	Any
Assurance-Level:	EAL6 assurance components: • ALC_CMC.5 • ALC_CMS.5 • ALC_DVS.2 at AVA_VAN.5 level

1.2 Version History

Version	Date	Comment/Editor/Changes
0.1	08.12.2017	First draft
1.0	13.12.2017	Release

Name	Function	Date approved
Christophe Bouly	NXP Security Manager	13/12/2017

2 SST Introduction

1 This Site Security Target (**HCL Gothenburg for NXP Site Security Target Lite**, **Version 1.0**) refers to the site **HCL for NXP**. As the site carries out IT systems management activities for NXP as a whole, and these are not directly related to a specific product type, this site is suitable for any type of NXP security product.

2.1 Identification of the Site

2 The site HCL for NXP is located at:

HCL DA

Gunnar Engellaur väg 3

Gothenburg 418 78

Sweden

3 The building is completely used by HCL. The area where the relevant activities take place is limited to a single room within this building: **room DAVB-S**. In the remainder of this SST, this room is referred to as the Secure Room.

4 The building is rented by HCL. HCL provides a smartcard-based access control system for physical access control. The location falls under the general HCL quality and security management system.

2.2 Site Description

5 The entire building specified in Section 2.1 is in the scope of the SST. The surrounding premises are not in the scope of the SST. Therefore the walls of the building form the physical boundary of the site.

6 Most of the site is involved in 3rd party IT Engineering & Support. The Secure Room provides 2nd and 3rd line IT support to NXP Business Units, such as the NXP Business Security & Connectivity (BU S&C). This consists of activities such as:

- Adding file storage space to existing NXP accounts
- Remote installation of Operating Systems
- General IT setup and maintenance (network and users' equipment)
- Remote installation of software upgrades and patches
- Making changes in user accounts
- Implementing requests from the NXP Change Control Board
- Resolving problems and responding to incidents

7 The personnel in the Secure Room are therefore **not** directly involved in designing, testing, producing, shipping etc. of NXP products. Therefore there are **no assets** inside

the site. However, the personnel have root level access to the electronic assets of the Business Units they manage and the is could therefore lead to threats to these assets. It is these threats that are the main subject of this Site Certification.

8 For smartcard products, their activities could therefore be related to any or all of the seven Phases of the Lifecycle Model in [5], depending on the roles that a managed Business Unit has in these Phases.

3 Conformance Claim

9 The evaluation is based on Common Criteria Version 3.1, release 5

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

- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April [2]

10 This SST is CC part 3 conformant and there are no extended components required for this SST for the HCL for NXP site.

11 For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology; Version 3.1, Revision 5, April [3]

- Minimum Site Security Requirement V1.1 June 2013 [8]

12 The evaluation of the site comprises the following assurance components[1]:

13 ALC_CMC.5, ALC_CMS.5 and ALC_DVS.2

14 The assurance level chosen for the SST is compliant to the Protection Profile (PP) [5] and therefore suitable for Security ICs.

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

[1] 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

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

4.1 Assets

17 Access[2] and access rights[3] to electronic files belonging to NXP Business Units. Some of these files contain assets that are relevant to secure products. In particular:

- Development data: The site can give access to electronic development data in relation to developed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected.
- Cryptographic keys: The site can give access cryptographic keys used for NXP key usage. Both the integrity and the confidentiality of these electronic data must be protected.
- Production data: The site can give access to electronic production data in relation to developed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected.
- Account with specific rights: The site uses specific account which can give access to BU S&C assets descried before. The confidentiality of these accounts must be protected.

4.2 Threats

18 The following threats are considered:

T.Smart-Theft: An attacker tries to access the Secure Room to gain access to a particular NXP Business Unit network and thereby access to the assets on that network (1) In this case development data, (2) cryptographic keys with the intention to violate confidentiality and possibly integrity. 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. In addition the attacker may be able to use specific working clothes of the site to camouflage the intention.

