Site Security Target – NXP ATMC Austin

Revision	v1.4

Table of Contents

Table of Figures

1. 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.

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

1.1 SST Referene

3 Company: NXP Semiconductors

4 Name of site: ATMC (Austin Technology & Manufacturing Center)

5 SST Title: Site Security Target – NXP ATMC Austin

6 EAL: SARs taken from EAL6

7 Ref, version, date: NXPOMS-1719007347-4730, 10/14/2021, v1.4

1.2 Site Reference

8 The site belongs to NXP and is located at:

NXP USA, Inc
ATMC (Austin Technology & Manufacturing Center)
3501 Ed Bluestein Boulevard, Austin
TX 78736
USA,
United States

1.3 Site Description

9 The site is contained in buildings joined together (W, X, Y and Z) which is a dedicated NXP site.

10 Areas where certified activities are performed are:

- the clean room, a YELLOW area[1] 13000 m2 in both Y and Z buildings (level1). All manufacturing operations for certified products are performed here.
- Secure Cage into Building Y (red area) for secure storage (level 2) and shipment area Z building(yellow and red areas) for shipment operations (level 1).
- A Security Operation Center located at building W (level2).
- IT operations performed from clean room area described above and from local datacenter (w1238)

11 This area is exclusively occupied by NXP with restricted need to know access controlled by NXP for authorize personnel only.

[1] Areas are defined in the NXP internal document „NXPOMS-1719007347-2404 "

12 The NXP ATMC Austin Fab adopts advanced 12-inch process technology to provide the optimal combination of processes for the manufacture of secure IC's. The site manufactures secure ICs from delivered secure mask set and 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

13 For smartcard products, the site activities can be related to Phases 3 of the Lifecycle Model in [5].

The activities are: IC manufacturing (Phase 3) as defined in ' 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084).

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

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

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

16 The following services and/or processes provided by ATMC Austin 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 during the production process.

1.3.1 Supporting services

- IT infrastructure, IT administration and IT support related to the production process;
- Security Operation Center.

1.3.2 ATMC services

- Security mask management;
- Security wafer manufacturing;
- Security wafer management;
- Secure scrap management;
- Warehouse and shipment of masks/wafers.

2. Conformance Claim

17 This SST is conformant with Common Criteria Version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017, [2]
- Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 5, April 2017,[3]

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

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

19 This SST is CC Part 3 conformant.

20 There are no extended components required for this SST for the ATMC Site.

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

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

23 The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profiles [5], and is therefore suitable for the evaluation of (software for) Security ICs.

24 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.

3. Security Problem Definition

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

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

3.1 Assets

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

Physical security objects: The site has physical security objects e.g. photomasks, wafers in relation to developed 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 (Product Quality Engineering Documents, Product Documents, Data and IT process objects specifications, etc.) in relation to developed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected.

28 Note: the integrity of any machine or tools used for production and testing of wafers is not considered as an asset. The machines, tools are commercial hardware and software customized by ATMC and correct processing is ensured through calibration and regular maintenance.

3.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of assets (1) Physical security objects in the form of masks or wafers. 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) Physical security objects in the form of masks or wafers.

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 software of different clients during development/production by accident.

T.Unauthorised-Staff: Employees or subcontractors not authorized to get access to assets by violating (1) Physical security objects in the form of masks or wafers.

T.Staff-Collusion: An attacker tries to get access to assets by getting support from one employee through extortion or bribery. (1) Physical security objects in the form of masks or wafers.

T.Attack-Transport: An attacker tries to get data, specifications, photomasks or wafers during the internal shipment with the intention to compromise confidentiality and/or integrity.

29 The protection of the internal shipment is related to the exchange of data and the transport of masks and wafers.

3.3 Organizational Security Policies

30 The documentation of the site under evaluation is under configuration management. This comprises all procedures regarding the evaluated data processing, wafers production flows and the security measures that are in the scope of the evaluation.

P.Config-Items: The configuration management system shall be able to uniquely identify configuration items. This includes in this case the unique identification of items that are used at the site as well as the received and transferred and/or provided items.

31 The configuration management relies completely on the naming and identification of the received configuration items. The consistency with the expected identification is verified after receipt and each item is assigned to an internal unique identification.

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.

