PV3-00202a

PV3-00202a Site Security Target Lite NXP Austin Fab

Publication Summary

Reference Number (OMS-ID)	PV3-00202
Reference Title	PV3-00202a Site Security Target Lite NXP Austin Fab
Publisher	Business Unit Identification
Classification	Company PUBLIC
Author	Gordon Caffrey
Owner	NXP Security
Archive Numbers	V1.0

Revision History

Revision	Description	Author	Approval - Date
1.0	First Draft	Gordon Caffrey	19 Apr 2017

Approvers

Sequence	Role	Name
Author	Security Manager	Gordon Caffrey
Acceptance	Security Manager	David Isaacson
Approval	Security Manager	David Case

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: PV3-00202a Site Security Target Lite NXP Austin Fab

Version: 1.0

Date: 4/19/2017

Company: NXP Semiconductors

Name of site: NXP Semiconductors 3501 Ed Bluestein Blvd, Austin, TX 78721, USA

EAL: SARs taken from EAL6

1.2 Version History

Version	Date	Comment
V1.0	22 Oct 2016	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 PV3-00202a Site Security Target Lite NXP Austin Fab

3 Version 1.0

2.2 Site Reference

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

NXP Semiconductors
3501 Ed Bluestein Blvd, Austin, TX 78721, USA

2.3 Site Description

5 The site is contained in Buildings which is a dedicated NXP site with all secure areas controlled by NXP.

6 This Fab area is a RED HS[1] (High Security) and exclusively occupied by NXP with restricted need to know access controlled by NXP for authorize personnel only. The site also has YELLOW areas which conform to well-defined NXP security levels.

7 The NXP Austin Fab adopts advanced 12-inch process technology to provide the optimal combination of processes for the manufacture of secure IC's. The site provides the services and/or processes covered in the scope of the site evaluation process as follows.

- Security mask management
- Security wafer manufacturing
- Security wafer management
- Warehouse mask/wafer scrap
- Secure Shipment

1 The terms NS, RS and HS are well defined security levels. Their definition can be found in the NXP internal document "PV3-00202 - Site Security Manual, Austin Fab" [8]

8 Within the secure areas, only authorized members of the manufacturing team are entitled to access sensitive information i.e. source code, confidential documentation, Masks, Wafers, etc

9 The activities are: IC Manufacturing (Phase 3) as defined in 'Security IC Platform Protection Profile' (PP-0035) and 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084)

10 To perform these activities the site uses the NXP BU S&C provided and manage the IT-infrastructure. Locally available IT equipment like workstations or VPN routers are also provided and managed by NXP BU S&C directly. The site works according to NXP BU S&C processes.

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

Activity	Area
Security mask management	NXP Secure Area
Security wafer manufacturing	NXP Secure Area
Security wafer management	NXP Secure Area
Secure scrap management	
Warehouse mask/wafer delivery	

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

- Production,
- Preparation,
- Operation,

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

- Production,
- Preparation,
- Operation,

14 Manufacture comprises of the creation of secure IC's from a delivered secure masks set.

15 Delivery comprises of the shipment of secure IC's in wafer form to and from NXP Semiconductors. All these processes remain within DVS and not DEL.

3. Conformance Claim

16 This SST is conformant with Common Criteria Version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, September 2012, [2]

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

17 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 [10]

18 This SST is CC Part 3 conformant.

19 There are no extended components required for this SST for the NXP Austin Fab Site.

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

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

21 The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profile [5] and is therefore suitable for the evaluation of software and Hardware design for Security ICs.

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

4. Security Problem Definition

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

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

4.1 Assets

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

Manufacturing tools: To perform its activities the site uses all tools expected in a Fab manufacturing process. The integrity of these tools (running on local or remote development systems) must be protected.

Physical security objects: The site has physical security objects (printed documents, engineering samples, masks, wafers, etc.) in relation to the 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 printed documentation or engineering samples (3) Development Tools in the form of IT 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 printed documentation or engineering samples (3) Development Tools in the form of IT infrastructure hardware.

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

(2) development computers with the intention to modify the development process.

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 printed documentation or engineering samples (3) Development Tools in the form of IT infrastructure hardware.

