Site Security Target Huawei Dongguan Data Center D1

Contents

1 Document Information 4
1.1 Reference 4
1.2 Version History 5
2 SST Introduction 6
2.1 SST Reference 6
2.2 Identification of the Site 6
2.3 Site Description 6
2.3.1 Physical Scope 6
2.3.2 Logical Scope 7
3 Conformance Claim 9
4 Security Problem Definition 10
4.1 Assets 10
4.2 Threats 10
4.3 Organisational Security Policies 12
4.4 Assumptions 12
5 Security Objectives 14
5.1 Security Objectives Rationale 15
6 Extended Assurance Components Definition 18
7 Security Assurance Requirements 19
7.1 Application Notes and Refinements 19
7.2 Security Assurance Rationale 21
8 Site Summary Specification 25
8.1 Preconditions Required by the Site 25
8.2 Services of the Site 25
8.3 Objectives Rationale 25
8.4 Security Assurance Requirements Rationale 27
8.5 Assurance Measure Rationale 29
8.6 Mapping of the Evaluation Documentation 31
9 References 36
9.1 Literature 36
9.2 Definitions 36
9.3 List of Abbreviations 36

Table of Figures

Table 1 Security Objectives Rationale 16
Table 2 Rationale for dependencies 21
Table 3 Rationale for ALC_CMC.5 23
Table 4 Rationale for ALC_CMS.5 24
Table 5 Rationale for ALC_DVS.2 24
Table 6 Mapping for ALC_CMC.5 33
Table 7 Mapping for ALC_CMS.5 34
Table 8 Mapping for ALC_DVS.2 35

1 Document Information

1.1 Reference

Title:	Site Security Target Huawei Dongguan Data Center D1
Version:	0.7
Date:	07 November 2022
Company:	Huawei Technologies Co.,Ltd.
Name of the site:	Huawei Dongguan Data Center D1
Product type:	Site certification
EAL-Level:	EAL6

1.2 Version History

Version	Date	Comment/Editor/Changes
0.1	04 April 2022	First draft.
0.2	08 June 2022	Internal update.
0.3	28 June 2022	Update after the internal review.
0.4	08 July 2022	Update the chapter 2.3 site description
0.5	05 August 2022	Update chapters 3, 4.3, 4.4 and 5
0.6	28 September 2022	Add the logical service “HIAPM” in chapter 2.3.2
0.7	07 November 2022	Update the scope in chapter 2.3

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 Dongguan Data Center D1

Version: 0.7

Date: 07 November 2022

2.2 Identification of the Site

The name of the site is Huawei Dongguan Data Center D1.

The site address is:

D1 building of Huawei South Factory, Huawei Songshan Lake Technology Campus,
No 6, Xincheng Street, Dongguan, Guangdong Province, P.R.China.

2.3 Site Description

2.3.1 Physical Scope

The site is the entire D1 building of the Huawei Songshan Lake Technology Campus. It consists of the entry areas and corridors inside the building premises, IT maintenance room and several server rooms.

Among the server rooms, the areas which in the scope of this SST are:

- Building D1: Modules M1 to M6 on the 1st floor and Modules M7 to M12 on the 3rd floor.

The IT maintenance room (CHN-DG-D1-1-B13R) is mainly for scrapping and storage of defective hard disks.

To support the maintenance of PKI service, engineers from the Huawei Chengdu office (the address is "Room U10-4, Building 1 of Southwest Phase III, Central Commercial Building, No. 200 Tianquan Road, China-Chengdu-High-tech Zone, Chengdu, Sichuan Province, P.R.China") can remotely connect to the PKI facilities hosted by this site. The maintenance activities can include:

- User and permission management: adding roles and assigning permissions to roles
- Internationalization management: configuration on the Chinese and English GUIs
- Lookup management: system parameters configuration
- Server Management: viewing system logs

As the Huawei Chengdu office only provides the remote maintenance activities to the PKI web services and the actual assets which contained by the PKI servers cannot be remotely manipulated, it is excluded from the scope of this SST.

The site is a secure area with restricted access where only authorized persons can enter. To enforce such access restriction, a combination of physical, procedural, personnel and logical measurements have been installed.

2.3.2 Logical Scope

This site supports activities of several organisations, but the only relevant area where activities take place is referred to as the Secure Rooms which include both the IT maintenance room and relevant server rooms as stated in chapter 2.3.1 Physical Scope.

The Huawei Dongguan Data Center D1 contains the following service:
Security-relevant services within scope: **secured remote access to servers**.

- Note that the servers will be used in relation with designing, testing, etc. of security-related Huawei Products. **The secured remote access to servers is the subject of this certification**.

The security-relevant system is only connected with other systems through VPN router provided by and remotely managed by Huawei development team to whom the data belongs. During processing, servers can manipulate encrypted and unencrypted data. The only connection to the outside world is protected through different means (e.g. MPLS VPN, HTTPS protocol and PGP encryption). Only the specific Huawei development team has the keys to encrypt/decrypt. Data are stored in specialized and specific data servers.

All logical activities in the secure rooms are performed remotely. For example: a Huawei employee in Shenzhen secure development room performs some design work on a security IC: the actual work is physically done in Shenzhen, but logically in the Secure Rooms. Administration of the servers in the Secure Rooms are performed remotely using encrypted lines.

The only personnel with physical access to the Secure Rooms is Huawei IT personnel or authorized subcontractors. They perform only the physical activities for the server maintenance. The IT personnel is therefore not directly involved in designing, testing, etc. of Huawei products.

However, as the site physically hosts electronic assets of Huawei development teams, confidentiality and integrity-related threats exist to these assets on this site. These threats are the main subject of this site certification.

For security product development, the site activities can be related to different life-cycle phases, depending on the roles that the Huawei development team uses this site

The site is served as a data center which hosts hardware servers and provides the following logical services:

- PKI service: A comprehensive key management platform for providing the services including key generate/storage/revocation/inquire, data encryption and decryption, Certificate services and image sign services. The site hosts the key management facilities (e.g. HSM, key servers, KMS server, etc.).
- DTS service: A bug tracking and management system used by Huawei development teams

- D-BOX service: A configuration management (CM) system used for the document management related to the intended TOE development and Huawei internal procedures.
- HiAPM service: A project management system that used to manage the status of project, such as project plan and progress, risk and problems management, minutes of project meeting.
- iRight service: A logical access right management platform used to create and maintain different permission groups for Huawei development teams.
- Configuration Management Cloud (CMC) service: used to manage the release versions of intended TOE. The binary image, technical documentation and signature are archived in the CMC platform.
- Offering release management (ORM) service: used for the management of version release requests.
- SVN service: A configuration management (CM) system used for the documentation and source code management.
- W3 account service: provide a unified login verification webpage for internal Huawei users for basic work account management.
- Data backup service: provide the encrypted data backup for intended TOE.
- IT systems setup and maintenance: Installation of operating system & software and patching; Hardware maintenance; Implementing approved requests for Huawei development team; Resolving technical issues and responding to incidents; IT scraps destruction.

The site can provide the above-mentioned services and Huawei development teams can choose the services on their own demands.

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[1]:

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

The activities of the site are not directly related to designing, testing, producing, shipping etc. of secure products. Therefore, this site does not claim conformance to ALC_DEL, ALC_TAT and ALC_LCD.

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 cannot be defined either. Therefore, this site does not claim conformance to ALC_TAT. The site is a data center which does not involve in product development or production activities. Therefore, this site does not claim conformance to ALC_LCD.

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.

Cryptographic keys:	The site stores cryptographic keys used for PKI services. Both the integrity and the confidentiality of these electronic data must be protected.
Development data:	The site stores electronic development data in relation to developed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected.
Production data	The site stores electronic production data in relation to developed TOEs. Both the integrity and the confidentiality of these electronic documents 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) Cryptographic keys and certificates with the intention to violate confidentiality and possibly integrity (3) 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 assets by violating (1) In this case development data (2) cryptographic keys (3) production data with the intention to violate confidentiality and possibly 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 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.