32 The product setup may include the following information (i) identification of the items, (ii) test program (iii) test limits and properties (iv) classification of the items (which are security relevant), (v) who (either Name of the site or the client) is responsible for destruction of defect devices, (vi) which address is used for external delivery and/or internal shipment.

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

33 The documentation with the process descriptions and the security measures of the site are under version control. Measures are in place to ensure that the evaluated status is

ensured. Tools are used to support the processes at the site. This comprises a commercial data base system.

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 product can be identified and a released production process is defined for the product. If applicable this aspect includes the check that all required information and data is available to process the items.

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 or externally delivered.

P.Zero-Balance: The site ensures that all wafers are separated and traced on a device basis. For each hand over, either an automated or an organisational “two-employees-acknowledgement” (four-eyes principle) is applied for functional and defect assets. According to the released production process the defect assets are either destroyed at the site.

P.Product-Transport: Technical and organisational measures ensure the correct labelling of the product. A controlled internal shipment and/or the external delivery is applied. The products are packed as required by the client. The in-house forwarder is used for the transfer of security products. Measures to support traceability during the transport are supported by ATMC (Austin Technology & Manufacturing Center).

P.Transfer-Data: Any data in electronic form (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 scrapped at the site in a way that the destructed items do not support any attacker.

3.4 Assumptions

34 Each site operating in a production flow must rely on preconditions provided by the previous site. Each site has to rely on the information received by the previous site/client. This is reflected by the assumptions defined below for the interface with ATMC (Austin Technology & Manufacturing Center).

A.Prod-Specification: The client must provide appropriate information (e.g. specifications, definitions, process limits, process parameters) in order to ensure an appropriate data processing and wafer production process. The

provided information includes the classification of the documents and product.

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

A.Internal-Shipment: The recipient (client) of the product is defined by the client. The client provides the address and shipping information to ATMC (Austin Technology & Manufacturing Center). The client defines the requirements for packing of security products. The address of the client is part of the setup.

A.ProdEnv-Provisionning: To enable that the site participates in the production of NXP products, NXP provides TOE items, documentation under CM and services to maintain configuration management. The configuration Managements used are under NXP Hamburg site certification.

35 The assumptions are outside the sphere of influence of ATMC (Austin Technology & Manufacturing Center). 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.

4. Security Objectives

36 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.

37 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.

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

39 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.

40 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.

41 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.

42 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 authorized 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.

43 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.

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

45 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 process to classify and introduce changes for services and/or processes of released products. Minor changes 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 classification and release of changes. This team comprises specialists for all aspects of the services and/or processes. The services and/or processes can be changed by authorised personnel only. Automated systems support configuration management and production control.

46 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 development and production of the product, 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.

47 O.Acceptance-Product: wafers are tested according to test limits in order to ensure compliance with the specification. The test results are logged to support tracing and the identification of systematic failures.

48 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.

49 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 atall times.

50 O.Zero-Balance: The site ensures that all masks and wafers are separated and traced on a device basis. Automated control and/or two employees acknowledgement during hand over is applied for functional and defective devices. According to the agreed production flow the defect devices are sent back to the client.

51 O.Reception-Control: Upon reception of masks an immediate incoming inspection is performed. 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.

52 O.Internal-Shipment: The recipient of a physical configuration item is identified by the assigned client address. The internal shipment procedure is applied to the configuration item. 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.

53 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.

-

4.1 Security Objectives Rationale

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

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

T.Rugged-Theft	O.Physical-Access O.Control-Scrap O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	O.Physical-Access ensures that the Secure Areas are physically partitioned off, so that a burglar cannot just walk in. O.Control-Scrap ensures that scrap material cannot be accessed by an authorized party O.Security-Control ensures that an attacker will be detected when trying to reach the assets through the Secure Room O.Alarm-Response supports O.Physical_Access and O.Security_Control by ensuring that a response will be given to the alarm systems and that this response is quick enough to prevent access to the assets. O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T.Rugged_Theft
T.Computer-Net	O.Logical-Operation O.Logical-Access O.Internal-Monitor O.Maintain-Security O.Staff-Engagement	O.Logical-Operation ensures that all computer systems used to manage the network are kept up to date minimizing IT weaknesses. O.Logical-Access ensures protection of the production environment from the external. O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). Together, these objectives will therefore counter T.Computer-Net.