T.Rugged-Burglary: An experienced thief with specialised equipment for burglary, who may be paid to perform the attack tries to access the Secure Room to gain access to a particular NXP Business Unit network and thereby access to the assets on that network(1) In this case development data, (2) cryptographic keys (3) account with specific rights with the intention to violate confidentiality and possibly integrity. The attacker has sufficient time to investigate the site outside the controlled boundary.

[2] That is: these files could be viewed, edited and/or deleted from the Secure Room. People from the Secure Room do not access these files.

[3] That is, the read/write/execute rights to these files could be altered from the Secure Room (e.g. to give somebody else access to them). People from the Secure Room do not change these access rights.

T.Staff-Collusion: An attacker may try bribing or extorting a Secure Room employee into giving him copies of assets or access to a particular NXP Business Unit network and thereby access to the assets on that network. (1) In this case development data (2) cryptographic keys (3) account with specific rights (4) production data with the intention to violate confidentiality and possibly integrity.

T.Unauthorized-Staff: Unauthorised employees or subcontractors try to access the Secure Room to gain access to a particular NXP Business Unit network and thereby access to the assets on that network (1) In this case development data (2) cryptographic keys (3) production data with the intention to violate confidentiality and possibly integrity.

T.Computer-Net: A hacker, with no physical access to the Secure Room, with substantial expertise, standard equipment, who may be paid to attempt to remotely access the network in the Secure Room and leverage this access to gain access to a particular NXP Business Unit network and thereby access to the assets on that network (1) In this case development data (2) cryptographic keys (3) account with specific rights (4) production data with the intention to violate confidentiality and possibly integrity

4.3 Organisational Security Policies

P.Config-Items: The configuration management system shall be able to uniquely identify configuration items[4]. This includes the unique identification of items that are created, generated, developed or used at a site as well.

P.Config-Process: The services and/or processes provided by a site are controlled in the configuration management plan. This comprises the documentation that describes the services and/or processes provided by a site.

4.4 Assumptions

A.Serv-Specification: The Business Unit that is being managed must provide appropriate information and means in order to allow the Secure Room to provide 2nd and 3rd line IT support to the Business Unit.

A.Secure_Conn The Business Unit that is being managed must arrange an encrypted network connection from the Secure Room to its network. This includes the provisioning of robust network encryption equipment to the Secure Room, key management for this equipment etc.

[4] The site is only intended for in IT Engineering & Generic Support and no TOE development. Therefore the only configuration items that are internal site security documents and procedures, IT hardware.

5 Security Objectives

The Security Objectives are related to physical, technical and organisational security measures, the configuration management.

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.

O.Security-Control: 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.

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 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.Exclusive-Access: The only way to access the Business Unit network is through management workstations connected to the encryption equipment provided by the Business Unit[5]. There is no internal network access to the encryption equipment.

O.Logical-Operation: 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).

[5] See A.Secure_Conn.

O.Control-Scrap: The site will return any scrap to NXP. In this case the only possible scrap would be faulty hardware that will be only handled by NXP or authorized NXP 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: The Secure Room has a configuration management system that assigns a unique internal identification to each version of the internal procedures and guidance. NXP has a configuration management system that assigns a unique internal identification to each equipment installed in cage.

5.1 Security Objectives Rationale

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	Rationale
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Control-Scrap O.Maintain-Security	O.Physical-Access ensures that the Secure Room is physically partitioned off, so that a burglar cannot just walk in. 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.Control_Scrap ensures that burglars are not aided by any sensitive data lying around O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T.Smart_Theft

Threat and OSP	Security Objective	Rationale
T.Rugged-Burglary	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Control_Scrap	O.Physical-Access ensures that the Secure Room is physically partitioned off, so that a burglar cannot just walk in. 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.Control_Scrap ensures that burglars are not aided by any sensitive data lying around O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T.Rugged_Burglary
T.Staff-Collusion	O.Staff-Engagement O.Internal-Monitor O.Maintain-Security	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. Together, these objectives will therefore counter T.Staff-Collusion.
T.Unauthorized-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Staff-engagement O.Config-Items	O.Security_Control ensures that all unauthorised 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 unauthorised people cannot circumvent this (see the rationale for T.Smart-Theft for more details on this) O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. O.Staff-Engagement ensures that all staff is aware of its responsibilities (not providing access without sufficient authorisation). O.Config-Items assigns unique numbers to the internal procedures and guidance. Together, these objectives will therefore counter T.Unauthorized-Staff.

