HiPandaCC V100 Site Security Target lite Shenzhen-Huawei Base D3-4A17R

Huawei Technologies Co.Ltd

Contents

1 Document Information

1.1 Reference

Title:	HiPandaCC V100 Site Security Target lite Shenzhen-Huawei Base D3-4A17R
Version:	1.0
Date:	14 Dec 2021
Company:	Huawei Technologies Co.,Ltd.
Name of the site:	Shenzhen-Huawei Base D3-4A17R
Product type:	Site certification
EAL-Level:	EAL6

1.2 Version History

Version	Date	Comment/Editor/Changes
1.0	14 Dec 2021	First formal version

2 SST Introduction

The SST describes security features of the site and defines the scope of the site. This chapter is divided into two sections “SST reference and Site reference” and “Site description”.

2.1 SST Reference

Title: HiPandaCC V100 Site Security Target lite Shenzhen-Huawei Base D3-4A17R

Version: 1.0

Date: 14 Dec 2021

2.2 Identification of the Site

The name of the site is Shenzhen-Huawei Base D3-4A17R. It is located at:

Huawei Base D region, D3 building, 4th Floor.

Wuhe Street, Longgang district, Shenzhen, China

2.3 Site Description

2.3.1 Physical Scope

The site is an isolated area on the 4th floor of D3 building in Huawei Base D region. It consists of an entry region, a development room, a testing room, a meeting room and an IT server room. Among these areas, three different security levels area employed:

- Level1: The entry region
- Level2: The development room, the testing room and the meeting room
- Level3: The IT server room

The site is a secure area with restricted access where only authorized persons can enter. Within the development area, only members of the development team are entitled to access sensitive information like source code, design material and confidential development documentation. To enforce such access restriction, a combination of physical, procedural, personnel and logical measurements have been installed.

2.3.2 Logical Scope

The activities are: Security IC Embedded Software Development (Phase 1), IC Embedded Software and Testing (Phase 1), IC Design (Phase 2), IC Dedicated Software and Testing (Phase 2) as defined in ‘Security IC Platform Protection Profile with Augmentation Packages’ (PP-0084)

To perform its activities the site uses the Huawei provided and managed remote IT infrastructure. Locally available IT equipment like workstations or VPN router is also provided and managed by Huawei IT authorized support directly or remotely.

The site performs secure shipment, which only refers to internal shipments and/or shipments between sites and not to shipment to customer or end user. Therefore ALC_DEL is not scope.

The site performs secure scrap activities and has measures in place to either securely destruct assets (e.g. paper shredder) or return them to the client and/or to a certified site to perform higher scrap requirements.

3 Conformance Claim

The evaluation is based on Common Criteria Version 3.1:

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

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology; Version 3.1, Revision 5, April 2017, [3]
- JIL – Minimum Site Security Requirements v3.0, February 2021, [6]

The evaluation of the site comprises the following assurance components[1]:

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

The assurance level chosen for the SST template is compliant to the Protection Profile (PP) [5] and therefore suitable for Security ICs.

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

[1] The activities of the site are not directly related to production and shipping of secure products. Therefore, this site does not claim conformance to ALC_DEL. Since there is no specific TOE included in the site certification, the development tools ca not be defined either. Therefore, this site does not claim conformance to ALC_TAT.

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 and the security management of the site.

4.1 Assets

The following section describes the assets handled at the site.

Physical security objects	The site has physical security objects (samples, printed documents, etc.) in relation to developed TOEs. Both the integrity and the confidentiality of these must be protected
Development data:	The site has access to (and optionally copies thereof) electronic development data (specifications, guidance documentation, source code, etc.) in relation to developed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected
Development tools:	To perform its development activities the site uses tools (e.g. synthesis, layout and simulation tools) to transform design code, schematics and library elements into a design database. The integrity of these tools (running on local or remote development computers) must be protected.

4.1.1 Security IC Embedded Software Development

- software specifications
- source code in any form
- pre-personalisation data
- guidance documentation

4.1.2 IC Development

- hardware and IC Dedicated Software specifications
- source code for software and hardware
- layout data for the hardware
- pre-personalisation data
- keys for the personalisation
- guidance documentation

4.2 Threats

The threats at this site are considered as followed

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 access to (1) development data with the intention to violate confidentiality and possibly integrity (2) development computers with the intention to modify the development process

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 projects or different clients during development by accident.

Employees, contractors or student trainees that are not trained may take products or influence development 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 development or test. 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 development, production or test get access to products or affect configuration systems, so that the confidentiality and/or the integrity of the product is violated.

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 and/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 development 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 development flow and the security measures of the site. In addition, they shall allow an appropriate mapping to the Security Assurance Requirements (SAR).