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

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

4.3 Organizational Security Policies

P.Config_IT-env: The site uses programs and servers in addition to configuration management systems for file versioning and problem tracking. For file versioning unique repositories shall be used to support proper management of multiple products and the site internal procedures and helps meet the objective of (O.Config_IT-env). The team members are instructed to use only project related IT equipment provided by NXP with the provided tools.

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

(1) Description of configuration management systems and their usage;
(2) A configuration items list;
(3) Site security;
(4) The development process;
(5) The development tools.
These help meet the objective of O.Lifecycle-Doc

P.Config_Activities: The activities of the site shall be performed in accordance with the life cycle documentation (P.Config_IT-env) and helps meet the objective of IT-environment (O.Config_Activities).

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

The internal transport covers the shipment of produced wafers as well as the shipment of masks either for repair or for final scrapping.

P.Reception-Control: The reception activities of the site shall be performed in accordance with the life cycle documentation. 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. All assets will be identified and moved immediately to the correct security level.

4.4 Assumptions

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

A.Setup-Projects: To enable that the site participates in the development of products NXP provides services to setup the necessary development computers (tools, user accounts, etc.) and configuration management systems (user accounts, repositories etc.).

A.Product-Setup: The site participates in the development of products. To define the participation of the site in the development while maintaining quality, for each product NXP will manage the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results by NXP.

A.Shipment: To enable the site to realize shipment such that assurance of integrity is assured throughout transport of physical security objects NXP will manage the shipment method as described in the life cycle documentation.

5. Security Objectives

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

O.Config_IT-env: The site uses programs and servers in addition to configuration management systems for file versioning and problem tracking. For file versioning unique repositories shall be used to support proper management of multiple products and the site internal procedures.

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

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

O.Config_Activities: The activities of the site are performed in accordance with the life cycle documentation (O.Config_IT-env) using the IT-environment (O.LifeCycle-Doc).

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

O.Control-Scrap: The site has measures in place to either securely destroy assets (e.g. paper shredder) or return them to NXP for destruction. O.Transfert-Data

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.Internal-Shipment: The recipient of finished wafers and defect masks are identified by the assigned address. An appropriate internal shipment procedure is applied for both configuration items. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of configuration items during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined.

O.Transfer-Data: The NXP logical infrastructure ensures that the transfer for all secure data is contained within the secure networks or delivered via encryption complaint to company policy.

O.Reception-Control: Upon reception of masks an immediate incoming inspection is per-formed. The inspection comprises the received amount of masks and the identification and assignment of the product to a related internal production process. The received mask comes from mask division in the site.

O.Zero-Balance: The site ensures that all wafers (intended TOE of different clients) and masks are separated and traced on a wafer respectively mask basis. Automated control and/or two employees acknowledgement during hand over is applied for functional and defective wafers and masks. According to the agreed production flow the defect wafers are either destroyed at the site or sent to the client.

5.1 Security Objectives Rationale

27 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 and Table 2)

28 Note that the assumptions of the SST cannot be used to cover any threat or OSP of the site. They are seen as pre-conditions fulfilled either by the site providing the sensitive configuration items or by the site receiving the sensitive configuration items. Therefore, they do not contribute to the security of the site under evaluation.

Threat and OSP	Security Objective(s)	Rationale

T.Smart-Theft	O.Lifecycle-Doc O.Physical-Access O.Control-Scrap O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Config_Activities O.Zero-Balance O.Reception-Control	O.Lifecycle-Doc ensure that procedures are documented which assist in preventing Theft. 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. O.Config_Activities activities of the site are performed in accordance with the life cycle documentation. O.Zero-Balance and O.Reception-Control ensures that all items are traced and accounted for. Together, these objectives will therefore counter T.Smart_Theft.