Threat and OSP	Security Objective	Rationale
T.Computer-Net	O.Exclusive-Access O.Logical-Operation O.Internal-Monitor O.Maintain-Security O.Control_Scrap	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 attackers cannot obtain sensitive data that may come from the Secure Room. Together, these objectives will therefore counter T.Computer-Net.
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 and guidance. As the site processes no other configuration items, this is sufficient to meet P.Config-Items.

Threat and OSP	Security Objective	Rationale
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 processed provided by the site are described in the internal procedures and guidance. As these are kept under CM (see the rationale above), this is sufficient to meet P.Config-Process.

Table 5.1: Security Objectives Rationale

6 Extended Assurance Components Definition

19 There are no extended assurance components in this Site security target.

7 Security Assurance Requirements

20 Sites using this SST may require an evaluation against evaluation assurance level **EAL6**. Therefore, the Security Assurance Requirements are a superset of the SARs included in the Security IC Platform Protection Profile [5].

21 The Security Assurance Requirements (SARs) are:

Class ALC: Life-cycle support

CM capabilities (ALC_CMC.5)

CM scope (ALC_CMS.5)

Development security (ALC_DVS.2)

22 The Security Assurance Requirements listed above fulfil the requirements of [4] because all claimed assurance components are at least at the same hierarchical level.

7.1 Application Notes and Refinements

23 The description of the site certification process [4] includes specific application notes. The main item is that a product that is considered as intended TOE (i.e. any TOE type) is not available during the evaluation. Since the term “TOE” is not applicable in the SST the associated processes for the handling of products or “intended TOEs” are in the focus and described in this SST. These processes are subject of the evaluation of the site.

7.1.1 CM Capabilities (ALC_CMC.5)

24 Refer to subsection ‘Application Notes for Site Certification’ in [4] 5.1 ‘Application Notes for ALC_CMC’.

25 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.

26 Items like wafers, dice, products are not in scope. The CM system is therefore relatively simple.

27 Items like source code, design information are considered electronic files (development or production data) and are therefore in the scope.

28 Due to the nature of the site, the refinements on ALC_CMC from [5] are not applicable.

7.1.2 CM Scope (ALC_CMS.5)

29 Refer to subsection ‘Application Notes for Site Certification’ in [4] 5.2 ‘Application Notes for ALC_CMS’.

30 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.

31 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 Development Security documentation for this site

32 Due to the nature of the site, the refinements on ALC_CMS from [5] are not applicable.

7.1.3 Development Security (ALC_DVS.2)

33 Refer to subsection 'Application Notes for Site Certification' in [4] 5.4 'Application Notes for ALC_DVS'.

34 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 Unit7. 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).**

- **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.**

7.2 Security Requirements Rationale

7.2.1 Security Requirements Rationale - Dependencies

35 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.

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	O.Config_items	O.Config-Items also states that NXP uses a configuration management system. This is included in ALC_CMC.5.

SAR	Security Objective	Rationale
ensure an appropriate and consistent labeling.		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
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

SAR	Security Objective	Rationale
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	O.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 identify all other configuration items that are affected by the change of a given configuration 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
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

SAR	Security Objective	Rationale
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 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

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 has the internal procedures and guidance under CM. This is a subset of the CM list specified by ALC_CMS.5 (which also includes the SST).
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config_items	O.Config-Items also states that NXP has the internal procedures and guidance under CM. This is a subset of the CM list specified by ALC_CMS.5 (which also includes the SST).
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 has the internal procedures and guidance under CM. This is a subset of the CM list specified by ALC_CMS.5 (which also includes the SST).

Table 3 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 TOE design and implementation in its development environment.	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Exclusive-Access 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.2.2C: 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-Access 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-Access 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

SAR	Security Objective	Rationale
		(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

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

- The Business Unit that is being managed must provide appropriate information and means in order to allow the Secure Room to provide 2nd and 3rd line IT support to the Business Unit.
- The Business Unit that is being managed must arrange an encrypted network connection from the Secure Room to its network. This includes the provisioning of robust network encryption equipment to the Secure Room, key management for this equipment etc.

