Site Security Target Lite

of

ACT Dongguan Technology Limited

Date: 12 June 2024

Version：1.0

Public

Content

List of Tables

1 Document Information

1.1 Document Invariants

c	Title	Value
Classification:	Public	Public
Title:	Site Security Target Lite of ACT Dongguan Technology Limited	Site Security Target Lite of ACT Dongguan Technology Limited
Site (short):	ACTDG	ACTDG
Site (long):	ACT Dongguan Technology Limited	ACT Dongguan Technology Limited
Address:	Dong Guan	Dong Guan
Sponsor:	Apply Card Technology Ltd.	Apply Card Technology Ltd.
Assurance Level:	EAL6	EAL6

1.2 Version History

Version	Date	Comment/Editor/Changes
1.0	12 June 2024	Lite version based on SST v2.0

2 SST Introduction

This document is based on the Eurosmart Site Security Target Template [7] with adaptations such that it fits the site.

This chapter is divided into the sections “Identification of the site” and “Site Description”.

The Site Security Target Lite (title: "Site Security Target of ACT Dongguan Technology Limited", Version 1.0, 12 June， 2024) refers to the site ACT Dongguan Technology Limited in DongGuan. The site is used as part of the production flow of inlays & modules.

2.1 Identification of the site

The company ACT Dongguan Technology Limited is located at:

Building B,

Shang Sha Industrial Centre,

6 Xin Chun Road,

Chang An, Dongguan,

China 523841

2.2 Site Description

The following areas of the plant specified in Section 2.1 are in the scope of the SST.

2.2.1 Physical Scope

ACT Dongguan Technology Limited is the site consists of Building A， and Building B. Only Building B is in the scope of this site certification. Building B has a total of 4 levels. The 1/F is used for logistic, scrapping and warehouse, IC chipset & wafer storage cleanroom function. 2/F is used for production of the secure products. 3/F is used for the production of the secure products. 4/F is used partially for the production of IC modules, and also partially used for the production of secure products. The secure products refer to the finished products or semi-finished products consisted of the IC modules. The IC modules refer to integrated circuits that are specifically designed to be embedded within our application for banking cards or identity cards, etc. The border of the site is determined by the fence/gate all around the building. There is a data room at 2/F which is never in use anymore. It is renamed as the spare room, which is not allowed any unauthorized person to go to this room.

Access into the building is restricted and is documented and controlled.

The site enforces 3 different security levels of access control with respect to sensitive areas at the site. The access control measures ensure that only registered employees and registered visitors can access level 0. Sensitive products are handled in areas requiring access level 2. Any person enters the building B but not to areas contain any sensitive products, requiring access level 1.

2.2.2 Logical Scope

The following services/processes provided by ACTDG are in the scope of the site evaluation process:

- Manufacturing of inlays & IC modules
- Electrical Test of finished inlays & IC modules, such that ACTDG does not perform wafer testing, but electric test only. No security relevant test is provided in ACTDG.
- Destruction of defect inlays & IC modules

The complete logical production of the inlays & IC modules at the site is covered by the Site Security Target. In addition, the management of the inlays & IC modules related processes and the site security are covered by the Site Security Target.

The product flow of the inlays on the site comprises the reception of modules of the intended TOE, as well as, the delivery of the provided modules. The site only provides the assembled modules to the manufacturers of smart cards.

The product flow of the IC module packaging on the site comprises the reception of wafers of the intended TOE, perform module packaging, required testing as well as the delivery of the finished modules.

The following departments are involved in the inlays & IC modules process: Order Management Department, Project Manager, IT (Facility Manager, Document Manager, and Project Manager), Store Department, Packaging, Production, Quality Control, Process Engineer, and Test Engineer.

The services provided by ACTDG are part of the life cycle phase 4 according to the life cycle definition provided in [5] and [6]. The following production steps of the inlays are subject of the Site Security Target:

- Inlay & IC module production
- Standard Packaging of inlays & IC modules for delivery for all clients.

3 Conformance Claim

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

- Common Criteria, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

- Common Criteria, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

- Common Criteria, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

- For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

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

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

The chosen assurance components are derived from the assurance level EAL6 of the assurance class "Life-cycle Support". The assurance components are compliant or augmented compared to the Protection Profile [6]. The life cycle described in [6] can include the module packaging, the assembly and embedding process like the inlay assembly. Therefore, this site evaluation supports product evaluations conformant to Part 3 up to the assurance level EAL6.

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.

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 intended TOE and the security management of the site.

This SST template is based on the life-cycle defined in the Security IC Platform Protection Profile [6]. The assets (4.1), threats (4.2) and Organisational Security Policies (OSP) (4.3) defined in this template are derived from the life-cycle defined in that PP.

The Security Problem Definition comprises two major so called security problems. The first set of security problems comprises all kind of 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 Organisational Security Policies (OSP).

4.1 Assets

The following section describes the assets handled at the site.

The site specific internal documentation and data that is relevant to maintain the confidentiality and integrity of an intended TOE is considered as asset. This comprises the site security concept and the associated security measures as well as keys and cryptographic tools for the encrypted exchange of data. These items are not explicitly listed in the list of assets below.

The integrity of any machine or tool used for development, production, testing and personalisation is not considered as an asset. However, appropriate measures must be defined for the site to ensure this important condition. These items normally consist of standard hardware and software which are programmed or customised for their purpose at ACTDG.

If the equipment stores sensitive data related to testing, the data is considered as assets.

The assets are:

- Modules
- Inlays or other packages
- Product specifications
- Wafers

4.2 Threats

All threats endanger the integrity and confidentiality of the intended TOE and the representation of parts of the TOE.

The following threats are described in a general way. However, they are applicable to each site that provides services handling the items listed in section 4.1 above. The explanation below the threats will help to address the Security Objectives according to the site specific aspects.

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive configuration 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.

This attack already includes a variety of targets and aspects with respect to the various assets listed in the section above. It shall cover the range of individuals that try to get unregistered or defect devices that can be used to further investigate the functionality of the device and search for possible exploits. Such an attacker will have limited resources and a low financial budget to prepare the attack. However the time that can be spent by such an attacker to prepare the attack and the flexibility of such an attacker will provide notable risk.

It is expected that such an attacker can be defeated by state of the art physical, technical and procedural security measures like access control and surveillance. In general an access control concept with two or three levels shall be implemented. If two levels are implemented, the more restrictive level of the access control shall prevent the simple access using a lost or stolen access token. Other restrictions may be the need for parallel access by two employees. The technical measures shall include automated measures to support the surveillance.

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

Although this attack is applicable for each site the risk may be different regarding the assets. These attackers may be prepared to take high risks for payment. They are considered to be sufficiently resourced to circumvent security measures and do not consider any damage of the affected company. The target of the attack may be products that can be sold or misused in an application context. This can comprise devices at a specific testing or personalisation state for cloning or introduction of forged devices. Those attackers are considered to have the highest attack potential.

Such attackers may not be completely defeated by the physical, technical and procedural security measures. Special measures like storage of items in safes or strong rooms or the

splitting of sensitive data like keys provide additional support against such attacks. Also the unique registration of the products can support the protection if they can be disabled or blocked.

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 test data or other sensitive production data or modify the testing or production process at the site.

A logical attack against the network of the site provides the lowest risk for an attacker. The target of such an attack is to access the company network to get information that may allow to attack a product or manipulate a product or retrieve information to allow or change the configuration or the personalisation. In addition, a successful access to a company network leads to loss of reputation of the company processing the product or the company that produces the product.

Such attackers are considered to have high attack potential because the attacker may have appropriate technical equipment to perform such an attack. Furthermore, the attacker may have the resource to develop or buy software or hardware which can exploit known vulnerabilities within the tools and software used by the company.

Therefore, also for the company network a protective concept with more than one level is expected. This shall comprise a firewall to the external network, and further limitations of the network users and the network services for internal sub-networks. In addition, computer users shall have individual accounts which require authentication (e.g. password). For specific tasks or processes standalone networks may be required. The protection must be supported by appropriate measures to update and maintain the computer and network systems and analyse logs that may provide indications for attack attempts.

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

Employees, contractors or student trainees that are not trained may take products or influence production systems without considering possible impacts or problems. This threat includes accidental changes e.g. due to working tasks of student trainees or maintenance tasks of contractors within the development, production or test area.

Such accidental changes can include the modification of configurations for tools that may have an impact on the TOE, the wrong assignment of tools for a dedicated process step. Further examples may be machine failure or misalignment between operators that are responsible for products of different clients or different products of the same client are mixed during production. This also includes the disposal of sensitive products using the standard flow and not the controlled destruction.

T.Unauthorised-Staff: Employees or subcontractors not authorised to get access to products or systems used for production get access to products or affect production systems or configuration systems, so that the confidentiality and/or the integrity of the product is violated. This can apply to any production step and any configuration item of the final product as well as to the final product or its configuration.

Especially maintenance tasks of subcontractors may require the access to computer systems storing sensitive data. The implemented security measures may not work because a special dedicated access may be used to the network or specific tools may be used for this dedicated task. This comprises e.g. tools which process the layout data e.g. in the design center, the mask shop and/or the wafer foundry as well as sensitive test and/or configuration data within the test center.

Also other subcontractors like cleaning staff or maintenance staff for the building get limited access that may allow them to start an attack. The disposal of defect equipment and/or sensitive configuration items must be considered.

The attack potential depends on the trustworthiness of the subcontracted company and the access required within the company. Related to this different measures are required.

T.Staff-Collusion: An attacker tries to get access to material processed at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.

Personal accountability shall be traceable as far as possible. Handover procedures with dual control, enforcement of parallel access by two authorised employees and the split of sensitive knowledge like personalisation keys can be implemented to prevent such an attack. The measures depend on the assets that must be protected at the site.

T.Attack-Transport: An attacker might try to get data, specifications or products during the internal shipment and/or the external delivery. The target is to compromise confidential information or violate the integrity of the products during the stated internal shipment and/or the external delivery process to allow a modification, cloning or the retrieval of confidential information after further production steps. Confidential information comprises design data, customer and/or consumer data like code and data (including personalisation data and/or keys) stored in the ROM and/or EEPROM or classified product documentation.

The protection of the internal shipment and/or the external delivery depends on the configuration items that are exchanged. The protection is related to the assets that must be considered during the site evaluation.

4.3 Organisational Security Policies

The following policies are introduced by the requirements of the assurance components of ALC for the assurance level EAL6. The chosen policies shall support the understanding of the production flow including optional initialization and the security measures of the site. In addition they allow an appropriate mapping to the assurance requirements.

The documentation of the site under evaluation is under configuration management. This comprises all procedures regarding the evaluated production flow 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 the unique identification of items that are created, generated, developed or used at a site as well as the received and transferred and/or provided items.

The configuration management may rely completely on the naming and identification of the received configuration items. In this case at least the consistency with the expected values must be verified and the unique identification must be ensured. This holds also for test programs or other items that are provided to the site for local use. For configuration items that are created, generated or developed at the site the naming and identification must be specified. For data like configuration, initialisation or personalisation data the identification and handling must be described.

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.

The product setup may include the following information (i) identification of the product, (ii) properties of the product when received at the site (iii) properties of the product when internally shipped or externally delivered, (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) how the product is tested after assembly, (vii) any configuration of the processed item as part of the services provided by the site, (viii) which address is used for external delivery and/or internal shipment.

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

Measures are in place to ensure that the evaluated status is ensured. In most cases tools are used to support the production of the site. This comprises e.g. scripts and batch routines developed by the site as well as a commercial data base system. This comprise the initialization data and parameters for testing and quality checks.

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 sensitive items (security relevant parts of the intended TOEs of different clients) are separated and traced on a device basis. For each hand over, either an automated or an organisational “two-employees-acknowledgement” (four-eye principle) is applied for functional and defect assets. According to the released production process the defect assets are destructed or sent back to the client.

P.Shipping-Support: Technical and organisational measures shall ensure the correct labelling of the product. A controlled internal shipment and/or the external delivery shall be applied. The transport supports traceability up to the acceptor. If applicable or required this policy shall include measures for packing if required to protect the product during transport.

P.Scrap-Items: Any item that is defect, end-of-life or that does not comply with the quality requirements is shipped back to the client for destruction or is scrapped at the site in a way that the destructed item does not support any attacker.

4.4 Assumptions

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 that must be defined for the interface.

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

A.Prod-Specification: The client must provide appropriate information (e.g. specifications, definitions, process limits, process parameters, test requirements, test limits, bond plans) in order to ensure an appropriate development or 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.External-Delivery: The recipient of the product is defined by the client. The client provides the address and shipping information (selected forwarder) to ACTHK/ACTDG. The client defines the requirements for packing of the security products in case the standard procedure of ACTHK/ACTDG is not applicable.

A.Product-Integrity: The self-protecting features of the devices are fully operational and it is not possible to influence the configuration and behaviour of the devices based on insufficient operational conditions or any command sequence generated by an attacker or by accident.

The assumptions are outside the sphere of influence of ACTDG. They need to provide an appropriate production process, assign the product to the released production process and ensure the proper handling, storage and destruction of all configuration items related to the product.

5 Security Objectives

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

O.Physical-Access: The physical separation between the different access control levels in addition with the technical and organisational security measures allow 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 reject of unauthorised people. The site enforces two or three level (level 0 to level 2) of access control to sensitive areas of the site. The access control measures ensure that only registered employees and registered visitors can access level 0. Sensitive products are handled in areas requiring access level 2.

O.Security-Control: Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like 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, contractors and suppliers.

O.Alarm-Response: The technical and organisational security measures ensure that an alarm is generated before an unauthorised person gets access to any sensitive configuration item (asset). After the alarm is triggered the unauthorised person still has to overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack.

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. Sensitive processes may be controlled within a shorter time frame to ensure a sufficient protection.

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

O.Logical-Access: The site enforces a logical separation between the internal network and the internet by a firewall. The firewall ensures that only defined services

and defined connections are accepted. Furthermore, the internal network is separated into a production network and an office network. Additional specific networks for production and configuration are physically separated from any internal network to enforce access control. Access to the production network and related systems is restricted to authorise employees that work in the related area or that are involved in the configuration tasks or the production systems. Every user of an IT system has its own user account and password. An authentication using user account and password is enforced by all computer systems.

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

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

O.Config-Control: The site applies a release procedure for the setup of the production process for each new product. In addition, the site has a 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.

O.Process-Config: 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 optimisations of the process flow as well as for the documentation that describes the services and/or processes provided by a site.

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

O.Staff-Engagement: All employees who have access to sensitive configuration items and who can move parts of the product out of the defined production flow

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

O.Zero-Balance: The site ensures that all sensitive products (intended TOE of different clients) 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 destructed or sent to the client.

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

O.Shipping-Support: Supports the shipment that is controlled by the client. The address of the receiver is maintained for each product. Finished products are packed and labelled as defined by the client. Before handover the identity of the forwarders is checked based on the information provided by the client.

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

5.1 Security Objectives Rationale

The SST includes a Security Objectives Rationale with two parts. The first part includes a tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part include a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives.

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

5.1.1 Mapping of Security Objectives

Threat or OSP	Security Objective	Note
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	Adequate reaction on an attack is ensured by these measures.

Threat or OSP	Security Objective	Note
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	Adequate reaction on an attack is ensured by these measures.
T.Computer-Net	O.Logical-Access O.Logical-Operation O.Internal-Monitor O.Staff-Engagement O.Maintain-Security	The measures prevent an interfering access to the internal network.
T.Accident-Change	O.Logical-Access O.Logical-Operation O.Acceptance-Test O.Staff-Engagement O.Zero-Balance O.Process-Config	The automated measures and the control procedures avoid this threat.
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Maintain-Security O.Alarm-Response O.Logical-Operation O.Logical-Access O.Internal-Monitor O.Config-Control O.Zero-Balance O.Scrap-Control O.Staff-Engagement	Physical and logical access control limit the access to the assigned tasks. Control procedures and personal accountability hinder uncontrolled access.
T.Staff-Collusion	O.Zero-Balance O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Scrap-Control	Control procedures and personal accountability hinder uncontrolled access.
T.Attack-Transport	O.Shipping-Support	The measures allow to detect attack attempts. The objective is applicable for the internal shipment and the external delivery.
P.Config-Items	O.Reception-Control O.Config-Items	All relevant items are covered by the control.
P.Config-Control	O.Config-Items O.Config-Control O.Logical-Access	The scope comprises the introduction of production flows and their controlled change.
P.Config-Process	O.Process-Config	The scope comprises the production processes and the documentation of the site.
P.Reception-Control	O.Reception-Control	The control ensures the correct identification and assignment of configuration items.
P.Accept-Product	O.Acceptance-Test O.Config-Control O.Process-Config	Ensures the compliance of the finished product with the specifications

Threat or OSP	Security Objective	Note
P.Zero-Balance	O.Zero-Balance O.Internal-Monitor O.Scrap-Control O.Staff-Engagement	All functional and non-functional products are in the scope of the traceability
P.Shipping-Support	O.Shipping-Support O.Process-Config	The correct destination address, the controlled packing and the tracing of the transport ensure the correct external delivery and internal shipment
P.Scrap-Items	O.Scrap-Control	The scrapped products are scrapped subjected to customer confirmation in advance in the scrap room using the specific scrap machine to scrap the IC modules into powder form under the two person four eyes practice.

Table 1: Mapping of threats and Organisational Security Policies versus Security Objectives

6 Extended Assurance Components Definition

No extended components are defined in this SST.

7 Security Assurance Requirements

Sites using this Site Security Target require an evaluation against evaluation assurance level EAL6. The security assurance requirement ALC.CMC.5 improvement involves the following: justification of the acceptance procedures, advanced Configuration Management System including mostly automated means to identify all other configurations items that are affected by the change of a given configuration item, identification of the version of the implementation representation. Therefore this security assurance requirement is also included in the Security IC Platform Protection Profile [6].

The Security Assurance Requirements (SAR) are:

Class ALC: Life-cycle support

CM capabilities (ALC_CMC.5)

CM scope (ALC_CMS.5)

Development security (ALC_DVS.2)

Life-cycle definition (ALC_LCD.1)

The Security Assurance Requirements listed above cover the minimum set of SAR required by [5] and they are extended by SAR of the assurance component "Life-cycle definition" (ALC_LCD.1).

7.1 Application Notes and Refinements

The description of the site certification process [5] 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 SST the associated processes for the handling of products are in the focus and described in this SST. These processes are subject of the evaluation of the site.

7.1.1 Overview and Refinements regarding CM Capabilities (ALC_CMC)

A production control system is employed to guarantee the traceability and completeness of different production charges or lots. The number of wafers, dice and/or packaged products (e.g. modules/inlays) is tracked by this system. Appropriate administration procedures are implemented for managing wafers, dice and/or packaged products, which are being removed from the production-process in order to verify and to control predefined quality standards and production parameters. It is ensured, that wafers, dice or assembled devices removed from the production stage (i) are returned to the production stage from where they were removed or (ii) are securely stored and destroyed.

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 application notes in [5] are defined for ALC_CMC.5.

The configuration control and a defined change process for the procedures and descriptions of the site under evaluation are mandatory. The control process must include all procedures that have an impact on the evaluated production processes as well as on the site security measures.

The life cycle described in [6] includes complex production processes that cannot be controlled at each state within the production process. In such a case the control of the product after such a production process must include sufficient verification steps to ensure the specified and expected result. Test procedures, verification procedures and the associated expected results are under configuration management for these cases.

The configuration items for the considered product type are listed in section 4.1. The CM documentation of the site is able to maintain the items listed for the relevant life cycle step and the CM system is able to track the configuration items.

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

7.1.2 Overview and Refinements 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 for the claimed life-cycle SAR and the configuration items handled at the site.

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 4.1 that are considered as “TOE implementation representation” which include:

- Logical design data,

- Physical design data,

- IC Dedicated Software,

- final physical design data In addition process control data, test data and related procedures and programs can be in the scope of the configuration management.

7.1.3 Overview and Refinements regarding Development Security (ALC_DVS)

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

The TOE Manufacturer must ensure that the development and production of the TOE is secure so that no information is unintentionally made available for the operational phase of the TOE. The confidentiality and integrity of design information, test data, configuration data and pre-personalisation data must be guaranteed, access to any kind of samples (client specific samples or open samples) development tools and other material must be restricted to authorised persons only, and scrap must be 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.

7.1.4 Overview and Refinements regarding Life-Cycle Definition (ALC_LCD)

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 Protection Profile [6] provides a life cycle description there specific life-cycles steps can be assigned to the tasks at site. This comprise a change of the life-cycle state if e.g. testing or initialisation is performed at the site or not.

The Protection Profile [6] does 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.

7.2 Security Assurance Rationale

The security assurance rationale maps the content elements of the selected assurance components of [3] to the security objectives defined in this Site Security Target. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of the products. If the site already receives configuration items, this process is based on the assumption that the delivered configuration items are appropriately labelled 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 configuration items in most cases. In specific cases it is replaced by product as intended TOE.

Security Assurance Requirement	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.Reception-Control O.Config-Items	Each item is already labelled when it is received at the site, this is checked by O.Reception-Control. The received items are mapped to an internal product identification as defined by O.Config-Items.
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Config-Items O.Config-Control	Registration of each product and each client/customer is applied according to O.Config-Items. Unique identification and assignment for each released product is ensured according to O.Config-Control. The related processes ensure unique labels and assignments. This applies also for data used for initialisation or upload.
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.Process-Config	O.Process-Config ensures a controlled configuration management and release process. During the release as well as for major changes the client is involved in the release approval supporting appropriate review.
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 check if all items received can be identified uniquely. O.Config-Items comprises the unique identification of components used to produce and initialise and or upload software for each product. O.Config-Control defines the processes and procedures including initialisation scripts and upload script for the production/initialisation/upload for a dedicated product. Also the site documentation can be uniquely identifed.

Security Assurance Requirement	Security Objective	Rationale
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.Process-Config O.Logical-Access	O.Config-Control comprises the product data base that allows for only one script version per product. When a new version is introduced, the previous versions is disabled or a new unique product derivative is created in the data base. O.Process-Config requires the authentication of each user before any change in the data base can be applied. O.Logical-Access supports user authentication and logical separation of tools and IT-systems.
ALC_CMC.5.6C: The CM system shall support the production of the configuration items by automated means.	O.Config-Control O.Zero-Balance O.Acceptance-Test	According to O.Config-Control components and processes for production and/or initialisation and/or upload are stored in a data base and used to setup and configure the production environment. O.Zero-Balance ensures the control of all products during production with automated tracking for functional devices. O.Acceptance-Test implements automated testing at defined production steps and after the production.
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.Process-Config O.Acceptance-Test	O.Process-Config provides the required separation of roles supported by the tool setup and the organisational setup. According to O Acceptance-Test the quality control is also responsible for acceptance of the finished devices.
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	O.Config-Items	The security functionality is provided by the security IC that is a configuration item according to O.Config-Items. The security IC is packages at the site. The package as well as the initialisation and/or upload of software does not change the security functionality of the device.

Security Assurance Requirement	Security Objective	Rationale
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the configuration items by automated means, including the originator, date, and time in the audit trail.	O.Config-Control O.Process-Config O.Zero-Balance	According to O.Config-Control all changes for a product can be tracked and according to O.Process-Config all changes for the processes including configuration management can be tracked. O.Zero-Balance supports the tracking of each device during production, initialisation and software upload.
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.Process-Config	The package and minor changes related to the package do not have an impact on the security functionality of the security IC and O.Config-Control and O.Process-Config are defined accordingly.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the delivered configuration items are generated.	O.Config-Items O.Config-Control O.Zero-Balance O.Acceptance-Test	O.Config-Items and O.Config-Control cover the unique labelling and management of the client configuration items. The logging supported by O.Zero-Balance and O Acceptance-Test ensure traceability of each inlay.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.Config-Control O.Process-Config	According to O.Config-Control the CM plan is defined for each product. CM process documentation is available and maintained according to O.Process-Config.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the production of the configuration items.	O.Config-Control O.Process-Config	CM plan describes product release process from development start to qualified product according to O.Config-Control. The processes for the configuration management are defined according to O.Process-Config.
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of an intended TOE.	O.Config-Items O.Config-Control O.Process-Config O.Reception-Control	O. Process-Config includes the change management that is part of the CM plan. The acceptance process comprises internal approval and approval by the client as part of O.Process-Config. The new products must be set up as required by O.Config-Control. At the end of the introduction process the configuration item can be identified according to O.Config-Items. The complete process is supported by O.Reception-Control.

Security Assurance Requirement	Security Objective	Rationale
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Config-Control O.Process-Config O.Reception-Control O.Zero-Balance O.Acceptance-Test O.Shipping-Support	According to O.Config-Control each product must be assigned to a production recipe. O.Process-Config is the overall control process for the configuration management. O.Reception-Control ensure the expected input for the production, O.Zero-Balance and O.Acceptance-Test ensure the tracking during production and the final testing after production. O.Shipping-Support ensures the preparation for shipment based on the procedure defined by the client.
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.Reception-Control O.Process-Config O.Acceptance-Test	O.Reception-Control ensures that only identified items are used for production. According to O.Process-Config the site controls its services/processes using a configuration management concept and requires release approvals before production. O.Acceptance-Tests ensures the compliance of the finished products with the functional requirements and the quality requirements defined in the CM plan.

Table 2: Rationale for ALC_CMC.5

Security Assurance Requirement	Security Objective	Rationale
ALC_CMS.5.1C: The configuration list shall include the following: the configuration items; the evaluation evidence required by the SARs; the parts that comprise the configuration items; the implementation representation; security flaw reports and resolution status; and development tools and related information.	O.Config-Items O.Config-Control O.Process-Config	Since the development of the Security IC is finished the scope is limited to the assets listed in section 4.1. O.Config-Items includes the unique identification of the configuration items as described above. O.Config-Control comprises a defined production process with optional module assembly, and/or initialisation for each product. O.Process-Config ensures the control and change management for all processes at the site. The tools and scripts are related to the initialization

Security Assurance Requirement	Security Objective	Rationale
		and they are under configuration management according to O.Config-Items and O.Config-Control.
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config-Items O.Config-Control O.Process-Config O.Reception-Control O.Shipping-Support	Products are described with unique part and version numbers as well as configuration options according to O.Config-Items, supported by O. Reception-Control. Also the CM System supports automated unique version control according to O.Config-Control. The control of the processes is applied according to O.Process-Config. According to O.Shipping-Support the preparation for shipment is also part of the product configuration.
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer/ subcontractor of the item.	O.Reception-Control O.Config-Control	The security IC for assembly is delivered by the client and controlled according to O.Reception-Control and O.Config-Control.

Table 3: Rationale for ALC_CMS.5

Security Assurance Requirement	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Scrap-Control	Site security manual describes all physical measures according to O.Physical-Access, supported by O.Security-Control and O.Alarm-Response. Also the 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. O.Scrap-Control requires the protection of defect and obsolete sensitive items until they are

Security Assurance Requirement	Security Objective	Rationale
		destructed or returned to clients in case of security ICs
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.Maintain-Security O.Logical-Operation O.Zero-Balance O.Reception-Control O.Shipping-Support	O.Internal-Monitor, O.Maintain-Security and O.Logical-Operation comprise measures to control and justify the application and effectiveness of the security measures. Further the intended TOE is traced and a 4-eye principle is implemented with personal accountability for items that cannot be tracked automatically according O.Zero-Balance. The incoming control supports the detection of attack attempts of the incoming products according to O.Reception-Control. The controlled packing and tracing during the transport according to O.Shipping-Support.

Table 4: Rationale for ALC_DVS.2

Security Assurance Requirement	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the configuration items.	O.Config-Control O.Process-Config	The processes used for identification, production and initialization of the product are defined in the documentation required by O.Config-Control and O.Process-Config
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	O.Process-Config O.Acceptance-Test O.Zero-Balance	Products and scripts aren't developed by ACTDG but bought as certified products. Control is maintained throughout overall ACTDG production process by O.Process-Config. In addition the quality control as defined by O.Acceptance-Test provides the necessary control. O.Zero-Balance ensures that all products are controlled.

Table 5: Rationale for ALC_LCD.1

Since this SST references the PP [6], the life-cycle module used in this PP includes also the processes provided by site under evaluation. The provided description must be conformed to this life-cycle model.

8 Site Summary Specification

The following sections describe the services provided by ACTDG in more detail. These details include the required deliverable and conditions needed to provide the evaluated services by ACTDG. The description shall support the integration of ACTDG as a subcontractor within the production process for inlays.

8.1 Preconditions required by the Site

The items and data required by the site depend on the scope of the services provided by ACTDG. For the production of inlays & IC modules, the following items need to be delivered:

- Security related products such as inlays & IC modules come with clearly defined and fitting interfaces for the production at ACTDG. The wafer & IC modules are uniquely identifiable. The information required for the assembly of inlays & IC modules such as specifications, assembly guidance, test requirements and inlay plans.

- Also, the shipping process including shipping address and packaging requirements for the shipment are specified by the client. This includes the procedure for identifying the forwarder.

- During production, the site tracks the modules using their WIP system and each module will have their own unique log number. Their measurement equipment is able to track the unique ID of the production lot.

In general, the site assumes that the self-protecting measures of the modules are fully operational. The client has to ensure that the self-protecting features of the modules are fully operational before the modules are delivered to the site.

Note that goods such as wire material, plastic foils, glue, etc. are not considered to be security relevant. For each released inlay batch, these goods are defined in the specification for production but they are not considered to have any impact on the behaviour with respect to the security of the intended TOE.

8.2 Services of the site

ACT Dongguan Technology Limited is focusing its business mainly on inlays & IC modules, with its service scope ranging from IC module packaging inlay assembling, with the corresponding electrical tests to be done for both IC module packaging and inlay assembling processes respectively. Final testing and quality control verify the compliance of the finished product with the product specification.

The raw materials are delivered to the site and picked up at the site. ACTDG supports the preparation of the shipment according to the requirements of the client. This includes the labelling (product information and shipping address).

Defected pieces are replaced piece by piece at QA stage; details are captured on manual forms. Defected pieces are destructed or with all functional pieces shipped to client. Thus, we do not keep any pieces in the factory.

8.3 Objectives Rationale

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

O.Physical-Access:

> The physical separation between the different access control levels in addition with the technical and organisational security measures allow 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 individuals. The site enforces 3 different security levels of access control with respect to sensitive areas at the site. The access control measures ensure that only registered employees and registered visitors can access level 0. Sensitive products are handled in areas requiring access level 2.

O.Security-Control:

> Assigned personnel of the site and guards operate the systems for access control, surveillance and respond to alarms. Technical security measures like video control, motion and similar sensors support the enforcement of access control. These personnel is also responsible for registering visitors, contractors, and suppliers.

O.Alarm-Response:

> A series of border alarms are installed to provide a warning system for entering the premises by T.Smart-Theft and T.Rugged-Theft. Force entering in the premises will trigger border alarm. The alarm system will trigger an acoustic alarm in the security control room manned by security personnel. The personnel in the control room are in position to monitor and access the situation through the CCTV system and dispatch the security personnel to the location where the presence is needed. The security staff patrols the site periodically and can reach the spot in a few minutes. The system consisting of CCTV cameras monitored by security guards will detect unauthorised access.

O.Internal-Monitor:

> The management shall be responsible for presiding over the review of the information security established according to the requirement of iso27001:2013 standard once a year to ensure the detection of T.Smart-Theft and T.Rugged-Theft. to ensure the continuous suitability, sufficiency and effectiveness of the information security management. The review shall include evaluating opportunities for improvement and needs for change in information security management, strategies, performance and

trends, and identifying opportunities for change or improvement. The review ensures that information security is implemented and run in accordance with organisational policies and procedures.

O.Maintain-Security:

The security officer will check the CCTV daily to ensure all cameras are working, lenses are clean and picture quality is clear. The alarm systems is to prevent T.Rugged-Theft and T.Smart-Theft are checked. The access logs are stored for at least 3 months.

The access control system has to be operated in line with the 4-eye principle, 2 security personnel will be present to operate the system in secure server room. Network security is consistently monitored by the IT department to prevent T.Computer-Net.

O.Logical-Access:

ACTDG uses firewall, anti-virus, and anti-spam solutions.

ACTDG has separated networks between Building A and B for production and office (to prevent T.Unauthorised-Staff, T.Accident-Change and T.Computer-Net).

ACTDG uses a system to control users, password, local policy, security policy and authorisation to access shared folder. Every user is required to log on using their unique username and password. These measures counter T.Unauthorised-Staff and T.Accident-Change.

O.Logical-Operation:

ACTDG has a backup procedure including off-site backup. Access to IT equipment and location is limited to authorised ACTDG employees.

Updates in the network are controlled by the IT department. These security measures prevent T.Computer-Net, T.Unauthorised-Staff and T.Accident-Change.

O.Config-Items:

Products use their unique part number with job order number for product configuration management (according to P.Config-Items), along manufacturing process product will be tracked by tag card and data will be confirmed by supervisor or quality manager.

According to P.Config-Control, the Process Management Plan will specify information regarding which assembly steps and option processes are applied to a product. This information will be transferred during process transfer from new product development team to mass production. Any changes in file naming conventions will be followed using the “Engineering Change Control” process.

O.Config-Control:

Product has a procedure that describes process of new product/sample which gets requirements from clients and will record all parameters/configuration that is used

during sample manufacturing. The information will be transferred to mass production in process of new product transfer as required by P.Accept-Product. Any change in mass production which deviates from initial product transfer will be handled by “Engineering Change Control” procedure according to P.Config-Control.

O.Process-Config:

The product has a “Process Management Plan” according to P.Process-Config as process configuration management which has detail of process control, parameter that needs to be controlled, inspection method, and equipment that are used for the control of products as required by P.Accept-Product.

O.Acceptance-Test:

After assembly the quality control according to O.Acceptance-Test ensures that the finished product complies with the product specification according to P.Accept-Product. These measures are also detect errors to prevent T.Accident-Change. This is achieved by In-Process Quality Control and Control of nonconforming product. All product will be sampling / inspect base on configuration that defined in PMP. Any non-conforming unit will be segregated and corrective action request will be issues to concern department.

O.Staff-Engagement:

The appointment of staff will be dependent on two major factors: 1. the experience and suitability of the candidate to prevent T.Accident-Change, ensure P.Zero-Balance. 2. The personal history of the candidate. Job applications are submitted on a pre-printed company form to prevent T.Staff-Collusion. The Security manager, in concert with the Personnel Manager, will ensure that all details are carefully checked. This will involve direct personal contact with schools, previous employers and references to confirm details A confidentiality agreement has to be signed up by all employees to prevent T.Staff-Collusion, T.Computer-Net. Depending on the designated role of the staff member they get keys, computer passwords and other codes related to specific tasks to prevent T.Unauthorised-Staff.

O.Zero-Balance:

Zero Balance is achieved at the site by the tracking of production lots using manual forms throughout the entire production cycle. Each lot has its unique identification number.

According to the released production process the defect assets are destructed or sent back to the client with all functional pieces. Thus, we do not keep any pieces in the factory.

O.Reception-Control:

Upon reception of any goods an immediate incoming inspection (according to P.Reception (Control) is performed, including invoice number, product specific parameters and quantity. The quality inspection staff will perform quality tests on random samples for each shipment. The scale of sample tests is depending on the delivered quantity and is defined for each product in a separate document. Every good

is identified by an unique internal material number according to P.Config-Item. Upon request the inventory control creates new material numbers for new goods or derivatives.

O.Shipping-Support:

To prevent T.Shipment-Attack the shipping preparation is performed in the level 1 warehouse area. The goods and necessary documentation are transferred to the control of the Store Area Supervisor. The packing procedure is defined for each product. These procedures include packing, labelling and sealing. The label includes the shipping address. The shipping address is defined during the purchase order. Barcodes are used to verify the correct labelling and controlled handover to the forwarder according P.Shipping-Support.

O.Scrap-Control:

The site has measures in place to shred rejected or defect modules and inlays in case the destruction on site is requested by the client. Otherwise the scrap is returned to the client. The site has further measures in place to shred sensitive documentation and destruct electronic media and other sensitive configuration items. All items are destroyed in a way that they do not support attackers to prevent T.Unauthorised-Staff, T.Staff-Collusion and support P.Zero-Balance.

8.4 Security Assurance Requirements 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.

8.4.1 ALC_CMC.5

The chosen assurance level ALC_CMC.5 of the assurance family "CM capabilities" is suitable to support the production of high volumes due to the formalized acceptance process and the automated support. The identification of all configuration items supports an automated and industrialised production process. The requirement for authorized changes support the integrity and confidentiality required for the products. Therefore these security assurance requirements meet the requirements for the configuration management.

8.4.2 ALC_CMS.5

The chosen assurance level ALC_CMS.5 of the assurance family "CM scope" supports the controlled environment for production, testing, initialisation and software upload. This includes the documentation of the site security and the procedures for the configuration management as well as documentation of the product specific processes. 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

The chosen assurance level ALC_DVS.2 of the assurance family "Development security" is required since a high attack potential is assumed for potential attackers. The information used at the site during the production, initialization of the product and software upload can be used by potential attackers during the development of attacks. Based on the assumed self-protection of the products the information is needed to apply an attack within considerable time and effort. The keys used during the initialization process and/or software upload also support the security during the shipment. Therefore the handling is applied to split keys and a special storage of electronic keys is implemented. Further on the Protection Profiles [5] and [6] require this protection for sites involved in the life-cycle of Security ICs development and production.

8.4.4 ALC_LCD.1

The chosen assurance level ALC_LCD.1 of the assurance family "Life-cycle definition" is suitable to support the controlled development and production process. This includes the documentation of these processes and the procedures for the configuration management. Because the site provides only a limited support of the described life-cycle for the development and production of Security ICs the focus is limited to this site. However the assurance requirements are considered to be suitable to support the application of the site evaluation results for the evaluation of an intended TOE.

8.5 Assurance Measure Rationale

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 intended TOE design and implementation in its development environment. Thereby this objective is suitable to meet the 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 intended TOE design and implementation including the initialization and software upload in its production and testing environment. Thereby this objective is suitable to meet the Security Assurance Requirement.

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 intended TOE design and implementation including the initialization and software upload in its production and testing environment. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Internal-Monitor:

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Maintain-Security:

ALC_DVS.2.1C: The development security requires the correct functionality of the technical security measures. The associated control is defined by O.Maintain-Security. ALC_DVS.2.2C: The development security documentation shall justify the security measures provide the necessary level of protection. Also this is part of O.Maintain-Security. Thereby this objective is suitable to meet the 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 intended TOE design and implementation including the initialization in its development and production environment. In addition the configuration requirement ALC_CMC.5.5C requires that only authorised changes are made to configuration items. For computer systems the authentication is automatically enforced. Thereby this objective is suitable to meet the Security Assurance Requirements.

O.Logical-Operation:

ALC_DVS.2.1C: The computer systems are operated to provide the necessary level of protection to maintain the confidentiality and integrity of the processed data. The available data also contributes to ALC_DVS.2.2C: The development security documentation shall justify the security measures provide the necessary level of protection. Thereby this objective is suitable to meet the Security Assurance Requirements.

O.Config-Items:

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. A method used to uniquely identify the configuration items is required by ALC_CMC.5.2C. In addition ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.8C requires that the CM system shall identify the configuration items that comprise the however this is not directly applicable because only the configuration item "security IC" provides security functionality. ALC_CMC.5.11C requires that the CM system shall be able to identify the version of the implementation representation from which the product is generated. ALC_CMC.5.14C requires that the intended TOE can be identified as uniquely if it is either a new product or a new version of the intended product. The configuration list required by ALC_CMS.5.1C 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.

O.Config-Control:

ALC_CMC.5.2C requires the description how the configuration items are uniquely identify. ALC_CMC.5.4C requires to uniquely identify all configuration items. ALC_CMC.5.5C and ALC_CMC.5.6C requires automated measures so that only authorized changes are made. ALC_CMC.5.9C requires the support of audit information for all changes to the TOE by automated means including the originator, date and time. ALC_CMC.5.10C requires that 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 requires that production processes used for production and data for initialisation and/or upload can be identified. ALC_CMC.5.12C requires a CM documentation that includes a CM plan. ALC_CMC.5.13C requires to describe how the CM system is used for the development of the product. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the intended TOE. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. The identification of each configuration item (here the device and optionally the initialization data, software package for upload and keys is required by ALC_CMS.5.1C, ALC_CMS.5.2C, ALC_CMS.5.3C. Further on ALC_LCD.1.1C requires to maintain the intended products within the production environment. The objective meats the set of Security Assurance Requirements.

O.Process-Config:

ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items. The provision of automated measures such that only authorized changes are made to the configuration items as required by ALC_CMC.5.5C. ALC_CMC.5.7C requires that the CM system ensures that the person responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.9C requires the support of audit information for all changes to the TOE by automated means including the originator, date and time. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a

change given to a configuration item. ALC_CMC.5.12C requires that the CM documentation includes a CM plan. ALC_CMC.5.13C requires that the CM plan describe how the CM system is used for the development of the intended TOE. ALC_CMC.5.14C requires that the CM plan includes measure to accept modified or newly created configuration items. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires that the CM system is used as required by the CM plan and that related evidence is available. The configuration list required by ALC_CMS.5.1C 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_LCD.1.1C and ALC_LCD.1.2C require the maintenance of the intended products within the production environment and the associated control. The objective meats the set of Security Assurance Requirements.

O.Acceptance-Test:

The testing of the products is considered as automated procedure as required by ALC_CMC.5.6C. ALC_CMC.5.7C requires that the CM system ensures that the person responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.11C requires that production processes used for assembly and the integrated security IC can be identified. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. The operation of the CM system in accordance with the CM plan is required by ALC_CMC.5.16C. In addition ALC_LCD.1.2C requires control over the development and maintenance of the intended TOE. Thereby the objective fulfils this combination of Security Assurance Requirements.

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 intended TOE design and implementation in its development environment. Thereby the objective fulfils this combination of Security Assurance Requirements.

O.Zero-Balance:

ALC_CMC.5.6C requires that the CM system supports the production of the intended TOE by automated means. ALC_CMC.5.9C requires the support of audit information for all changes to the TOE by automated means including the originator, date and time. ALC_CMC.5.11C requires that production processes used for assembly and the integrated security IC can be identified. ALC_CMC.5.15C requires evidence that all configuration items are maintained. ALC_DVS.2.2C requires a rational that the security measures for all configuration items are fulfilled. ALC_LCD.1.2C requires that the processes for a controlled production environment are described. Thereby this objective is suitable to meet the set of Security Assurance Requirements.

O.Reception-Control:

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.14C required a process to accept modified or new configuration items. ALC_CMC.5.15C required evidence for the control of the configuration items. The operation of the CM system in accordance with the CM plan is required by ALC_CMC.5.16C. ALC_CMS.5.2C and ALC_CMS.5.3C required the identification of all configuration items. ALC_DVS.2.2C requires a rational for the identification of sensitive configuration items. Thereby this objective is suitable to meet the set of Security Assurance Requirements.

O.Shipping-Support:

ALC_CMC.5.15C requires that configuration items including the final parts that are intended for the delivery are maintained under the CM system, ALC_CMS.5.2C requires that all parts are uniquely identified in the configuration list. ALC_DVS.2.2C requires the confidentiality and integrity of the configuration items during internal shipment. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Data-Transfer:

ALC_DVS.2.2C The development security documentation shall justify the security measures provide the necessary level of protection to ensure confidentiality and integrity of the intended TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.

No sensitive data involved currently.

O.Scrap-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 intended TOE design and implementation in its production environment including initialisation and software upload and prevent misuse of non-conform security ICs. Thereby this objective is suitable to meet the Security Assurance Requirement.

8.6 Mapping of the Evaluation Documentation

The scope of the evaluation according to the assurance class ALC_CMS comprises the security products, the complete documentation of the site provided for the evaluation and the configuration and initialisation data as well as associated tools. The specifications and descriptions provided by the client are not part of the configuration management at ACTDG.

The mapping between the internal site documentation and the Security Assurance Requirements is only available within the full version of the Site Security Target.

9 Bibliography

[1] Common Criteria, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[2] Common Criteria, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[3] Common Criteria, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

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

[6] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014

[7] Site Security Target Template, Version 1.0, published by Eurosmart," Eurosmart, 21.06.2009