T.Rugged-Theft	O.Lifecycle-Doc O.Physical-Access O.Control-Scrap O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Config_Activities O.Zero-Balance O.Reception-Control	O.Lifecycle-Doc ensure that procedures are documented which assist in preventing Theft. 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. O.Config_Activities activities of the site are performed in accordance with the life cycle documentation. O.Zero-Balance and O.Reception-Control ensures that all items are traced and accounted for. Together, these objectives will therefore counter T.Rugged_Theft

T.Computer-Net	O.Config_IT-env O.Lifecycle-Doc O.Physical-Access O.Logical-Operation O.Internal-Monitor O.Maintain-Security O.Control-Scrap O.Staff-Engagement O.Config_Activities O.Transfer-Data:	O.Config_IT-env assigns unique numbers to the internal procedures and guidance. This helps enforce segregation of duties and the need to know principals. O.Lifecycle-Doc ensure that procedures are documented which assist in preventing Unauthorised Staff access. O.Physical-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.Physical-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.Config_Activities activities of the site are performed in accordance with the life cycle documentation. O.Staff-Engagement ensures that all staff is aware of its reponsibilities (signing NDAs, and being trained). O.Transfer-Data ensures the integrity of the secure delivery of data 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.Config_IT-env O.Logical-Operation O.Control-Scrap O.Config_Activities O.Lifecycle-Doc O.Staff-Engagement O.Zero-Balance O.Transfer-Data:	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 unauthrised 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.Config_IT-env assigns unique numbers to the internal procedures and guidance. This helps enforce segregation of duties and the need to know principals. O.Control-Scrap ensures that scrap material cannot be accessed by an authorized party O.Config_Activities activities of the site are performed in accordance with the life cycle documentation. 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.Lifecycle-Doc ensure that procedures are documented which assist in preventing Unauthorised Staff access. O.Staff-Engagement ensures that all staff is aware of its reponsibilities (signing NDAs, and being trained). O.Zero-Balance ensures that all items are traced and accounted for. O.Transfer-Data ensures the integrity of the secure delivery of data Together, these objectives will therefore counter T.Unauthorised-Staff.

T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Config_IT-env O.Control-Scrap O.Config_Activities O.Lifecycle-Doc O.Zero-Balance O.Transfer-Data O.Physical-Access	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.Config_IT-env assigns unique numbers to the internal procedures and guidance. This helps enforce segregation of duties and the need to know principals. O.Control-Scrap ensures that scrap material cannot be accessed by an authorized party O.Config_Activities activities of the site are performed in accordance with the life cycle documentation. O.Lifecycle-Doc ensure that procedures are documented which assist in preventing Unauthorised Staff access. O.Zero-Balance ensures that all items are traced and accounted for. O.Transfer-Data ensures the integrity of the secure delivery of data O.Physical-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.Physical-Access also ensures that all such connections are not connected to the encryption equipment. Together, these objectives will therefore counter T.Staff-Collusion.

T.Attack-Transport	O.Transfer-Data O.Internal-Shipment O.Zero-Balance O.Internal-Monitor O.Maintain-Security O.Lifecycle-Doc O.Reception-Control	O.Transfer-Data ensures the integrity of the secure delivery of data O.Internal-Shipment ensure the traceability and security of masks and wafer during shipment. O.Zero-Balance and O.Reception-Control ensures that all items are traced and accounted for. O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. O.Lifecycle-Doc ensure that procedures are documented which assist in preventing Unauthorised Staff access. Together, these objectives will therefore counter T.Attack-Transport.
P.Config_IT-env	O.Config_IT-env O.Transfer-Data:	The Security Objective directly enforces the OSP. O.Config_IT-env assigns unique numbers to the internal procedures and guidance. O.Transfer-Data ensures the integrity of the secure delivery of data As the site processes no other configuration items, this is sufficient to meet P.Config_IT-env.
P.Config_Activities	O.Config_Activities O.Transfer-Data: O.Physical-Access	The Security Objective directly enforces the OSP. O.Config_Activities activities of the site are performed in accordance with the life cycle documentation. O.Transfer-Data ensures the integrity of the secure delivery of data O.Physical-Access also ensures that all such connections are not connected to the encryption equipment. The services and processes 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_Activities.
P.LifeCycle-doc	O.LifeCycle-doc	The Security Objective directly enforces the OSP. This ensures life cycle documentation that describes configuration management systems, Site security, development process and tools providing a CM_Plan is sufficient to meet P.LifeCycle-doc.

P.Reception-Control	O.Internal-Shipment O.Reception-Control	The Security Objective directly enforces the OSP. O.Internal-Shipment and 0.Reception-Control ensure the traceability and security of masks and wafer during shipment. These measures are sufficient to meet the requirements of P.Reception-Control
P.Product-Transport	O.Internal-Shipment O.Reception-Control	The Security Objective directly enforces the OSP. O.Internal-Shipment and 0.Reception-Control ensure the traceability and security of masks and wafer during shipment. These measures are sufficient to meet the requirements of P.Product-Transport

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

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:

- [10] 'Minimum Site Security Requirements'

- [5] Eurosmart Protection Profile.

7.1 Application Notes and Refinements

33 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)

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

7.1.2 CM Scope (ALC_CMS.5)

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

7.1.3 Development Security (ALC_DVS.2)

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

7.2 Security Requirements Rationale

7.2.1 Security Requirements Rationale - Dependencies

37 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_DEL.1: None
- ALC_DVS.2: None

38 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'.

7.2.2 Security Requirements Rationale – Mapping

SAR	Security Objective	Rationale
ALC_CMC.5.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling.	O.Config_IT-env O.LifeCycle-Doc O.Config_Activities	Appropriate and consistent labelling is ensured through the application (O.Config_Activities) of the CM-Plan (O.LifeCycle-Doc) and the use of the configuration management systems (O.Config_IT-env).
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.LifeCycle-Doc	The method used to uniquely identify the configuration items is described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMC.5.3C: The CM documentation shall justify that the	O.LifeCycle-Doc	The adequate and appropriate acceptance procedures for configuration items are described

SAR	Security Objective	Rationale
acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.		in the CM-Plan (O.LifeCycle-Doc).
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.Config_IT-env O.LifeCycle-Doc O.Config_Activities	Unique identification of all CIs is realized by performing the CM activities (O.Config_Activities) in accordance with the CM-Plan (O.LifeCycle-Doc) using the Configuration management systems (O.Config_IT-env)
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config_IT-env O.LifeCycle-Doc O.Config_Activities	The configuration management systems (O.Config_IT-Env) used (O.Config_Activities) according to the CM-Plan (O.LifeCycle-Doc) enforces automated measures such that only authorized changes are made to the configuration items
ALC_CMC.5.6C: The CM system shall support the production of the product by automated means.	O.Config_IT-env O.LifeCycle-Doc O.Config_Activities	The software on the development computers (O.Config_IT-env) supports automated production of products when used (O.Config_Activities) in accordance with the CM-Plan (O.LifeCycle-Doc)
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	O.LifeCycle-Doc O.Config_Activities	As described in the CM-Plan (O.LifeCycle-Doc) the activities performed (O.Config_Activities) are such that the person responsible for accepting a configuration item into CM is not the person who developed it.
ALC_CMC.5.8C: The CM system shall clearly identify the configuration items that comprise the TSF.	O.Config_IT-env O.LifeCycle-Doc	The CM-Plan (O.LifeCycle-Doc) identifies the configuration items that comprise the TSF possibly supported by the configuration management system (O.Config_IT-env)
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the TOE by automated	O.Config_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configuration management systems (O.Config_IT-env) are

SAR	Security Objective	Rationale
means, including the originator, date, and time in the audit trail.		configured such that an audit trail (showing originator, date and time) is automatically generated.
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O.Config_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configurations management system and software installed on the development workstations and servers (O.Config_IT-env) provide automated means to identify all other configuration items that are affected by the change of a given configuration item.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.	O.Config_IT-env O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configurations management system (O.Config_IT-env) identifies the version of the implementation representation from which the TOE is generated through baselines.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) describes how the CM system is used for the development of the product.
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE	O.LifeCycle-Doc	The acceptance procedures for modified or newly created configuration items are described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.LifeCycle-Doc	All configuration items are listed in the CI-list (O.LifeCycle-Doc)

SAR	Security Objective	Rationale
ALC_CMC.5.16C: The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.	O.Config_IT-env O.LifeCycle-Doc	The CI-list (O.LifeCycle-Doc) is generated from the configuration management systems (O.Config_IT-env)

Table 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.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan and a CI-List with the items required by ALC_CMS.5.1C
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.LifeCycle-Doc	The CI-List (O.LifeCycle-Doc) uniquely identifies the configurations items as described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.	O.LifeCycle-Doc	The CI-List (O.LifeCycle-Doc) indicates the developer/subcontractor for each configuration items as described in the CM-Plan (O.LifeCycle-Doc).