8.2 Services of the Site

37 The Secure Room provides 2nd and 3rd line IT support to NXP Business Units, such as the NXP Business Unit S&C (BUS&C). This consists of activities such as:

- Adding file storage space to existing NXP accounts
- Remote installation of Operating Systems
- General IT setup and maintenance
- Remote installation of software upgrades and patches
- Making changes in user accounts
- Implementing requests from the NXP Change Control Board
- Resolving problems and responding to incidents

8.2.1 Aspects of SARs

8.2.1.1 ALC_CMC.5 and ALC_CMS.5

38 As defined in [4], 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. Configuration Management of the Configuration Items used within the site only is described in [7] and [9].

8.2.1.2 ALC_DVS.2

39 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). This is described in detail in [6]. All other information is internal to the site, and does not need to be provided (para 87, [4]).

- 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.

- 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)

40 Configuration Management is described in [7], [9] and [10].

41 For full detail and evidences please view Section 7.2.2

8.3.2 CM scope (ALC_CMS.5)

42 Configuration Management is described in [7], [9] and [10].

43 For full detail and evidences please view Section 7.2.2

8.3.3 Development Security (ALC_DVS.2)

44 Development Security is described in [6].

45 For full detail and evidences please view Section 7.2.2

8.4 Objectives Rationale

46 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

47 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.

48 Thereby the threats T.Smart-Theft and T.Rugged-Burglary 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.Unauthorized-Staff is addressed. Also addresses the OSP P.Config_Items and P.Config_Process

8.4.2 O.Security-Control

49 The site is managed 24/7 but during office off hours the guard patrol the internal of the building and the alarm system is used to monitor the site with a dedicated in 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 office off-hours.

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

8.4.3 O.Alarm-Response

51 The site is managed 24/7 and the guards monitor 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.

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

8.4.4 O.Internal-Monitor

53 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.

54 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.

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

8.4.5 O.Staff-Engagement

56 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.

57 This addresses the threats T.Staff-Collusion and T.Unauthorised-Staff

8.4.6 O.Control-Scrap

58 Scrap may exist in a number of forms on this site redundant hardware/movable media. Hardware scrap is returned to NXP head office for controlled secure destruction. Transport and actual destruction of security products is done under supervision of a qualified employee in collaboration with the destructor.

59 Supported by O.Physical-Access and O.Staff-engagement this addresses the threats T.Computer-Net, T.Smart-Theft, T.Rugged-Burglary .

8.4.7 O.Maintain-Security

60 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 authorized 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

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

8.4.8 O.Exclusive-Access

62 Access to the secure cage from and to the outside is using encrypted links (CISCO equipments) provided by the BUs. This addresses the threat T.Computer-Net.

8.4.9 O.Logical-Operation

63 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.

64 This addresses the threats T.Computer-Net

8.4.10 O.Config_Items

65 All items configuration information is stored in colabnet on the NXP secure network. The information is under configuration management in a managed and restricted network.

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

9 References

9.1 Literature

[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] Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology; Version 3.1, Revision 5, April 2017

[4] Supporting Document, Site Certification, October 2007, Version 1.0, Revision 1, CCDB-2007-11-001

[5] Security IC Platform Protection Profile with Augmented packages, Version 1.0, Eurosmart, BSI-CC-PP-0084-2014

[6] [DVS] HCL Gothenburg BUS&C Secure Room DVS Ver 1.2 09-10-2017

[7] "BU S&C ALC-CM Common Criteria Documentation, NXPOMS-1719007347-2549".

[8] [MSSR] Minimum Site Security Requirement V1.1 June 2013

[9] BU S&C Configuration and Data Management Procedure, NXPOMS-1719007347-2524

[10] HCL Configuration List, Version 1.0

9.2 Definitions

None.

9.3 List of Abbreviations

CC	Common Criteria
BU S&C	Business Unit Security & Connectivity
EAL	Evaluation Assurance Level
IC	Integrated Circuit
IT	Information Technology
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation