Site Security Target Huawei Hangzhou Z8-2-B30 Development Site

Contents

Table of Figures

1 Document Information

1.1 Reference

Title:	Site Security Target Huawei Hangzhou Z8-2-B30 Development Site
Version:	1.1
Date:	17 October 2023
Company:	Huawei Technologies Co.,Ltd.
Name of the site:	Huawei Hangzhou Z8-2-B30 Development Site
Product type:	Site certification

1.2 Version History

Version	Date	Comment/Editor/Changes
0.1	02 August 2023	First draft.
0.2	15 August 2023	Modify as the reviewer suggest.
0.3	16 August 2023	Correct the claimed EAL in chapter 3.
0.4	16 August 2023	Modify as the reviewer suggest.
0.5	8 September 2023	Update the mapping of the evaluation documentation references in chapter 8.5.
0.6	12 September 2023	Update the description of physical scope, logical scope in chapter 2.3 and assets in chapter 4.1.
1.0	22 September 2023	Initial version and ready to release.
1.1	17 October 2023	Add the description of life-cycle definition rationale in 8.3.4

2 SST Introduction

The chapters 1 to 8 of this document are based upon the Eurosmart Site Security Target Template [6] with adaptations such that it fits the site.

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

2.1 SST Reference

Title: Site Security Target Huawei Hangzhou Z8-2-B30 Development Site

Version: 1.1

Date: 17 October 2023

2.2 Identification of the Site

The name of the site is Huawei Hangzhou Z8-2-B30 Development Site.

The site address is:

Room Z8-2-B30 of building Z8-B, Huawei Hangzhou research and development base, No. 410 Jianghong Road, Binjiang District, Hangzhou City, P.R.China.

2.3 Site Description

2.3.1 Physical Scope

The site is located at a campus owned entirely by Huawei. The secure development area is located in the Room B30, 2nd floor of Building Z8 on the campus, which is classified as yellow zone area within Huawei. The site performs intended TOE development, testing, and shipment activities, meanwhile it includes a secure IT server room which hosts the servers for development tools, CM system and physical security system.

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.

The additional security relevant area which falls into the site scope and supports the protection of intended TOE assets is the Central Control Room of campus (room Z2-1-09) on the 1st floor of building Z2. The main entrances of the Z8 building are equipped with turnstile which have card swiping or facial recognition functions.

There are three physical security levels defined for Huawei premises:

- Green zone area: All Huawei employees have the access.
- Yellow zone area: Huawei employees who belong to a dedicated development team can have the access.

- Red zone area: Huawei employees who belong to the development team of confidential projects can have the access. However, none of the site areas falls into this group.

2.3.2 Logical Scope

The site performs activities are Security IC Embedded Software Development (Phase 1), IC Embedded Software Testing (Phase 1) 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 and servers or VPN router is also provided and managed by Huawei IT authorized support directly or remotely.

The site performs secure shipment to the client, 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.

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), Evaluation Methodology; Version 3.1, Revision 5, April 2017 [3]
- JIL Minimum Site Security Requirements v3.0, February 2021 [5]

The evaluation of the site comprises the following assurance components:

ALC_CMC.5, ALC_CMS.5, ALC_DVS.2 (at AVA_VAN.5), and ALC_LCD.1.

The chosen assurance components are derived from the assurance level EAL6 of the assurance class "Life-cycle Support". Therefore, this site supports product evaluations up to EAL6. The activities of the site are not directly related to production and shipment 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 cannot 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.

This Site Security Target is based on the product life cycle defined by the type of product being developed. The assets (Section 4.1), threats (Section 4.2) and Organizational Security Policies (OSP) (Section 4.3) defined in this document are derived from the life cycle definition.

4.1 Assets

The following section describes the assets handled at the site.

Physical objects:	The site has physical objects (samples, printed documents etc.) in relation to the intended TOE. Both the integrity and the confidentiality of these must be protected.
Development data:	The site has access to or even copies of electronic development data in relation to intended TOEs. Both the integrity and the confidentiality of these electronic documents must be protected. • Firmware Development (e.g. specifications, source code) • Test Software/Data/Documents (e.g. specifications, test script/code) • Product Documents (e.g. datasheets, specification) • Evaluation Documents (e.g. design reports, guidance documentation)
Development tools:	To perform its development activities the site uses tools (e.g. compiler) to transform source code into binaries. The integrity of these tools (running on local or remote development computers) must be protected.
Physical equipment (include IT equipment and physical security equipment:	The site provides corresponding services based on IT hardware devices such as server hosts and network equipment, meanwhile it is physically secured by security equipment. Thereby the integrity of these devices must be protected.

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.Unauthorised-Staff: Employees or subcontractors not authorized to get access to in this case (1)development data with the intention to violate confidentiality and possibly integrity (2)development tools with the intention to violate integrity (3)physical equipment with the intention to violate integrity (4)physical objects with the intention to violate integrity.

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.

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 these 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.

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. In this case the unique identification of items is solely the IT hardware used for these services.

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 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.Transfer: Transfer of protected material out of the development environment and between different development sites is performed in accordance with defined acceptance procedures.

The documentation indicates that intend TOE development data is encrypted and transmitted within the internal secure network. The firewall device is implemented to protect the secure network. There is no physical transportation between these sites.

4.4 Assumptions

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, test or production process. The provided information includes the classification of the documents and product.

A.Item-Identification: Each sensitive configuration data or item received by the site can be uniquely identified.

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

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 centre.

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, logical 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 must 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.Date-Transfer: Sensitive electronic configuration items (data or documents) are protected by applying cryptographic algorithms to ensure confidentiality and/or integrity (as required) during internal shipment. In case asymmetric cryptographic algorithms are applied, the associated cryptographic keys must be assigned to individuals to ensure that only authorised employees are able to extract the sensitive electronic configuration items. Alternatively, symmetric key or password-based exchanges methods might be used (e.g. symmetric key encrypted files, password encrypted archives) which don't allow assignment of individuals. In the latter case it has to be ensured that only authorised users have access to the cryptographic keys or passwords. The cryptographic keys and/or passwords are exchanged based on secure measures and they are sufficiently protected.

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-Operation: 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. 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: Huawei has a configuration management system that assigns a unique internal identifier for all equipment installed in Secure Rooms and to each version of the internal procedures and guidance. This helps ensure P.Config_Items and P.Config_Process.

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 by documentation that describes the services and/or processes provided by a site.

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.Exclusive-Access: The only way to access the Security-Relevant System from the Huawei development team is through dedicated Huawei development infrastructure and internal network.

O.Control-Scrap: The site has measures in place to destruct electronic media and paper document and erase/format sensitive data, 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.Control-Scrap	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. O.Control-Scrap ensures that scrap material cannot be accessed by an authorised party. 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.Control-Scrap	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. O.Control-Scrap ensures that scrap material cannot be accessed by an authorised party. Therefore, the threat is effectively addressed by these objectives
T.Computer-Net	O.Internal-Monitor O.Maintain-Security O.Logical-Operation O.Staff-Engagement O.Exclusive-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.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Operation O.Staff-Engagement O.Control-Scrap	O.Physical-Access, O.Alarm-Response, O.Logical-Operation, O.Staff-Engagement 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.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. O.Control-Scrap prevent the attacker get the sensitive data from the unuse media or paper documents. Therefore, the threat is effectively addressed by these objectives.
OSP	Security Objective	Note
P.Config-Items	O.Physical-Access O.Config-Items	O.Physical-Access ensures that unauthorized people cannot circumvent this (see the rationale for T.Smart-Theft for more details on this). O.Config-Items assigns unique numbers to the internal procedures. As the site processes no other configuration items, this is sufficient to meet P.Config-Items.
P.Config-Control	O.Physical-Access O.Config-Items O.Config-Control	O.Physical-Access ensures that unauthorized people cannot circumvent this (see the rationale for T.Smart-Theft for more details on this). The services and processes provided by the site are described in the internal site procedures and guidance. O.Config-Items as are kept under CM (see the rationale above),
P.Config-Process	O.Config-Process	The Security Objective directly enforces the OSP.
P.Transfer:	O.Date-Transfer	The encryption technique used in transferring data and procedures used in internal shipment can ensure the integrity of the configuration items.

Table 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.

The Security Assurance Requirements (SAR) are chosen from the class ALC (Life-cycle support) as defined in [2]:

- 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.

As the scope of the configuration management system is rather limited (see section 7.1.2), the configuration management system only needs to keep a few documents under CM.

Items such as wafers, dice, products, etc. are not in scope.

Items such as source code, binary image, design documentation are considered electronic files are therefore in scope. The CM system is therefore relatively simple.

The configuration management system controlling activities will be in scope.

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. The configuration list contains all evaluation documentation for the certification of this site.

In the particular case of a Security IC the scope of the configuration management can include a number of configuration items. The configuration items already defined in section 4.1 that are considered as “TOE implementation representation” include:

- Hardware and software specifications
- Source code for software and hardware.

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)

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

- The combination of physical partitioning between the different access control levels together with technical and 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.
- Assigned personnel of the site operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, unauthorised Huawei employees, contractors and suppliers.
- The technical and organisational security measures ensure that an alarm is generated before an unauthorised person gets access to any asset. After the alarm is triggered, the unauthorised person still has to overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack.
- The site performs security management meetings at least every six months. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures.
- Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only 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.
- The only way to access Huawei development team network is through management workstations connected to the encryption equipment. There is no internal network access to the encryption equipment.
- The computer systems in the Secure Rooms that are connected to the encryption equipment are kept up-to-date (software updates, security patches, virus protection, spyware protection).
- The Secure Rooms have measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive configuration items so that they do not support an attacker.
- All employees who have access to assets are checked regarding security concerns and must sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.

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 document provides a life-cycle description and there are 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.

For this site regarding Life Cycle, the following phases are relevant:

1. Security IC embedded software development
2. Security IC embedded software testing
3. Software Release

7.2 Security Assurance Rationale

7.2.1 Security Assurance Rationale - Dependencies

The dependencies for the assurance requirements are as follows:

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

Assurance Family	Dependencies
ALC_CMC.5	ALC_CMS.1 ALC_DVS.2 ALC_LCD.1
ALC_CMS.5	No dependencies
ALC_DVS.2	No dependencies
ALC_LCD.1	No dependencies

Table 2 Rationale for dependencies

7.2.2 Security Assurance Rationale – Mapping

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 configuration items.

SAR	Security Objective	Rationale
ALC_CMC.5.1C: The TOE shall be labelled with its unique reference.	O.Config-Items	O.Config-Items states that Huawei uses a configuration management system. This is included in ALC_CMC.5. Therefore ALC_CMC.5 and ALC_CMS.5 are suitable to meet O.Config-Items

ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Config-Items O.Config-Control O.Config-Process	O.Config-Items states that Huawei uses a configuration management system. 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.Config-Items O.Config-Control O.Config-Process	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.Config-Items O.Config-Control	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-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-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.Config-Process comprises the automated management of the development processes.
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	O.Config-Process O.Logical-Operation	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 identify the configuration items that comprise the TSF.	O.Config-Items O.Config-Control O.Config-Process	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-Items O.Config-Control O.Config-Process	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.
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.Config-Items O.Config-Control O.Config-Process	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.Config-Items O.Config-Control O.Config-Process	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.Config-Control O.Config-Process	O.Config-Control, O.Config-Process ensure that only released client part IDs are produced.
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.Config-Control comprises a release procedure as evidence. O.Config-Process ensures the compliance of the process.

Table 3 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
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.	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	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
ALC_CMS.5.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	O.Config-Items	According to O.Config-Items all configuration items for secure products are identified.

Table 4 Rationale for ALC_CMS.5

SAR	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Control-Scrap O.Exclusive-Access O.Date-Transfer	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-Operation. The personnel security measures are provided by O.Staff-Engagement. The sensitive information is securely destroyed according to O.Control-Scrap. The security of transmission is ensured by O.Exclusive-Access and O.Date-Transfer.
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.Exclusive-Access O.Date-Transfer	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. The security of transmission is ensured by O.Exclusive-Access and O.Date-Transfer.