T.Accident-Change	O.Logical-Access O.Logical-Operation O.Acceptance-Product O.Staff-Engagement O.Config-Items O.Config-Control O.Config-Process	O.Logical-Access ensures protection of the production environment from the external O.Logical-Operation ensures that all computer systems are kept up to date minimizing IT weaknesses. O.Acceptance-Product ensures that non agreed job by the client is done O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Config-Items ensures that all masks/wafers have their own identifier. O.Config-Control and O.Config-Process ensure that only authorized people are able to change process.
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Logical-Access O.Config-Control O.Config-Process O.Zero-Balance	O.Security_Control ensures that all unauthorized people who have a legitimate need to visit the Secure Areas are always accompanied. O.Physical-Access, O.Security-Control and O.Alarm-Response ensures that the unauthorized people cannot circumvent this O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Logical-Access ensures protection of the production environment due to user account and password. O.Config-Control and O.Config-Process ensure that only authorized people are able to change process. O.Zero-Balance ensures that all sensitive material are under control. Together, these objectives will therefore counter T.Unauthorised-Staff.

T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Zero-Balance O.Transfer-Data	O.Internal-Monitor and O.Maintain-Security ensure that physical accesses is well managed and maintained. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Zero-Balance ensures that all sensitive material are under control. O.Transfer-Data ensures that sensitive data are protected using encryption. Together, these objectives will therefore counter T.Staff-Collusion.
T.Attack-Transport	O.Internal-Shipment O.Transfer-Data	O.Internal-Shipment ensures that the transport is securely managed O.Transfer-Data ensures that sensitive data are protected using encryption during transport. Together, these objectives will therefore counter T.Attack-Transport.
P.Config-Items	O.Config-Items O.Reception-Control	The Security Objectives enforce the OSP. O.Config-Items ensures that all wafers have their own identifier. O.Reception-Control ensures identification to a production process. These objectives are sufficient to meet P.Config-Items.
P.Config-Control	O.Config-Items O.Config-Control O.Config-Process O.Logical-Access	The Security Objectives enforce the OSP. O.Config-Items ensures that all wafers have their own identifier. O.Config-Control and O.Config-Process ensure that only authorized people are able to change process. O.Logical-Access ensures protection of the production environment due to user account and password. These objectives are sufficient to meet P.Config-Control.
P.Config-Process	O.Config-Process O.Logical-Access	O.Config-Process ensures that documentation and production processes are under configuration management. O.Logical-Access ensures protection of the production environment due to user account and password. These objectives are sufficient to meet P.Config-Process.
P.Reception-Control	O.Reception-Control	O.Reception-Control ensures identification to a production process. This objective is sufficient to meet P.Reception-Control.

P.Accept-Product	O.Acceptance-product	O.Acceptance-product ensures that verifications are performed by the client. This objective is sufficient to meet P.Accept-Product.
P.Zero-Balance	O.Internal-Monitor O.Staff-Engagement O.Zero-Balance	O.Internal-Monitor ensures that the site is well managed at a security point of view. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Zero-Balance ensures that all sensitive material are under control. These objectives are sufficient to meet P.Zero-Balance.
P.Product-Transport	O.Config-Control O.Internal-Shipment	O.Config-Control ensures that the site has specialist for transport activities. O.Internal-Shipment ensures that the transport is securely managed These objectives are sufficient to meet P.Product-Transport.
P.Transfer-Data	O.Transfer-Data	O.Transfer-Data ensures that the site uses cryptographic algorithms to ensure confidentiality and integrity. This objective is sufficient to meet P.Transfer-Data
P.Scrap-Items	O.Control-Scrap	O.Control-Scrap ensures that the site is responsible for scrapping. This objective is sufficient to meet P.Scrap-Items

Table 1 Threats and OSP - Security Objectives Rationale

5. Extended Assurance Components Definition

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

6. Security Assurance Requirements

56 ATMC using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profiles [5].

57 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)
- Life-cycle definition (ALC_LCD.1)

58 The Security Assurance Requirements listed above fulfill the requirements of [6] 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 [6]) are used in this Site Security Target.

6.1 Application Notes and Refinements

59 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.

6.1.1 **CM Capabilities (ALC_CMC.5)**

60 According to [6] the processes rather than a TOE are in the focus of the CMC examination.

61 The configuration items for the development of the considered product type are listed in section 3.1. and in ALC_CMS.5. The CM documentation of the site must be able to maintain the items listed for the relevant life-cycle step and the CM system must be able to track the configuration items.

62 A CM system has to be employed to guarantee the traceability and completeness of the different configuration items. Appropriate administration procedures have to be provided in order to maintain the integrity and confidentiality of the configuration items.

63 For further details refer to subsection ‘Application Notes for Site Certification’ in [6] 5.1 ‘Application Notes for ALC_CMC’.

6.1.2 CM Scope (ALC_CMS.5)

64 Refer to subsection ‘Application Notes for Site Certification’ in [6] 5.2 ‘Application Notes for ALC_CMS’.

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

66 In the particular case of a Security IC the scope of the configuration management can include a number of configuration items. The configuration items already defined in section 3.1 that are considered as “TOE implementation representation” include:

- masks;
- wafers;

6.1.3 Development Security (ALC_DVS.2)

67 Refer to subsection ‘Application Notes for Site Certification’ in [6] 5.4 ‘Application Notes for ALC_DVS’.

68 If the transfer of configuration items between two site involved in the production flow is included in the scope of the evaluation (life-cycle covered by the product evaluation) this is considered as internal shipment. In general, the security requirements for confidentiality and integrity are the same but it must clearly distinguished to ensure the correct subject of the evaluation.

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

- **The combination of physical partitioning between the different access control levels together with technical and 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.**
- **Assigned personnel of the site operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, unauthorized ATMC employees, contractors and suppliers.**
- **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 or guards is short enough to prevent a successful attack.

- **The site performs security management meetings at least every six months. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures.**

- **Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorized employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.**

- **The computer systems for production are kept up-to-date (software updates, security patches, virus protection, spyware protection).**

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

6.1.4 Life-cycle Definition (ALC_LCD.1)

70 The site is not equal to the entire development environment. Therefore, the ALC_LCD criteria are interpreted in a way that only those life-cycle phases have to be evaluated which are in the scope of the site. The PPs [5] provide a life-cycle description there specific life-cycles steps can be assigned to the tasks at site. This may comprise a change of the life-cycle state if e.g. testing or initialization is performed at the site or not.

71 The PPs [5] do not include any refinements for ALC_LCD. For a site under evaluation the dependencies to other sites must be explained if they are not covered by the obvious deliverables.

72 More information can be found in the subsection ‘Application Notes for Site Certification’ in [6] 5.6 ‘Application Notes for ALC_LCD’.

6.2 Security Requirements Rationale

6.2.1 Security Requirements Rationale - Dependencies

73 The dependencies for the assurance requirements are as follows (see [3], 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

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

- ALC_LCD.1 is only partially fulfilled as the site does not represent the development environment. This is in-line with and further explained in [6] 5.6 ‘Application Notes for ALC_LCD’.

75 Refinements introduced into the SAR are in *italic*.

6.2.2 Security Requirements Rationale – Mapping

SAR	Security Objective	Rationale	Reference
ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling*.	O.Config-Items	Appropriate and consistent labelling is ensured through the CM-Plan and use of the site configuration management systems (O.Config-Items).	[7], [8]
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	Incoming inspection are based on O.Reception-Control product identification that ensures associated labeling. Labeling is mapped to the internal identification as defined by O.Config-Items. This ensures the unique identification of security products. O.Config-Control ensures that handling of each client item is released based on a defined process. This includes changes that are related to a client item. The configurations can only be done by authorized person. O.Config-Process provides a configured and controlled production process.	[7], [8]
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.Reception-Control	The adequate and appropriate acceptance procedures for configuration items are based on O.Reception-Control.	[7], [8]

ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.Reception-Control O.Config-Items O.Config-Control	O.Reception-Control includes the incoming labeling and the mapping to internal identifications. O.Config-Items includes the internal unique identification of all items that belong to a client item. Each product is setup according to O.Config-Control including all necessary items.	[7], [8]
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config-Control O.Config-Process O.Logical-Access O.Logical-Operation	O.Config-Control assigns the setup including processes and items for the production of each client item. O.Config-Process includes the control of the production processes. O.Logical-Access and O.Logical-Operation support the control by limiting the access and ensuring the correct operations for all tasks to the authorized staff.	[7], [8]
ALC_CMC.5.6C: The CM system shall support the production of the intended TOE by automated means.	O.Reception-Control O.Config-Process	O.Reception-Control includes the incoming labeling and the mapping to internal identifications using an automated database. O.Config-Process includes the automated management of the production processes.	[7], [8]
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	O.Config-Process O.Logical-Access O.Logical-Operation	O.Config-Process includes the control of the production processes. O.Logical-Access and O.Logical-Operation support the control by limiting the access and ensuring the correct authorized person for all tasks.	[7], [8]
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	O.Config-Control O.Config-Process O.Config-Items	The CM-Plan (O.Config-Control , O.Config-Process) identifies the configuration items that comprise the TSF possibly supported by the configuration management system (O.Config-Items)	[7], [8]
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the intended TOE by	O.Config-Control	O.Config-Control ensures that handling of each client item is released based on a defined process. This includes changes that are related to a client item.	[7], [8]

automated means, including the originator, date, and time in the audit trail.		The configurations can only be done by authorized person. All changes are stored in the CM system support an audit.	
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-Control	O.Config-Control ensures that handling of each client item is released based on a defined process. This includes changes that are related to a client item. Any change will result in a new process for a client item, thus implicitly indentifying all other configuration items that are affected by the change.	[7], [8]
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the intended TOE is generated.	O.Reception-Control O.Config-Items O.Config-Process	O.Reception-Control supports the identification of configuration items in order to associate to the relevant production process. O.Config-Items includes the internal unique identification of all items that belong to a client item. O.Config-Process includes the control of the production processes including all client items.	[7], [8]
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.Config-Control O.Config-Process	According to O.Config-Control the setup of each client item includes an associated CM plan including the release. O.Config-Process ensures the reliability of the processes and tools based on dedicated CM plans.	[7], [8]
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the intended TOE.	O.Config-Control O.Config-Process O.Acceptance-Product	O.Config-Control describes the management of the client items at the site. According to O.Config-Process the CM plans describe the services provided by the site. O.Acceptance-Product ensures that masks are checked according to specification.	[7], [8]
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as	O.Reception-Control O.Config-Process O.Acceptance-Product	O.Reception-Control supports the identification of configuration items in order to associate to the relevant production process.	[7], [8]

part of an intended TOE.		O.Config-Process ensures the automated control of released items. O.Acceptance-Product ensures that the masks are checked according to the specifications.	
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Reception-Control O.Config-Control O.Config-Process O.Zero-Balance	The objectives O.Reception-Control, O.Config-Control, O.Config-Process ensure that only released client items are processed. This is supported by O.Zero-Balance ensuring the tracing of all security products.	[7], [8]
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.Acceptance-Product	The verification and final check of the wafers includes the verification of the associated productions logs O.Acceptance-Product.	[7], [8]

Table 2 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale	Reference
ALC_CMS.5.1C: The configuration list shall include the following: *clear instructions how to consider these items in the list*; the evaluation evidence required by the SARs *of the life-cycle*; *development and production tools* and security flaw reports and resolution status.	O.Config-Items O.Config-Control O.Config-Process	Since the process is subject of the evaluation no products are part of the configuration list. O.Config-Items ensure unique part IDs including a list of all items and processes for this part. O.Config-Control describes the release process for each client item. O.Config-Process defines the configuration control including part IDs, procedures and processes.	SST, [11]
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config-Items O.Config-Control O.Config-Process O.Reception-Control O.Internal-Shipment	Items, products and processes are uniquely identified by the data base system according to O.Config-Items. Within the production process the unique identification is supported by automated tools according to O.Config-Control and O.Config-Process.	SST, [11]

SAR	Security Objective	Rationale	Reference
		The identification of received products is defined by O.Reception-Control. The labeling and preparation for the transport is defined by O.Internal-Shipment.	
ALC_CMS.5.3C: For each *configuration item*, the configuration list shall indicate the developer/*subcontractor* of the item.	O.Config-Items	The CI-List (O.Config-Items) indicates the developer/subcontractor for each configuration items.	SST, [11]

Table 3 Rationale for ALC_CMS.5

SAR	Security Objective	Rationale	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.	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Internal-Shipment O.Control-Scrap O.Staff-Engagement O.Logical-Access O.Logical-Operation	The development security documentation describes the physical (O.Physical-Access, O.Security-Control, O.Alarm-Response), procedural (O.Internal-Monitor, O.Maintain-Security, O.Internal-Shipment, O.Control-Scrap), personnel (O.Staff-Engagement), and logicaly (O.Logical-Operation, O.Logical-Access) security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	[9]
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.Internal-Monitor O.Logical-Operation O.Maintain-Security O.Zero-Balance O.Control-Scrap O.Reception-Control	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous justification is subject of the objectives O.Internal-Monitor, O.Logical-Operation, O.Reception-Control and O.Maintain-Security. All	[9]

SAR	Security Objective	Rationale	Reference
	O.Transfer-Data	devices including functional and non functional are traced according to O.Zero-Balance. Defective devices are securely disposed according to O.Control-Scrap. During transport, data are encrypted according to O.Transfer-Data.	

Table 4 Rationale for ALC_DVS.2

SAR	Security Objective	Rationale	Reference
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the intended TOE.	O.Config-Control O.Config-Process	The production process is defined by O.Config-Control and O.Config-Process.	[7]
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the intended TOE.	O.Config-Process O.Acceptance-Product.	The applied production process is controlled according to O.Config-Process, the wafers are checked according to O.Acceptance-Product.	[7]

Table 5 Rationale for ALC_LCD.1

7. Site Summary Specification

7.1 Preconditions required by the Site

76 This section provides background information on the assumptions defined in chapter 3.4

77 The Client (NXP) must provide appropriate information for the servcices/processes as mentionned in chapter 1.3.

Assumption	How the assumption is met with this site
A.Prod-Specification	Information necessary for wafers processing and checking process according to NXP specification are sent before activities by NXP.
A.Item-Identification	To enable the site to be able to correctly identify the products NXP needs to provide appropriately labelled items to the site (A.Item-Identification) to ensure a correct mapping to site activities.
A.Internal-Shipment	Shipment and exchanges between ATMC and NXP, they need to agree about the shipment details.
A.ProdEnv-Provisioning	TOE items, documentation necessary for production are under configuration management evaluated during the NXP Hamburg site certification.

78 Applicable policies and processes are documented and available.

7.2 Services of the Site

79 The site participates in :

- Security mask management;
- Security wafer manufacturing;
- Security wafer management;
- Secure scrap management;
- Warehouse and shipment of masks/wafers.

Moreover, the site offers for its own activities the following internal and supporting service

- IT support for production process including IT administration and IT support for tools related to the production

- A Security Operation Center managing local physical security activities.

7.3 Objectives Rationale

7.3.1 **CM capabilities (ALC_CMC.5)**

80 Configuration Management is described in [6].

81 For full detail and evidences please view Section 6.2.2

7.3.2 **CM scope (ALC_CMS.5)**

82 Configuration Management is described in [6].

83 For full detail and evidences please view Section 6.2.2

7.3.3 **Development Security (ALC_DVS.2)**

84 Development Security is described in [6].

85 For full detail and evidences please view Section 6.2.2

86 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.

87 O.Security-Control: The site is using dedicated personnel for guard services. This personnel is 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.

88 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.

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

90 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.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

91 O.Logical-Access: The used workstations for production purposes are using authentication measures for the users of these systems. Hence the threats T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff is prevented and the OSP P.Config-Control and P.Config-Process addressed.

92 O.Logical-Operation: The network used at the site is connected only to dedicated trustworthy systems. All network segments are separated and the computer systems are kept up-to-date. This prevents the threats T.Computer-Net, T.Accident-Change.

93 O.Config-Items: All wafers are tracked during the manufacturing are based on a unique number. This prevents the threat T.Accident-Change and directly addresses the OSP P.Config-Items as well as the OSP P.Config-Control.

94 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 process to classify and introduce changes for services and/or processes of released products. The services and/or processes can be changed by authorised personnel only. By the combination of these measures the threat T.Accident-Change and T.Unauthorised-Staff can be prevented and directly addresses the OSP P.Config-Control and P.Product-Transport.

95 O.Config-Process: The site controls its services and/or processes using a configuration management plan. This includes also shipping and thus addresses the threats T.Accident-Change, T.Unauthorised-Staff and the OSPs P.Config-Control and P.Config-Process.

96 O.Acceptance-Product: The data processing and manufacturing of the wafers comprises verification steps either by the client or internally according to specifications. This prenvents T.Accident-Change and addresses also the OSP P.Accept-Product.