The documentation of the site under evaluation is under configuration management. This comprises all procedures regarding the evaluated development 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 relies completely on the naming and identification of the received configuration items. In this case, 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 development 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 development process ensures that sufficient information is provided by the client.

The product setup may include the following information (1) identification of the product, (2) properties of the product when received at the site (3) properties of the product when internally shipped or externally delivered, (4) classification of the items (which are security relevant), (5)

who (either Name of the site or the client) is responsible for destruction of defect devices, (6) how the product is tested after assembly, (7) any configuration of the processed item as part of the services provided by the site, (8) 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.

The documentation that includes the process descriptions and the security measures of the site is under version control. Measures are in place to ensure that the evaluated status is ensured. In most cases automated tools are used to support and control the development at the site. This comprises graphical parameters for each layer as well as parameters of test structures produced together with the functional devices. In addition, it comprises scripts or batch routines developed by the site to track the development process of the intended TOE. This can also comprise service levels or quality parameters.

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 development 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 TOEs of different clients) are separated and traced on a device basis. For each handover, either an automated or an organizational “two-employees-acknowledgement” (four-eye principle) is applied for functional and defect assets. As per the released development process the defect assets are sent back to a certified site and/or consumer (depending on the development-setup).

P.Product-Transport: 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.Transfer-Data: Any data in electronic form (e.g. product specifications, test programs, release information etc.) that is classified as sensitive or higher security level by the client is encrypted to ensure confidentiality of the data. The

integrity of the data is ensured by the signed signature. The entire IT configuration fulfils the Huawei requirements.

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.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.Internal-Shipment: The recipient (client) of the product is identified by the address of the client site. The address of the client is part of the product setup.

A.Init-Data: To enable that the site participates in the development of products the client provides services to setup and maintain the necessary development environment (e.g. workstations, tools) and configuration management systems (e.g. user accounts in project repositories) including a CM plan. The client also provides a secure connection between the IT equipment of the site and a secure remote IT infrastructure of the client. These services are provided by the client in a secure way in order to properly protect the assets of the site.

This includes the enforcement of a trustworthy access policy to the site equipment and data using the secure connection based on a “need-to-know” principle and offering a secure storage of the hardware design data in a remote data center..

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.

A.Destruct-Scrap: Scrap configuration items are also transferred and they are destructed at the receiving site so that they are useless for an attacker.

5 Security Objectives

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

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organisational security measures allows a sufficient separation of employees to enforce the “need to know” principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorised people. The site enforces three levels (level 1 to level 3) of access control to sensitive areas of the site. The access control measures ensure that only registered employees and vendors can access restricted areas. Sensitive products are handled in restricted areas only.

O.Security-Control: Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like 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 physical and/or 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 development network and an office network. Additional specific networks for development and configuration are physically separated from any internal network to enforce access control. Access to the development

network and related systems is restricted to the authorised 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. 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 development 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 development control.

O.Config-Process: The site controls its services and/or processes using a configuration management plan. The configuration management is controlled by tools and procedures for the development and development 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.

O.Staff-Engagement: All employees who have access to sensitive configuration items and who can move parts of the product out of the defined development flow are checked regarding security concerns and have to sign a nondisclosure 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 development flow, the defect devices are sent to the client or the consumer. This defect device delivery is an internal delivery.

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 development process.

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

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

O.Control-Scrap: 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	Security Objective	Note
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	O.Physical-Access and O.Alarm-Response detect unauthorized access, O.Security-Control responds to the detected incidents and O.Internal-Monitor and O.Maintain-Security control and maintain these security measures. Therefore, the threat is effectively addressed by these objectives

T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	O.Physical-Access and O.Alarm-Response detect unauthorized access, O.Security-Control responds to the detected incidents and O.Internal-Monitor and O.Maintain-Security control and maintain these security measures. Therefore, the threat is effectively addressed by these objectives
T.Computer-Net	O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement	O.Logical-Access, O.Logical-Operation and O.Staff-Engagement prevent unauthorized access from the internal and external network, and O.Internal-Monitor and O.Maintain-Security control and maintain these security measures. Therefore, the threat is effectively addressed by these objectives.
T.Accident-Change	O.Logical-Access O.Logical-Operation O.Config-Items O.Config-Process O.Acceptance-Test O.Staff-Engagement O.Zero-Balance	O.Logical-Access, O.Logical-Operation, O.Staff-Engagement, O.Zero-Balance and O.Control-Scrap, O.Config-Items prevent unauthorised access and changes to assets. O.Config-process ensures a proper process of the change is followed. Therefore, the threat is effectively addressed by these objectives. .
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Zero-Balance O.Control-Scrap	O.Physical-Access, O.Alarm-Response, O.Logical-Access, O.Logical-Operation, O.Staff-Engagement, O.Zero-Balance and O.Control-Scrap prevent unauthorised access to assets, O.Security-Control responds to the detected incidents and O.Internal-Monitor and O.Maintain-Security control and maintain these security measures. Therefore, the threat is effectively addressed by these objectives.
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Zero-Balance O.Control-Scrap	O.Staff-Engagement ensures that all staff is aware of its responsibilities, and O.Internal-Monitor and O.Maintain-Security control and maintain these security measures. Therefore, the threat is effectively addressed by these objectives.
T.Attack-Transport	O.Internal-Shipment O.Transfer-Data	O.Transfer-Data ensures that the sensitive item transferred to the external company are protected with the secure measures. O.Internal-Shipment ensures that the internal delivery procedure are applied to the sensitive item. Therefore, the threat is effectively addressed by these objectives.

OSP	Security Objective	Note
P.Config-Items	O.Reception-Control O.Config-Items	O.Config-Items directly enforces the OSP. O.Reception-Control ensures the incoming items follows the reception procedures and uniquely labelled.
P.Config-Control	O.Config-Items O.Config-Control O.Logical-Access	O.Config-Control directly enforces the OSP. O.Config-Items ensures all configuration items are uniquely labelled and identified. O.Logical Access ensures only authorised personnel can setup the development process.
P.Config-Process	O.Config-Process	The Security Objective directly enforces the OSP.
P.Reception-Control	O.Reception-Control	The Security Objective directly enforces the OSP.
P.Accept-Product	O.Config-Control O.Config-Process O.Acceptance-Test	O.Acceptance-Test directly enforces the OSP. O.Config-Control and O.Config-Process ensures the accepted items are recorded and labelled in a correct way. The items can be identified and traced correctly in the site.
P.Zero-Balancing	O.Internal-Monitor O.Staff-Engagement O.Zero-Balance O.Control-Scrap O.Internal-Shipment	O.Zero-Balance directly enforces the OSP. O.Internal-Shipment and O.Control-Scrap ensure the sent-out items are well controlled. O.Staff-Engagement and O.Internal-Monitor ensure the internal policy is updated on time and fulfilled by the employees.
P.Transfer-Data	O.Transfer-Data	The Security Objective directly enforces the OSP.

Table 5.1: Security Objectives Rationale

6 Extended Assurance Components Definition

No extended components are currently defined in this SST.

7 Security Assurance Requirements

Clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Security IC Platform Protection Profile [5].

The Security Assurance Requirements (SAR) are:

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 fulfil the requirements of [4] 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 [MSSR]) are used in this Site Security Target.

7.1 Application Notes and Refinements

The description of the site certification process [4] 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)

According to [4] the processes rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below.

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 development processes as well as on the site security measures.

The life-cycle described in [5] is a complex development process. Only parts of this development process are normally provided at a specific site. In such a case the control of the product during such a development process must include sufficient verification steps to ensure the specified and expected result. Test procedures, verification procedures and the associated expected results must be 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 must be able to maintain the items listed for the relevant life-cycle step and the CM system must be able to track the configuration items.

A CM system has to be employed to guarantee the traceability and completeness of different development 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.

According to [5], 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” include:

- Hardware and software specifications
- Source code for software and hardware.
- layout data for the hardware
- keys for the personalisation
- pre-personalisation data
- guidance documentation
- Development tools and samples

In addition, 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 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 as described in [5].

The TOE developer 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 (customer specific samples or open samples) development tools and other material must be restricted to authorised 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 and integrity are the same but it must clearly distinguished to ensure the correct subject of the evaluation.

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 PP [5] provides a life-cycle description there specific life-cycles steps can be assigned to the tasks at site. This may comprise a change of the life-cycle state if e.g. testing or initialisation is performed at the site or not.

The PP [5] 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 [2] 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 the products. If the site already receives configuration items, this process is based on the assumption that the received configuration items are appropriately labelled and identified, refer to A.Item-Identification.

SAR	Security Objective	Rationale
ALC_CMC.5.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	O.Config-Items	O.Config-Item describes that the TOE is labelled with its unique reference by the configuration management system
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	Incoming inspection according to O.Reception-Control ensures product identification and the associated labelling. This labelling is mapped to the internal identification as defined by O.Config-Items. This ensures the unique identification of security products. O.Config-Control ensures that each client part ID is setup and released based on a defined process. This comprises also changes related to a client part ID. The configurations can only be done by authorised staff. O.Config-Process provides a configured and controlled development process.
ALC_CMC.5.3C: The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	O.Reception-Control ensures the incoming changed configuration items from the client can be recognized and labelled correctly. O.Config-Items and O.Config-Control ensures the changes to both the internal and external configuration items are recorded and reviewed. O.Config-Process ensures that only authorised staff can apply changes. This comprises changes related to process flows, procedures and items of

		clients. Teams are defined to assess and release changes.
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 comprises the incoming labelling and the mapping to internal identifications. O.Config-Items comprises the internal unique identification of all items that belong to a client part ID. Each product is setup according to O.Config-Control comprising all necessary items.
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Config-Control O.Config-Process O.Logical-Access O.Logical-Operation	O.Config-Control assigns the setup including processes and items for the development of each client part ID. O.Config-Process comprises the control of the development processes. O.Logical-Access and O.Logical-Operation support the control by limiting the access and ensuring the correct operation for all tasks to authorised staff.
ALC_CMC.5.6C: The CM system shall support the production of the product by automated means.	O.Config-Process O.Zero-Balance O.Acceptance-Test	O.Config-Process comprises the automated management of the development processes. O.Zero-Balance ensures the control of all security products during development. O.Acceptance-Test provides an automated testing of the functionality and supports the tracing.
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.Reception-Control O.Acceptance-Test O.Config-Process O.Logical-Access	O.Reception-Control ensures the reception procedure of the physical configuration item. Since the site is only receiving physical configuration item from the client, the person responsible for accepting the physical configuration item cannot be the developer. O.Acceptance-Test ensures the test results are recorded in the CM. O.Config-Process ensures the procedure of the CM plan. It is required in the procedure that the CM manager is not the CM developer. O.Logical-Access ensures the configuration item developer cannot accept the configuration items in the CM system.

ALC_CMC.5.8C: The CM system shall clearly identify the configuration items that comprise the TSF.	O.Config-Control O.Config-Process O.Config-items	O.Config-Items comprises the internal unique identification of all items that belong to a client part ID. O.Config-Control describes the management of the client part IDs O.Config-Process describes the scope of the configuration items.
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.	O.Config-Control O.Config-Process O.Config-items O.Acceptance-Test	O.Config-Control describes the management of the client part IDs at the site.ID. O.Config-items ensures the changes of the configuration items are recorded. O.Config-Process ensures that the changes are recorded automatically by the CM system. O.Acceptance-Test ensures the changes from the acceptance test are recorded automatically.
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O.Config-Control O.Config-Process	O.Config-Control describes the management of the configuration items received from the client and delivered to the client. According to O.Config-Process the CM plans provides a service to generate a related report containing the affected configuration items.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	O.Reception-Control comprises the control of the incoming configuration items. O.Config-Items and O.Config-Control cover identifies the version of the implementation representation from which the intended TOE is generated through baselines. O.Config-Process ensures that only controlled changes are applied.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O.Config-Control O.Config-Process	According to O.Config-Control the setup of each client part ID includes an associated CM plan including the release. O.Config-Process ensures the reliability of the processes and tools based on dedicated CM plans.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE.	O.Config-Control O.Config-Process	O.Config-Control describes the management of the client part IDs at the site. According to O.Config-Process the CM plans describe the services provided by the site.

ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	O.Reception-Control supports the identification of configuration items at the site. O.Config-Items ensures the unique identification of each product produces at the site by the client part ID. O.Config-Control ensure a release for each new or changed client part ID. O.Config-Process ensures the automated control of released products
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Reception-Control O.Config-Control O.Config-Process O.Zero-Balance O.Internal-Shipment	The objectives O.Reception-Control, O.Config-Control, O.Config-Process ensure that only released client part IDs are produced. This is supported by O.Zero- Balance ensuring the tracing of all security products. O.Internal-Shipment include the packing requirements, the reports, logs and notifications including the required evidence.
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan	O.Config-Control O.Config-Process O.Acceptance-Test O.Internal-Shipment	O.Config-Control comprises a release procedure as evidence. O.Config-Process ensures the compliance of the process. O.Acceptance-Test comprises the control that all finished parts based on the test assigned to this part ID. The finished products are returned to the client according to O.Internal-Shipment.

Table 7.1 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMS.5.1C: The configuration list includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.	O.Config-Items O.Config-Control O.Config-Process	Since the process is subject of the evaluation no products are part of the configuration list. O.Config-Items ensures unique part IDs including a list of all items and processes for this part. O.Config-Control describes the release process for each client part ID. O.Config-Process defined the configuration control including part IDs, procedures and processes.

ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config-Items O.Config-Control O.Config-Process O.Reception-Control O.Internal-Shipment	Items, products and processes are uniquely identified by the database system according to O.Config-Items. Within the development process the unique identification is supported by automated tools according to O.Config-Control and O.Config-Process. The identification of received products is defined by O.Reception-Control. The labelling and preparation for the transport is defined by O.Internal-Shipment
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.	O.Config-Items	According to O.Config-Items all configuration items for secure products are identified.

Table 7.2 Rationale for ALC_CMS.5

SAR	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Control-Scrap	The physical protection is provided by O.Physical-Access, supported by O.Security- Control, O.Alarm-Response, and O.Maintain-Security. The logical protection of data and the configuration management is provided by O.Logical-Access and O.Logical-Operation. The personnel security measures are provided by O.Staff-Engagement. The sensitive information is securely destroyed according to O.Control-Scrap.
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O.Internal-Monitor O.Logical-Operation O.Maintain-Security O.Zero-Balance O.Acceptance-Test O.Transfer-Data	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous justification is subject of the objectives O.Internal-Monitoring, O.Logical-Operation and O.Maintain-Security. All devices including functional and non-functional are traced according to O.Zero-Balance. O.Acceptance-Test supports the integrity control by functional testing of the finished products. O.Transfer-Data ensures the data is transferred in a secure method.

		The confidentiality and integrity is protected during the transfer.

Table 7.3 Rationale for ALC_DVS.2

SAR	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	O.Config-Control O.Config-Process	The processes used for identification and development are covered by O.Config-Control and O.Config-Process.
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	O.Acceptance-Test O.Config-Process O.Zero-Balance	O.Acceptance-Test describes the necessary test on the configuration items. O.Config-Process describes the necessary control over the development and the maintenance of the TOE in each phase. All security products are traced according O.Zero-Balance.

Table 7.4 Rationale for ALC_LCD.1

Since this SST references the PP [5], 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

8.1 Preconditions Required by the Site

The site performs some development and verification services for the construction of secure IC hardware and software. To perform these services in a secure way, the client of the site needs to support the security processes of the site. The following paragraphs denote preconditions of the client that are required to ensure the security measures of the site to protect its assets.

For the setup of the development process, the relevant specifications and product information is required by Huawei. In general, the release process can only be finished, if the required information is provided by the client. All these data/information has to be provided to Huawei in encrypted format or via a secure channel. All finished products are tested. The tests are configured based on the provided specifications. The test environment allows functional tests to verify the operation after completion of the development. This cover the assumption **A.Prod-Specification**.

Huawei has procedures in place to protect and maintain classified products and properties of his clients. The protection is based on the classification agreed with the client or printed on the received item or document. Any received configuration items are appropriately labelled and identified by the client. This covers the assumptions **A.Product-Integrity** and **A.Item-Identification.**

Secure physical destruction and scrap handling are supported by the client. The site does not provide a secure physical destruction process as a service. All scraps are securely shipped to the client. This covers the assumption **A.Destruct-Scrap.**

The shipping after the development is supported by labelling and packaging the finished products. The products are labelled and packed as specified by the client. This includes the address of the receiver. The forwarder is selected by the client. Huawei verifies the secure label based on the provided pre-announcement by the client before any charge is handed over. The pre-announcement is performed for each transport. The tracing and further control and security measures for that transport is under the responsibility of the client. This covers the assumption **A.Internal-Shipment.**

Further, the client needs to setup and maintain the used configuration management systems and provide a project specific CM plan. This includes the setup and maintenance of user accounts in the project repositories and other required configuration management tools. The client needs to agree about the configuration management methods and the usage of the configuration management tools. The configuration management methods and tools by the client ensure the correct handling of the configuration items according to Common Criteria.

In addition, the client needs to setup and maintain a secure connection between the IT equipment of the site and a remote secure IT infrastructure of the client. The enforced access policy to the equipment and data of the site using this secure connection need to be restrictive and based on a “need-to-know” principle. Meanwhile, a secure data center is provided by the client to ensure the hardware design data is stored in a secure manner. Therefore, the assumption **A.Init-Data** is covered.

8.2 Services of the Site

The following services and/or processes provided by Shenzhen-Longgang-Huawei Base D3-F4-A17R are in the scope of the site evaluation process:

Security IC Embedded Software Development (Phase 1), IC Embedded Software and Testing (Phase 1), IC Design (Phase 2), IC Dedicated Software and Testing (Phase 2) as defined in 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084)

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

Development comprises

- The generation of the GDSII layout of Smart Card ICs, the source code of embedded and IC dedicated software and the creation of development related documents.
- The verification and validation processes: verification comprises the simulation and emulation of hardware & software designs on dedicated test environments. The purpose of verification is the preparation of the design freeze and sample development. Validation comprises verification of the design with real samples. The purpose of validation is to release the product to the Operations organization that facilitates the volume ramp up.

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 site is a closed area, armed by the infrared alarms, the glass breaking detection and the intrusion detection. The access to the area is only possible via access controlled doors. The enabling of the alarm system and the additional external control are graduated according to the running operation at the site. The physical, technical and organizational security measures ensure a separation of the site into three security levels. The access control ensures that only registered persons can access sensitive areas. This is supported by O.Security-Control that includes the maintenance of the access control and the control of visitors. The physical security measures are supported by O.Alarm-Response providing an alarm system.