Table 5 Rationale for ALC_DVS.2

SAR	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the 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.Config-Control O.Config-Process	See ALC_LCD.1.1C

Table 6 Rationale for ALC_LCD.1

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 firmware. 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 must 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 assumption **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 centre 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 the site are in the scope of the evaluation process:

1. Security IC embedded software development
2. Security IC embedded software testing
3. Software Release.

The typical Life Cycle model for Smart Cards usually comprises the following phases: (i) Development, (ii) Validation, (iii) Mass 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 source code of Security IC embedded software, test scripts/codes and the creation of development documentation.

Validation comprises the simulation and emulation of hardware and software designs on dedicated test environments. The purpose of verification is the preparation of the design freeze and sample development.

8.3 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.

8.3.1 CM capabilities (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 all configuration items have been and are being maintained under the CM system.

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 supports the integrity and confidentiality required for the products. Therefore, these security assurance requirements meet the requirements for configuration management.

8.3.2 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.

8.3.3 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, and testing of the TOE can be used by potential attackers for the development of attacks. Therefore, the handling and storage of these items must be sufficiently protected. Therefore, the handling and storage of these items must be sufficiently protected.

8.3.4 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. One site provides only limited support of the described lifecycle for the development and production of the intended TOE. However, the assurance requirements are suitable to support the application of the site evaluation results for the evaluation of an "intended TOE".

8.4 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.Date-Transfer

ALC_DVS.2.1C requires that all information considered sensitive will be manipulated and transferred under proper security controls, and ALC_DVS.2.2C justifies these measures. Thereby this objective is suitable 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-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 configuration items. 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 related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_CMS.5.2C requires the uniqueness of configuration item is indicated in the configuration list. The objective meets the set of Security Assurance Requirements.

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.

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.

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.Exclusive-Access

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 sites and the secure rooms. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Control-Scrap

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.

8.5 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. As there is no processing on this site the Configuration Management of the site relevant documentation is controlled on the other Huawei site. The mapping between the internal site documentation and the Security Assurance Requirements is described in the following tables.

SAR	References
ALC_CMC.5.1C: The TOE shall be labelled with its unique reference.	• HROT-FirmwareHZ-ALC-CMC
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	• HROT-FirmwareHZ-ALC-CMC
ALC_CMC.5.3C: The CM documentation shall justify that the acceptance procedures provide for an	• HROT-FirmwareHZ-ALC-CMC

SAR	References
adequate and appropriate review of changes to all configuration items.	
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	• HROT-FirmwareHZ-ALC-CMC
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	• HROT-FirmwareHZ-ALC-CMC
ALC_CMC.5.6C: The CM system shall support the production of the TOE by automated means.	• HROT-FirmwareHZ-ALC-CMC
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.	• HROT-FirmwareHZ-ALC-CMC
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	• HROT-FirmwareHZ-ALC-CMC
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.	• HROT-FirmwareHZ-ALC-CMC
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.	• HROT-FirmwareHZ-ALC-CMC
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.	• HROT-FirmwareHZ-ALC-CMC
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	• HROT-FirmwareHZ-ALC-CMC
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE.	• HROT-FirmwareHZ-ALC-CMC
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.	• HROT-FirmwareHZ-ALC-CMC
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	• HROT-FirmwareHZ-ALC-CMC

SAR	References
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	• HROT-FirmwareHZ-ALC-CMC

Table 7 Mapping for ALC_CMC.5

SAR	References
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.	• HROT-FirmwareHZ-ALC-CMS
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	• HROT-FirmwareHZ-ALC-CMS
ALC_CMS.5.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	• HROT-FirmwareHZ-ALC-CMS

Table 8 Mapping for ALC_CMS.5

SAR	References
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.	• HROT-FirmwareHZ-ALC-DVS
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.	• HROT-FirmwareHZ-ALC-DVS

Table 9 Mapping for ALC_DVS.2

SAR	References
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	• HROT-FirmwareHZ-ALC-LCD
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	• HROT-FirmwareHZ-ALC-LCD

Table 10 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), Evaluation Methodology, Version 3.1, Revision 5, April 2017.

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

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

[6] Eurosmart Site Security Target Template, Version 2.0, 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