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.LifeCycle-Doc 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.LifeCycle-Doc) describes the physical (O.Physical-Access, O.Security-Control, O.Alarm-Response), 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 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.LifeCycle-Doc	The development security documentation (O.LifeCycle-Doc) justifies the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.
ALC_DVS.2.3C: The evidence shall justify that the security measures provide the necessary level of protection to	O.LifeCycle-Doc O.Physical-Access O.Security-Control O.Internal-	The development security documentation (O.LifeCycle-Doc) describes the physical (O.Physical-Access, O.Security-Control),

SAR	Security Objective	Rationale
maintain the confidentiality and integrity of the TOE.	Monitor O.Maintain-Security O.Logical-Operation O.Control-Scrap O.Staff-Engagement	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 development environment.

Table 4 Rationale for ALC_DVS.2

8. Site Summary Specification

8.1 Preconditions required by the Site

39 NXP Austin provides mask handling services to manufacture wafers. In order to perform the aforementioned services, NXP requires to fulfil the following preconditions. The following paragraphs describe preconditions of NXP.

40 For the setup and control of the production process, NXP is required to provide the appropriate specification and relative manufacturing information.

41 The production process includes the tool configuration and set-up for manufacturing processes. The released production process further includes the parameters and limits that must be fulfilled by the mask that are used by the wafer Fab. In addition the process allows the electrical testing of the finished wafer by the wafer Fab.

42 For the shipment of security product, the recipient of the finished wafers are identified by the address of the respective site. The packing of finished wafers and preparation of the shipment adhere to the standard procedure of the site, unless the specific requirement from NXP. NXP is responsible for delivery and transfer of the finished wafers, comprising the selection of the forwarder and the provision of data for the verification of the transport order.

43 NXP must perform the appropriate functional testing of the finished wafer. The testing of the finished wafer at the site is restricted to the testing of the process control modules that are added on the wafer.

44 The site activities are performed using an IT infrastructure consisting of workstations, servers manufacturing tools and configuration management systems. All of these are provided, configured and maintained by the NXP.

45 In case of necessary updates to the life cycle documentation NXP will co-ordinate, communicate and deliver.

46 To enable the site to realize shipment such that assurance of integrity is assured throughout transport of physical security objects NXP will manage the shipment method.

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

8.2 Services of the Site

48 The site does not directly contribute to the development of the intended TOE in the sense of Common Criteria. The site ensures a reproducible production process within the limits defined for the released wafer production process. Therefore relevant parameters are controlled during the production process. This is subject of the configuration management. Using the received set of masks (the masks are manufactured at Toppan's mask division and will be delivered to NXP), then the site produces security wafers.

49 Functional testing must be performed before the intended TOE can be delivered to the consumer. Since the functional testing is not performed at the site, the wafers are delivered to the functional testing site of the related security product. Therefore the site does not perform delivery to the consumer, but internally within NXP.

50 Thus the site does not comply to any aspects that are covered by ALC_DEL. Internal shipment is covered under ALC_DVS.2.

8.3 Security Assurance Rationale

8.3.1 CM capabilities (ALC_CMC.5)

51 Configuration Management is described in [7], [8] and [12].

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], [8] and [12].

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

8.3.4 Life-cycle definition (ALC_LCD.1)

57 Life-cycle definition is described in [7] and [8].

58 For full detail and evidences please view Section 7.2.2

8.3.5 Tools and techniques (ALC_TAT.3)

Tools and techniques is described in [8].

59 For full detail and evidences please view Section 7.2.2

8.4 Objectives Rationale

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

8.4.1 O.Config_IT-env

61 The configuration of the IT environment is designed in such way to ensure segregation of duties and the need to know principals. These measures address T.Computer-Net, T.Staff-Collusion and T.Unauthorized-Staff. Also addresses the OSP P.Config-IT-env.

8.4.2 O.Physical-Access

The physical access is supported by O.Security-Control that includes the maintenance of the access control and the control of visitors. The physical security measures are supported by O.Alarm-Response providing an alarm system.

Thereby the threats T.Smart-Theft, T.Rugged-Theft can be prevented. The physical security measures together with the security measure provided by O.Security-Control enforce the recording of all actions. Thereby also T.Computer-Net, T.Staff-Collusion and T.Unauthorized-Staff is addressed. Also addresses the OSP P.Config-Activities.

8.4.3 O.Security-Control

62 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.

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

8.4.4 O.Alarm-Response

64 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.

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

8.4.5 O.Internal-Monitor

66 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).

67 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.

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

8.4.6 O.Logical-Operation

69 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.

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

8.4.7 O.Staff-Engagement

71 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.

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

8.4.8 O.Control-Scrap

73 Scarp may exist in a number of forms on this site printed secure objects, test samples or redundant hardware/movable media. Transport and actual destruction of security products is done under supervision of a qualified employee in collaboration with the destructor. Sensitive information and information storage media are collected internally in a secure location and destroyed in a supervised and documented process. Any secure documentation on site will be destroyed by means of a Level 5 security shredder.

74 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

8.4.9 O.Config_Activities

75 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 IDs with are linked to the unique ID numbers of the associated WIP system (PROMIS).

76 This is addressing the threat T.Rugged-Theft, T.Computer-Net, T.Staff-Collusion, T.Unauthorised-Staff, T.Smart-Theft and the OSP P.Config-Activities

8.4.10 O.Maintain_Security

77 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

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

8.4.11 O.LifeCycle_doc

79 The security of the site is maintained according to the sites security documentation covering all physical and logical measures to ensure the security of the site.

80 These security measures are necessary to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unautorised-Staff, T.Staff-Collusion and T.Attack-Transport. Also addressing the OSP P.Lifecycle-Doc

8.4.12 O.Internal-Shipment

81 The recipient of a production lot is linked to production system and can be modified by authorized users. Packing procedures are documented in the product configuration. This includes specific requirement of the client. This security objective is supported by O.Staff-Engagement and O.Config-Items.

The threat T.Attack-Transport and the OSP P.Product-Transport are addressed by the internal shipment.

8.4.13 O.Reception-Control

82 At reception each configuration item including security products are identified by the shipping documents, labels and information in the system supported by O.Config-Items. Inspection at reception is counting the amount of boxes and checking the shipping list if applicable. Thereby only correctly identified masks are accepted for production.

83 These security measures are necessary to prevent the threats T.Smart-Theft, T.Rugged-Theft T.Attack-Transport and OSP P.Product-Transport and P.Reception-Control are addressed by the reception control.

8.4.14 O.Transfer-Data

84 The integrity of the data transfer from/to the site, specifically GDS data and mask data and within the site is ensured by appropriate secure measures.

85 Supported by O.Logical-Access and O.Staff-Engagement this addresses the threats T.Staff-Collusion, T.Computer-Net, T.Unauthorised-Staff and T.Attack-Transport as well as the OSP's P.Config_IT-env and P.Config-Activities.

8.4.15 O.Zero-Balance

86 Products are uniquely identified throughout the whole process. For each hand over, either an automated or an organizational "two-employees-acknowledgement" (four-eyes principle) is applied for functional and defect assets. Scrap is following the good products through the whole production process. At every process step the registration of functional and scrap products is updated. Before a production order is closed a zero balance calculation is documenting the history of functional and scrap parts of this order. This security objective is sup-ported by O.Physical-Access, O.Config-Items and O.Staff-Engagement.

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

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 Version 1.0," Eurosmart, 15.06.2007.

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

[7] "BU S&C ALC-CM Common Criteria Documentation, PV4-00805".

[8] ATMC Austin – Site Security Manual v0.3 March 30, 2017

[10] Minimum Site Security Requirement V1.1 June

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

[12] NXP Austin Fab Configuration List, 10th November 2016

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