Thereby the threats T.Smart-Theft, T.Rugged-Theft can be prevented. The physical security measures together with the security measure provided by O.Security-Control enforce the recording of all actions. Thereby also T.Unauthorized-Staff is addressed.

O.Security-Control

The guard service monitors the site and surveillance systems continuously. The CCTV system supports these measures because it is always enabled. Further on the security control is supported by O.Physical-Access requiring different level of access control for the access to security product during operation as well as during off-hours.

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

O.Alarm-Response

The guard service is monitoring the alarm system continuously. The guard is also maintaining and alarm log for review and audit purposes. O.Physical-Access requires certain time to overcome the different level of access control. The response time of the guard and the physical resistance match to provide an effective alarm response.

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

O.Internal-Monitor

Regular security management meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This comprises also logs and security events of security relevant systems like Firewall, Virus protection and access control. Major changes of security systems and security procedures are reviewed. Upon introduction of a new process a formal review and release for mass production is made before being generally introduced.

This addresses T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance

O.Maintain-Security

The security relevant systems enforcing or supporting O.Physical-Access, O.Securitycontrol and O.Logical-Access are checked and maintained regularly by the suppliers. In addition the configuration is updated as required either by employees (for the access control system) of the supplier. Logging files are checked regularly for technical problems and specific maintenance requests.

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

O.Logical-Access

The internal network is separated from the internet. The internal network is further separated into subnetworks by internal firewalls. These firewalls allow only authorized information exchange between the internal subnetworks. Each user is logging into the system with his personalised user name and password. The objective is supported by O.Internal-Monitor based on the checks of the logging regarding security relevant events. The individual accounts are addressing T.Computer-Net. All configuration is stored in the database of the configuration management system.

Supported by O.Config-Items this addresses the threats T.Accident-Change and T.Unauthorised-Staff and the OSP P.Config-Control.

O.Logical-Operation

All logical protection measures are maintained and updated as required. The firewall configuration is set by Huawei IT team. The IT infrastructure fulfils Huawei IT requirements and is evaluated based on a regular manner. The backup is sufficiently protected and is only accessible for the administration.

This is addressing the threats T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff

O.Config-Items

All product configuration information is stored in the database of the configuration management system. Products are identified by unique client part IDs with are linked to the unique ID numbers of the associated configuration items.

This is addressing the threat T.Accident-Change and the OSP P.Config-Items and P.Config-Control

O.Config-Control

The configuration management covers the release and management of development. The development is initialised and maintained in a data base. In addition, the development and change of internal procedures is released according to the quality process.

Supported by O.Config-Items this addresses the threats T.Unauthorised-Staff, T.Accident-Change and the OSP P.Config-Control, P.Accept-Product

O.Config-Process

The configuration management comprises automated measures to ensure the correct set up of a development and to ensure constant results within the development appropriate procedures are defined. Further on a team of employees responsible for the product handling and the development is defined to plan, organise and control the development process. This includes also the change of development steps.

This addresses the threat T.Accident-Change and the OSP P.Config-Process and P.Accept-Product

O.Acceptance-Test

Acceptance tests are introduced and released based on the client’s approval. The tools, specifications and procedures for these tests are controlled by the means of O.config-Items and O.Config-Control. Acceptance test results are logged and linked to a work order in the configuration management system.

This addresses the threat T.Accident-Change and the OSP P.Accept-Product.

O.Staff-Engagement

All employees are interviewed before hiring. They must sign an NDA and a code of conduct for the use of computers before they start working in the company. The formal training and qualification includes security relevant subjects and the principles of handling and storage of security products. The security objectives O.Physical-Access, O.Logical-Access and O.Config-Items support the engagement of the staff.

This addresses the threats T.Computer-Net, T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance

O.Zero-Balance

The automated tracing of the functional and defect devices ensure that no security devices are lost during the development and testing. This security objective is supported by O.Physical-Access, O.Config-Items and O.Staff-Engagement.

This addresses the threats T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance.

O.Reception-Control

The incoming inspection ensures the correct identification of security product and the verification of the security measure applied to control the integrity during shipment. The process is the starting point of the internal tracing. If an assignment cannot be applied the product is separated until the identification is clarified.

The OSPs P.Config-Items and P.Reception-Control are addressed by the reception control.

O.Internal-Shipment

The recipient of secure products is linked to the work order in the management system and can only be modified by authorized users. Packing procedures are documented in the product configuration. This includes specific requirement of the client. This security objective is supported by O.Staff-Engagement and O.Config-Items.

The threat T.Attack-Transport is addressed by the internal transport.

O.Transfer-Data

Classified electronic data and documents are protected with cryptographic algorithms during transfer. The keys are assigned to authorised employees only.

Supported by O.Logical-Acces and O.Staff-engagement this addresses the threats T.Staff-Collusion and T.Attack-Transport as well as the OSP P.Transfer-Data

8.4 Security Assurance Requirements Rationale

The SAR Rationale does not explicitly address the developer action elements defined in [2] 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. This includes the requirement that the procedures are applied as written and explained in the documentation.

8.4.1 ALC_CMC.5

ALC_CMC.5.1C The TOE shall be labelled with its unique reference.

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 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 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 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 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 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 chosen assurance level ALC_CMC.5 of the assurance family "CM capabilities" is suitable to support the development of high volumes due to the formalized acceptance process and the automated support. The identification of all configuration items supports an automated and industrialised development 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 CM scope (ALC_CMS.5)

ALC_CMS.5.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.

ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.5.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

The chosen assurance level ALC_CMS.5 of the assurance family "CM scope" supports the control of the development and test environment. This includes product related documentation and data as well as the documentation for the configuration management and the site security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE these security assurance requirements are considered to be suitable.

8.4.3 Development Security (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 TOE design and implementation in its development environment.

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

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 configuration items and information handled at the site during development, testing of the product can be used by potential attackers for the development of attacks. Therefore the handling and storage of these items must be sufficiently protected. Further on, the Protection Profile (Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014) requires this protection for sites involved in the life-cycle of security ICs development and production.

8.4.4 Life-cycle definition (ALC_LCD.1)

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

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 TOE design and implementation

in its development environment. Thereby this objective contributes 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 TOE design and implementation in its development and production environment. Thereby this objective contributes 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 TOE design and implementation in its development and production environment. Thereby this objective contributes 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 TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Maintain-Security

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 TOE design, implementation and in its development and production environment. Thereby this objective contributes to meet the Security Assurance Requirement. 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. Thereby this objective contributes to meet the Security Assurance Requirement.

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 TOE design, implementation and in its development and production environment. Thereby this objective is suitable to meet the Security Assurance Requirement. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items. Thereby this objective contributes to meet the Security Assurance Requirement. 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.

O.Logical-Operation

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 TOE design, implementation and in its development and production environment. Thereby this objective contributes to meet the Security Assurance Requirement. 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. Thereby

this objective is suitable to meet the Security Assurance Requirement. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Config-Items

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. ALC_CMC.5.2C requires to describe the method used to uniquely identify the configuration items. The acceptance procedures provide for an adequate review of changes to the CIs is required by ALC_CMC.5.3C. In addition ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.9C requires the CM system shall support the audit of changes to TOE by automated means. ALC_CMC.5.14C requires that the CM plan describes the procedures used to accept modified or newly created configuration items as part of the TOE. 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_CMS.5.2C requires that the developer of each TSF relevant configuration item is indicated in the configuration list. The objective meets the set of Security Assurance Requirements.

O.Config-Control

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires 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 requires a unique identification of all configuration items by the CM system. 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 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.5.10C requires that the system automatically identifies all configuration items that are affected by a change given to a configuration item. ALC_CMC.5.11C requires that the version of test programs and the development processes can be identified. ALC_CMC.5.12C requires a CM documentation that includes a CM plan. ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development (production) of the TOE. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE. 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 evidence shall demonstrate that the CM system is operated in accordance with the CM plan. 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. In addition ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products. The objective meets the set of Security Assurance Requirements.

O.Config-Process

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires an adequate and appropriate review

of changes to all configuration items. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. 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.5.6C requires that the CM system supports the production by automated means. ALC_CMC.5.7C requires that the person or team accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.9C requires the CM system shall support the audit of changes to TOE by automated means. 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.5.11C requires that the version of test programs, internal procedures and processes used at the site can be identified. 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 TOE. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE. 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 evidence shall demonstrate that the CM system is operated in accordance with the CM plan. 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 requires that the lifecycle definition documentation describes the model used to develop and maintain the products. ALC_LCD.1.2C requires control over the development and maintenance of the TOE. The objective meets 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.5.9C requires the CM system shall support the audit of changes to TOE by automated means. ALC_CMC.5.13C requires that the CM plan describe how the CM system is used to accept finished configuration items. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items. 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 TOE. ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the TOE during development, testing and production. 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 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 TOE by automated means. ALC_CMC.5.15C requires evidence that all configuration items are being maintained under the CM system. ALC_DVS.2.2C requires security measures that are necessary to protect the confidentiality and integrity of the TOE. ALC_LCD.1.2C requires control over the

development and maintenance of the TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Reception-Control

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires 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 requires a unique identification of all configuration items by the CM system. ALC_CMC.5.7C requires that the person accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.11C requires that the version of design data used to generate the test scripts can be identified. ALC_CMC.5.14C requires that the version of test programs and the development processes can be identified. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the TOE during internal transport. Thereby this objective is suitable to meet the Security Assurance Requirement

O.Internal-Shipment

ALC_DVS.2.2C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE. This includes also the protection during internal transport. 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 evidence shall demonstrate that the CM system is operated in accordance with the CM plan. ALC_CMS.5.2C according the unique identification of the packing as configuration item. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Transfer-Data

ALC_DVS.2.2C: 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. This includes also the protection during the transport between development sides. 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 comprises the processing and handling of security products and the complete documentation of the site provided for the evaluation. The specifications and descriptions provided by the client are not part of the configuration management at INESA. The mapping between the internal site documentation and the Security Assurance Requirements is described in the following tables.

SAR	Aspect
ALC_CMC.5.1C: The TOE shall be labelled with its unique reference.	The sources are labelled in the version control system, which is owned by the site. The version control system is used as per project. Documents are labelled with a DOC-number, -title, -owner. Configuration Items are identified via the identifiers that are automatically provided by the

SAR	Aspect
	system as well as the baseline labels that are given by the configuration manager.
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	All items can be uniquely identified by the version control system, which is owned by the site. Documents can be uniquely identified using the labelling described above. Configuration Items are identified via the identifiers that are automatically provided by the system as well as the baseline labels that are given by the configuration manager.
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.	Review board is in place for every project.
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	All items can be uniquely identified by the version control system, which is owned by the site.
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	Different CM tools like SVN as well as Gitlab provides automated measures to only allow authorized changes to configuration items. Restricted access allows only authorized persons to do changes and the authorization for the change is approved by the Change Control Board using the change process
ALC_CMC.5.6C: The CM system shall support the production of the TOE by automated means.	The above-mentioned tools support the development of the intended 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.	Specific roles in tools are defined in a way that the person responsible for accepting a configuration item into CM is not the person who developed it. The role CM administrator publishes a document written by an author.
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	There is no specific TOE in the focus.

SAR	Aspect
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.	Different CM tools like SVN or Gitlab provide automated means to support the audit of all changes. Documents stored in SVN are under version control
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.	In case a source file has been changed, the code is compiled again and all affected items are identified via the implementation module mapping. Documents are checked for consistency via the document mapping.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.	Different CM tools like SVN or Gitlab provide means to tag a release version from which the intended TOE is generated. The version information of documents is stored in SVN.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	The development environment used is set up centrally as per project specific CM plan.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE.	The development environment used is set up centrally as per project specific CM plan.
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.	The development environment used is set up centrally as project specific CM plan. Documents are created by the developer. The new/modified document is reviewed by the administrator and pushed into the repository after approval.
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	The development environment used is set up centrally as project specific CM plan. Documents are stored in the project repository. Evidences can be provided during a site visit
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being	The development environment used is set up centrally as project specific CM plan.

SAR	Aspect
operated in accordance with the CM plan.	Documents are stored in the project repository. Evidences can be provided during a site visit

Table 8.1 Mapping for ALC_CMC.5

SAR	Aspect
ALC_CMS.5.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.	In terms of site certification, on the one hand the configuration list is provided in form of the tables at hand. On the other hand, the configuration list is represented by the list of all applicable documents.
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	Since no TOE is subject of the site evaluation the principles are defined. All configuration items are maintained in the CM systems provided by the site. Every document can be uniquely identified as stated above for ALC_CMC.5.1C
ALC_CMS.5.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	The configuration list in case of site certification is the list of all applicable documents. In the document the author of each item is listed.

Table Mapping for ALC_CMS.5

SAR	Aspect
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	Access control to wings, surveillance, alarm system and on campus guard services to prevent access to the wings for unauthorized persons. Handling of physical objects, zero balancing, disposal of security products. Trustworthiness and training of staff Physical security system: operation, emergency procedures, incident handling and reporting.

SAR	Aspect
	The procedure of granting and revoking the physical or the logical access right. A secure network topology is used to ensure the logical assets are securely protected.
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	The justification is provided in this security target because it shows that all threats are addressed by the measures. In addition the measures are monitored to control the effectiveness

Table 8.3 Mapping for ALC_DVS.2

SAR	Aspect
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	The intended TOE is developed and maintained as development process.
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	The development control of each phase provides the necessary control and compliance of the development environment in use.

Table 8.4 Mapping for ALC_LCD.1

9 References

9.1 Literature

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

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

[3] Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology; Version 3.1, Revision 5," April 2017

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

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

[6] JIL, Minimum Site Security Requirements, Version 3.0, February 2021.

9.2 Definitions

Client: The site providing the Site Security Target may operates as a subcontractor of the TOE manufacturer. The term “client” is used here to define this business connection. It is used instead of customer since the terms “customer” and “consumer” are reserved in CC. In this document the terms words “customer” and “consumer” are only used here in the sense of CC.

9.3 List of Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
IC	Integrated Circuit
IT	Information Technology
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation