Site Security Target Lite -Huawei Cyber Security Compliance Testing Center

Author	Reviewer	Approver
Xiaoping Cheng	Xiaoxin Gong	Junning Yao

Version Control

Version	Date	Description
0.1	20/05/2021	Initial version
0.2	08/11/2021	Update regarding ORs
0.3	20/12/2021	Update regarding ORs
0.4	17/02/2022	Update regarding ORs
0.5	28/02/2022	Update regarding ORs

Contents

1 Document Information 5
1.1 Reference 5
2 SST Introduction 6
2.1 Identification of the Site 6
2.2 Site Description 6
2.3 Testing Center 8
3 Conformance Claim 9
4 Security Problem Definition 10
4.1 Assets 10
4.2 Threats 11
4.3 Organizational Security Policies 12
4.4 Assumptions 13
5 Security Objectives 14
5.1 Configuration management 14
5.2 Security measures 14
5.2.1 Physical Security measures 15
5.2.2 Personal measures 15
5.2.3 Logical measures 16
5.3 Security Objectives Rationale 18
5.3.1 Mapping of Security Objectives 18
5.3.2 Justification of Security Objectives mapping 20
6 Extended Assurance Components Definition 25
7 Security Assurance Requirements 26
7.1 Application Notes and Refinements 26
7.1.1 Overview regarding CM capabilities (ALC_CMC) 26
7.1.2 Overview regarding CM Scope (ALC_CMS) 27
7.1.3 Overview regarding Development Security (ALC_DVS) 27
7.1.4 Overview regarding Life-Cycle Definition (ALC_LCD) 27
7.2 Security Assurance Rationale 27
7.2.1 Rationale for ALC_CMC.4 28
7.2.2 Rationale for ALC_CMS.4 29
7.2.3 Rationale for ALC_DVS.1 30
7.2.4 Rationale for ALC_LCD.1 30
8 Site Summary Specification 32
8.1 Preconditions Required by the Site 32

8.2 Services of the Site 32
8.3 Objectives Rationale 33
8.4 SAR Rationale 38
8.4.1 ALC_CMC 38
8.4.2 ALC_CMS 39
8.4.3 ALC_DVS 39
8.4.4 ALC_LCD 39
8.5 Assurance Measure Rationale 39
8.6 Mapping of the Evaluation Documentation 43
9 References 43

1 Document Information

1.1 Reference

Title: Site Security Target Lite Huawei Cyber Security Compliance Testing Center

Version: 0.5

Date: 28/02/2022

Company: Huawei Technology Co., Ltd

Name of the site: Huawei Cyber Security Compliance Testing Center

Product Type: Information and communication technology (ICT) products and solutions

Service content: Testing design and compliance testing

Evaluation Assurance Components: ALC_CMC.4, ALC_CMS.4, ALC_DVS.1 and ALC_LCD.1.

2 SST Introduction

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

This Site Security Target refers to the following site:

Huawei Cyber Security Compliance Testing Center

This site is used for testing design and compliance testing for information and communication technology (ICT) products and solutions.

Along this document, the word testing will be used as a general concept for the testing performance under the development phase. This development phase is considered as design and production phases. Development concept is stick to the definition in (1)

2.1 Identification of the Site

The site name is Huawei Cyber Security Compliance Testing Center (hereinafter referred to as "HCSCTC") is located at;

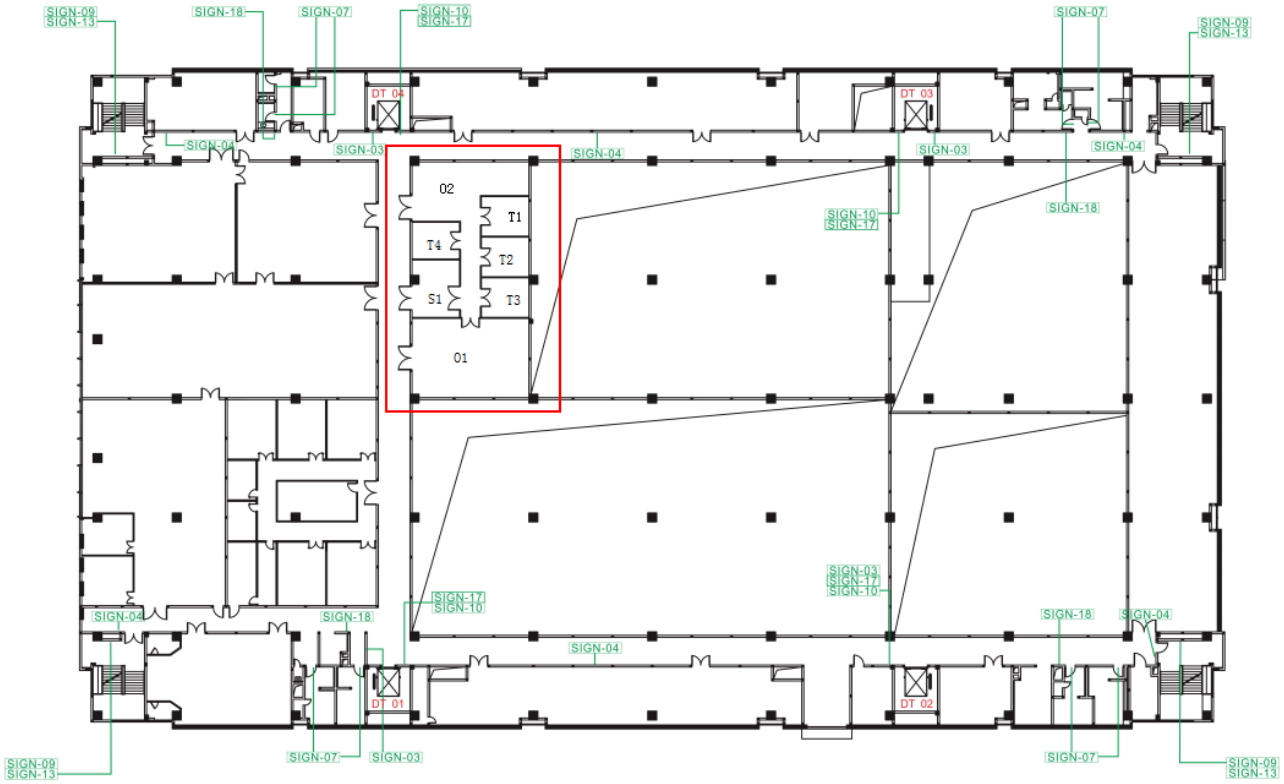
2F D4 D Area Administration Building,
Southern Factory of Huawei Technologies Co., Ltd.,
No. 6 Xincheng Avenue,
Songshan Lake Technology Industrial Park,
Dongguan City, 523808, P.R.C

2.2 Site Description

The whole HCSCTC site is in the scope of this SST. The Huawei campus is surrounded by a fence that each of its entrance is guarded by security guards and surveillance cameras 24 hours a day, all of the employees and trying to enter the campus should be verified by showing their ID card, all of the drivers of the vehicles entering the entrance are required to swipe their ID cards. The building D4 must be entered with the ID card. There are two entrances in the building, one is the main entrance, and the other one is the entrance from the cargo loading platform at the back of the building. Each entrance is guarded by security guards and monitored by surveillance cameras 24 hours a day. The site is located on the second floor, its entrances and office area are monitored by surveillance cameras.

Below is the layout of the campus:

Below is the layout of the second floor of D4:



The following zones in red box marked in the above figure have been taking into account in this security target and therefore they are the scope of the site certification regarding the physical measures implemented in their local perimeter.

- O1, O2: office room
- T1-T4: testing room

- S1: seminar room

2.3 Testing Center

HCSCTC is a secure testing center that provides testing design and compliance testing for information and communication technology (ICT) products and solutions, such as taxonomy Data encryption storage devices / tools, Firewall, Network Access Control Devices. Wireless Network Devices, Mobile devices, Routers, Network management tools, other devices – Virtualization software, Operating systems, Switches, Smart Cards and similar devices and Data exchange gateways. The client will provide ICT products and solutions to HCSCTC. After analysis, the testing center will perform a test design. This testing design will be related with security standards, such as the class ATE in common criteria (CEMv3.1R5). The HCSCTC will test if the product behaves as described in the ST and as specified in the evidence provided by the client, which is considered as the compliance testing.

The HCSCTC testing efforts consist not only of creating and running tests, but also of assessing the adequacy of the developer's tests and re-running a subset of them. This will be reported in a final report provided to the client.

HCSCTC designs and tests to determine the extent to which they are sufficient to demonstrate that TSFI perform as specified, and to understand the developer's approach to testing. Similarly, the testing center will design the tests and comply to determine the extent to which they are sufficient to demonstrate the internal behavior and properties of the TSF.

After running the test, HCSCTC will provide a report compliant with the testing methodology used for this purpose. Furthermore, HCSCTC will provide connection to specific devices to provide a testing environment with the client for their own product.

3 Conformance Claim

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

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

For the evaluation, the methodology will be used:

- Common Methodology for Information Technology Security Evaluation: Evaluation methodology. Version 3.1, Revision 5, April 2017, (4)

This Site Security Target (SST) is CC Part 3 conformant and the following CC assurance components are covered:

ALC_CMC.4, ALC_CMS.4, ALC_DVS.1, ALC_LCD.1

The assurance components are chosen in order to reuse the results in evaluations up to EAL4. It also has been assumed that the security measures are resistant to attacks performed by attackers with a High attack potential. IN this sense ALC_TAT is omitted, because the development tools and its versions are TOE specific and therefor it is more efficient to cover the whole ALC_TAT together with the product evaluation process.

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

In this site security target are not included any extended component.

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. The configuration management covers the integrity of the products and the security management of the site.

This Site Security Target is based on the life cycle defined by Huawei. 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.

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

4.1 Assets

The following section describes the assets handled at the site.

Id	Asset	Asset value
A.TOE	The products that will be evaluated and pre-evaluated.	Confidentiality Integrity
A.PROT	Products prototypes or parts of the TOEs before packaging and shipping.	Confidentiality Integrity
A.INFO	All the documentation and information of the products and certification/pre-evaluation (guidance, test tools/data) or information related to the processes in whatever format.	Confidentiality Integrity
A.EQUI	Equipment used in the network topology.	Integrity
A.INFOSEC	All the documentation or information regarding the systems and security mechanisms configuration (machines and perimeter protection	Confidentiality Integrity

	devices audit data, configuration, cryptographic keys, passwords, etc.).	
A.DEVSEC	Protection devices or mechanisms.	Integrity Availability

4.2 Threats

All threats endanger the integrity and confidentiality of the intended TOE and the representation of parts of the TOE. Such a product intended to be tested in HCSCTC, is sensitive to be vulnerable in this phase of the development.

The following threats are described in a general way. However, they are applicable to the site that provides services handling the items listed in Section 4.1 above. The explanation below the threats shall support the mapping to the Security Objectives of the site.

T.Physical-Theft

An attacker, with sufficient time to investigate the site from outside the site boundary using simple equipment to carry out a robbery or manipulate TOE components or other of the mentioned assets. This includes the possibility that the attack occurs during the daily working time and the agent intend impersonating an employee of the services company (e.g. cleaning). The attacker can use specific working clothes of the site to camouflage and trying to access sensitive areas.

All the assets may be affected by the attack as any information obtained may be used to investigate the TOE functionality, both directly (TOE, etc.), and indirectly, getting security systems information and attempt to violate and subsequently access to the TOE information.

These agents have limited resources but they have enough time to prepare the attack.

T.Logical-Theft

The agent has experience for compromising logical devices installed by the company to avoid attacks through the wire. He may be paid for the work. This attack would allow access to the company network. If the development computer were accessible, they can be manipulated dumping information.

The objective is to obtain confidential information of the TOEs or to manipulate the development or testing process. Also, the configuration information of the security devices may be manipulated.

These agents have resources and experience to develop the attack.

T.Accidental-Change

The agent, considered as an internal worker can commit an error during his daily work in TOEs configuration.

T.Unauthorized -Staff

The agent is a company employee without authorisation for accessing the development areas. The attacker circumvents the security, entering a restricted area with the aim of stealing TOEs information. Also, the configuration information of the security devices may be accessed.

The agent has not resources or technical knowledge for performing more than a simple robbery, but the information may be useful if he conspires with someone outside.

His motivation may be high as he may be paid for performing the work or he may be subjected to coercion.

T.Authorized-Access

The agent is a malicious TOEs tester whose goal can be the theft of TOEs information or the TOEs modification during the testing/working process or carry out a sabotage during his testing. The employee might be paid for the work or might be cahoots with someone outside.

The tester has enough technical knowledge for modifying the TOEs, but he has not experience in physical or logical security disciplines.

His motivation may be high as he may be paid for performing the work or he may be subjected to coercion.

4.3 Organizational Security Policies

The following policies are introduced by the requirements of the assurance components of ALC for the assurance level EAL4. 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 evaluation of the documentation of the site is under configuration management.

P.Config-Man

The organization has implemented a configuration management system documented in the associated CM plan.

The CM system guarantees the assignment of uniquely identifier to the TOEs configuration items, implements version and changes control. This includes the unique identification of sensitive configuration data or items that are created, generated, developed or used at a site as well as the received and transferred and provided sensitive configuration data or items.

The objective of this policy is to contribute to the integrity guarantee of the final product.

P.Transfer

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

P.Backup

Backups will be created, stored and destroyed according to an approved procedure.

4.4 Assumptions

Each site operating in a development flow must rely on preconditions provided by the previous site. Each site has to rely on the information received by the previous site/client. This is reflected by the assumptions that must be defined for the interface.

The following assumptions are considered to be applicable to all sites.

A.Init-Data: The software and guidance shall be provided by the client of the product.

A.Prod-Specification: The client must provide appropriate software and procedures in order to perform the testing. This includes the delivery of correct data for development, secured by appropriate means against modification and/or disclosure, if necessary.

A.Prod-Release: The client is responsible for the release of the products to be produced.

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

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

5 Security Objectives

This section defines the security objectives for the SST area allowing the resolution of the security problem described in the previous section.

The security objectives are focused in the logical (technical, personnel, procedural) and physical security measures application to the HUAWEI development areas defined in the scope of this site security target, the configuration management of the items conforming the TOEs and the development and security maintenance life cycle.

5.1 Configuration management

O.CM.LABEL

It shall be implemented a configuration management system assigning uniquely identifiers to the configuration items of TOEs under configuration control.

A version control will be managed so that obsolete versions of the configuration items will be clearly identified.

The CM system will maintain under configuration management the TOEs, the parts of the TOEs, testing data, documentations and evidences used in evaluation and pre-evaluation.

O.CM.RECEPTION.CONTROL

Upon reception of a physical product an incoming inspection is performed. The inspection comprises the received amount of products and the identification according to the documentation of the supplier. For electronic items that require authenticity, the authenticity is verified upon reception.

O.CM.CHANGE.CONTROL

The configuration management system shall implement an access control policy controlling the services and information accessible for the employees.

In addition, a change control procedure shall be implemented. This procedure is supported by the access control mechanism guaranteeing that only authorized changes to the configuration items are performed.

O.CM.PROCESS

The site controls its services and/or processes using a configuration management plan. The configuration management is supported by tools and procedures for the development of the product, for the management of flaws and optimisations of the process flow as well as for the documentation that describes the services and/or processes provided by the site.

5.2 Security measures

5.2.1 Physical Security measures

O.PERIMETERS

The development areas are protected by:

- Global security perimeter: implements the security measures controlling the access to the company; e.g. security fence, identification and authentication control, global perimeter intrusion detection systems (sensors, alarms, CCTV, etc.).
- Local security perimeter: implements the security measures controlling the access to the restricted areas; eg. Access control mechanisms, identification and authentication control, global perimeter intrusion detection systems (sensors, alarms, CCTV, etc.).

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 data or item 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.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.

5.2.2 Personal measures

O.STAFF.ENGAGEMENT

All employees who have access to sensitive configuration data or 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 non-disclosure agreement. All employees are trained and qualified for their job. The personnel shall be aware of their responsibilities, be proactive and shall communicate any security incident to the security responsible.

The team members are aware of the dangers of logical attacks through modifying the IT systems and development machines with which they work and inappropriate Internet usage, e-mail attachments, accidental malware import etc. They should also be aware of the company policy regarding material destruction and backups and ‘working from home’ (if applicable).

Access rights will only be granted to employees as part of an approved management procedure once they have received the security training.

O.REVOKING

If someone is removed from the team list due to disciplinary matters or dismissal, then their rights will be revoked and the person who is responsible within the developers own organization for overall security is made aware of this.

O.VISITORS

All visitors to the development area must be identified, logged and then escorted at all times once in the development environment.

5.2.3 Logical measures

O.INTERNAL.MONITOR

The site performs security management meetings on a regular basis. 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 at least every year to verify the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure a sufficient protection.

O.DATA.TRANSFER

Sensitive electronic configuration items (data or documents in electronic form) are protected by applying cryptographic algorithms to ensure confidentiality and/or integrity (whatever is 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.INTERNAL.SHIPMENT

The recipient of a physical configuration item is identified by the assigned client address. The recipient(s) of an electronic configuration item (e.g. source code) can be identified in different ways. The specific way is defined in the internal shipment procedure. The internal shipment procedure is applied to all shipped configuration data or items. The recipient for shipment can only be changed by a controlled process. The packaging (if any) is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of configuration data or items during internal shipment. For every sensitive configuration data or item, the protection measures against manipulation are defined (e.g. sealed boxes, encryption, integrity protection, electronic signature).

O.AC

Logical access to development machines shall be limited to approved development team members and system administrators.

The logical access mechanism to the operating system and also to the CM system will be based in identification of the individual and not at group level.

O.PASSWD

Weak passwords are not allowed. A password policy guaranteeing the passwords strength shall be implemented:

- Passwords shall be changed periodically
- The same password may not be used for both the underlying operating system and the CM system.
- An inactivity period for screen blocking shall be established, requiring re-authentication for unblocking.

O.LOGICAL.ACCESS

The site enforces a logical separation between the internal network and the internet by a firewall. The firewall ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into a testing network and an office network. Additional specific networks for testing are physically or logically separated from any internal network to enforce access control. Access to the testing network and related systems is restricted to authorized employees that work in the related area or that are involved in the configuration tasks. Every user of an IT system has its own user account and password. All computer systems with access to sensitive data require successful authentication by user name and password.

O.LOGICAL.OPERATION

The equipment's Hard Disk are encrypted. The equipment has updated anti-virus.

Backups will be created, stored and destroyed according to an approved procedure. Members of the development teams should be aware that no unauthorized backups may be made that are then taken outside the development area.

The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.

O.AC.REM

It is only possible to access the testing environment from outside the development area (i.e. work at home) on a company issued computer with commercial grade software then helps create an encrypted network connection with mutual authentication of both end parties.

O.INSTALL

The development machines should be configured with a controlled, restrictive user security policy that prevents the installation of additional unauthorized functionality.

O.RIP

Materials that are no longer used within the development area (through the whole development life cycle) must be destroyed in such a way that they cannot be used in any meaningful way that might affect the confidentiality of the materials in the development area.

5.3 Security Objectives Rationale

The SST includes a Security Objectives Rationale with a map, which shows how the threats and OSPs are covered by the Security Objectives.

Note that the assumptions defined in this Site Security Target cannot be used to cover any threat or OSP of the site. They are seen as preconditions 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.

5.3.1 Mapping of Security Objectives

Threats and OSP	Security Objective	Note
T.Physical-Theft	O.PERIMETERS O.ALARM.RESPONSE O.INTERNAL.MONITOR O.REVOKING O.VISITORS O.LOGICAL.OPERATION O.SECURITY.CONTROL O.RIP	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threat.
T.Logical-Theft	O.INTERNAL.MONITOR O.STAFF.ENGAGEMENT O.LOGICAL.OPERATION O.LOGICAL.ACCESS O.REVOKING O.AC O.PASSWD O.AC.REM O.INSTALL	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threats.
T.Accidental-Change	O.CM.LABEL O.CM.RECEPTION.CONTROL O.CM.CHANGE.CONTROL O.CM.PROCESS O.STAFF.ENGAGEMENT	The automated measures and the control and verification procedures avoid accidental changes of sensitive items.
T.Unauthorized - Staff	O.PERIMETERS O.ALARM.RESPONSE O.SECURITY.CONTROL O.INTERNAL.MONITOR O.REVOKING O.VISITORS O.LOGICAL.OPERATION O.LOGICAL.ACCESS O.STAFF.ENGAGEMENT	Physical and logical access control limits the access to sensitive data to authorized persons. In addition, organizational measures prevent uncontrolled access to products or product related items.

	O.RIP O.AC O.PASSWD O.AC.REM O.INSTALL	
T.Authorized-Access	O.INTERNAL.MONITOR O.STAFF.ENGAGEMENT O.RIP O.DATA.TRANSFER	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees prevent unauthorized access to the sensitive data or items.
P.Config-Man	O.CM.LABEL O.CM.RECEPTION.CONTROL O.CM.CHANGE.CONTROL O.CM.PROCESS	The CM labels all the relevant configuration items including received items. Access control to the CM ensures the integrity of the configuration items. Together with used CM plan supported by tools and procedures, configuration management is accomplished. Additional record of CM can be used for audit purpose.
P.Transfer	O.DATA.TRANSFER O.INTERNAL.SHIPMENT	The encryption technique used in transferring data and procedures used in internal shipment can ensure the integrity of the configuration items.
P.Backup	O.LOGICAL.OPERATION	Authorized backups can be done for protecting the integrity of the configuration items.

TABLE 1 MAPPING OF SECURITY OBJECTIVES

The following is a table that demonstrates full coverage of Threats being countered and that all Organizational Security Policies are at least enforced by one or more Security Objective of the site.

	O.CM.LABEL	O.CM.RECEPTION.CONTROL	O.CM.CHANGE.CONTROL	O.CM.PROCESS	O.PERIMETERS	O.ALARM.RESPONSE	O.SECURITY.CONTROL	O.STAFF.ENGAGEMENT	O.REVOKING	O.VISITORS	O.INTERNAL.MONITOR	O.DATA.TRANSFER	O.INTERNAL.SHIPMENT	O.AC	O.PASSWD	O.LOGICAL.ACCESS	O.LOGICAL.OPERATION	O.AC.REM	O.INSTALL	O.RIP
T.Physical-Theft					■	■	■		■	■	■						■			■
T.Logical-Theft								■	■		■			■	■	■	■	■	■	
T.Accidental-Change	■	■	■	■				■												
T.Unauthorized-Staff					■	■	■	■	■	■	■			■	■	■	■	■	■	■
T.Authorized-Access								■			■	■								■
P.Config-Man	■	■	■	■																
P.Transfer												■	■							
P.Backup																■				

TABLE 2 MAPPING BETWEEN POLICIES/THREADS COVERING OBJECTIVES

5.3.2 Justification of Security Objectives mapping

The T.Physical-Theft describes the adverse action of an attacker, with sufficient time to investigate the site from outside the site boundary using simple equipment to carry out a robbery or manipulate TOE components or other of the mentioned assets. This includes the possibility that the attack occurs during the daily working time and the agent intend impersonating an employee of the services company (e.g. cleaning). The attacker can use specific working clothes of the site to camouflage and trying to access sensitive areas. The following security objectives are considered to be sufficient counteracting the threat:

- O.PERIMETERS: implements security mechanisms for the global and local security perimeters to restrict the access to authorised personnel therefore minimizing the possibility of a theft occurrence performed by an outsider;
- O.ALARM.RESPONSE: ensures that an attacker undertaking an unauthorised access attempt cannot get access to sensitive areas of the site for manipulation or theft of sensitive data or items.
- O.INTERNAL.MONITOR: defines the internal assessments and ensures that the required level of security to prevent unauthorised access attempts is established at all times.
- O.REVOKING: ensures that some who belonged to the development team but no longer belongs to it, do not have access rights anymore;
- O.VISITORS: outsiders with rights are identified and always escorted once in the development environment.

- O.LOGICAL.OPERATION: the equipment has Hard Disk encrypted and updates anti-virus to the latest version, which ensures the physical theft cannot extract sensitive data from the equipment.
- O.SECURITY.CONTROL: the security control mechanisms like access control and surveillance cameras and the work of the security staff are defined here which ensure that any attempts of unauthorised access to the site are detected and alarms are triggered.
- O.RIP: if the outsider achieves stealing materials that are no longer used within the development area, they will be not useful as the information will have been destroyed in such a way that they cannot be used in any meaningful way that might affect the confidentiality of the materials in the development area.

The T.Logical-Theft describes the adverse action of an attacker, with experience for compromising logical devices installed by the company to avoid attacks through the wire. This attack would allow access to the company network. The following security objectives are considered to be sufficient counteracting the threat:

- O.INTERNAL.MONITOR: defines the internal assessments and ensures that the required level of security to prevent unauthorised access attempts is established at all times.
- O.STAFF.ENGAGEMENT: the measures defined here which ensure that staff with access to sensitive items has the required skills not to compromise the security measures established at the site.
- O.LOGICAL.OPERATION: the equipment has Hard Disk encrypted and updates anti-virus to the latest version, which ensures the logical theft cannot extract sensitive data from the equipment.
- O.LOGICAL.ACCESS: the logical security measures defined here which prevent an attacker from unauthorised remote access to sensitive data.
- O.REVOKING: ensures that some who belonged to the development team but no longer belongs to it, do not have access rights anymore;
- O.AC: ensures that the logical access to development machines is limited to approved development team members and system administrators. The logical access mechanism to the operating system and also to the CM system is based in identification of the individual and not at group level.
- O.PASSWD: contributes to mitigate the threat as imposes a password policy guaranteeing the passwords strength.
- O.AC.REM: the remote access is controlled by creating an encrypted network connection with mutual authentication of both end parties.
- O.INSTALL: the development machines are configured with a controlled, restrictive user security policy preventing the installation of additional unauthorized functionality which can cause a security hole.

The T.Accidental-Change describes the adverse action of an agent who is a TOE developer committing an error during the TOE development or generation process issuing a vulnerable TOE configuration. The following security objectives are considered to be sufficient counteracting the threat:

- O.CM.LABEL: implements a configuration management system assigning uniquely identifiers to the configuration items of TOEs under configuration control and ensure every version of the configuration item can be found and recovered.
- O.CM.RECEPTION.CONTROL: the reception of physical products or electronic items will be verified and included in the CM system, which ensures the reception of items can be organized accurately and avoid accidental changes.
- O.CM.CHANGE.CONTROL: ensure only authorized access and authorized changes are acceptable.
- O.CM.PROCESS: ensures the site is using a configuration management plan supported by tools and procedures.
- O.STAFF.ENGAGEMENT: the measures defined here which ensure that staff with access to sensitive items has the required skills not to compromise the security measures established at the site.

The T.Unauthorized-Staff describes the adverse action of an insider without access rights circumventing the security, entering a restricted area with the aim of stealing TOEs information. Also the configuration information of the security devices may be accessed. The following security objectives are considered to be sufficient counteracting the threat:

- O.PERIMETERS: implements security mechanisms for the global and local security perimeters to restrict the access to authorised personnel therefore minimizing the possibility of a theft occurrence performed by an outsider;
- O.ALARM.RESPONSE: ensures that an attacker undertaking an unauthorised access attempt cannot get access to sensitive areas of the site for manipulation or theft of sensitive data or items.
- O.SECURITY.CONTROL: the security control mechanisms like access control and surveillance cameras and the work of the security staff are defined here which ensure that any attempts of unauthorised access to the site are detected and alarms are triggered.
- O.INTERNAL.MONITOR: defines the internal assessments and ensures that the required level of security to prevent unauthorised access attempts is established at all times.
- O.REVOKING: ensures that some who belonged to the development team but no longer belongs to it, do not have access rights anymore;
- O.VISITORS: outsiders with rights are identified and always escorted once in the development environment.
- O.LOGICAL.OPERATION: the equipment has Hard Disk encrypted and updates anti-virus to the latest version, which ensures the logical theft cannot extract sensitive data from the equipment.
- O.LOGICAL.ACCESS: the logical security measures defined here which prevent an attacker from unauthorised remote access to sensitive data.
- O.STAFF.ENGAGEMENT: the measures defined here which ensure that staff with access to sensitive items has the required skills not to compromise the security measures established at the site.

- O.RIP: if the outsider achieves stealing materials that are no longer used within the development area, they will be not useful as the information will have been destroyed in such a way that they cannot be used in any meaningful way that might affect the confidentiality of the materials in the development area.
- O.AC: ensures that the logical access to development machines is limited to approved development team members and system administrators. The logical access mechanism to the operating system and also to the CM system is based in identification of the individual and not at group level.
- O.PASSWD: contributes to mitigate the threat as imposes a password policy guaranteeing the passwords strength.
- O.AC.REM: the remote access is controlled by creating an encrypted network connection with mutual authentication of both end parties.
- O.INSTALL: the development machines are configured with a controlled, restrictive user security policy preventing the installation of additional unauthorized functionality which can cause a security hole.

The T.Authorized-Access describes the adverse action of an insider with access rights (a malicious TOE developer) whose goal can be the theft of TOE information or the TOE modification during the development process or carry out a sabotage during the same process. The following security objectives are considered to be sufficient counteracting the threat:

- O.INTERNAL.MONITOR: ensured that the security level of the site is maintained at all times by the security measures defined here.
- O.STAFF.ENGAGEMENT: the measures defined here which ensure that staff with access to sensitive items has the required skills not to compromise the security measures established at the site.
- O.RIP: if the insider achieves stealing materials that are no longer used within the development area, they will be not useful as the information will have been destroyed in such a way that they cannot be used in any meaningful way that might affect the confidentiality of the materials in the development area.
- O.DATA.TRANSFER: ensures the security of sensitive data during transfer.

The policy P.Config-Man specifies that the organization has implemented a configuration management system documented in the associated CM plan. The objective of the CM system is to ensure the assignment of uniquely identifier to the TOEs configuration items, the implementation of a version and changes control mechanisms (by means of procedures and the support of automated access control to the CM system) and provide an automated support for the TOE generation and their acceptance. The CM system maintains under configuration management the TOEs, the parts of the TOEs, the implementation representation, the documentation generated and security flaws and their resolution status. To enforce this policy, the following security objectives are considered necessary and sufficient:

- O.CM.LABEL: ensures that the items under configuration control are uniquely identified. The CM system maintains under configuration management the TOEs, the parts of the TOEs, the

implementation representation, the documentation generated and security flaws and their resolution status.

- O.CM.RECEPTION.CONTROL: the reception of physical products or electronic items will be verified and included in the CM system, which ensures the reception of items can be organized accurately and avoid accidental changes.
- O.CM.CHANGE.CONTROL: the objective contributes enforcing the policy as it implements an access control policy controlling the services and information accessible for the developers. In addition, a change control procedure is implemented. This procedure is supported by the access control mechanism guaranteeing that only authorised changes to the configuration items are performed.
- O.CM.PROCESS: ensures the site is using a configuration management plan supported by tools and procedures.

Therefore, it has been demonstrated that all the security objectives are needed for enforcing the policy. The sufficiency condition is direct as it covers all the points with individual objectives.

The Security Objectives O.DATA.TRANSFER and O.INTERNAL.SHIPMENT directly enforce the OSP P. Transfer.

The Security Objective O.LOGICAL.OPERATION directly enforces the OSP P. Backup.

6 Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

7 Security Assurance Requirements

The security assurance requirements for this Site Security Target are ALC_CMC.4, ALC_CMS.4, ALC_DVS.1 and ALC_LCD.1.

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

- ALC_CMC.4 (CM capabilities)
- ALC_CMS.4 (CM scope)
- ALC_DVS.1 (Development security)
- ALC_LCD.1 (Life-cycle definition)

The assurance requirements listed above fulfil the requirements of (5) because hierarchically higher components are used in this Site Security Target compared to the Minimum Requirements in (6).

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

ALC_CMC.4: ALC_CMS.1, ALC_DVS.1, ALC_LCD.1

ALC_CMS.4: None

ALC_DVS.1: None

ALC_LCD.1: None

The following dependencies are not fulfilled or not completely fulfilled:

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

7.1 Application Notes and Refinements

The term "TOE" used for the product under evaluation is considered as "intended TOE" here because a specific product is not considered 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.

Refinements regarding Security Assurance Requirements as defined in CC Part 3 (3) are written in italic. The term 'TOE' is replaced by 'product' or 'configuration item'.

7.1.1 Overview regarding CM capabilities (ALC_CMC)

According to the processes rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below. Since the application notes in (4) are defined for ALC_CMC.4. Since this SST claims ALC_CMC.4, only the relevant content elements are adapted.

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

7.1.2 Overview regarding CM Scope (ALC_CMS)

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

7.1.3 Overview regarding Development Security (ALC_DVS)

The site must ensure that the handling and storage of the configuration items is secure so that no information is unintentionally made available for the operational phase and no unauthorised modifications of security relevant parameters is possible. The confidentiality and integrity of design information, test data and configuration data must be guaranteed, access to any kind of samples (client's specific samples or open samples) development tools and other material must be restricted to authorized persons only, and scrap must be controlled and returned.

Based on these requirements the physical security as well as the logical security of the site are in the focus of the evaluation. Beside the pure implementation of the security measures, also the control and the maintenance of the security measures must be considered.

If the transfer of configuration items between two sites involved in the development flow is included in the scope of the evaluation (life-cycle covered by the product evaluation) this is considered as internal shipment. In general, the security requirements for confidentiality and integrity are the same but it must clearly distinguish to ensure the correct subject of the evaluation.

7.1.4 Overview 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.

For this site the Life Cycle only Develop/ Test and Quality phase relevant.

7.2 Security Assurance Rationale

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

The site has a process in place to ensure an appropriate and consistent identification of the products.

Note: The content elements that are changed from the original (4) according to the application notes in the process description (5) are written in italic. The term TOE can be replaced by configuration items or product.

7.2.1 Rationale for ALC_CMC.4

SAR	Security Objective	Rationale
ALC_CMC.4.1C: *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*	O.CM.LABEL O.CM.RECEPTION.CONTROL O.CM.PROCESS	Upon reception of an item from another site O.CM.RECEPTION.CONTROL ensures that authenticity is verified for the shipped item. With this it is ensured that the item has been labelled before delivery. After integration into the CM system O.CM.LABEL ensures appropriate and consistent labelling as well as unique identification of the item. O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures.
ALC_CMC.4.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.CM.LABEL	see ALC_CMC.4.1C
ALC_CMC.4.3C: The CM system shall uniquely identify all configuration items.	O.CM.LABEL	see ALC_CMC.4.1C
ALC_CMC.4.4C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	O.CM.CHANGE.CONTROL O.AC O.AC.REM	All configuration items are kept under configuration control according to O.CM.CHANGE.CONTROL. O.CM.CHANGE.CONTROL is supported by O.AC and O.AC.REM that logical access locally to development machines and CM system shall be limited to approved development team member and system administrators.
ALC_CMC.4.5C: The CM system shall support the *development* of the *product* by automated means.	O.CM.PROCESS	The CMS system supports automated development of products.
ALC_CMC.4.6C: The CM documentation shall include a CM plan.	O.CM.PROCESS	CM process documentation is available and maintained according to O.CM.PROCESS.

ALC_CMC.4.7C: The CM plan shall describe how the CM system is used for the development of the *product*.	O.CM.PROCESS	CM process documentation is available and maintained according to O.CM.PROCESS.
ALC_CMC.4.8C: The CM plan shall describe the procedures used to accept modified or newly created configuration items (as part of the *product*).	O.CM.CHANGE.CONTROL O.CM.PROCESS	Process descriptions are covered by O.CM.PROCESS, including modification or new generation of configuration items. Handling of change management for released products is covered by O.CM.CHANGE.CONTROL.
ALC_CMC.4.9C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.CM.LABEL O.CM.CHANGE.CONTROL	All configuration items are kept under configuration control according to O.CM.LABEL and O.CM.CHANGE.CONTROL.
ALC_CMC.4.10C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.CM.PROCESS	The operation of the CM system in accordance to the CM plan is ensured by O.CM.PROCESS.

TABLE 3 RATIONALE FOR ALC_CMC.4

7.2.2 Rationale for ALC_CMS.4

SAR	Security Objective	Rationale
ALC_CMS.4.1C: The configuration list shall include the following: *The evaluation evidence required by the SARs*	O.CM.LABEL O.CM.PROCESS	The unique identification of all configuration items is ensured by O.CM.LABEL. O.CM.PROCESS contains the CM documentation including clear instructions how to consider the configuration items in the configuration list.
ALC_CMS.4.2C: The configuration list shall uniquely identify the configuration items.	O.CM.LABEL O.CM.PROCESS	The unique identification of all configuration items is ensured by O.CM.LABEL. O.CM.PROCESS contains the CM documentation.

ALC_CMS.4.3C: For each *configuration item*, the configuration list shall indicate the developer of the item.	O.CM.PROCESS	O.Config-Process contains the CM documentation including clear instructions how to consider the configuration items in the configuration list (including developer information - no subcontractors are used).

TABLE 4 RATIONALE FOR ALC_CMS.4

7.2.3 Rationale for ALC_DVS.1

SAR	Security Objective	Rationale
ALC_DVS.1.1C: 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 *product* design and implementation in its development environment.	O.PERIMETERS O.ALARM.RESPONSE O.SECURITY.CONTROL O.STAFF.ENGAGEMENT O.REVOKING O.VISITORS O.INTERNAL.MONITOR O.DATA.TRANSFER O.INTERNAL.SHIPMENT O.AC O.AC.REM O.PASSWD O.LOGICAL.ACCESS O.LOGICAL.OPERATION O.INSTALL O.RIP	Physical measures are implemented according to O.PERIMETERS supported by O.SECURITY.CONTROL and O.ALARM.RESPONSE. In addition, all logical measures are described according to O.REVOKING, O.VISITORS, O.AC, O.AC.REM, O.PASSWD, O.INSTALL, O.LOGICAL.ACCESS and O.Logical-Operation. These measures are supported by the security awareness of the staff according to O.STAFF.ENGAGEMENT. Security during internal shipment is ensured by O.INTERNAL.SHIPMENT and O.DATA.TRANSFER. O.RIP, O.LOGICAL.OPERATION, O.PASSWD ensure that no unauthorised access to products is possible for an attacker.

TABLE 5 RATIONALE FOR ALC_DVS.1

7.2.4 Rationale for ALC_LCD.1

SAR	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the *product*.	O.CM.LABEL O.CM.CHANGE.CONTROL O.CM.PROCESS	During development no production of the intended TOE takes place. Therefore, only the maintenance of products is relevant for this site. Maintenance is done according to O.CM.LABEL,

		O.CM.CHANGE.CONTROL and O.CM.PROCESS.
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the *product*.	O.CM.LABEL O.CM.CHANGE.CONTROL O.CM.PROCESS	see ALC_LCD.1.1C

TABLE 6 RATIONALE FOR ALC_LCD.1

8 Site Summary Specification

The Site Summary Specification section identifies all evidence needed for the Site to meet the SARs, and describes aspects of how to fulfil them and, regarding ALC_DVS, how it fulfils the attack potential claim made in the SST.

This site only in charge of the cyber security and user privacy protection certification features for Huawei's products/systems, all phases of the cyber security and user privacy protection certification features related life cycle are carried out within the site which is the target of this SST, thus only Develop/ Test phase and Quality phase will be involved in this site.

The following sections identify the evidences provided by HUAWEI and describe how HCSCTC site meet the assurance requirements and how the security measures resist the attack potential "High" selected.

The internals of the procedures are described in so far as it has been considered necessary to demonstrate the fulfilment of the requirements and the security objectives.

8.1 Preconditions Required by the Site

Preconditions are described for the services of this site as following:

1. The client will provide the necessary software and guidance to properly install the intended TOE under product evaluation in case HCSCTC has not the specific ways to install it.
2. The client must provide appropriate software and procedures in order to perform the testing. This includes the delivery of correct data for development, secured by appropriate means against modification and/or disclosure, if necessary.
3. The client is responsible for the release of the products (e.g. by buying released products).
4. The client provides a method of unique identification for all items shipped to the site.
5. The client provides appropriate information for the delivery of produced goods as well as electronic data to be delivered. This information shall at least comprise address data for physical items.

8.2 Services of the Site

The following service and/or processes provided by HCSCTC are in the scope of the evaluation process:

- Testing design and compliance testing for products described in section 2.3 Testing Center products up to EAL4.
- Report generation for Testing performance.
- Only allow remote connection to the testing room IV where network devices placed there can be tested through remote control of third-party. Test data is generated from the process of interaction between remote third-party operator and the devices to be tested. Network devices to be tested and other devices supporting the testing process, network connection in

testing room IV are physically isolated from testing room I, II and III, therefore, remote connection in testing room IV cannot access sensitive data in testing room III.

8.3 Objectives Rationale

The following rationale provides a justification that shows that all threats and organisational security policies are effectively addressed by the security objectives.

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

Security Objective	Threats and OSPs
O.AC	T.Logical-Theft T.Unauthorized-Staff
O.AC.REM	T.Logical-Theft T.Unauthorized-Staff
O.ALARM.RESPONSE	T.Physical-Theft T.Unauthorized-Staff
O.CM.PROCESS	T.Accidental-Change P.Config-Man
O.CM.CHANGE.CONTROL	T.Accidental-Change P.Config-Man
O.CM.LABEL	T.Accidental-Change P.Config-Man
O.CM.RECEPTION.CONTROL	T.Accidental-Change P.Config-Man
O.DATA.TRANSFER	T.Authorized-Access P.Transfer
O.INSTALL	T.Logical-Theft T.Unauthorized-Staff
O.INTERNAL.MONITOR	T.Physical-Theft T.Logical-Theft T.Unauthorized-Staff T.Authorized-Access
O.INTERNAL.SHIPMENT	P.Transfer

O.LOGICAL.ACCESS	T.Unauthorized-Staff T.Logical-Theft
O.LOGICAL.OPERATION	T.Physical-Theft T.Logical-Theft T.Unauthorized-Staff P.Backup
O.PASSWD	T.Logical-Theft T.Unauthorized-Staff
O.PERIMETERS	T.Physical-Theft T.Unauthorized-Staff
O.REVOKING	T.Physical-Theft T.Logical-Theft T.Unauthorized-Staff
O.RIP	T.Physical-Theft T.Unauthorized-Staff T.Authorized-Access
O.SECURITY.CONTROL	T.Physical-Theft T.Unauthorized-Staff
O.STAFF.ENGAGEMENT	T.Logical-Theft T.Accidental-Change T.Unauthorized-Staff T.Authorized-Access
O.VISITORS	T.Physical-Theft T.Unauthorized-Staff

TABLE 7 OBJECTIVES RATIONALE

O.CM.LABEL

All configuration items are identified by a unique version number by the configuration management system. By this, different products can be identified. By this, the threat T.Accidental-Change is countered and the OSPs P.Config-Man is addressed.

O.CM.RECEPTION.CONTROL

Upon reception of an electronic item relevant to security from a different site, authenticity of this item is verified (e.g. verification of a PGP signature when sent via email). Identification is performed if necessary (i.e. requested by the client; the client has to provide information how to identify the

item). In case items are shared by a shared configuration management system between different sites or shared network drives, authenticity is implicitly assumed. By this, the threat T.Accidental-Change is countered and OSPs P.Config-Man is addressed.

O.CM.CHANGE.CONTROL

The application of released procedures for the setup of the intended TOE and the controlled introduction of changes ensures a development process according to clients' specifications. Procedures for setting up the development process as well as changes to the initial setup are done only by authorised personnel. The development process is supported by automated systems. By this the OSP P.Config-Man is addressed. In addition, the threat T.Accident-Change is covered.

O.CM.PROCESS

Configuration items are stored in the configuration management system according to the site's configuration managment plan. By this the threat T.Accidental-Change is countered and OSP P.Config-Man is addressed.

O.PERIMETERS

implemented security mechanisms for the global and local security perimeters to restrict the access to authorised personnel therefore minimize the possibility of a theft occurrence performed by an outsider. By this, threat T.Physical-Theft and T.Unauthorized-Staff are countered.

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 data or item 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. Therefore, by this, threat T.Physical-Theft and T.Unauthorized-Staff are countered.

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. Therefore, by this, threat T.Physical-Theft and T.Unauthorized-Staff are countered.

O.STAFF.ENGAGEMENT

All employees who have access to sensitive configuration data or 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 non-disclosure agreement. All employees are trained and qualified for their job. The personnel shall be aware of their responsibilities, be proactive and shall communicate any security incident to the security responsible. Situation mentioned above can counter the threat T.Authorized-Access and T.Unauthorized-Staff.

The team members are aware of the dangers of logical attacks through modifying the IT systems and development machines with which they work and inappropriate Internet usage, e-mail attachments, accidental malware import etc. They should also be aware of the company policy regarding material destruction and backups and 'working from home' (if applicable). Situation mentioned above can counter the threat T.Logical-Theft.

Access rights will only be granted to employees as part of an approved management procedure once they have received the security training. Situation mentioned above can counter the threat T.Accidental-Change.

Therefore, Threats T.Logical-Theft, T.Accidental-Change, T.Unauthorized-Staff and T.Authorized-Access can be countered by O.STAFF.ENGAGEMENT.

O.REVOKING

If someone is removed from the team list due to disciplinary matters or dismissal, then their rights will be revoked and the person who is responsible within the developers own organization for overall security is made aware of this. Therefore, by this, threats T.Physical-Theft, T.Logical-Theft and T.Unauthorized-Staff can be countered by O.REVOKING.

O.VISITORS

All visitors to the development area must be identified, logged and then escorted at all times once in the development environment. Therefore, by this, threats T.Physical-Theft and T.Unauthorized-Staff can be countered by O.VISITORS.

O.INTERNAL.MONITOR

The site performs security management meetings on a regular basis. 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 at least every year to verify the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure a sufficient protection. The measures mentioned above can improve the effectiveness of security measures, which means threat T.Physical-Theft, T.Logical-Theft, T.Unauthorized-Staff and T.Authorized-Access are countered by O.INTERNAL.MONITOR.

O.DATA.TRANSFER

Sensitive electronic configuration items (data or documents in electronic form) are protected by applying cryptographic algorithms to ensure confidentiality and/or integrity (whatever is 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. Therefore, the threat T.Authorized-Access is countered and OSP P.Transfer is addressed by O.DATA.TRANSFER.

O.INTERNAL.SHIPMENT

The recipient of a physical configuration item is identified by the assigned client address. The recipient(s) of an electronic configuration item (e.g. source code) can be identified in different ways. The specific way is defined in the internal shipment procedure. The internal shipment procedure is applied to all shipped configuration data or items. The recipient for shipment can only be changed by a controlled process. The packaging (if any) is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of configuration data or items during internal shipment. For every sensitive configuration data or item, the protection measures against manipulation are defined (e.g. sealed boxes, encryption, integrity protection, electronic signature). Therefore, the security measures for delivery above can address OSP P.Transfer

O.AC

Logical access to development machines shall be limited to approved development team members and system administrators.

The logical access mechanism to the operating system and also to the CM system will be based in identification of the individual and not at group level.

The two security measures mentioned above can ensure that threats T.Logical-Theft and T.Unauthorized-Staff are countered by O.AC.

O.PASSWD

Weak passwords are not allowed. A password policy guaranteeing the passwords strength shall be implemented:

- Passwords shall be changed periodically
- The same password may not be used for both the underlying operating system and the CM system.
- An inactivity period for screen blocking shall be established, requiring re-authentication for unblocking.

The password policy mentioned above can ensure that T.Logical-Theft and T.Unauthorized-Staff are countered.

O.LOGICAL.ACCESS

The separation of office network and production network can ensure that T.Unauthorized-Staff and T.Logical-Theft are countered by O.LOGICAL.ACCESS.

O.LOGICAL.OPERATION

The equipment's Hard Disk are encrypted. The equipment has updated anti-virus. The two measures above ensure that T.Physical_Theft, T.Logical-Theft and T.Unauthorized-Staff are countered by O.LOGICAL.OPERATION.

Backups will be created, stored and destroyed according to an approved procedure. Members of the development teams should be aware that no unauthorized backups may be made that are then taken outside the development area.

The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.

The backup measure mentioned above ensure that P.Backup is addressed by O.LOGICAL.OPERATION.

O.AC.REM

It is only possible to access the testing environment from outside the development area (i.e. work at home) on a company issued computer with commercial grade software then helps create an encrypted network connection with mutual authentication of both end parties. The measures mention above ensure that T.Logical-Theft and T.Unauthorized-Staff are countered by O.AC.REM.

O.INSTALL

The development machines should be configured with a controlled, restrictive user security policy that prevents the installation of additional unauthorized functionality. The measures mentioned above can minimize the possibility that the sensitive items can be accessed by logical theft and unauthorized staff. Therefore, by this, T.Logical-Theft and T.Unauthorized-Staff are countered by O.INSTALL.

O.RIP

Materials that are no longer used within the development area (through the whole development life cycle) must be destroyed in such a way that they cannot be used in any meaningful way that might affect the confidentiality of the materials in the development area. Because the destroyed materials cannot be used in any meaningful way, even the materials are accessed by a theft or unauthorized staff or authorized staff, there would be no harm for the site. Therefore, T.Authorized-Access, T.Unauthorized-Staff and T.Physical-Theft are countered by O.RIP.

8.4 SAR Rationale

The Security Assurance Requirements rationale does not explicitly address the developer action elements defined in (4) because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the preparation for the site visit. In addition, this includes that the procedures are applied as written and explained in the documentation.

8.4.1 ALC_CMC

The security assurance requirements of the assurance component ALC_CMC.4 are suitable to support the development of complex testing due to the formalized acceptance process and the automated production support. This comprises the identification of all configuration items and the automated control and tracking within the development area. The requirement for authorized changes and

separate roles for operation and release support the integrity and confidentiality required for the products. Therefore, this assurance level meets the requirements for the configuration management.

8.4.2 ALC_CMS

The chosen assurance level ALC_CMS.4 of the assurance family “CM scope” supports the control of the production 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 ALC_DVS

The chosen assurance level ALC_DVS.1 of the assurance family “Development Security” is required since a high attack potential is assumed for potential attackers. The configuration items and information handle at the site during development and testing of the intended TOE can be used by potential attackers. Therefore, the handling and storage of these items must be sufficiently protected.

8.4.4 ALC_LCD

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

8.5 Assurance Measure Rationale

O.AC

Logical access to development machines shall be limited to approved development team members and system administrators by sufficient security measures described in developer’s documentation. ALC_DVS.1.1C provides this fulfilment. ALC_CMC.4.4C ensures only authorized changes can be made.

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.AC.REM

Access to the testing environment is allowed to the clients with proper conditions described by the developer. ALC_DVS.1.1C provides this fulfilment. ALC_CMC.4.4C ensures only authorized changes can be made.

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.ALARM.RESPONSE

ALC_DVS.1.1C requires that the developer shall assure that the time to response for the alarm system will be enough to keep confidentiality and integrity of the TOE or related components. The alarm system is in place to foresee any problems.

Thereby this objective contributes to meet the Security Assurance Requirement.

O.CM.PROCESS

ALC_CMC.4.1C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.4.5C requires the CM system to support the production of the intended TOE by automated means. ALC_CMC.4.6C requires that the CM documentation shall include a CM plan. ALC_CMC.4.7C and ALC_CMC.4.8C requires that the CM plan describe how CM system is used for the development of the product and how are new configuration items being accepted in the same system. ALC_CMC.4.10 the CM plan shall demonstrate how CM System is being operated in accordance with the4 CM plan documentation that includes a CM plan.

ALC_CMS.4.1C, ALC_CMS.4.2C and ALC_CMS.4.3C ensure configuration items will be managed the CM system.

ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products. ALC_LCD.1.2C requires control over the development and maintenance of the TOE. The objective meets the set of Security Assurance Requirements listed here.

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.CM.CHANGE.CONTROL

ALC_CMC.4.4C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items This configuration management tool provides sufficient security measures for the integrity of the TOE or related components. ALC_CMC.4.8C requires that the CM plan describe how CM system is used for the development of the product and how are new configuration items being accepted in the same system. ALC_CMC.4.9C requires the evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products. ALC_LCD.1.2C requires control over the development and maintenance of the TOE. The objective meets the set of Security Assurance Requirements listed here.

Thereby this objective is suitable to meet the Security Assurance Requirement

O.CM.LABEL

The configuration list required by ALC_CMS.4.1C shall include the evaluation evidence for the fulfilment of the SARs and related information. ALC_CMS.4.2C addresses the same requirement as ALC_CMC.4.3C by identifying a uniquely the configuration items. ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system. ALC_CMS.4.1C, ALC_CMS.4.2C ensure configuration items will be managed the CM system.

ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products. ALC_LCD.1.2C requires control over the development and maintenance of the TOE.

The objective meets the set of Security Assurance Requirements.

O.CM.RECEPTION.CONTROL

ALC_CMC.4.1C requires a CM documentation that describes the method used to uniquely identify the configuration items.

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.DATA.TRANSFER

ALC_DVS.1.1C requires to make sure all information considered sensitive will be manipulated and transferred under proper security controls.

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.INSTALL

Integrity of the devices used in order to manage, develop or test any critical or sensitive data is required under ALC_DVS.1.1C.

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.INTERNAL.MONITOR

Internal audits are performed periodically. This is being required under ALC_DVS.1.1C.

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.INTERNAL.SHIPMENT

Transfer of physical/logical assets in the developer's premises is being required to be controlled under strict conditions. This is required by ALC_DVS.1.1C.

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.LOGICAL.ACCESS

Segregation of networks and proper security control checks are required by ALC_DVS.1.1C

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.LOGICAL.OPERATION

ALC_DVS.1.1C required to have sufficient logical security measures to keep integrity and confidentiality of the assets in the devices.

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.PASSWD

The DSD describes in the detail the security related topics for the logical security as required by ALC_DVS1.1C related with the logical access to the assets. Those are protected by different stopping layers only accessible by proper password check controls.

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.PERIMETERS

ALC_DVS.1.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE.

Thereby this objective contributes to meet the Security Assurance Requirement.

O.REVOKING

Access, management and revocation is being granted under strict control measures. These measures are being required under ALC_DVS.1.1C.

Thereby this objective is suitable to meet the Security Assurance Requirement.

O.RIP

This objective is being covered by the asset management described in the internal policies. Also any material that could be suitable to be stolen will be tracked by the company with as described in ALC_DVS1.1C in order to assess the physical and logical security implemented in the site.

Thereby this objective is suitable to meet the Security Assurance Requirement

O.SECURITY.CONTROL

The DSD describes in the detail the security related topics for the physical security as required by ALC_DVS1.1C. The physical security measures are considered to be sufficient to cover with the requirements of the family. Furthermore, the security policy detailed by corporate is aligned with the internal documentation for the services provided by the site. Thereby this objective is suitable to meet the Security Assurance Requirement

O.STAFF.ENGAGEMENT

ALC_DVS.1.1C 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.VISITORS

ALC_DVS.1.1C requires that all visitors are being monitored all the time in order to mitigate any threat related with the development activities performed in the HCSCTC. This is being covered by the internal policies described in corporate security in Huawei by means that every visitor must be accompanied since he enters a restricted zone. 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 associated data as well as the complete documentation of the site provided for the evaluation.

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

9 References

1. **Lab, Huawei Cyber Security Certification.** *HUA-C-LCD-0.7.*

2. **Common Criteria for Information Technology Security Evaluation.** *Part 1: Introduction and General Model.* Version 3.1, Rev. 5, April 2017.

3. —. *Part 3: Security Assurance Components.* Version 3.1, Rev. 5, April 2017.

4. **Common Methodology for Information Technology Secuirty Evaluation.** *Evaluation methodology.* Version 3.1, Rev.5, April 2017.

5. **Supporting Document Guidance.** *Site Certification.* Version 1.0, Rev.1, October 2007.

6. **Library, Join International.** *Minimum Site Security Requirements.* 2020 February. version 3.0.

7. **EUROSMART.** *Security IC Platform Protection Profile with Augmentation packages.* Version 1.0, 2014.