97 O.Control-Scrap: The material to be scrapped is stored in a secure area. This directly addresses the OSP P.Scrap-Items and helps to prevent the threats T.Rugged-Theft.

98 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, T.Accident-Change and T.Computer-Net and addresses the OSP P.Zero-Balance.

99 O.Zero-Balance: Products are uniquely identified throughout the whole process. Whithin the process flow, an automated tracking is in place completed by Four-eyes principle outside the process flow. This security objective is supported by O.Physical-Access, O.Config-Items and O.Staff-Engagement. The combination of measures addresses the threats T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance.

100 O.Reception-Control: Inspection at reception is counting the number of boxes and checking the shipping list if applicable. Thereby only correctly identified masks are accepted for production. OSPs P.Config-Items and P.Reception-Control are addressed by the reception control.

101 O.Internal-Shipment: The site implements protection measures to provide assurance of integrity throughout shipment of physical security objects. Hence, the threat T.Attack-Transport is prevented and the OSP P.Product-Transport addressed.

102 O.Transfer-Data: During transport of logical assets, protection against disclosure and modification is ensured by cryptographic means which are appropriate to resist against high attack potential. Cryptographic keys and passwords are protected against unauthorised access. The threats T.Staff-Collusion and T.Attack-Transport are prevented and the OSP P.Transfer-Data is addressed.

7.3.4 Life Cycle definition (ALC_LCD.1)

103 Life cycle definition is described in [6].

104 For full detail and evidences please view Section 6.2.2

7.3.5 Security Objectives and security requirements

105 The following section provides a rationale for each security objective for the development environment (as defined in chapter 4), why each of the assigned SARs (as given in section 6.2.2 is suitable to meet the security objective.

106 The justification is given at the level of SAR content elements (see Table 1 to Table 6).

7.3.6 O.Physical-Access

107 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.

7.3.7 O.Security-Control

108 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.

7.3.8 O.Alarm-Response

109 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.

7.3.9 O.Internal-Monitor

110 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. ALC_DVS.2.2C require the development security

documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby these SARs are suitable to meet the security objective.

7.3.10 **O.Maintain-Security**

111 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. ALC_DVS.2.2C require the development security documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby these SARs are suitable to meet the security objective.

7.3.11 **O.Logical-Access**

112 ALC_CMC.5.5C requires the CM system to provide automated measures such that only authorised changes are made to the configuration items. ALC_CMC.5.7C requires the CM system to ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.

113 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.

7.3.12 **O.Logical-Operation**

114 ALC_CMC.5.5C requires the CM system to provide automated measures such that only authorised changes are made to the configuration items. ALC_CMC.5.7C requires the CM system to ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.

115 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. ALC_DVS.2.2C require the development security documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby these SARs are suitable to meet the security objective.

116 Thereby this objective is suitable to meet the Security Assurance Requirement.

7.3.13 **O.Config-Items**

117 ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configura tion items. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.8C requires the CM system to identify the configuration items that comprise the TSF. ALC_CMC.5.11C requires the CM system to be able to identify the version of the implementation representation from which the product is generated.

118 ALC_CMS.5.1C requires that the configuration list shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_CMS.5.3C requires for each TSF relevant configuration item, that the configuration list indicated the developer of the item.

119 Thereby this objective is suitable to meet the Security Assurance Requirement.

7.3.14 O.Config-Control

120 ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.5C requires the CM system to provide automated measures such that only authorised changes are made to the configuration items. ALC_CMC.5.8C requires the CM system to identify the configuration items that comprise the TSF. ALC_CMC.5.9C requires the CM system to support the audit of all changes to the product 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.5.12C requires the CM documentation to include a CM plan. ALC_CMC.5.13C requires the CM plan to describe how the CM system is used for the development of the product. ALC_CMC.5.15C requires evidence to demonstrate that all configuration items are being maintained under the CM system.

121 ALC_CMS.5.1C requires that the configuration list shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.

122 ALC_LCD.1.1C requires that the life cycle documentation shall describe the model used to develop and maintain the intended TOE.

123 Thereby this objective is suitable to meet the Security Assurance Requirement.

7.3.15 O.Config-Process

124 ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.5C requires the CM system to provide automated measures such that only authorised changes are made to the configuration items. ALC_CMC.5.6C requires the CM system to support the production of the product by automated means. ALC_CMC.5.7C requires the CM system to ensure that the person responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.8C requires the CM system to identify the configuration items that comprise the TSF. ALC_CMC.5.11C requires the CM system to be able to identify the version of the implementation representation from which the product is generated. ALC_CMC.5.12C requires the CM documentation to include a CM plan. ALC_CMC.5.13C requires the CM plan to describe how the CM system is used for the development of the product. ALC_CMC.5.14C requires the CM plan to describe the procedures used to accept modified or newly created configuration items as part of the product. ALC_CMC.5.15C requires evidence to demonstrate that all configuration items are being maintained under the CM system.

125 ALC_CMS.5.1C requires that the configuration list shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C requires that the configuration list shall uniquely indetify the configurantion items.

126 ALC_LCD.1.1C requires that the life cycle documentation shall describe the model used to develop and maintain the intended TOE. ALC_LCD.1.2C requires that the life cycle model shall provide for the necessary control over the development and maintenacne of the intended TOE.

127 Thereby this objective is suitable to meet the Security Assurance Requirement.

7.3.16 **O.Acceptance-Product**

128 ALC_CMC.5.13C requires the CM plan to describe how the CM system is used for the development of the product. ALC_CMC.5.14C requires the CM plan to describe the procedures used to accept modified or newly created configuration items as part of the product. ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM suystem is neing operated in accordance with the CM plan.

129 ALC_LCD.1.2C requires that the life cycle model shall provide for the necessary control over the development and maintenacne of the intended TOE.

130 Thereby this objective is suitable to meet the Security Assurance Requirement.

7.3.17 **O.Control-Scrap**

131 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. ALC_DVS.2.2C require the development security documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby these SARs are suitable to meet the security objective.

7.3.18 **O.Staff-Engagement**

132 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.

7.3.19 **O.Zero-Balance**

133 ALC_CMC.5.15C requires evidence to demonstrate that all configuration items are being maintained under the CM system.

134 ALC_DVS.2.2C require the development security documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

135 Thereby this objective is suitable to meet the Security Assurance Requirement.

7.3.20 **O.Reception-Control**

136 ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires the CM documentation to justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.6C requires the CM system to support the production of the product by automated means. ALC_CMC.5.11C requires the CM system to be able to identify the version of the implementation representation from which the product is generated. ALC_CMC.5.14C requires the CM plan to describe the procedures used to accept modified or newly created configuration items as part of the product. ALC_CMC.5.15C requires evidence to demonstrate that all configuration items are being maintained under the CM system.

137 ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.

138 ALC_DVS.2.2C require the development security documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

139 Thereby this objective is suitable to meet the Security Assurance Requirement.

7.3.21 **O.Internal-Shipment**

140 ALC_CMS.5.2C requires that the configuration list shall uniquely indetify the configurantion items.

141 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.

142 Thereby this objective is suitable to meet the Security Assurance Requirement.

7.3.22 **O.Transfer-Data**

143 ALC_DVS.2.2C requires confidentiality and integrity of the product during internal shipment. Thereby this objective is suitable to meet the Security Assurance Requirement.

8. References

8.1 Literature

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

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

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

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

[5] „Security IC Platform Protection Profile with Augmentation Packages Version 1.0 (BSI-PP-0084),“ Eurosmart, 13.01.2014

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

[7] NXPOMS-1719007347-2549 ALC-CM Common Criteria Documentation

[8] NXPOMS-999116894-3989 NPI 3.0 Hanbook - CM slides

[9] Site Security Manual ATMC

[10] Minimum Site Security Requirements v3.0 Feb; 2020

[11] ATMC Configuration List

8.2 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.

Production Process — “Production Process” here refers to the processes and flows that are set up for internal shipment and external delivery (forwarding or storing and shipping of items).

8.3 List of Abbreviations/Glossary

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

8.4 Revision History

Revision	Description	Author	Approval - Date
1.2	Previous version with other template	Christophe Bouly	7 October 2019
1.3	Answering comments from Applus (CCENXP002R1-OR002-M0) and change reference 2798 to 4730	Christophe Bouly	12 August 2021
1.4	Based on september draft version: typos corrections due to ref change and details description on chapter 1.3	Christophe Bouly	14 October 2021

Approvers

Sequence	Role	Name
Acceptance	Security Manager	Christophe Bouly
Approval	Security Manager	Gordon Caffrey