PV3-00200

PV3-00200 Site Security Target Toppan Lite

Publication Summary

Reference Number (OMS-ID)	PV3-00200
Reference Title	PV3-00200 Site Security Target Toppan Lite
Publisher	Business Unit S&C
Classification	Company Public
Author	Gordon Caffrey
Owner	NXP Security
Archive Numbers	V1.0

Distribution of CONFIDENTIAL DOCUMENTS

The cover sheet of this document is published at the NXP internal websites: BU S&C – Security Procedures
Readers of this confidential document have to contact the author.

Revision History

Revision	Description	Author	Approval - Date
1.0	First Release	Gordon Caffrey	21 Mar 2017

Approvers

Sequence	Role	Name
Acceptance	Security Manager	Sylvain Bonfardin
Approval	Security Manager	Dirk Luetzelberger

Subscriber

Role	Name	Notification	PDF-file
n.a.	None, document not public		

Table of Contents

Table of Figures

1. Document Introduction

1.1 Reference

Title: PV3-00200 Site Security Target Toppan Lite

Version: 1.0

Date: 3/21/2017

Company: Toppan

Name of site: Toppan Round Rock, 400 Texas Ave, Round Rock, TX 78664, United States

EAL: SARs taken from EAL6

1.2 Version History

Version	**Date**	**Comment**
V1.0	21 Mar 2017	first release

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 belong to NXP BU S&C.

2.1 SST Reference

2 Title PV3-00200 Site Security Target Toppan Lite

3 Version 1.0

2.2 Site Reference

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

Toppan Round Rock, 400 Texas Ave, Round Rock, TX 78664, United States

2.3 Site Description

5 The entire Toppan building specified in Section 2.1 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 Toppan building supports activities of many other organisations, but only the secure NXP mask making activities are in the scope of this SST. Activities of other organisations are not in scope of this SST.

7 NXP will supply secure encrypted data to Toppan for the fracture and creation of secure masks.

8 All mask making processes, storage and shipping are under the complete control for Toppan.

9 No data will be stored in the Toppan site once the manufacturing process is complete.

10 For smartcard products, the site activities can be related to Phases 2 of the Lifecycle Model in [5].

11 The activities are: Photomask creation (Phase 2) as defined in ‘Security IC Platform Protection Profile’ (PP-0035) and ‘Security IC Platform Protection Profile with Augmentation Packages’ (PP-0084)

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

Activity	Area
Mask Maker	Toppan Round Rock Site

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

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

14 Only the **Production** phase is considered relevant for this certification.

3. Conformance Claim

15 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 4, September 2012, [2]

- Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, 4, September 2012, [3]

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

- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1, 4, September 2012, [4]

- Minimum Site Security Requirement V1.1 June 2013 [12]

17 This SST is CC Part 3 conformant.

18 There are no extended components required for this SST for the Toppan Site.

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

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

20 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.

4. Security Problem Definition

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

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

4.1 Assets

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

- Electronic files
- Photo Masks

NXP Development data: The site has access to electronic development data in relation to developed TOEs. Both the integrity and the confidentiality of this electronic data must be protected.

NXP Development tools: To perform its development activities the site uses tools to transform source code to usable data formats for mask making. The integrity of these tools must be protected.

NXP Physical security objects: The site has physical security objects e.g. photomasks in relation to developed TOEs. Both the integrity and the confidentiality of these must be protected.

4.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of assets (1) In this case development data with the intention to violate confidentiality and possibly integrity (2) Physical security objects in the form of masks (3) Development Tools in the form of mask making infrastructure hardware. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered.

T.Rugged-Theft: An attacker with specialized equipment for burglary, who may be paid to perform the attack, tries to access sensitive areas and manipulate or steal assets (1) In this case development data with the intention to violate confidentiality and possibly integrity (2) Physical security objects in the form of masks (3) Development Tools in the form of mask making infrastructure hardware.

T.Computer-Net: A possibly paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to (1) development data with the intention to violate confidentiality and possibly integrity (2) Physical security objects in the form of masks (3) Development Tools in the form of mask making infrastructure hardware.

