NXPOMS-1719007347-5162

Site Security Target NXP ATTJ

Publication Summary

Reference Number (OMS-ID)	NXPOMS-1719007347-5162
Reference Title	Site Security Target NXP ATTJ
Publisher	Competence Center Crypto & Security
Classification	PUBLIC
Author	Christophe Bouly
Owner	Yan Yu

Revision History

Revision	Description	Author	Date
0.1 (not released)	Initial Draft	Christophe Bouly	2021-07-26
0.2 (not released)	Include Security manual reference	Christophe Bouly	2021-08-06
0.3	Including preaudit remarks	Christophe Bouly	2021-09-15
0.4	Deleting ALC_TAT.3 and ALC_DEL.1 including partial answers related to NSCIB-SS-0432035-RR-AST-1.0 to allow EM.1+2 meetings	Christophe Bouly	2021-10-08
1.0	Answers to evaluator comments ([AILSA] 12136 NXP ATTJ Action item list (Site Audit)_v1.0)	Christophe Bouly	2021-11-05
1.1	Table of content change, typo correction with the shipping area	Christophe Bouly	2021-11-09
1.2	Changes related to Chapter 2.3.1	Christophe Bouly	2021-11-18

Approvers

Sequence	Role	Name
Acceptance	Security Manager	Christophe Bouly
Approval	Security Representative	Yan Yu

Subscriber

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

Contents

Table of Figures

1. Document Introduction

1.1 Reference

Title: Site Security Target NXP ATTJ

Version: 1.2

Date: 11/18/2021

Company: NXP Semiconductors

Name of site: NXP ATTJ

EAL: SARs taken from EAL6

2. SST Introduction

1 The chapters 1 to 9 of this document are based upon the Eurosmart Site Security Target Template [1] with adaptations such that it fits the site.

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

2.1 SST Reference

3 Title Site Security Target NXP ATTJ

4 Version 1.2

2.2 Site Reference

5 The site belongs to NXP and is located at:

NXP Tianjin Assembly and test manufacturing (ATTJ)
15#, Xinghua Avenue, Xiqing Economic Technology Development Area,
Tianjin
P.R. C

2.3 Site Description

2.3.1 Physical Scope

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

7 Physical scope includes also the warehouse located at a different address.

8 The warehouse is located at 16 Wei 2 Road, Xiqing Microelectronic Development Area Tianjin, P.R.C

9 All areas in scope are classified as YELLOW and RED[1] areas. These areas will be within the main building of ATTJ and described below

- Building A
  - 1 st floor yellow areas: wafer test room (WT[2]), receiving area[3] (R- E01A05A), shipping area[4] (S-E01A18) , Security Command Center (SCC)

[1] The terms YELLOW area and RED area are defined in the NXP internal document „NXPOMS-1719007347-2404 CCC&S Security Requirements Overview"

[2] Because VPM, FOI, final packing performed in this area
[3] Receiving raw wafers from clients
[4] Shipping tested wafers and scrap from building A to the warehouse

- 1 st floor red areas: Data center3 (DC3), Wafer test 5 area (WFT5 -MDF-E01C89)
- 1 M floor red area: Telecom room (DF-E01MB03A)
- 2nd floor red area: Data center1 (DC1- E02C41A)

- Industrial Warehouse (NXP Area) (see line 8 for location)
  - Yellow area: NXP warehouse (W) (1st floor shipping dock[5], 3rd floor warehousing area)
  - Red area: NXP Secure cage (SC) inside the 3rd floor warehousing area

10 A more detailed view of the layout is described in documentation referenced into the Site Security Manual (SSM) for ATTJ. All other yellow areas not detailed here are not part of the site certification scope.

11 Those locations contain security areas with restricted access where only authorized persons are allowed to enter.

12 Within those areas, only authorized people are entitled to access sensitive information. To enforce such access restriction, a combination of physical, procedural, personnel and logical measurements have been installed.

2.3.2 Logical Scope

13 The following life-cycle phases as defined in 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084) [3] are subject of the SST:

- Phase 3: IC Manufacturing

14 IT Manufacturing provides a Secure Production Network IT infrastructure.

2.3.2.1 The following services and/or processes provided by NXP ATTJ are in the scope of the site evaluation process. Some processes are directly part of the phases presented before and others are supporting processes which can be involved at any phase of the production. Supporting service

- IT support;
- Warehousing
- Shipment.

2.3.2.2 ATTJ Site Services related to [3] life cycle phases

- IC Manufacturing (Phase 3) under MES[6] Camstar system;
  - Die room
    - wafer storage.
  - Scraps collection and shipment

[5] Receiving (shipping) wafers from (to) the building A (clients)
[6] Manufacturing Execution System

- Wafer Test
  - Functional wafer test of security products (test program execution)
  - Quality & Quantity wafer inspection.

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 5, April 2017, [4]

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

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

17 Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017, [6]

18 This SST is CC Part 3 conformant.

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

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

21 The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profile [2], [3] and is therefore suitable for the evaluation of 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 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 as per NXPOMS-1719007347-2401 “Security Objects Document”. They can be grouped within the following categories:

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

Development data: The site has access to (and optionally copies thereof) electronic development data (Evaluation Documents, Product Quality Engineering Documents, Product Documents and Test program/Data/Documents as well as site- and IT process objects specifications, etc.) in relation to developed TOEs. Both the integrity and the confidentiality of these electronic documents 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. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered.

T.Rugged-Theft: An attacker with specialized equipment for burglary, who may be paid to perform the attack, tries to access sensitive areas and manipulate or steal assets.

T.Computer-Net: A possibly paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to (1) development data with the intention to violate confidentiality and possibly integrity, (2) production systems with the intention to modify the production process.

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

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

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

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

4.3 Organizational Security Policies

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

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

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

P.Config-Items: The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of items that are used for production as well as that are produced at the site.

P.Config-Control: The procedures for setting up the production process for a new product as well as the procedure that allows changes of the initial setup for a product shall only be applied by authorised personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The procedure for the initial set-up of a production process ensures that sufficient information is provided by the client.

P.Config-Process: The services and/or processes provided by the site are controlled in the configuration management plan. This comprises incoming items used for the production, the management of flaws and optimizations of the process flow as well as the documentation that describes the services and/or processes provided by the site. A released production process is defined for the wafers.

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

P.Zero-Balance: The site ensures that all sensitive items (security relevant parts of the TOEs of different clients) are separated and traced on a device basis. For each hand over, either an automated or an organizational “two-employees-acknowledgement” (four-eyes principle) is applied for functional and defect assets. According to the released production process the defect assets are stored by the site before to be sent to a certified supplier. The sent back procedures are controlled through internal compliance policies and procedures.

P.Accept-Product: The testing and quality control of the site ensures that the released products comply with the specification agreed with the client. The acceptance process is supported by automated measures. Records are generated for the acceptance process of the configuration items. Thereby, it is ensured that the properties of the product are ensured when internally shipped.

P.Product-Transport: Technical and organizational measures shall ensure the correct labelling of the product or item parts. 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.

P.Transfer-Data: Any data in electronic form (e.g. product specifications, test programs, test program specifications, release information etc.) that is classified as sensitive or higher security level by the client is encrypted to ensure confidentiality of the data. In addition measures are used to control the integrity of the data after the transfer.

P.Scrap-Items: Physical items that do not comply with the quality requirements are stored and scrapped by an external certified supplier in a way that the destructed items do not support any attacker.

P.Organise-Product: The configuration, pre-personalisation, initialisation or personalisation process is applied as specified by the client. If the data includes sensitive items like keys relevant for the life-cycle or configuration data that affect the security of the TOE appropriate measures must be in place. This includes the requirement that the knowledge of sensitive keys shall be split to at least two different persons. Furthermore, technical measures like crypto-boxes, separation of network, split access permission and secure storage shall be implemented for this kind of data.

4.4 Assumptions

26 The assumptions are outside the sphere of influence of NXP ATTJ site. They are needed to provide the basis for an appropriate production process, to assign the product to the released production process and to ensure the proper handling, storage and destruction of all configuration items related to the intended TOE.

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

A.Product-Setup: The site participates in the production of products. To define the participation of the site in the production 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.Transfer-Data: The test program is provided by the client. Related cryptographic measures will be agreed between the sender and receiver of the data to ensure integrity and/or confidentiality.

A.Item-Identification: Each configuration item received by the site is appropriately labelled by the previous site to ensure the identification of the configuration item.

A.Internal-Shipment: The recipient of the product is identified by its address or e-mail address. The address / e-mail address of the client is part of the product setup. 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

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

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

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

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organizational 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 unauthorized people. The access control measures ensure that only registered employees can access restricted areas. Assets are handled in restricted areas only.

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

O.Alarm-Response: The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any asset. After the alarm is triggered the unauthorized 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 incidents, 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-Access: The site enforces a logical separation between the internal network and the internet including a firewall. The security measures ensure that only defined services and defined connections are accepted on the internal network. The internal network is appropriately separated to prevent interference between the different environments (office, development and production environments). Additional specific networks for production and configuration are physically separated from any internal network to enforce access control. Access to the production network and associated systems is restricted to authorised employees working in the related area or involved in the configuration tasks of the production systems. Every user of an IT system has his/her own user account and password.

O.Logical-Operation: All network segments and the computer systems are kept up-to-date (software updates, security patches, virus protection, spyware protection). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.

O.Config-Items: The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify configuration items and allow an assignment to the client. Also the internal procedures and guidance are covered by the configuration management.

O.Config-Control: The site applies a release procedure for the setup of the production process for each new product. In addition, the site has a change management for changes requested by the client as well as internal changes within the production process for released products. Internal changes are classified and minor ones are handled by the site, major changes must be acknowledged by the client. A designated team is responsible for the release of new products and for the management of changes and their release. This team comprises specialists for all aspects of the services and/or processes. The services and/or

processes can be introduced or changed by authorized personnel only. Automated systems support configuration management and production control.

O.Config-Process: The site controls its services and/or processes using a configuration management plan. The configuration management is controlled by tools and procedures for the production, for the management of flaws and optimizations of the process flow as well as for the documentation that describes the services and/or processes provided by a site.

O.Control-Scrap: The site has measures in place to store assets to be scrapped.

O.Staff-Engagement: All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.

O.Zero-Balance: The site ensures that all physical asset are separated and traced. Automated control and/or two employees acknowledgement during hand over is applied for functional and defective material.

O.Reception-Control: Upon reception of TOE items an immediate incoming inspection is performed. The inspection comprises the received amount items and the identification and assignment of the product to a related internal production process.

O.Acceptance-Test: The site delivers configuration items that fulfil the specified properties. Parameter checks, functional and/or visual checks and tests are performed to ensure the compliance with the specification. The test results are logged to support tracing and the identification of systematic failures.

O.Internal-Shipment:The site has measures in place to provide assurance of integrity throughout transport of physical security objects. The recipient of finished 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 according to NXP policy. The forwarder supports the tracing of configuration items during internal shipment. Before shipping a pre-announcement is sent to the receiver to support the control during transport. For every sensitive configuration item, the protection measures against manipulation are defined.

O.Transfer-Data: Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorized employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected.

O.Organise-Product: For the configuration, pre-personalisation, initialisation or personalisation process it is ensured that the specified process is applied. The data integrity is controlled. Keys and other sensitive data can only be constructed by at least two employees. The operation is applied in crypto-boxes or similar devices. After the release process changes are only applied based on the request of the client. The update is done according to a controlled process.

5.1 Security Objectives Rationale

28 The SST includes a Security Objectives Rationale with two parts. The first part includes the tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part includes a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives (see column “Rationale” of table Table 1 and Table 2).

29 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.

5.1.1 Mapping of Security Objectives

Threat	Security Objective(s)	Rationale
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat.

Threat	Security Objective(s)	Rationale
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat.
T.Computer-Net	O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation	The combination of structural, technical and organizational measures detects and prevents unauthorized access which is an appropriate response on the threat.
T.Accident-Change	O.Logical-Operation O.Config-Items O.Logical-Access O.Config-Process O.Staff-Engagement O.Zero-Balance O.Acceptance-Test	Automated measures and control procedures allow preventing accidental changes on sensitive items.
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Zero-Balance O.Control-Scrap	Physical and logical access control prohibits access to assets. Secure destruction of scrap limits the amount of assets.
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Control-Scrap O.Transfer-Data O.Zero-Balance	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees limits unauthorized access to assets.

Threat	Security Objective(s)	Rationale
T.Attack-Transport	O.Internal-Shipment O.LifeCycle-Doc O.Transfer-Data	The shipment method and the organizational measures ensure that integrity changes of shipped objects are detected and appropriately responded upon.

Table 1 Threats - Security Objectives Rationale

OSP	Security Objective(s)	Rationale
P.Config_IT-env	O.Config_IT-env	The Security Objective directly enforces the OSP.
P.LifeCycle-Doc	O.LifeCycle-Doc	The Security Objective directly enforces the OSP.
P.Config-Items	O.Reception-Control O.Config-Items	The Security Objective (O.Reception-Control, O.Config-items) enforces the OSP.
P.Config-Control	O.Config-Items O.Config-Control O.Logical-Access	Network and logical protection (O.Logical-Access) and the usage of configuration management tools by authorised people (O.Config-Control, O.Config-Items) ensure the OSP.
P.Config-Process	O.Config-Process	The Security Objective directly enforces the OSP.
P.Reception-Control	O.Reception-Control	The Security Objective directly enforces the OSP.
P.Zero-Balance	O.Staff-Engagement O.Zero-Balance O.Control-Scrap O.Internal-Monitor	All assets are traced internally (O.Internal-Monitor) until their possible destruction (O.Zero-Balance, O.Control-Scrap) by trained and authorized people (O.Staff-Engagement) to enforce the OSP.
P.Accept-Product	O.Config-Control O.Config-Process O.Acceptance-Test	Application of a configuration management plan and change management monitored by authorized people ensure that the *intended TOE* is conformant

OSP	Security Objective(s)	Rationale
		to the accepted one by the customer (O.Config-Control, O.Config-Process, O.Acceptance-Test).
P.Organise-Product	O.Logical-Access O.Logical-Operation O.Config-Control O.Config-Process O.Organise-Product	Appropriate procedures and processes (O.Config-Process O.Organise-Product) using a protected environment (O.Logical-Access O.Logical-Operation O.Config-Control) enforce the OSP.
P.Product-Transport	O.Config-Process O.Transfer-Data O.Internal-Shipment	Appropriate procedures for internal shipment ensure correct labelling and traceability until the recipient.
P.Transfer-Data	O.Transfer-Data	The Security Objective directly enforces the OSP.
P.Scrap-Items	O.Control-Scrap	The Security Objective directly enforces the OSP.

Table 2 OSP - Security Objectives Rationale

6. Extended Assurance Components Definition

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

7. Security Assurance Requirements

31 Clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profile [2], [3].

32 The Security Assurance Requirements are chosen from the class ALC (Life-cycle support) as defined in [5]:

- CM capabilities (ALC_CMC.5)
- CM scope (ALC_CMS.5)
- Development Security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)

33 The Security Assurance Requirements listed above fulfill the requirements of [7] because hierarchically higher components than the defined minimum site requirements (ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, see section 3.2.3 of [7]) are used in this Site Security Target.

7.1 Application Notes and Refinements

34 The description of the site certification process [7] 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)

35 Refer to subsection ‘Application Notes for Site Certification’ in [7] 5.1 ‘Application Notes for ALC_CMC’.

7.1.2 CM Scope (ALC_CMS.5)

36 Refer to subsection ‘Application Notes for Site Certification’ in [7] 5.2 ‘Application Notes for ALC_CMS’.

37 Note: Due to these application notes the refinements from the Eurosmart PP [2], [3] (see section 6.2.1.3) are not applicable.

7.1.3 Development Security (ALC_DVS.2)

38 Refer to subsection ‘Application Notes for Site Certification’ in [7] 5.4 ‘Application Notes for ALC_DVS’.

39 Refer to ‘*Application Note 26’* in 6.2.1.2 ‘Refinements regarding Development Security (ALC_DVS)’ in the Eurosmart PP [2] and [3] (application note 27).

40 Refer to subsection *'Refinement'* in 6.2.1.2 'Refinements regarding Development Security (ALC_DVS)' in the Eurosmart PP [2] and [3].

41

7.1.4 Life-cycle Definition (ALC_LCD.1)

42 Refer to subsection 'Application Notes for Site Certification' in [7] 5.6 'Application Notes for ALC_LCD'.

7.2 Security Requirements Rationale

7.2.1 Security Requirements Rationale - Dependencies

43 The dependencies for the assurance requirements are as follows (see [5], appendix C):

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

44 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 [7] 5.1 'Application Notes for ALC_CMC'.

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 labelling.*	O.Config-Item O.Reception-Control O.Config_IT-env O.LifeCycle-Doc	O.Config-Item and O.Reception-Control assures correct and unique identification. Appropriate and consistent labeling is ensured through the application of the CM-Plan (O.LifeCycle-Doc) and the use of the configuration management systems (O.Config_IT-env).
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.LifeCycle-Doc O.Reception-Control O.Config-Control O.Config-Process	The method used to uniquely identify the configuration items is described in the CM-Plan (O.LifeCycle-Doc) using a process and a configuration

SAR	Security Objective	Rationale
		management system (O.Config-process, O.config-control). At each step, the configuration item is inspected and identified (O.Reception-Control)
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-Item O.LifeCycle-Doc O.Config-Control	O.Config-Item assures correct and unique identification The adequate and appropriate acceptance procedures for configuration items are described in the CM-Plan (O.LifeCycle-Doc). Change acceptance is managed by authorized people only (O.Config-Control)
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.Config_IT-env O.Config-Items O.Config-Process O.LifeCycle-Doc	Unique identification of all CIs is realized by performing the CM activities in accordance with the CM-Plan (O.LifeCycle-Doc, O. Config-Process) using the Configuration management systems (O.Config_IT-env, O.Config-Items)
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config_IT-env O.Config-Items O.Config-Process O.LifeCycle-Doc O.Config-Control O.Acceptance-Test	The configuration management systems (O.Config_IT-env, O.Config-Items) used according to the CM-Plan (O.Config-Process, O.LifeCycle-Doc, O.Config-Control) enforces automated measures such that only authorized changes are made to the configuration items according to specifications (O.Acceptance-Test).
ALC_CMC.5.6C: The CM system shall support the production of the product by automated means.	O.Organise-Product O.Config_IT-env O.Config-Items O.Config-Process O.LifeCycle-Doc O.Zero-Balance	Production is performed according to the process (O.Organise-Product) by automated means when used in accordance with the CM-Plan (O.LifeCycle-Doc, O.Config-Process) using

SAR	Security Objective	Rationale
		items followed by CM (O.Config_IT-env O.Config-Items). Zero-Balancing is performed at each step (O.Zero-Balance)
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-Process	As described in the CM-Plan (O.LifeCycle-Doc, O.Config-Process) the activities performed are such that the person responsible for accepting a configuration item into CM is not the person who developed it.
ALC_CMC.5.8C: The CM system shall clearly identify the configuration items that comprise the TSF.	O.Config_IT-env O.Config-Items O.Config-Process O.LifeCycle-Doc	The CM-Plan (O.LifeCycle-Doc, O.Config-Process) identifies the configuration items that comprise the TSF possibly supported by the configuration management system (O.Config_IT-env, O.Config-Items)
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the *intended TOE* by automated means, including the originator, date, and time in the audit trail.	O.Config_IT-env O.Config-Items O.Config-Process O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc, O.Config-Process) the configuration management systems (O.Config_IT-env, O.Config-Items) are configured such that an audit trail (showing originator, date and time) is automatically generated.
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O.Config_IT-env O.Config-Items O.Config-Process O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc, O.Config-Process) the configurations management system and software installed on the development workstations and servers (O.Config_IT-env, O.Config-Items) 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	O.Config_IT-env O.Config-Items	As described in the CM_Plan (O.LifeCycle-Doc,