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-Process: The processes provided by this site are controlled and documented. This 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 configuration items at the site.

4.4 Assumptions

A.Serv-Specification: The Huawei development team that is being managed must store data it wishes to keep secure on the Security-Relevant System in the secure network

A.Secure_Conn: Huawei must arrange a secure network connection from the Security-Relevant System to its network.

The site is only intended for IT Engineering & Generic Support and is not intended for TOE development or production. Therefore, the only configuration items are this SST, internal site security documents and procedures

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 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-Operation: The computer systems in the Secure Rooms enforce that every user authenticates using a unique user ID and password and also including two-factor authentication.

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-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.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. 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-Process	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). 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),

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)

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)

Refer to subsection ‘Application Notes for Site Certification’ in [4] 5.1 ‘Application Notes for 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, cryptographic keys and certificates, design documentation are considered electronic files are therefore in scope. The CM system is therefore relatively simple.

The configuration management system of the Data Center controlling activities will be in scope.

7.1.2 Overview and Refinements regarding CM Scope (ALC_CMS)

Refer to subsection ‘Application Notes for Site Certification’ in [4] 5.2 ‘Application Notes for 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.

As this site is not directly involved with designing, testing, producing, storing or delivering the TOE, the only relevant configuration items are

- This Site Security Target for this site
- The CM documentation for this site
- The site security documentation for this site

7.1.3 Overview and Refinements regarding Development Security (ALC_DVS)

Refer to subsection ‘Application Notes for Site Certification’ in [4] 5.4 ‘Application Notes for 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.

7.2 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

Assurance Family	Dependencies	Rationale
ALC_CMC.5	ALC_CMS.1 ALC_DVS.2 ALC_LCD.1	All included except ALC_LCD.1. ALC_LCD.1 is not included as it is related to the intended TOE development where this site is not involved in development.
ALC_CMS.5	No dependencies	N/a, no dependencies
ALC_DVS.2	No dependencies	N/a, no dependencies

Table 2 Rationale for dependencies

As there is no processing on this site the Configuration Management of the site relevant documentation is controlled on the other Huawei site.

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 CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	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-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.5.3C: The CM documentation shall justify that the acceptance procedures	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

provide for an adequate and appropriate review of changes to all configuration items.		and ALC_CMS.5 are suitable to meet O.Config-Items
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	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.5.5C: The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	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.5.6C: The CM system shall support the production of the product by automated means.	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.5.7C: 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-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.5.8C: The CM system shall clearly identify the configuration items that comprise the TSF.	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.5.9C: 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-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.5.10C: 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-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.5.11C: 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-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.5.12C: The CM documentation shall include a CM plan.	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.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE.	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.5.14C: 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-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.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	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.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan	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

Table 3 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	O.Config-Items	O.Config-Items states that Huawei has the internal procedures and guidance under CM. This is a subset of the CM list specified by ALC_CMS.5 (which also includes the SST).

information. The CM documentation shall include a CM plan.		
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config-Items	O.Config-Items states that Huawei has the internal procedures and guidance under CM. This is a subset of the CM list specified by ALC_CMS.5 (which also includes the SST).
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.	O.Config-Items	O.Config-Items states that Huawei has the internal procedures and guidance under CM. This is a subset of the CM list specified by ALC_CMS.5 (which also includes the SST).

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	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
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	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

Table 5 Rationale for ALC_DVS.2

8 Site Summary Specification

8.1 Preconditions Required by the Site

There are two preconditions that must be fulfilled in order to make use of the site:

- The Huawei development team that is being managed must provide appropriate information and means in order to allow the Secure Rooms to provide IT support to the development environment. This covers the assumption **A.Serv-Specification**.
- The Huawei development team must arrange an secure network connection from the Secure Rooms to its network. This covers the assumption **A.Secure_Conn**.

8.2 Services of the Site

S.IT_Support: The Secure Rooms provide various IT support to Huawei development teams. This consists of activities such as:

- IT systems setup and maintenance
  - Installation of operating system & software and patching
  - Hardware maintenance
  - Implementing approved requests for Huawei development team
  - Resolving technical issues and responding to incidents
  - IT scraps destruction
- User account creation, user account maintenance and revocation (iRight)
- Providing bug management service, such as bug state and flow management (DTS)
- Providing document configuration management service (DBOX)
- Providing project management service (HiAPM)
- Providing the management for version release requests (ORM)
- Providing the intended TOE release management service (CMC)
- Providing document and code configuration management service (SVN)
- Providing secure data backup for encrypted data of intended TOE
- Providing PKI service (including key generate/storage/revocation/inquire, data encryption and decryption, certificate service and image sign service)
- Providing internal user account management service (W3)

S.IT_Protection: The site provides physical protection for IT the infrastructure.

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 andT.Staff-Collusion

O.Maintain-Security

The security relevant systems enforcing or supporting O.Physical-Access and O.Security-control 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-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 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 the OSP P.Config-Items and P.Config- Process

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 and O.Config-Items support the engagement of the staff.

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

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.Unauthorised-Staff and T.Staff-Collusion

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.Exclusive-Access

Access to the Secure Rooms, from and to the outside uses encrypted links provided by the Huawei development team.

This addresses the threat T.Computer-Net

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.

8.5 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-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.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.

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. 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	Aspect	References
ALC_CMC.5.1C: The TOE shall be labelled with its unique reference.	The configuration items 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 system as well as the baseline labels that are given by the configuration manager.	• HWPKI-ALC_CMC, Configuration Management Capability
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.	• HWPKI-ALC_CMC, Configuration Management Capability
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.	• HWPKI-ALC_CMC, Configuration Management Capability

SAR	Aspect	References
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.	• HWPKI-ALC_CMC, Configuration Management Capability
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	CM system 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	• HWPKI-ALC_CMC, Configuration Management Capability
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	• HWPKI-ALC_CMC, Configuration Management Capability
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.	• HWPKI-ALC_CMC, Configuration Management Capability
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	There is no specific TOE in the focus.	• HWPKI-ALC_CMC, Configuration Management Capability
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.	CM tool provides automated means to support the audit of all changes. Documents stored in DBOX are under version control	• HWPKI-ALC_CMC, Configuration Management Capability
ALC_CMC.5.10C: The CM system shall provide an automated means to identify all other configuration items that are affected by the change	In case a source file has been changed, the code is compiled again and all affected items are identified via the implementation module mapping.	• HWPKI-ALC_CMC, Configuration Management Capability

SAR	Aspect	References
of a given configuration item.	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.	CM tool provides means to tag a release version from which the intended TOE is generated. The version information of documents is stored in DBOX.	• HWPKI-ALC_CMC, Configuration Management Capability
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.	• HWPKI-ALC_CMC, Configuration Management Capability
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.	• HWPKI-ALC_CMC, Configuration Management Capability
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.	Documents are created by the manger. The new/modified document is reviewed by the administrator and pushed into the repository after approval.	• HWPKI-ALC_CMC, Configuration Management Capability
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	Documents are stored in the project repository. Evidences can be provided during a site visit	• HWPKI-ALC_CMC, Configuration Management Capability
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	Documents are stored in the project repository. Evidences can be provided during a site visit	• HWPKI-ALC_CMC, Configuration Management Capability

Table 6 Mapping for ALC_CMC.5

SAR	Aspect	References
ALC_CMS.5.1C: The configuration list shall include the following: the TOE itself; the	In terms of site certification, on the one hand the configuration list is provided in form of the tables at	• HWPKI-ALC_CMS, Configuration

SAR	Aspect	References
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.	hand. On the other hand, the configuration list is represented by the list of all applicable documents.	Management Scope
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	• HWPKI-ALC_CMS, Configuration Management Scope
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.	• HWPKI-ALC_CMS, Configuration Management Scope

Table 7 Mapping for ALC_CMS.5

SAR	Aspect	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.	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. The procedure of granting and revoking the physical or the logical access right.	• HWPKI Site V100_ALC_DVS, Site Security

SAR	Aspect	References
	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	• Chapter 8 of this document

Table 8 Mapping for ALC_DVS.2

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