T.Unauthorised-Staff: Employees or subcontractors not authorized to get access to assets by violating (1) In this case development data with the intention to violate confidentiality and possibly integrity (2) Physical security objects in the form of masks (3) Development Tools in the form of mask making infrastructure hardware.

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

T.Attack-Transport: An attacker tries to get access to shipped physical security objects when shipped in or out of the site with the intention to compromise confidentiality and/or integrity of the product design data, customer and/or consumer data like code and data.

4.3 Organizational Security Policies

P.LifeCycle-Doc: The site uses life cycle documentation that describes:

(1) Description of configuration management systems and their usage;
(2) A configuration items list;
(3) Site security;
(4) The Mask making process;
(5) The mask making tools.

P.Config_Activities: The activities of the site shall be performed in accordance with the life cycle documentation using the IT-environment (P.LifeCycle-Doc).

4.4 Assumptions

A.Inherit-secure-IT: The local IT equipment is connected to a secure IT-Infrastructure through a secure (encrypted) network connection. The local workstations, the secure IT-infrastructure and the secure connection to it will satisfy all relevant ALC requirements and are provided and managed by Toppan. The workstations are configured such that any assets are contained within the encrypted network.

A.Secure_Conn NXP have arranged an encrypted network connection for delivery of secure databases to Toppan. Toppan will receive and securely store encrypted data until required.

5. Security Objectives

24 The Security Objectives are related to physical, technical, and organizational security measures, the configuration management as well as the internal shipment and/or the external delivery.

O.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. Toppan 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 be responsible for any scrap. In this case the only possible scarp would be faulty hardware the contractor will wipe all data and re-work. In the case of a ROM mask this will be destroyed.

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: Toppan has a configuration management system that assigns a unique internal identification to all masks. This helps ensure P.Config_Activities.

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

5.1 Security Objectives Rationale

25 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 Areas are 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.Physical-Access O.Security-Control O.Logical-Operation O.Internal-Monitor O.Maintain-Security O.Control-Scrap O.Staff-Engagement O.Config-Items	O.Physical-Access ensures that the Secure Areas are physically partitioned off, so that the attacker also cannot use other networks that lead into the Secure Room as O.Physical-Access also ensures that all such connections are not connected to the encryption equipment. O.Security-Control ensures that an attacker will be detected when trying to reach the assets through the Secure Room In addition, O.Logical-Operation ensures that all computer systems used to manage the 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.Config-Items as are kept under CM (see the rationale above), this is sufficient to meet P.Config-Process. Together, these objectives will therefore counter T.Computer-Net.

T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Control-Scrap O.Staff-Engagement O.Logical-Operation O.Config-Items	O.Security_Control ensures that all unauthorized people who have a legitimate need to visit the Secure Areas 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) 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). In addition, O.Logical-Operation ensures that all computer systems used to manage the network are kept up to date (software updates, security patches, virus and spyware protection) O.Config-Items as are kept under CM (see the rationale above), this is sufficient to meet P.Config-Process. 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 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.

T.Attack-Transport	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Staff-Engagement	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) 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 reponsibilities (signing NDAs, and being trained).
P.LifeCycle-Doc	O.Config-Items	The Security Objective directly enforces the OSP. The lifecycle 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.LifeCycle-Doc
P.Config-Activities	O.Config-Items O.Physical-Access	The Security Objective directly enforces the OSP. 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-Activities and O.Physical_Access.

Table 1 Threats and OSP - Security Objectives Rationale

6. Extended Assurance Components Definition

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

7. Security Assurance Requirements

27 Toppan using this Site Security Target requires a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profile [5].

28 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)

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

- [12] 'Minimum Site Security Requirements'

- [5] Eurosmart Protection Profile.

7.1 Application Notes and Refinements

30 The description of the site certification process [6] includes specific application notes. The main item is that a product that is considered as intended TOE is not available during the evaluation. Since the term "TOE" is not applicable in the Site Security Target, the associated processes for the handling of products, or "intended TOEs" are in the scope of this Site Security Target and are described in this document. These processes are subject of the evaluation of the site.

7.1.1 CM Capabilities (ALC_CMC.5)

31 Refer to subsection 'Application Notes for Site Certification' in [6] 5.1 'Application Notes for ALC_CMC'.

32 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.

