Tongxin Microelectronics Co., Ltd.

Site Security Target Lite TMC Development Center

Confidential Level: 【Public】

Version	A
Date	2024-3-18

Contents

List of tables

1 Document Information

1.1 Reference

Title: Site Security Target Lite TMC Development Center

Version/Date: Version A/18.3.2024

Company: Tongxin Microelectronics Co., Ltd.

Name of the site: TMC Development Center

Product Type: Security IC hardware and software (such as the Crypto Library, the boot code of the chip which namely the firmware) design and development, IC embedded software development.

Evaluation Assurance Components: ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1 and ALC_DEL.1.

2 SST Introduction

This chapter is divided into the sections 2.1 Identification of the Site and 2.2 Site Description.

This site security target refers to the following site:

TMC Development Center

The site is used for security IC hardware and software design and development and IC embedded software development.

Tongxin Microelectronics Co., Ltd.(hereinafter referred to as ‘TMC’)

2.1 Identification of the Site

The TMC Development Center is located at:

Floor 1 and 4, Building B1, Zhongguancun Dongsheng Science and Technology Park, 66 XiXiaokou Road, Haidian District, Beijing, China.

TMC Development Center will be abbreviated by ‘TDC’ throughout the rest of the document.

2.2 Site Description

The TMC is located in one building inside a campus where the security guards and anti-tailgating access control door is deployed at the campus main entrance. TDC site belonging to TMC and is incharge of the development for security IC software and hardware. Only four areas in TMC fall in the scope of this SST - that termed TDC. The rest of the TMC areas are used for

administration affairs, general non-security IC product R&D and some testing activities.

There is one main entrance at the 1st floor for this site, only TMC employees can access. The entrance is monitored by CCTV, reception employee and security guard at real time for 24/7 and with the access control system protected.

The warehouse and IT server room are located at the 1st floor of TDC site, enclosed R&D area and data transmit area are located at the 4th floor where the security IC dedicated software and hardware, embedded software development activities are conducted. Both of these 4 areas are classified as high security areas by TMC and with the most strict protection security measures such as access control door with badge and PIN, door left open alarm, CCTV, sensors for infrared intrusion detection, glass breaking and wall vibration deployed.

The following areas within the building fall in the scope of audit:

- Warehouse
- IT Server Room
- Enclosed R&D Area
- Data Transmit Area

The following services and processes provided by TDC are in the scope of the evaluation process:

- Security IC software and hardware design and development, layout data such as GDS file formulation and sending to wafer foundry.
- IC embedded software development, management, storage and shipment.
- Sample receiving, management, storage and shipment.

- (In some rare cases) Enciphered IC embedded software (Chip OS, termed as COS)receiving, management, storage.
- CP/FT(Final test) testing program/instruction formulation, management, storage and delivered to CP testing site and packaging site.
- CP/FT testing result receiving, management and storage.
- Production data(such as COS downloading/testing, Personalization production/testing vector, production instruction, etc.) formulation and sending to packaging site and card manufacture.
- Product User Manual(IC and COS) formulation and sending to customer.

TDC conducts security IC hardware and software(crypto library, the boot code of the chip) development and the IC embedded software in enclosed R&D and data transmit area, During the IC design process, GDS file will be the output and sent to the IC manufactures for data handling from data transmit area, then the mask data will be transferred to mask manufactures for mask production, the mask will be delivered to wafer foundry for wafer production. Then the testing program and instruction will be formulated and sent to CP testing site for CP test to distinguish the die quality on wafer. After CP testing, the wafer will be delivered to packaging site. During the packaging process, the production and final test instruction will be formulated and sent to packaging site for chip packaging and final test. Besides, samples will be produced and sent to TDC for inspection before mass production. The IC product user manual will be formulated and sent to customer for future usage.

Regarding the IC embedded software development process, COS file and vectors will be the output and sent to the packaging site or the card manufactures

for downloading and testing. Besides, the product manual will also be formulated and sent to the client to develop the applet.

Cause the network used for security IC software/hardware development and IC embedded software development is physically isolated, data transmit area is the connection point between the internal and outside network.

Supporting Services of TDC site include the following:

- Security measures internal audit (access control system and IT infrastructure logs audit, etc.) and maintenance
- Network separation and IT system access control
- IT infrastructure maintenance (software updates, security patches, virus protection, etc.)
- Sensitive data and security relevant logs backup and backup access control
- Employee training, background check and NDA signing.

The TDC covers phase 1(IC embedded software development) and phase 2(IC Development) according to protection profile [1].

Since a site certification formally does not cover 'TOEs' in the sense of CC but only sites which handle items related to a TOE in a product certification, the term 'TOE related item' is widely used instead of TOE in this document. This comprises all items that belong to a future TOE like source code files and guidance documentation, etc. Please note that a reference to 'TOE related items' in this document might not necessarily covers all TOE related items but only some of them. When the document refers to a TOE which is expected to be developed at this site the term 'future TOE' is used.

3 Conformance Claim

The evaluation is based on Common Criteria Version 3.1, Revision 5.

- Common Criteria for Information Technology Security Evaluation, Part1: Introduction and general model; Version 3.1, Revision 5, April 2017, [2]
- Common Criteria for Information Technology Security Evaluation, Part3: Security assurance components; Version 3.1, Revision 5, April 2017, [3]

For the evaluation, the methodology will be used:

- Common Methodology for Information Technology Security Evaluation: Evaluation methodology. Version 3.1, Revision 5, April 2017, [4]
- Supporting Document, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007, [5]
- JIL-Minimum Site Security Requirements v3.0, February 2020, [6]

The assurance components chosen for the Site Security Target are taken from the definition of the EAL 6 package defined in [3].

This Site Security Target (SST) is CC Part 3 conformant, which consists of the following CC assurance components:

ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1 and ALC_DEL.1

For the assessment of the security measures attackers with high attack potential are assumed. This allows an evaluation of products using this site according to the assurance component AVA_VAN.5.

Note:

ALC_TAT is omitted, because the development tools and its versions are TOE specific and therefore it is more efficient to cover the whole ALC_TAT together at the product evaluation time.

4 Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site and security problems derived from the configuration management requirements. The configuration management covers the integrity of the TOE related items and the security management of the site.

The Security Problem Definition comprises two major so called security problems. The first set of security problems comprises various attacks regarding theft (e.g. samples) or disclosure (e.g. design data) or manipulation of assets. These security problems are described in terms of Threats. The second set of security problems comprises the requirements for the configuration management (e.g.controlled modification) and the control of security measures. These security problems are described in terms of Organizational Security Policies (OSP).

4.1 Assets

The following section describes the assets handled at the site:

Name and ID	Type	Asset Value
A.DOC Security documentation (such as TMC internal management procedures and policies, instructions, specifications, guidance or any other documentations related to the development process, the confidential product documentation.)	Electronic documentation	Confidentiality Integrity
A.SAMPLE Samples delivered from chip packaging	Physical object	Confidentiality

site and card manufactures to TDC for conducting evaluation and qualification before mass production.		Integrity
A.DATA Sensitive data or items (such as source code in any form, CP/FT testing program, GDS file, COS file, layout data for the hardware and other data related with the security IC software and hardware development and IC embedded software development process)	Electronic data	Confidentiality Integrity

4.2 Threats

The term ‘sensitive configuration item’ has been replaced by ‘sensitive data or items’, because not only the theft or modification of sensitive configuration items but also of other data kept outside the configuration management system might compromise the security of TOE related items or future TOEs.

T.Attack-Transport: An attacker might try to get sensitive data and items, documentation or samples during the shipment. The target is to compromise confidential information or violate the integrity of the TOE related items during the stated shipment to allow a modification, cloning or the retrieval of confidential data and product documentation.

T.Computer-Net: A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get data such as source code or sensitive data or modify security relevant processes such as the development process at the site.

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

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive data or items. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered. In addition, the attacker may be able to use specific working clothes of the site to camouflage the intention.

T.Staff-Collusion: An attacker tries to get access to sensitive data or items stored or processed at the site. The attacker tries to get support from one or more employees through an attempted extortion or an attempt at bribery.

T.Unauthorised-Staff: Employees or subcontractors not authorised to get access to products or systems used for development, get access to sensitive data or items or affect development systems or configuration systems, so that the confidentiality and/or the integrity of TOE related items is violated. This can apply to development and any TOE related item as well as to the future TOE, its configuration or other sensitive data.

4.3 Organizational Security Policies

The following policies are introduced by the requirements of the assurance components of ALC for the assurance level EAL 6. The chosen policies support the understanding of the development flow and the security measures of the site. In addition, they shall allow an appropriate mapping to the Security Assurance Requirements (SAR).

P.Accept-Product: In case the client requires formal release of the developed items, the quality control of the site ensures that the released future TOEs comply with the specification agreed with the client. The acceptance process is supported by automated measures. Records are generated for the acceptance process of TOE related items. Thereby, it is ensured that the properties of the future TOE are ensured when internally shipped or externally delivered.

P.Config-Control: The procedures for setting up the development process for a future TOE as well as the procedure that allows changes of the initial setup for a future TOE shall only be applied by authorized personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes.

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

P.Config-Process: The services and processes provided by the site are controlled in the configuration management plan. This comprises tools used for the development of the future TOE, the management of flaws and optimizations of the process flow as well as the documentation that describes the services and processes provided by the site.

P.Organise-Product: The development process is applied as specified by the site's quality management documentation. If the related data includes sensitive items appropriate measures must be in place.

P.Product-Transport: Technical and organizational measures shall ensure the correct labeling of the future TOE and samples. A controlled shipment process 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 future TOE and samples during transport.

P.Reception-Control: The inspection of incoming requirements specifications from the client or samples from chip packaging site or card manufactures done at the site ensures that developed future TOEs comply with the requirements specified by the client. The inspection of incoming requirements from the chip manufacturer (i.e. datasheets and security manuals) at the site ensures that the developed future TOEs comply with the requirements specified by the chip manufacturer.

4.4 Assumptions

Each site operating in a development or 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 that must be defined for the interface.

The following assumption is considered to be applicable to all sites.

A.Item-Identification: Each configuration item shipped from the client to the development site is uniquely labeled by the client to ensure the identification of the configuration item.

A.Internal-Shipment: The recipient (client) of the future TOE is identified by the address of the client site for physical items and by corresponding information (e.g. email address) for electronic items.

A.Prod-Specification: The client must provide appropriate requirements in order to perform the development process.

5 Security Objectives

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

O.Acceptance-Test: The site delivers future TOE (in the form of GDS file) that fulfil the specified properties. The formal prove for that will be provided by the site. Before the software and hardware development process finished, all the functions of the security IC and the units of code are verified and tested, all the bugs are fixed, besides, the reviewing meeting will be held and with the approval is made by the project manager. Upon release of the future TOE, verification and functional simulation, design checklist reviewing are performed to ensure the compliance with the specification and requirement. The above tape out process results are logged as report to support tracing and the identification of systematic failures.

O.Alarm-Response: The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any sensitive TOE related item (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.

O.Config-Control: The site applies a release procedure for each new future TOE. In addition, the site has a process to classify and introduce changes for released future TOEs. A designated team is responsible for the release of new future and for the classification and release of changes.This team comprises specialists for all aspects of the services and/or processes.

Changes can be conducted by authorized personnel only. Automated systems support configuration management and development control.

O.Config-Items: The site has a configuration management system that assigns a unique internal identification to each configuration item. In addition, any future TOE consisting of several configuration items can be uniquely identified by unique labels management.

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 of future TOEs and for the management of security flaws.

O.Control-Scrap: The site has measures in place to destroy sensitive documentation and erase electronic media so that they do not support an attacker.

O.External-Delivery: The recipient of the product user manual(including the IC and COS product user manual) is identified by the assigned consumer email address. The external delivery procedure is applied to the product user manual. The recipient for shipment can only be changed by a controlled process. The PGP encryption mechanism is deployed for the item confidentiality and integrity verification.

O.Internal-Monitor: The site performs security management meetings once a year. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures.

O.Internal-Shipment: The recipient of a physical TOE related item is identified by the assigned client address. The recipient(s) of an electronic TOE related item or future TOE (e.g. CP testing program and GDS file) can be identified in different ways. The specific way is defined in the internal shipment procedure. The internal shipment procedure is applied to all shipped TOE related items or future TOE. The recipient 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 TOE related items or future TOE during internal shipment. For every sensitive TOE related item or future TOE, the protection measures against manipulation are defined (e.g. sealed boxes, encryption, integrity protection, electronic signature).

O.Logical-Access: The site enforces a logical separation between the internal network and the internet by a firewall system. The firewall ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into a enclosed development network which is physically isolated from internet and an office network. Access to the enclosed development network and related systems is restricted to authorized employees that work in the related area or that are involved in the configuration tasks or the development systems. Every user of an IT system has its own user account and password. Authentication using user account and password is enforced by all computer systems.

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

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 authorized employees have access to sensitive areas as well as computer and network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.

O.Organise-Product: For the development process it is ensured that the specified process and implementation standards are applied.

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organizational security measures allow a sufficient separation of employees to enforce the 'need to know' principle. The access control shall support the limitation of access to these areas including the identification and rejection of unauthorized people. The access control measures ensure that only registered employees and visitors can access restricted areas. Sensitive TOE related items are handled in restricted areas only.

O.Reception-Control: Upon reception of samples by the warehouse staff, the authenticity of the samples is verified. Upon reception of a requirement from a client the authenticity of the requirement is verified.

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

O.Staff-Engagement: All employees who have access to sensitive TOE related items and who can move them out of the defined development flow are checked regarding security concerns and must sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.

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

5.1 Security Objectives Rationale

The SST includes a Security Objectives Rationale with two parts. The first part describes a tracing which shows how the threats and OSPs for the development site 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.

5.1.1 Mapping Security Objectives and Rationale

Threat and OSP	Security Objective	Rationale
T.Attack-Transport	O.External-Delivery O.Internal-Shipment O.Transfer-Data	O.External-Delivery, O.Internal-Shipment and O.Transfer-Data ensures the address for recipient is identified by the assigned physical location and logical email address or webportals. The data encryption is needed to prevent modification or disclosure during transmission. Besides, the applied security measures on physical items during internal shipment allow detection of attempted attacks. Therefore these security objectives are suitable to prevent this threat.
T.Computer-Net	O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement	O.Logical-Access ensures the network is separated (physically isolated towards the enclosed R&D network) and firewall protected, access control to the network is also deployed. O.Logical-Operation ensures the latest updates for the system. O.Maintain-Security ensures the logs are checked to detect the intrusion and also ensures the logical system is properly working. O.Internal-Monitor ensures the internal audit is conducted to review the logical protection measures.

		O.Staff-Engagement ensures the employees are secured through the training, NDA signing and background checking. Therefore these security objectives are suitable to prevent this threat.
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	O.Physical-Access ensures the area is protected by access control system, only the authorized persons could access to the corresponding areas. Visitors are escorted all the time. Besides the access control, O.Alarm-Response and O.Security-Control ensure the site is protected by the CCTV and infrared/wall vibration/glass breaking sensors. The dedicated personnel will monitor the alarm system at real time and respond to the event immediately. O.Internal-Monitor ensures the internal audit is conducted to review the physical protection measures. O.Maintain-Security ensures the facilities condition is good and logs are checked to keep the proper working.Therefore these security objectives are suitable to prevent this threat.
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	O.Physical-Access ensures the area is protected by access control system, only the authorized persons could access to the corresponding areas. Visitors are escorted all the time. Besides the access control, O.Alarm-Response and O.Security-Control ensure the site is protected by the CCTV and infrared/wall vibration/glass breaking sensors. The dedicated personnel will monitor the alarm system at real time and respond to the event immediately. O.Internal-Monitor ensures the internal audit is conducted to review

		the physical protection measures. O.Maintain-Security ensures the security facilities condition is good and logs are checked to keep the proper working. Therefore these security objectives are suitable to prevent this threat.
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Transfer-Data O.Control-Scrap	O.Internal-Monitor ensures the internal audit is conducted annually to assess all the protection measures are working well. O.Maintain-Security ensures the security facilities condition is good and logs are checked to keep the proper working. O.Staff-Engagement ensures the employees are secured through the training(employees have a good knowledge of information security requirement), NDA signing and background checking. O.Transfer-Data and O.Control-Scrap ensures the data is encrypted and secured during the transmission and disposal to avoid the disclosure by an attacker. Therefore these security objectives are suitable to prevent this threat.
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.Control-Scrap	O.Physical-Access ensures the area is protected by access control system, only the authorized persons could access to the corresponding areas. Visitors are escorted all the time. Besides the access control, O.Alarm-Response and O.Security-Control ensure the site is protected by the CCTV and infrared/wall vibration/glass breaking sensors. The dedicated personnel will monitor the alarm system at real time and respond to the intrusion event immediately. O.Internal-Monitor ensures the internal audit is conducted to review the protection measures. O.Maintain-Security ensures the

		facilities condition is good and logs are checked to keep the proper working. O.Logical-Access and O.Logical-Operation ensure that only the authorized employees have the accounts to access the PC, network and systems. O.Staff-Engagement ensures the employees have a good knowledge of information security requirement by training.O.Control-Scrap ensures the data is encrypted and secured during the transmission and disposal to avoid the disclosure. Therefore these security objectives are suitable to prevent this threat.
P.Accept-Product	O.Config-Control O.Config-Process O.Acceptance-Test	O.Config-Control and O.Config-Process ensures the automatic CM system is operating properly based on the CM plan to support the future TOE acceptance. O.Acceptance-Test directly cover the P.Accept-Product. Therefore these security objectives are suitable to cover this OSP.
P.Config-Control	O.Config-Control O.Logical-Access	O.Logical-Access ensure that only the authorized employees have the accounts to access the PC, network and CM system. O.Config-Control directly cover the P.Config-Control. Therefore these security objectives are suitable to cover this OSP.
P.Config-Items	O.Config-Items	O.Config-Items directly enforce P.Config-Items. Therefore this security objective is suitable to cover this OSP.
P.Config-Process	O.Config-Process	O.Config-Process directly enforce P.Config-Process. Therefore this security objective is suitable to cover this OSP.

P.Organise-Product	O.Logical-Operation O.Logical-Access O.Config-Control O.Config-Process O.Organise-Product	O.Logical-Operation and O.Logical-Access ensure sensitive data can only be handled in the isolated and secured IT environment, only the dedicated employees have the access to these items. O.Config-Control and O.Config-Process ensure that automatic CM system is operating properly based on the CM plan defined for the sensitive data management. O.Organise-Product directly cover P.Organise-Product. Therefore these security objectives are suitable to cover this OSP.
P.Product-Transport	O.Config-Items O.External-Delivery O.Internal-Shipment O.Transfer-Data	O.Config-Items ensures the unique and correct labelling. O.External-Delivery, O.Internal-Shipment and O.Transfer-Data ensure the physical goods and logical data is secured during the internal shipment and external delivery. The traceability could also be tracked. Therefore these security objectives are suitable to cover this OSP.
P.Reception-Control	O.Reception-Control	O.Reception-Control directly enforce P.Reception-Control. Therefore this security objective is suitable to cover this OSP.

Table 1: Security problem definition to security objectives mapping

6 Extended Components Definition

No extended components are defined in this Site Security Target.

7 Security Assurance Requirements

The security assurance requirements for this Site Security Target are ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1 and ALC_DEL.1.

The Security Assurance Requirements (SAR) for the Class ALC (Life-cycle support) are:

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

The Security Assurance Requirements listed above fulfil the requirements of [5] 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 [5]) are used in this SST.

The dependencies for the assurance requirements named above are as follows:

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

The following dependency is not fulfilled or not completely fulfilled:

ALC_LCD.1: ALC_LCD.1 is part of this Site Security Target but doesn't cover TOE specific information of the life-cycle definition.

NOTE: ALC_TAT is omitted, because the development tools and its versions are TOE specific and therefore it is more efficient to cover the whole ALC_TAT together at the product evaluation time.

7.1 Application Notes and Refinements

The description of the site certification process [5] includes specific application notes. The main item is that a future TOE is not available during the evaluation. Since the term 'TOE' is not applicable in the SST the associated processes for the handling of TOE related items are in the focus and described in this SST. These processes are subject of the evaluation of the site.

Refinements regarding Security Assurance Requirements as defined in CC Part 3 [3] are written in *italic*. The term 'TOE' is replaced by 'future TOE' or 'TOE related items' depending on the specific case.

7.1.1 Overview regarding CM capabilities (ALC_CMC)

A configuration management system is used to manage all sensitive data of a future TOE under development.

According to [5] the processes rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below.

The use of the configuration management system and the application of a defined change process for the procedures of the site under evaluation are mandatory. The control process must include all procedures that have an

impact on the evaluated development processes as well as on the site security measures.

All items listed as assets in section 4.1 are kept within the configuration management system.

7.1.2 Overview regarding CM scope (ALC_CMS)

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

For this site all items listed as assets in section 4.1 are kept within the configuration management system.

7.1.3 Overview regarding Development Security (ALC_DVS)

The CC assurance components of family ALC_DVS refer to (i) the 'development environment', (ii) to the 'TOE' or 'TOE design and implementation'. The component ALC_DVS.2 'Sufficiency of security measures' requires additional evidence for the suitability of the security measures.

The manufacturer of the future TOEs must ensure that the development and production of the future TOEs is secure so that no information is unintentionally made available for the operational phase of the future TOEs. The confidentiality and integrity of design information, test data, configuration data must be guaranteed, access to any kind of samples, development tools and other material must be restricted to authorized persons only, and scrap must be controlled and destroyed.

Based on these requirements the physical security as well as the logical security of the site are in the focus of the evaluation. Beside the pure

implementation of the security measures also the control and the maintenance of the security measures must be considered.

If the transfer of configuration items between two sites involved in the development 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 are the same but it must clearly distinguish to ensure the correct subject of the evaluation. In addition, internal shipment between two development sites has to be covered by ALC_DVS.

7.1.4 Overview regarding Life-cycle definition (ALC_LCD)

The site is not necessarily 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. For this site the Life Cycle phase ‘Development’ is relevant.

7.1.5 Overview regarding Delivery (ALC_DEL)

The delivery aspect refers to the delivery of IC and COS product user manuals to the consumer.

7.2 Security Assurance Requirements Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components of [3] to the Security Objectives defined in this SST. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of future TOEs. If the site already receives TOE related items,

this process is based on the assumption that the delivered TOE related items are appropriately labeled and identified, refer to A.Item-Identification.

Note: The content elements that are changed from the original CEM [4] according to the application notes in the process description [5] are written in *italic*. The term 'TOE' can be replaced by 'TOE related items' or 'future TOE'.

7.2.1 Rationale for ALC_CMC.5

SARs	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-Items O.Reception-Control	Upon reception of an item from another site O.Reception-Control ensures that authenticity is verified for the shipped item. With this it is ensured that the item has been labeled before delivery. After integration into the CM system, O.Config-Items ensures appropriate and consistent labeling as well as unique identification of the item.
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Config-Process	O.Config-Process ensures the site is using the configuration management plan supported by tools and procedures to uniquely identify the configuration items.
ALC_CMC.5.3C: The CM documentation shall justify that the acceptance	O.Config-Process	The adequate and appropriate acceptance procedures for configuration items are described in the CM-Plan which is ensured by O.Config-Process.

procedures provide for an adequate and appropriate review of changes to all configuration items.		
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.Config-Items	O.Config-Items ensures appropriate and consistent labelling as well as unique identification of the item.
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	O.Config-Control O.Config-Process O.Logical-Access	The configuration management systems used according to the CM-Plan (required by O.Config-Process) enforces automated measures (required by O.Config-Control) and (required by O.Logical-Access) such that only authorized changes are made to the configuration items.
ALC_CMC.5.6C: The CM system shall support the production of the *future TOE* by automated means.	O.Config-Control	O.Config-Control ensures the automated CM system supports development of products.
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is	O.Config-Control O.Config-Process	As described in the CM-Plan (required by O.Config-Process) the activities performed (required by O.Config-Control) are such that the person responsible for accepting a configuration item into CM is not the person who developed it.

not the person who developed it.		
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	O.Config-Process	The CM-Plan as described by O.Config-Process identifies the configuration items that comprise the TSF, supported by the configuration management system.
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the *future TOE* by automated means, including the originator, date, and time in the audit trail.	O.Config-Process	As described in O.Config-Process the site is using the configuration management plan supported by tools which is 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-Process	O.Config-Process ensures the site is using the configuration management plan supported by tools and procedures, and that the CM system deployed at the site has the function to automatically identify all other configuration items that are affected by the change of a given configuration item.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation	O.Config-Process	O.Config-Process ensures the site is using the configuration management plan supported by tools and procedures, and that the CM system supports the version identification of future TOE implementation representation.

from which the *future TOE* is generated.		
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.Config-Process	CM documentation includes a CM plan which is ensured by O.Config-Process.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the *future TOE*.	O.Config-Process	O.Config-Process ensures the CM plan describes how the CM system is used for the development of the future TOE.
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *future TOE*.	O.Config-Process	The acceptance procedures for modified or newly created configuration items are described in the CM plan ensured by O.Config-Process.
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Config-Items O.Config-Process	All configuration items are uniquely identified and listed in the CM list and controlled under the CMS tools and procedures which are ensured by O.Config-Items and O.Config-Process.
ALC_CMC.5.16C: The evidence shall	O.Config-Process	The automatic tools and procedures operation for the CM system in accordance to the CM plan is ensured by

demonstrate that the CM system is being operated in accordance with the CM plan.		O.Config-Process.

Table 2: Rationale for ALC_CMC.5

7.2.2 Rationale for ALC_CMS.5

SARs	Security Objective	Rationale
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*; the parts that comprise the *future TOE*; security flaw reports and resolution status; and development tools and related information.	O.Config-Items O.Config-Control O.Config-Process	The unique identification of all configuration items is ensured by O.Config-Items. O.Config-Process contains the CM plan and CM list is also included with the items as required by ALC_CMS.5.1C. O.Config-Control covers the handling and identification of released future TOE.
ALC_CMS.5.2C: The configuration list shall uniquely identify the	O.Config-Items O.Config-Control O.Config-Process	The unique identification of all configuration items is ensured by O.Config-Items. O.Config-Process contains the CM plan and CM list is also included with the items as required by ALC_CMS.5.1C. O.Config-Control covers the handling and

configuration items.		identification of released future TOEs.
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer of the item.	O.Config-Process	O.Config-Process contains the CM documentation including clear instructions how to consider the configuration items in the configuration list (including developer information).

Table 3: Rationale for ALC_CMS.5

7.2.3 Rationale for ALC_DVS.2

SARs	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 *future TOE* design and implementation in its development environment.	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Internal-Shipment O.Transfer-Data O.Control-Scrap	The physical protection is provided by O.Physical-Access, supported by O.Security-Control and O.Alarm-Response. In addition, all logical measures are described according to O.Logical-Access and O.Logical-Operation. These measures are supported by the security awareness of the staff according to O.Staff-Engagement and the measures that ensure the functionality of the technical security measures of the site according to O.Maintain-Security. Security during internal shipment is ensured by O.Internal-Shipment and O.Transfer-Data. O.Control-Scrap ensures that no unauthorised access to future TOEs is possible for an attacker.
ALC_DVS.2.2C: The development security documentation	O.Internal-Monitor O.Internal-Shipment	Sufficiency of the security measures is verified according to O.Internal-Monitor. Security during internal shipment is ensured by O.Internal-Shipment,and

shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *future TOE*.	O.Transfer-Data	O.Transfer-Data.

Table 4: Rationale for ALC_DVS.2

7.2.4 Rationale for ALC_LCD.1

SARs	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the *future TOE*.	O.Config-Control O.Organise-Product	The processes used for development and maintenance of the future TOE are defined in the documentation related to O.Config-Control and O.Organise-Product.
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the *future TOE*.	O.Acceptance-Test O.Config-Process O.Organise-Product	Control over the development and maintenance of the future TOE is maintained by O.Config-Process and O.Organise-Product supported by the quality assurance measures defined by O.Acceptance-Test.

Table 5: Rationale for ALC_LCD.1

7.2.5 Rationale for ALC_DEL.1

SARs	Security Objective	Rationale
ALC_DEL.1.1C: The delivery	O.Transfer-Data O.External-Delivery	All external deliveries including the product manuals are controlled according to the procedures defined in

documentation shall describe all procedures that are necessary to maintain security when distributing versions of the *TOE related items* to the consumer.		O.External-Delivery and O.Transfer-Data.

Table 6: Rationale for ALC_DEL.1

8 Site Summary Specification

8.1 Preconditions required by the site

This section provides background information on the assumptions defined in section 4.4.

The client must provide appropriate requirements regarding the requested development services.

For every shipment expected from the development site by the client, the client has to provide the site with appropriate address data. This shall be address data for physical items and equivalent address data (e.g. email address) for the delivery and shipment of electronic items. All the configuration items received by the site from client are uniquely labeled by the client properly to guarantee the traceability.

8.2 Services of the site

This site provides the service of IC embedded software development in Phase 1 and security IC software and hardware development in Phase 2 according to PP [1]. This comprises:

- Security IC software and hardware design and development, layout data such as GDS file formulation and sending to wafer foundry.
- IC embedded software development, management, storage and shipment.
- Sample receiving, management, storage and shipment.
- (In some rare cases) Enciphered IC embedded software (Chip OS, termed as COS)receiving, management, storage.

- CP/FT(Final test) testing program/instruction formulation, management, storage and delivered to CP testing site and packaging site.
- CP/FT testing result receiving, management and storage.
- Production data(such as COS downloading/testing, Personalization production/testing vector, production instruction, etc.) formulation and sending to packaging site and card manufacture.
- Product User Manual(IC and COS) formulation and sending to customer.

Supporting Services includes the following:

- Security measures internal audit (access control system and IT infrastructure logs audit, etc.) and maintenance
- Network separation and IT system access control
- IT infrastructure maintenance (software updates, security patches, virus protection, etc.)
- Sensitive data and security relevant logs backup and backup access control
- Employee training, background check and NDA signing.

8.3 Objectives rationale

The following table shows which security objectives cover which threats and OSPs.

Security Objectives / Threats / OSPs	O.Acceptance-Test	O.Alarm-Response	O.Config-Control	O.Config-Items	O.Config-Process	O.Control-Scrap	O.External-Delivery	O.Internal-Monitor	O.Internal-Shipment	O.Logical-Access	O.Logical-Operation	O.Maintain-Security	O.Organise-Product	O.Physical-Access	O.Reception-Control	O.Security-Control	O.Staff-Engagement	O.Transfer-Data

T.Attack-Transport							■		■									■
T.Computer-Net								■		■	■	■					■	
T.Rugged-Theft		■						■				■		■		■		
T.Smart-Theft		■						■				■		■		■		
T.Staff-Collusion						■		■				■					■	■
T.Unauthorised-Staff		■				■		■		■	■	■		■		■	■	
P.Accept-Product	■		■		■													
P.Config-Control			■							■								
P.Config-Items				■														
P.Config-Process					■													
P.Organise-Product			■		■					■	■		■					
P.Product-Transport				■			■		■									■
P.Reception-Control															■			

Table 7: Security Objectives and Threats/OSPs Mapping

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

O.Acceptance-Test

On request of the client release of the developed future TOE or developed TOE related items are subjected to a release process under supervision of the site's related project management staff.

This addresses the OSP P.Accept-Product.

O.Alarm-Response

Several alarm and detection sensors are installed to provide a protection system for entering the premises by T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff. The trained security guard and reception staff are able to monitor and access the situation throughout surveillance cameras. Security guard and reception staff are dispatched to the location where presence is needed. Security guard and reception staff are present at any location 24/7.

O.Config-Control

A future TOE release can be performed on request of the client. Released future TOEs are identified by a unique identification based on the internal configuration management procedures with the help of automated CM system. Regarding the changes towards the configuration items, the reviewing will be conducted by corresponding project members through the meetings or emails, after approval by the project manager the changes are implemented and applied to the future TOE by the authorized development staff.

This addresses the OSPs P.Config-Control, P.Accept-Product and P.Organise-Product.

O.Config-Items

All configuration items are identified by a unique version number by the configuration management system. The configuration management system allows unique labeling of any set of configuration items in the configuration management system. By this different future TOEs and configurations thereof can be identified. This ensures that only correct version of TOE related items or future TOE are internally shipped or externally delivered.

This addresses the OSPs P.Config-Items and P.Product-Transport.

O.Config-Process

Configuration items are stored in the configuration management system according to the site's configuration management plan. In addition, security flaws are also managed through the configuration management system.

This addresses the OSPs P.Accept-Product, P.Config-Process and P.Organise-Product.

O.Control-Scrap

Security relevant items (e.g. documentation and electronic media that contain confidential information) are securely destroyed if no longer required. By this no employee could get uncontrolled access to scrap which might be helpful to support an attack.

This prevents the threats T.Unauthorised-Staff and T.Staff-Collusion.

O.External-Delivery

Security relevant electronic items (including the IC and COS product manuals) are externally shipped using secure communication measures. This might be signed and/or encrypted emails.

This prevents the threats T.Attack-Transport and addresses the P.Product-Transport.

O.Internal-Monitor

The security meetings are conducted with all security staff on a regular basis. During this meeting security procedures are reviewed and corrective actions are initiated (if necessary). In case security related incident occurred since the last security meeting, they will be addressed. In addition,

internal audits are performed on a regular basis to ensure the application of the security measures.

This prevents threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

O.Internal-Shipment

Security relevant physical items are internally shipped either by security transport (e.g. sealed boxes) or in person by company's internal staff. Security relevant electronic items are internally shipped using secure communication measures. This might be PGP signed and encrypted or similar (e.g. SSL secured webportals).

This prevents the threats T.Attack-Transport and addresses the P.Product-Transport.

O.Logical-Access

The IT network is logically separated from the internet by a firewall system which ensures that only authorized connections from and to the company network are possible.

Each user has an individual account. To access data on the company network, every user has to authenticate himself by login name and password. Multiple successive failed authentication attempts lead to a blocked the account. The number of retries depends on the authentication method.

Access rights to all network resources are set according to a need-to-know and need-to-have basis, respectively. Access rights of users who do not need access to network any longer (e.g. change of jobs) are revoked. In particular, all accounts of employees who leave the company are deactivated.

This prevents the threats T.Computer-Net and T.Unauthorised-Staff and addresses the OSPs P.Organise-Product and P.Config-Control.

O.Logical-Operation

Virus protection and patch management for operating systems and applications ensure the correct operation of the systems and prevent the systems from malfunction. They ensure that protective measures of the IT workplaces are up-to-date (virus definitions, security patches of operating system, security patches of programs, etc.). In addition, regular backups are applied to all network shares related to the configuration management system to prevent loss of data and protected against unauthorized modification and disclosure.

This addresses the OSP P.Organise-Product and prevents the threats T.Computer-Net and T.Unauthorised-Staff.

O.Maintain-Security

All security related alarm and detection systems are checked on a regular basis. Logs for building access or site access as well as access to especially secured areas are stored and checked on a regular basis. Network security is monitored permanently by the IT department.

This prevents threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

O.Organise-Product

The development process are defined and applied according to the site's quality management system. By this the OSP P.Organise-Product is addressed.

O.Physical-Access

The turnstile access control door and CCTV is deployed at the entrance of campus, CCTV are monitored by the campus security guards in real time. The dedicated reception desk is set at one entrance of the building, security guard and reception employee are responsible for the visitor registration and CCTV monitor in real time. Badge is needed to enter the campus and building, PIN is extra needed for entering the high security areas. Towards the areas which are in the scope of this SST, glass breaking sensor, wall vibration sensor and infrared intrusion sensor are also deployed to protect and ensures that only registered and authorized persons can access corresponding areas or related assets.

This prevents threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff.

O.Reception-Control

Upon reception of a requirements from a client or samples, authenticity of these items are verified (e.g. verification of a PGP signature when sent via email and the shipment list).

The OSP P.Reception-Control is addressed by the O.Reception-Control.

O.Security-Control

Trained staff is in charge of operating all security related systems. This especially holds for monitoring surveillance cameras, granting access rights. etc. Visitors are escorted by the company's security staff or collected by company internal staff from the building entrance reception desk.

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

O.Staff-Engagement

All employees working at the site and having access to sensitive information or data have to sign a non-disclosure agreement to provide legal liability to protect sensitive information against disclosure. In addition, all employees are trained regarding information security to support the security awareness. The background check will be conducted for the sensitive post employees before they are hired.

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

O.Transfer-Data

Sensitive electronic TOE related items are protected against modification and/or disclosure by cryptographic means during transfer. Either asymmetric means or password protection are applied (as appropriate). Cryptographic keys and password used for secure communication are sufficiently protected against unauthorized access and disclosure.

This prevents the threats T.Staff-Collusion and T.Attack-Transport as well as the OSP P.Product-Transport.

8.4 SAR Rationale

The Security Assurance Requirements rationale does not explicitly address the developer action elements defined in [3] because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the preparation for the site

visit. In addition, this includes that the procedures are applied as written and explained in the documentation.

Note: The content elements that are changed from the original CEM [4] according to the application notes in the process description [5] are written in *italic*. The term TOE can be replaced by 'TOE related items' in most cases. In specific cases it is replaced by 'future TOE'.

8.4.1 ALC_CMC.5

- ALC_CMC.5.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*
- ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.
- ALC_CMC.5.3C:The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.
- ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.
- ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.
- ALC_CMC.5.6C: The CM system shall support the production of the *future TOE* by automated means.
- 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.
- ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.

- ALC_CMC.5.9C: The CM system shall support the audit of all changes to the *future TOE* by automated means, including the originator, date, and time in the audit trail.
- 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.
- ALC_CMC.5.11C:The CM system shall be able to identify the version of the implementation representation from which the *future TOE* is generated.
- ALC_CMC.5.12C:The CM documentation shall include a CM plan.
- ALC_CMC.5.13C:The CM plan shall describe how the CM system is used for the development of the *future TOE*.
- ALC_CMC.5.14C:The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *future TOE*.
- ALC_CMC.5.15C:The evidence shall demonstrate that all configuration items are being maintained under the CM system.
- ALC_CMC.5.16C:The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

The security assurance requirements of the assurance class 'CM capabilities' listed above are suitable to support the secure and efficient development of future TOEs due to the formalized acceptance process and the automated support. The identification of all configuration items allows a parallel development of different future TOEs. The requirement for authorized changes support the integrity and confidentiality required for the future TOEs. Therefore this assurance level meets the requirements for the configuration management.

8.4.2 ALC_CMS.5

- 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*; the parts that comprise the *future TOE*; security flaw reports and resolution status; and development tools and related information.
- ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.
- ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer of the item.

The security assurance requirements of the assurance class 'CM scope' listed above are suitable to define a controlled environment for the future TOE development. This includes the documentation of the site security and the procedures for the configuration management. Since the site certification process focuses on the processes based on the absence of a concrete TOE these assurance requirements are considered to be suitable.

8.4.3 ALC_DVS.2

- 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 *future 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 *future TOE*.

The security assurance requirements of the assurance class 'Development security' listed above are required since a high attack potential is assumed for potential attackers. The information used at the site during the development of the future TOE can be used by potential attackers for the development of attacks. This information is needed to apply an attack within considerable time and effort.

8.4.4 ALC_LCD.1

- ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the *future TOE*.
- ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the *future TOE*.

The security assurance requirements of the assurance class 'Life-cycle definition' listed above are suitable to support the controlled development process and maintenance of already developed future TOEs. This includes the documentation of these processes and the procedures for the configuration management. The site supports only the phases development of the described life cycle. The assurance requirements are considered to be suitable for this site.

8.4.5 ALC_DEL.1

- ALC_DEL.1.1C: The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the *TOE related items* to the consumer.

The security assurance requirement of the assurance class "Delivery" listed above is suitable to define a controlled process for delivery IC and COS product manual to the consumer using this site. The confidentiality and integrity of the IC and COS product user manual during transport is addressed by this assurance class. The assurance requirement is considered to be suitable for this site.

8.5 Assurance Measures Rationale

O.Acceptance-Test

ALC_LCD.1.2C requires control over the development and maintenance of the future TOE. The site conducts verification and testing towards all the functions of the future TOE and holds the acceptance meeting to review. Thereby this objective fulfils this Security Assurance Requirements.

O.Alarm-Response

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the future TOE design and in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Config-Control

ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items. ALC_CMC.5.6C requires the CM system to support the production of the future TOE by automated means. ALC_CMC.5.7C requires that CM system shall ensure that the

person responsible for accepting a configuration item into CM is not the person who developed it. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs of the life-cycle, development tools and security flaw reports and resolution status. ALC_CMS.5.2C requires that all configuration items are identified uniquely. ALC_LCD.1.1C requires a description of the model used to develop and maintain the future TOE. The objective meets the set of Security Assurance Requirements.

O.Config-Items

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. In addition, ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the CM system. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs of the life-cycle, development tools and security flaw reports and resolution status. ALC_CMS.5.2C requires that all configuration items are identified uniquely. The objective meets the set of Security Assurance Requirements.

O.Config-Process

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 so that only authorised changes are made to the configuration items. ALC_CMC.5.7C

requires that CM system shall ensure 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. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs of the life-cycle, development tools and security flaw reports and resolution status. ALC_CMS.5.2C requires that all configuration items are identified uniquely. ALC_CMS.5.3C requires that for each configuration item the developer is indicated in the configuration list. ALC_LCD.1.2C requires that the life-cycle model provides the necessary control over the development and maintenance or the future TOE. The objective meets the set of Security Assurance Requirements.

O.Control-Scrap

The controlled destruction of scrap is necessary to ensure the confidentiality and integrity of future TOEs as required by ALC_DVS.2.1C.

O.External-Delivery

ALC_DEL.1.1C requires the delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE related items to the consumer. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Internal-Monitor

ALC_DVS.2.2C requires the development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the future TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Internal-Shipment

ALC_DVS.2.1C requires that 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 future TOE design and implementation in its development environment. ALC_DVS2.2C requires the justification that the described measures are appropriate to provide the necessary level of protection. This protection also includes internal shipments. Thereby the objective is suitable to meet this combination of Security Assurance Requirements.

O.Logical-Access

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation including the initialization in its development environment. 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 objective is suitable to meet the Security Assurance Requirements.

O.Logical-Operation

ALC_DVS.2.1C: The development security documentation shall describe the security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation in its development environment. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Maintain-Security

ALC_DVS.2.1C: The development security documentation shall describe the security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Organise-Product

ALC_LCD.1.1C requires a description of the model used to develop and maintain the future TOE. ALC_LCD.1.2C requires that the life-cycle model provides the necessary control over the development and maintenance or the future TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Physical-Access

ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Reception-Control

ALC_CMC.5.1C requires a process is in place to ensure an appropriate and consistent labeling. And O.Reception-Control ensures the items received from other sites has been labelled uniquely before delivery. Thereby this objective is suitable to meet this Security Assurance Requirement.

O.Security-Control

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation including the initialization in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Staff-Engagement

ALC_DVS.2.1C requires the description of personnel security measures that are necessary to protect the confidentiality and integrity of the future TOE design and implementation in its development environment. Thereby the objective fulfils this combination of Security Assurance Requirements.

O.Transfer-Data

ALC_DVS.2.1C requires 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 future TOE design and implementation in its development environment. ALC_DVS2.2C requires the justification that the described measures are appropriate to provide the necessary level of protection. This protection also includes internal shipments. ALC_DEL.1.1C requires the delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE related items to the consumer. Thereby this objective is suitable to meet the combination of Security Assurance Requirements.

9 References

9.1 Literature

[1] Security IC Platform Protection Profile with Augmentation Packages Version 1.0, BSI-PP-0084-2014, January 13, 2014

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

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

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

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

[6] JIL-Minimum Site Security Requirements v3.0, February 2020