SAR	Security Objective	Rationale
able to identify the version of the implementation representation from which the *intended TOE* is generated.	O.Config-Process O.LifeCycle-Doc	O.Config-Process) the configurations management system (O.Config_IT-env, O.Config-Items) identifies the version of the implementation representation from which the *intended TOE* is generated through baselines.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the *intended TOE*.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) describes how the CM system is used for the development of the product.
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *intended TOE*.	O.LifeCycle-Doc O.Config-Control	The acceptance procedures for modified or newly created configuration items are described in the CM-Plan (O.LifeCycle-Doc, O.Config-Control).
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 under configuration system and listed in the CI-list (O.LifeCycle-Doc)
ALC_CMC.5.16C: The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.	O.Config_IT-env O.Config-Process O.LifeCycle-Doc	The CI-list (O.LifeCycle-Doc) is generated from the configuration management systems (O.Config_IT-env, O.Config-Process)

Table 3 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMS.5.1C: The configuration list	O.LifeCycle-Doc	The life cycle documentation

SAR	Security Objective	Rationale
includes the following: the *intended TOE* itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the *intended TOE*; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.		(O.LifeCycle-Doc) 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 indicates the developer/subcontractor for each configuration items as described in the CM-Plan (O.LifeCycle-Doc).

Table 4 Rationale for ALC_CMS.5

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

SAR	Security Objective	Rationale
	O.Staff-Engagement O.Zero-Balance O.Transfer-Data	confidentiality and integrity of the *intended TOE* design and implementation in its development environment.
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *intended TOE*.	O.LifeCycle-Doc	The development security documentation (O.LifeCycle-Doc) justifies the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

Table 5 Rationale for ALC_DVS.2

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

Table 6 Rationale for ALC_LCD.1

8. Site Summary Specification

8.1 Preconditions required by the Site

45 The site performs production and test services for the construction of secure IC hardware (details in chapter 2.3.2)

46 In order to perform these services in a secure way, the client of the site needs to support the security processes of the site. The following paragraphs denote preconditions of the client that are required to ensure the security measures of the site in order to protect its assets.

Precondition	Assumption
The client needs to setup and maintain the used configuration management systems and provide a project specific CM plan. This includes the setup and maintenance of user accounts in the project repositories and other required configuration management tools (collabnet). The client needs to agree about the configuration management methods and the usage of the configuration management tools. The configuration management methods and tools by the client ensure the correct handling of the configuration items according to Common Criteria.	A.Setup-Projects
For each project setup, the client needs to agree on the activities to be performed by the site, the different items used (samples for analysis/failure analysis, wafer), the specifications of the input (design document when relevant, tests limits) for the site and the acceptance of the results from the site. Regarding a destruction of certain physical assets, the client need to to give instructions for the secure destruction of the assets.	A.Product-Setup,
When necessary, the site and stakeholders have to agree on cryptographic means to exchange secure data (customer code)	
The different activities can only be performed if the client and the site agree on product/item identifications.	A.Transfer-Data
Shipment related to internal (NXP or subcontractors) must follow secure shipment process. The address of the recipient must be given by the client.	A.Item-Identification

Precondition	Assumption
	A.Internal-Shipment

Table 7 Mapping of Preconditions to Assumptions

8.2 Services of the Site

47 The typical Life Cycle model for Smart Cards usually comprises the following phases: (i) Development, (ii) Validation, (iii) Production, (iv) Delivery, (v) Preparation, (vi) Operation whereas the site under evaluation supports only the life cycle phase (iii) Production

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

Phase 3: IC Manufacturing as defined in 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084), as well as characterization/validation testing of secure smart card ICs.

49 The services provided by the site are fully described in chapter 2.3.2 .

8.3 Objectives Rationale

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

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

52 O.Config-Items: The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify configuration items and allow an assignment to the client. This directly addresses the OSP P.Config-Items and P.Config-Control.

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

54 O.Physical-Access: The site implements a “need to know” principle by separation measures using a combination of physical partitioning together with technical and organisational security measures. The access control measures support the enforcement of the separation and the “need to know” principle. The handling of assets is restricted to separates security areas. By the combination of these measures

the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

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

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

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

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

59 O.Logical-Access: An Appropriate separation between the different working environment (office, development and production) including separate access control ensure access to only authorized people. This helps to prevent T.Computer-Net, T.Accident-Change, T.Unauthorised-Staff and to address P.Config-Control, P.Organise-Product.

60 O.Logical-Operation: The used workstations for development purposes are using authentication measures for the users of these systems. Hence this helps to prevent T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff to address P.Organise-Product.

61 O.Config-Items: The different items part of a TOE and the TOE itself is under configuration management. This helps to prevent T.Accident-Change and to address the OSP P.Config-Items, P.Config-Control.

62 O.Config-Control: TOE development is performed by authorized people using configuration management plan and change management. Automated tools are used for configuration management and for production control. This helps to address P.Config-Control, P.Organise-Product, P.Accept-Product.

63 O.Config-Process: Configuration management is used by the services and/or processes and all the documentation is under configuration management. This helps

to prevent T.Accident-Change and to address P.Config-Process, P.Accept-Product, P.Organise-Product and P.Product-Transport.

64 O.Internal-Shipment: The site implements protection measures to provide assurance of integrity throughout transport of physical security objects. This helps to prevent T.Attack-Transport and to address P.Product-Transport.

65 O.Control-Scrap: The security of scrap handling is ensured by either securely destruct assets (e.g. paper shredder) or return them to the client. This helps to prevent the threats T.Unauthorised-Staff and T.Staff-Collusion and addresses the OSP P.Zero-Balance and P.Scrap-Items.

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

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

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

69 O.Acceptance-Test: the site ensures products are compliant with the specifications. This addresses the OSP P.Accept-Product and addresses the threat T.Accident-Change.

70 O.Transfer-Data: The protection of exchanged sensitive data is performed using crypto algorithms and key management is well done. This helps to address P.Product-Transport and P.Transfer-Data, T.Staff-Collusion, T.Attack-Transport.

71 O.Organise-Product: The operations are ensured as planned. This helps to address P.Organise-Product,

8.4 Assurance Measure Rationale

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

73 The justification is given at the level of SAR content elements (see Table 3 to 6).

8.4.1 O.Config_IT-env

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

75 All these content elements of the SAR define required properties of the used configuration management system. Thereby this SAR is suitable to meet the security objective.

8.4.2 O.LifeCycle-Doc

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

ALC_CMC.5.12C requires that the CM documentation includes a CM plan. ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development of the TOE. ALC_CMC.5.14C requires that the CM plan describe the procedures used to accept modified or newly created configuration items as part of the TOE. ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system. ALC_CMS.5.1C requires that the CL includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan. ALC_CMS.5.2C requires that the CL uniquely identify the configuration items. ALC_CMS.5.3C requires that for each configuration item, the configuration list indicates the developer/subcontractor of the item.

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

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

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

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

81 All these content elements of the mentioned SARs require dedicated content of the CM documentation and the configuration list, properties of the SM system, content of the development security documentation and of the life-cycle and tools documentation. Thereby these SARs are suitable to meet the security objective.

8.4.3 O.Physical-Access

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

8.4.4 O.Security-Control

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

8.4.5 O.Alarm-Response

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

8.4.6 O.Internal-Monitor

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

8.4.7 O.Maintain-Security

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

8.4.8 O.Logical-Access

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

8.4.9 O.Logical-Operation

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

8.4.10 O.Config-Items

89 ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items. ALC_CMC.5.6C requires that the CM system supports the production of the product by automated means. ALC_CMC.5.8C requires that the CM system clearly identifies the configuration items that comprise the TSF. ALC_CMC.5.9C requires that the CM system supports the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail. ALC_CMC.5.10C requires that the CM system provides an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.11C requires that the CM system is able to identify the version of the implementation representation from which the TOE is generated.

90 All these content elements of the SAR define required properties of the used configuration management system. Thereby this SAR is suitable to meet the security objective.

8.4.11 O.Config-Control

91 ALC_CMC.5.2C requires that the CM documentation describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires that the CM documentation justifies that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items. ALC_CMC.5.14C requires that the CM plan describe the procedures used to accept modified or newly created configuration items as part of the TOE.

92 All these content elements of the SAR define required properties of the used configuration management system. Thereby these SARs are suitable to meet the security objective.

8.4.12 O.Config-Process

93 ALC_CMC.5.2C requires that the CM documentation describes the method used to uniquely identify the configuration items. ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items. ALC_CMC.5.6C requires that the CM system supports the production of the product by automated means. ALC_CMC.5.7C requires that the CM system ensures that the person responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.8C requires that the CM system clearly identifies the configuration items that comprise the TSF. ALC_CMC.5.9C requires that the CM system supports the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail. ALC_CMC.5.10C requires that the CM system provides an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.11C requires that the CM system is able to identify the version of the implementation representation from which the TOE is generated. ALC_CMC.5.16C requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system.

94 All these content elements of the SAR define required properties of the used configuration management system. Thereby these SARs are suitable to meet the security objective.

8.4.13 O.Internal-Shipment

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

8.4.14 O.Control-Scrap

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

8.4.15 O.Staff-Engagement

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

8.4.16 O.Zero-Balance

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

8.4.17 O.Reception-Control

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

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

8.4.18 O.Acceptance-Test

101 ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items. Thereby this SAR is suitable to meet the security objective.

8.4.19 O.Transfer-Data

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

8.4.20 O.Organise-Product

103 ALC_CMC.5.6C requires that the CM system supports the production of the product by automated means. Thereby this SAR is suitable to meet the security objective.

8.5 Mapping of the Evaluation Documentation

104 The scope of the evaluation according to the assurance class ALC comprises the processing and handling of security products and the complete documentation of the site provided for the evaluation. The specifications and descriptions provided by the client are not part of the configuration management at NXP ATTJ.

SAR	Aspects	Reference
ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*	The sources are labelled in the version control system, which is owned by CCC&S and in the local system for local procedures. The version control system is used according to O.Config_IT-env. Documents are labelled with a DOC-number, -title, -owner. Configuration Items are identified via the identifiers that are automatically provided by the system as well as the baseline labels that are given by the configuration manager.	• [NXPOMS-999116894-3989] NPI3.0 Handbook, the slide on Configuration management • [NXPOMS-999116894-3989] NPI3.0 Configuration Management References and Templates • Manage OMS Documents
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	All items can be uniquely identified by the version control system, which is owned by CCC&S or by ATTJ system for local procedures. Documents can be uniquely identified using the labelling described above. Configuration Items are identified via the identifiers that are automatically provided by the system as well as the baseline labels that are given by the configuration manager.	• [NXPOMS-999116894-3989] NPI3.0 Handbook, the slide on Configuration management • [NXPOMS-999116894-3989] NPI3.0 Configuration Management References and Templates • Manage OMS Documents
ALC_CMC.5.3C: The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate	Review board is in place for every project. Steering is done by BLs. For local procedure, reviews and acceptance are part of the DCC system.	• [NXPOMS-999116894-3989] NPI3.0 Handbook, the slide on Configuration management, Change Control Board - CCB &

SAR	Aspects	Reference
review of changes to all configuration items.		Change Control Process Outline • [NXPOMS-999116894-3989] NPI3.0 Handbook, the slide on NPI 3.0 Key Review overview – NPI Lifecycle • [NXPOMS-999116894-3989] NPI3.0 Configuration Management References and Templates • Manage OMS Documents
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	All items can be uniquely identified by the version control system, which is owned by BLs or by the local ATTJ documentation system (DCC)	• [NXPOMS-999116894-3989] NPI3.0 Handbook, the slide on Configuration management • [NXPOMS-999116894-3989] NPI3.0 Configuration Management References and Templates • Manage OMS Documents • [NXPOMS-610690506-43437] Test program Control
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	Different CM tools provide automated measures to only allow authorized changes to configuration items. Restricted access allow only authorized persons to do changes and the authorization for the change is approved by the Change Control Board using the change process	• [NXPOMS-999116894-3989] NPI3.0 Handbook, the slide on Configuration management • [NXPOMS-999116894-3989] NPI3.0 Configuration Management References and Templates • Manage OMS Documents • [NXPOMS-610690506-43437] Test program Control
ALC_CMC.5.6C: The CM system shall support the production of the TOE by automated means.	The tools used at ATTJ support the development of the TOE by automated means.	• [NXPOMS-999116894-3989] NPI3.0 Handbook, the slide on Configuration management

SAR	Aspects	Reference
		• [NXPOMS-999116894-3989] NPI3.0 Configuration Management References and Templates • Manage OMS Documents • [NXPOMS-610690506-43437] Test program Control
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	Specific roles in tools are defined in a way that the person responsible for accepting a configuration item into CM is not the person who developed it. The role Documentation Office publishes a document written by an author.	• [NXPOMS-999116894-4839] – Instruction Project Setup in CollabNet • [NXPOMS-999116894-2030] BL STI ECR Approval Form, • [NXPOMS-999116894-3989] NPI 3.0 Handbook • [NXPOMS-999116894-3989] NPI 3.0 Roles and Responsibilities.pptx • Manage OMS Documents
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	According to [7] there is no specific TOE in the main focus, therefore this is only applicable to the CM documentation and the MES Camstar. The items can be identified in the tool EnoviaNXP.	• [V6R2009] Enovia Synchronicity • Product/project specific CM plans and the CI list that is used for CC evaluation.
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.	Different CM tools like DesignSync or CollabNet provide automated means to support the audit of all changes. Documents stored in EnoviaNXP are under version control.	• [TeamForge] Technical Design - CollabNet service for BLs • [V6R2009] Enovia Synchronicity -
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the	In case a source file has been changed, the code is compiled again and all affected items are identified. Documents are checked for consistency.	• Tool documentation • [V6R2009] Enovia Synchronicity -

SAR	Aspects	Reference
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.	Different CM tools like DesignSync or CollabNet provide means to tag a release version from which the TOE is generated. The version information of documents is stored in EnoviaNXP.	• [V6R2009] Enovia Synchronicity
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	The development environment used is set up centrally according to the reference documents and a project specific CM plan.	• [NXPOMS-999116894-3989] NPI 3.0 Handbook • Product specific configuration management plan (CMP) available.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE.	The development environment used is set up centrally according to the reference documents and a project specific CM plan.	• [NXPOMS-999116894-3989] NPI 3.0 Handbook • Product specific configuration management plan (CMP) available.
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.	The development environment used is set up centrally according to the reference documents and a project specific CM plan. Documents are handled centrally after creation by the Documentation Officer.	• [NXPOMS-999116894-3989] NPI3.0 Handbook (slides referring to change control board, CCB process), • BLs Configuration Management Procedure Product specific configuration management plan (CMP) available.
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	The development environment used is set up centrally according to the reference documents and a project specific CM plan. Documents are stored in project vaults. Evidences can be provided during a site visit	• [NXPOMS-999116894-3989] NPI3.0 Handbook (slides referring to the configuration management) The development environment used is set up centrally and organized according to a project specific CM plan • Product specific configuration

SAR	Aspects	Reference
		management plan (CMP) available.
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	The development environment used is set up centrally according to the reference documents and a project specific CM plan. Documents are stored in project vaults. Evidences can be provided during a site visit	• [NXPOMS-999116894-3989] NPI3.0 Handbook (slides referring to the configuration management) The development environment used is set up centrally and organized according to a project specific CM plan

Table 8 Mapping of the Evidence for the Configuration Management Capabilities

SAR	Aspects	Reference
ALC_CMS.5.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.	In terms of site certification on the one hand the configuration list is provided in form of the tables at hand. On the other hand the configuration list is represented by the list of all applicable documents.	• Document list/Bibliography
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	Since no TOE is subject of the site evaluation the principles are defined. All configuration items are maintained in the CM systems provided by the client BLs. Every document can be uniquely identified as stated above for ALC_CMC.5.1C.	Not Applicable
ALC_CMS.5.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	The configuration list in case of site certification is the list of all applicable documents. In the document the author of each item is listed. Not applicable according to [7].	• Document list/Bibliography

Table 9 Mapping of the Evidence for the Scope of the Configuration Management

SAR	Aspects	Reference
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	Access control to wing, surveillance, alarm system and on campus guard services to prevent access to the wing for unauthorized persons.	• [NXPOMS-1719007347-5169] Site Security Manual - NXP Semiconductors ATTJ Tianjin
	Visitors, external suppliers and cleaning personnel handling	• [NXPOMS-1719007347-5169] Site Security Manual - NXP Semiconductors ATTJ Tianjin
	Handling of physical objects, zero balancing, disposal of security products	• [NXPOMS-1719007347-5169] Site Security Manual - NXP Semiconductors ATTJ Tianjin
	Trustworthiness and training of staff	• [NXPOMS-1719007347-5169] Site Security Manual - NXP Semiconductors ATTJ Tianjin
	Physical security system: operation, emergency procedures, incident handling and reporting	• [NXPOMS-1719007347-5169] Site Security Manual - NXP Semiconductors
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.	The justification is provided in this security target because it shows that all threats are addressed by the measures. In addition the measures are monitored to control the effectiveness.	• Chapter 8 of this document

Table 10 Mapping of the Evidence for the Development Security

SAR	Aspects	Reference
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	The TOE is developed and maintained according to the reference documents.	• [NXPOMS-999116894-3989] NPI3.0 Handbook
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	The sites and client procedures, tools and techniques provide the necessary control and compliance of the development environment in use.	• [NXPOMS-999116894-3989] NPI3.0 Handbook • NPI3.0 Intranet site

Table 11 Mapping of the Evidence for the Developer defined Life-Cycle Model

105 The evidence in the tables above is mapped according to the main purpose and content of the referenced documents. Nevertheless, the procedures support each other. Especially the physical and technical security measures as well as the organizational security measures including maintenance of security measures supplement each other. Also, the control during development assures the configuration management and support the personal accountability and tracing of the sources. The table above shows that all aspects of the assurance components are covered by the implemented procedures.

9. References

9.1 Literature

[1] „Site Security Target Template, Version 1.0, published by Eurosmart,“ Eurosmart, 21.06.2009.

[2] „Security IC Platform Protection Profile (BSI-PP-0035), Version 1.0,“ Eurosmart, 15.06.2007.

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

[4] Common Criteria, „Common Criteria for Information Technology Security Evaluations, Part 1: Introduction and General Model; Version 3.1, Revision 5,“ April 2017.

[5] Common Criteria, „Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5,“ April 2017.

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

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

9.2 Definitions

Client — The site providing the Site Security Target may operate as a subcontractor of the TOE manufacturer. The term “client” is used here to define this business connection. It is used instead of customer since the terms “customer” and “consumer” are reserved in CC. In this document, the terms “customer” and “consumer” are only used in the sense of the CC. Note that in this special case the client is always NXP, to which the site also belongs to.

9.3 List of Abbreviations

CC	Common Criteria
CI	Configuration Item
CL	Configuration List
CM	Configuration Management
EAL	Evaluation Assurance Level
FOI	Final Outgoing Inspection
HSM	High secure module
IC	Integrated Circuit
IP	Intellectual Property
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SSM	Site Security Manual
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation
VPM	Vacuum packing Machine