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

34 Items like design information and reticules are therefore in scope. The CM system is therefore relatively simple.

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

7.1.2 CM Scope (ALC_CMS.5)

36 Refer to subsection 'Application Notes for Site Certification' in [6] 5.2 'Application Notes for ALC_CMS'.

37 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.

38 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

39 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.

7.1.3 Development Security (ALC_DVS.2)

40 Refer to subsection 'Application Notes for Site Certification' in [6] 5.4 'Application Notes for ALC_DVS'.

41 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 Toppan 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 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

42 The dependencies for the assurance requirements are as follows:

- ALC_CMC.5: ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
- ALC_CMS.5: None
- ALC_DVS.2: None
- ALC_LCD.1: None
- ALC_TAT.3: ADV_IMP.1

43 Some of the dependencies are not (completely) fulfilled:

- ALC_LCD.1 is only partially fulfilled as the site does not represent the entire development environment. This is in-line with and further explained in [6] 5.1 ‘Application Notes for ALC_CMC’.

- ADV_IMP.1 is not fulfilled as there is no specific TOE. This is in-line with and further explained in [6] 5.7 ‘Application Notes for ALC_TAT’.

-

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

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	Appropriate and consistent labelling is ensured through the application (O.Config-Items) of the CM-Plan (O.Config-Items) and the use of the configuration management systems ().
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Config-Items	The method used to uniquely identify the configuration items is described in the CM-Plan (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	The adequate and appropriate acceptance procedures for configuration items are described in the CM-Plan (O.Config-Items).
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.Config-Items	Unique identification of all CIs is realized by performing the CM activities (O.Config-Items) in accordance with the CM-Plan (O.Config-Items) using the Configuration management systems ()
ALC_CMC.5.5C: The CM	O.Config-Items	The configuration management

SAR	Security Objective	Rationale
system shall provide automated measures such that only authorized changes are made to the configuration items.		systems () used (O.Config-Items) according to the CM-Plan (O.Config-Items) 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-Items	The software on the development computers () supports automated production of products when used (O.Config-Items) in accordance with the CM-Plan (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	As described in the CM-Plan (O.Config-Items) the activities performed (O.Config-Items) are such that the person responsible for accepting a configuration item into CM is not the person who developed it.
ALC_CMC.5.8C: The CM system shall clearly identify the configuration items that comprise the TSF.	O.Config-Items	The CM-Plan (O.Config-Items) identifies the configuration items that comprise the TSF possibly supported by the configuration management system ()
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	As described in the CM_Plan (O.Config-Items) the configuration management systems () 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-Items	As described in the CM_Plan (O.Config-Items) the configurations management system and software installed on the development workstations and servers () 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	O.Config-Items	As described in the CM_Plan (O.Config-Items) the configurations management system () identifies the version of

SAR	Security Objective	Rationale
representation from which the TOE is generated.		the implementation representation from which the TOE is generated through baselines.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.Config-Items	The life cycle documentation (O.Config-Items) includes a CM-Plan.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE.	O.Config-Items	The life cycle documentation (O.Config-Items) describes how the CM system is used for the development of the product.
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE	O.Config-Items	The acceptance procedures for modified or newly created configuration items are described in the CM-Plan (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	All configuration items are listed in the CI-list (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. 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	O.Config-Items	The life cycle documentation (O.Config-Items) includes a CM-

SAR	Security Objective	Rationale
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.		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.Config-Items	The CI-List (O.Config-Items) uniquely identifies the configurations items as described in the CM-Plan (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	The CI-List (O.Config-Items) indicates the developer/subcontractor for each configuration items as described in the CM-Plan (O.Config-Items).

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	O.Config-Items O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Operation O.Control-Scrap O.Staff-Engagement	The development security documentation (O.Config-Items) describes the physical (O.Physical-Access, O.Security-Control, O.Alarm-Response), procedural (O.Internal-Monitor, O.Maintain-Security, O.Control-Scrap), personnel

SAR	Security Objective	Rationale
confidentiality and integrity of the TOE design and implementation in its development environment.		(O.Staff-Engagement), and other O.Logical-Operation security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O.Config-Items	The development security documentation (O.Config-Items) justifies the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.
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.Config-Items O.Physical-Access O.Security-Control O.Internal-Monitor O.Maintain-Security O.Logical-Operation O.Control-Scrap O.Staff-Engagement	The development security documentation (O.Config-Items) describes the physical (O.Physical-Access, O.Security-Control), procedural (O.Internal-Monitor, O.Maintain-Security, O.Control-Scrap), personnel (O.Staff-Engagement), and other O.Logical-Operation security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its

SAR	Security Objective	Rationale
		development environment.

Table 4 Rationale for ALC_DVS.2

8. Site Summary Specification

8.1 Preconditions required by the Site

44 The site activities for Toppan are performed using IT infrastructure consisting of development workstations, servers and configuration management systems. All of these are provided, configured and maintained by the Toppan.

45 The Toppan IT infrastructure consists of local and remote equipment connected using an encrypted connection. Toppan IT provides, configures and maintains the local workstations and router (used for the encrypted connection) and all remote equipment such that they are secure. The workstations are configured such that any assets are contained within encrypted containers.

46 The site follows the development processes of NXP. Applicable policies and processes are documented and available.

8.2 Services of the Site

47 The site participates in the development of masks for NXP.

48 Delivery of encrypted secure databases

49 Creation of mask sets for NXP

50 Delivery of masks to NXP

8.3 Security Assurance Rationale

8.3.1 CM capabilities (ALC_CMC.5)

51 Configuration Management is described in [7].

52 For full detail and evidences please view Section 7.2.2

8.3.2 CM scope (ALC_CMS.5)

53 Configuration Management is described in [7].

54 For full detail and evidences please view Section 7.2.2

8.3.3 Development Security (ALC_DVS.2)

55 Development Security is described in [8].

56 For full detail and evidences please view Section 7.2.2

8.4 Objectives Rationale

57 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, T.Attack-Transport, T.Rugged-Theft and T.Computer_Net 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_activities

8.4.2 O.Security-Control

58 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.

59 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, T.Attack-Transport and T.Computer_Net are addressed.

8.4.3 O.Alarm-Response

60 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.

61 This addresses the threats T.Smart-Theft, T.Attack-Transport, T.Rugged-Theft and T.Unauthorised-Staff

8.4.4 O.Internal-Monitor

62 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.

63 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.

64 This addresses T.Smart-Theft, T.Attack-Transport, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion

8.4.5 O.Staff-Engagement

65 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.

66 This addresses the threats T.Computer-Net, T.Attack-Transport, T.Staff-Collusion and T.Unauthorised-Staff

8.4.6 O.Control-Scrap

67 All scarp may existing in the form of reticules will be returned to Toppan for destruction. Sensitive information and information storage media will be deleted as soon as the mask creation process is complete, there will be no back up data or storage.

68 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

69 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

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

8.4.8 O.Logical-Operation

71 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.

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

8.4.9 O.Config-Items

73 All product configuration information is stored in the database on the NXP secure network. The information stored is covering process specifications, acceptance test instructions and specifications, and test programs. Products are identified by unique customer part IDs with are linked to the unique ID numbers of the associated configuration items.

74 This is addressing the threat T.Unauthorised-Staff, T.Computer-Net and the OSP P.Config-Activities and P.LifeCycle-Doc

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 4," September 2012.

[3] Common Criteria, "Common Criteria for Information Technology Security Evaluation, Part3: Security Assurance Requirements; Version 3.1, Revision 4," September 2012.

[4] Common Criteria, "Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 4," September 2012.

[5] Security IC Platform Protection Profile with augmentation Version 1.0," Eurosmart, 13.01.2014.

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

[7] USUL-1000/AT1 - OE AND TP INSTRUCTION FOR NON-ITAR SECURE SWR ATTACHMENTS

[8] RRUL-3000 - ROUND ROCK SITE INFORMATION SECURITY INSTRUCTIONS

[9] RRUL-1000/AT2 - TPIRR DEFINED SECURE REQUIREMENTS

[10] USUL-0000 – SECURITY DOCUMENT

[11] GLIT-1000 - GLOBAL INFORMATION TECHNOLOGY EMPLOYEE MANUAL

[12] Minimum Site Security Requirement V1.1 June

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

[14] Toppan Configuration List

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