FILENAME: HiSi-21120301-INT-0-CC-Site-Security-Target-Lite(Bristol)
DMS REF: CC-000051-PS
VERSION: 6
DATE: 2022-01-17

Site Security Target Lite

- Huawei Bristol CC Design Centre

Author	Reviewer	Approver
Tom Thomas	Bristol CC Site Security Committee	Bristol CC Site Security Committee

Version Control

Version	Date	Description
1.0	03/12/2021	Based on SST v1.0
1.1	07/01/2022	Removed site floorplan details
5	17/01/2022	Switched to Cognidox DMS versioning style Removed watermark
6	17/01/2022	Corrected version number in Section 1.1

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 Design Centre 6
3 Conformance Claim 7
4 Security Problem Definition 9
4.1 Assets 9
4.2 Threats 10
4.3 Organizational Security Policies 11
4.4 Assumptions 12
5 Security Objectives 13
5.1 Configuration management 13
5.2 Security measures 14
5.2.1 Physical Security measures 14
5.2.2 Personal measures 14
5.2.3 Logical measures 15
5.3 Security Objectives Rationale 17
5.3.1 Mapping of Security Objectives 17
6 Extended Assurance Components Definition 20
7 Security Assurance Requirements 21
7.1 Application Notes and Refinements 21
7.1.1 Overview regarding CM capabilities (ALC_CMC) 21
7.1.2 Overview regarding CM Scope (ALC_CMS) 22
7.1.3 Overview regarding Development Security (ALC_DVS) 22
7.1.4 Overview regarding Life-Cycle Definition (ALC_LCD) 22
7.2 Security Assurance Rationale 22
7.2.1 Rationale for ALC_CMC.5 23
7.2.2 Rationale for ALC_CMS.5 26
7.2.3 Rationale for ALC_DVS.2 26
7.2.4 Rationale for ALC_LCD.1 28
8 Site Summary Specification 29
8.1 Services of the Site 29
8.2 SAR Rationale 30

8.2.1 ALC_CMC 30
8.2.2 ALC_CMS 31
8.2.3 ALC_DVS 31
8.2.4 ALC_LCD 32
8.3 Assurance Measure Rationale 32
8.4 Mapping of the Evaluation Documentation 37
9 References 38
External 38

1 Document Information

1.1 Reference

Title: Site Security Target Lite - Huawei Bristol CC Design Centre

Version: 6

Date: 17/01/2022

Company: Huawei Technology Co., Ltd

Name of the site: Huawei Bristol CC Design Centre

Product Type: TOE Architecture and Firmware Development Site

Evaluation Assurance Components: ALC_CMC.5, ALC_CMS.5, ALC_DVS.2 and ALC_LCD.1.

2 SST Introduction

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

This Site Security Target Lite refers to the following site:

Huawei Bristol CC Design Centre (part of Huawei Technologies R&D UK Ltd - Bristol site)

This site is used for developing architectural specifications and embedded firmware for Huawei silicon products.

2.1 Identification of the Site

The physical site is 'Huawei Technologies R&D (UK) Ltd' and is located at:

290 Park Avenue,
Aztec West,
Almondsbury,
Bristol,
UK
BS32 4TR

2.2 Site Description

The Huawei R&D UK Ltd (Bristol) site is located on a business park in the north of Bristol. The office occupies part of the first floor of a two storey office building. Only part of the office facility is in scope for this SST – that termed 'Bristol CC Design Centre'. The rest of the office is used for administration and general integrated circuit hardware and software design activities. The main office front door is accessed with Huawei ID cards, issued to Bristol-based employees only.

There are two entrances to the building, one is the main entrance, and the other is the entrance from the courtyard/fire escape area. Each entrance is monitored by surveillance cameras 24 hours a day.

Further site schematics are only available within the full version of the Site Security Target.

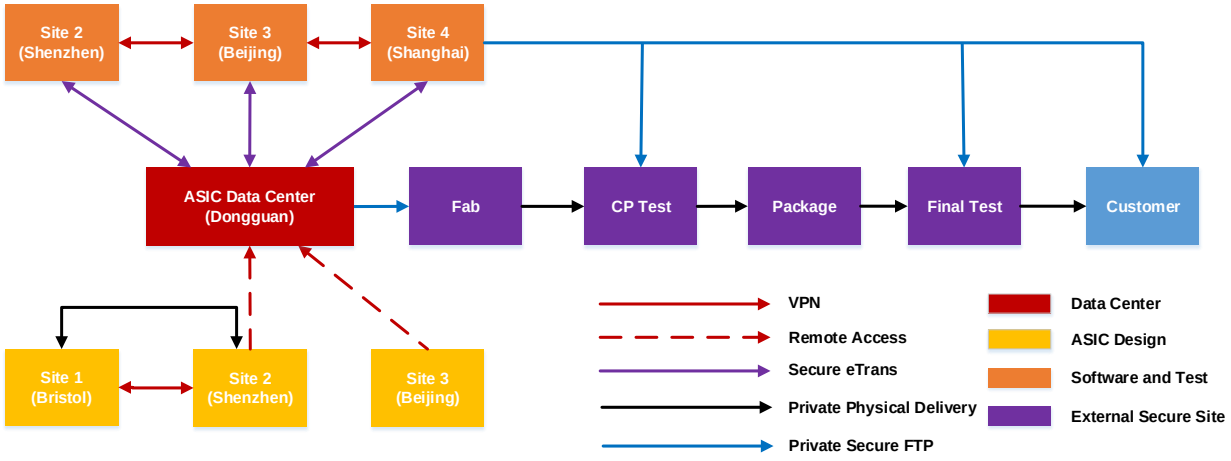
2.3 Design Centre

The Bristol CC Design Centre part of Huawei Bristol is a secure development facility that is responsible for a) architecture of silicon hardware and software, b) architecture and design of embedded firmware intended for incorporation into security sensitive products such as ePassports, consumer IoT and automotive products, and c) limited testing of embedded firmware on chip samples. Products such as these are subject to strict industry certification regimes.

The following services and processes provided by Huawei Bristol are in the scope of the evaluation process:

- Hardware architecture of security-related silicon IP and subsystems
- Firmware architecture, design and development for security-related silicon IP and subsystems
- Software architecture for security-related silicon IP and subsystems
- Receiving of manufactured prototype and production silicon and associated development boards and tools; management and storage of these assets
- Testing of manufactured silicon and associated firmware
- Curation, management and oversight of security policy and procedures on other Huawei sites which contribute or are involved in the life cycles of Bristol-derived security assets

Downstream development activities such as silicon design, silicon verification, manufacture, silicon validation and qualification will be carried out at other Huawei sites.



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, (1)
- Common Criteria for Information Technology Security Evaluation, Part3: Security assurance components; Version 3.1, Revision 5, April 2017, (2)

For the evaluation, the methodology will be used:

- Common Methodology for Information Technology Security Evaluation: Evaluation methodology. Version 3.1, Revision 5, April 2017, (3)

This Site Security Target Lite (SST Lite) is CC Part 3 conformant with EAL6 and therefore covers the following CC assurance components:

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

The assurance components are chosen in order to reuse the results in evaluations up to EAL6. 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 therefore it is more efficient to cover the whole ALC_TAT together at the product evaluation time.

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

The Security Problem Definition comprises two major security problems. The first set of security problems comprises various 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.INFO	All the documentation and information of the products and certification/pre-evaluation (specifications, designs, guidance, test tools/data, source code) or information related to the processes in whatever format.	Confidentiality Integrity
A.PROT	Products prototypes or parts/modules of the TOEs.	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 devices, audit data, configuration, cryptographic keys, passwords, etc.).	Confidentiality Integrity

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 intended TOE. Such a product intended to be designed at Huawei Bristol 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 mentioned assets. This includes the possibility that the attack occurs during the daily working time and the agent impersonates an employee of the services company (e.g. cleaning). The attacker may use specific working clothes of the site to camouflage and attempt 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, design information, etc.), and indirectly, getting security systems information and attempt to violate and subsequently gain 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 in compromising logical devices installed by the company to avoid attacks over 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.Logical-theft is ‘emergent’, i.e. in order to perform the logical theft, one of several vectors can be adopted by the attacker, including T.Physical-Theft, T.Authorised-Access and T.Unauthorised-Staff.

T.Accidental-Change

The agent, considered as an internal worker can commit an error during their 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 does not have 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 developer whose goal may be the theft of TOE information, the TOEs modification during the development process, or sabotage during the TOE development. The employee might be paid for the work or might be in conspiracy with someone outside.

The employee has enough technical knowledge to modifying the TOEs, but does not have experience in physical or logical security disciplines.

His motivation may be high as they may be paid for performing the work or they 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 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 evaluation of the documentation of the site is under configuration management control.

P.Config-Man

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

The CM system guarantees the assignment of unique identifiers to the TOE’s configuration items and implements version and change 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 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. The sender of the product is identified by the address of the sender site for physical items and by corresponding information (e.g. email address) for electronic items by the address provided by the sender.

The following assumption is applicable to the Bristol CC Design Centre:

A.Backup-Site: For the purposes of having the option of a geo-diverse backup facility, there is an assumption that there is a network connection to another Huawei development site, and this connected will be over a secure VPN, with minimal necessary services over this connection, and all data transferred over this connection pre-encrypted.

5 Security Objectives

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

The security objectives are focused on the logical (technical, personnel, procedural) and physical security measures applicable to the Huawei development areas defined in the scope of this SST, the configuration management of the items for the intended TOEs and the development and security maintenance life cycle.

5.1 Configuration management

O.CM.LABEL

A configuration management system shall be implemented, assigning unique identifiers to the configuration items of intended TOEs under configuration control.

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

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

O.CM.RECEPTION.CONTROL

A signature is required to be requested as part of incoming deliveries and is required for outgoing deliveries. 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, and checking of tamperproof measures. For electronic items that require authenticity, the authenticity is verified upon reception. Evidence of manipulation or improper observation of procedure shall invoke raising of a security incident.

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 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; i.e. main door electronic lock, global perimeter intrusion detection systems (sensors, alarms, CCTV, etc.).
- Local security perimeter: implements the security measures controlling the access to the restricted area; i.e. access control mechanisms, identification and authentication control, local 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 alarm response company is short enough to prevent a successful attack.

O.SECURITY.CONTROL

Assigned personnel of the site or the systems for access control and surveillance respond to alarms (out of hours, alarm response is supplemented by an alarm response company). Technical security measures such as CCTV, motion sensors and similar kinds of sensors support the enforcement of the access control. These site 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 shall also be aware of the company policy regarding material destruction and backups and ‘working from home’ (if applicable).

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

O.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 or physical signature). Evidence of manipulation or improper observation of procedure shall invoke raising of a security incident.

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 shall be based on 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.
- An inactivity period for screen locking shall be established, requiring re-authentication for locking.

O.LOGICAL.ACCESS

The site enforces a physical separation between the secure area network and the internet. A firewall ensures that only defined services and defined connections are accepted (i.e. to local network machines and other sites by VPN). Access to the secure area network and related systems is restricted to authorized employees that work in the secure area or that are involved in the configuration tasks. Every user of an IT system has their own user account and password. All computer systems with access to sensitive data require successful authentication by user name and password and 802.1x certificate based authentication.

O.LOGICAL.OPERATION

All server and desktop equipment hard disks are encrypted. The equipment anti-virus software is updated periodically.

Backups will be created, stored and destroyed according to an approved procedure. Members of the development teams shall 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.INSTALL

The development machines shall 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 Lite 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.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 O.RIP O.AC	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.PASSWD 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.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

6 Extended Assurance Components Definition

No extended components are defined in this Site Security Target Lite.

7 Security Assurance Requirements

The security assurance requirements for this Site Security Target Lite are ALC_CMC.5, ALC_CMS.5, ALC_DVS.2 and ALC_LCD.1.

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

- ALC_CMC.5 (CM capabilities)
- ALC_CMS.5 (CM scope)
- ALC_DVS.2 (Development security)
- ALC_LCD.1 (Life-cycle definition)

The assurance requirements listed above fulfil the requirements of (4) because hierarchically higher components are used in this Site Security Target Lite compared to the Minimum Requirements in (5).

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

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

ALC_CMS.5: None

ALC_DVS.2: None

ALC_LCD.1: None

The following dependencies are not fulfilled or not completely fulfilled:

ALC_LCD.1: ALC_LCD.1 is part of this Site Security Target Lite but does not 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 ‘intended TOE’ are in the focus and described in this SST. These processes are subject of the evaluation of the site.

The term 'TOE' is replaced by ‘intended TOE’ or 'configuration item'.

7.1.1 Overview regarding CM capabilities (ALC_CMC)

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 (3) are defined for ALC_CMC.5. Since this SST claims ALC_CMC.5, 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-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 regarding Life Cycle, the following phases are relevant:

1. Silicon product architecture
2. Silicon product firmware development
3. Sample product (and FPGA prototype) firmware validation

7.2 Security Assurance Rationale

The security assurance requirements rationale maps the content elements of the selected assurance components of (2) to the security objectives defined in this Site Security Target Lite. 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 (3) according to the application notes in the process description (4) are written in italic. The term TOE can be replaced by configuration items or product.

7.2.1 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMC.5.1D: The developer shall provide the *intended TOE* and a reference for the *intended TOE*.	O.CM.LABEL	O.CM.LABEL ensures appropriate and consistent labelling as well as unique identification of the item.
ALC_CMC.5.2D: The developer shall provide the CM documentation.	O.CM.PROCESS	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures.
ALC_CMC.5.3D: The developer shall use a CM system	O.CM.PROCESS	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures.
ALC_CMC.5.1C: The *intended TOE* shall be labelled with its unique reference.	O.CM.LABEL	O.CM.LABEL ensures appropriate and consistent labelling as well as unique identification of the item.
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.CM.PROCESS	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures.
ALC_CMC.5.3C: **The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.**	O.CM.PROCESS	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures.
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.CM.LABEL	O.CM.LABEL ensures appropriate and consistent labelling as well as unique identification of the item.

ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	O.CM.PROCESS	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures.
ALC_CMC.5.6C: The CM system shall support the production of the *intended TOE* by automated means.	O.CM.PROCESS	The CMS system supports automated development of products.
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.CM.PROCESS O.CM.CHANGE.CONTROL O.AC	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures. All configuration items are kept under configuration control according to O.CM.CHANGE.CONTROL. O.CM.CHANGE.CONTROL is supported by O.AC such that logical access locally to development machines and CM system shall be limited to approved development team members and system administrators.
ALC_CMC.5.8C: **The CM system shall identify the configuration items that comprise the TSF.**	O.CM.PROCESS	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures.
ALC_CMC.5.9C: **The CM system shall support the audit of all changes to the *intended TOE* by automated means, including the originator, date, and time in the audit trail.**	O.CM.PROCESS	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures. The CM system supports automated development of products.
ALC_CMC.5.10C: **The CM system shall provide an automated means to identify all other configuration items**	O.CM.PROCESS	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures, and that the CM system supports automated CI dependency tracking.

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 *intended TOE* is generated.**	O.CM.PROCESS	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures, and that the CM system supports identification of TOE implementation representation elements.
ALC_CMC.5.12C: 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.5.13C: The CM plan shall describe how the CM system is used for the development of the *intended TOE*.	O.CM.PROCESS	CM process documentation is available and maintained according to O.CM.PROCESS.
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *intended TOE*.	O.CM.PROCESS O.CM.CHANGE.CONTROL	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures. All configuration items are kept under configuration control according to O.CM.CHANGE.CONTROL.
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.CM.PROCESS	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures.
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.CM.PROCESS	O.CM.PROCESS ensures the site is using the configuration management plan supported by tools and procedures.

TABLE 3 RATIONALE FOR ALC_CMC.5

7.2.2 Rationale for ALC_CMS.5

SAR	Security Objective	Rationale
ALC_CMS.5.1D: The developer shall provide a configuration list for the *intended TOE*.	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.5.1C: The configuration list shall include the following: the *intended TOE*; the evaluation evidence required by the SARs; the parts that comprise the *intended TOE*; the implementation representation; security flaw reports and resolution status; **and development tools and related information.**	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.5.2C: 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.5.3C: For each TSF relevant 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 on how to consider the configuration items in the configuration list (including developer information - no subcontractors are used).

TABLE 4 RATIONALE FOR ALC_CMS.5

7.2.3 Rationale for ALC_DVS.2

SAR	Security Objective	Rationale
ALC_DVS.2.1D: The developer shall produce and provide development		

security documentation.		
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 *intended TOE* design and implementation in its development environment.	O.PERIMETERS O.ALARM.RESPONSE O.SECURITY.CONTROL O.STAFF.ENGAGEMENT O.REVOKING O.VISITORSO.INTERNAL.MONITOR O.DATA.TRANSFER O.INTERNAL.SHIPMENT O.AC 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.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.
ALC_DVS.2.2C: **The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *intended TOE*.**	O.PERIMETERS O.ALARM.RESPONSE O.SECURITY.CONTROL O.STAFF.ENGAGEMENT O.REVOKING O.VISITORSO.INTERNAL.MONITOR O.DATA.TRANSFER O.INTERNAL.SHIPMENT O.AC O.PASSWD O.LOGICAL.ACCESS O.LOGICAL.OPERATION O.INSTALL O.RIP	See ALC_DVS.2.1C. In addition, the measures are appropriate for the type of development that will occur at the site.

TABLE 5 RATIONALE FOR ALC_DVS.2

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 O.CM.RECEPTION_CONTROL	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, O.CM.PROCESS, and O.CM.RECEPTION_CONTROL.
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 O.CM.RECEPTION_CONTROL	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.

The following sections identify the evidences provided by Huawei and describe how the Bristol site meets 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.

The site activities are performed using an IT infrastructure consisting of development workstations, servers and configuration management systems. All of these are provided, configured and maintained by Huawei.

The IT infrastructure consists of local and remote equipment with encrypted offsite backup. Huawei provides, configures and maintains the local workstations and router such that they are secure. The workstations are configured such that any assets are contained within encrypted containers, disks or volumes.

To enable that the site participates in the development of products Huawei provides services to setup the necessary development computers (tools, user accounts, etc.) and configuration management systems (user accounts, repositories etc.).

To enable the site to realize shipment such that assurance of integrity is assured throughout, transport of physical security objects will adhere to the materials transfer procedure.

Physical assets will be securely disposed of as per the prescribed policy.

To define the participation of the site in the development while maintaining quality, for each product, the site and other sites partaking in the product life-cycle agree on the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results by the project team.

The site follows the development processes of Huawei. Applicable policies and processes are documented and available from Huawei to the site.

8.1 Services of the Site

The following services and/or processes provided by Bristol CC Design Centre are in the scope of the evaluation process:

- Hardware and software architecture of secure integrated circuits up to EAL6.

- Development and testing of firmware for secure integrated circuits up to EAL6.
- The site uses a shipment method such that assurance of integrity is assured throughout transport of physical security objects.

8.2 SAR Rationale

The Security Assurance Requirements rationale does not explicitly address the developer action elements defined in (3) because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the preparation for the site visit. In addition, this includes that the procedures are applied as written and explained in the documentation.

8.2.1 ALC_CMC

The security assurance requirements of the assurance component ALC_CMC.5 are suitable to support the development of a TOE product due to the formalized acceptance process. This comprises the identification of all configuration items and the automated control and tracking within the development environment. 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.

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.

8.2.2 ALC_CMS

The security assurance requirements of the assurance component ALC_CMS.5 support the control of the TOE 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.

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.

8.2.3 ALC_DVS

The security assurance requirements of the assurance component ALC_DVS.2 is required since a high attack potential is assumed for potential attackers. The configuration items and information handled at the site during development and testing of the intended TOE can be used by potential attackers. Therefore, the handling and storage of these items must be sufficiently protected.

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.

8.2.4 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. The assurance requirements are considered to be suitable to support the application of the site evaluation results for the development of an intended TOE.

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

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

8.3 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.2.1C, ALC_DVS.2.2C and ALC_CMS.5.7C provide this fulfilment.

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

O.ALARM.RESPONSE

ALC_DVS.2.1C and ALC_DVS.2.2C require 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.5.2D and ALC_CMC.5.3D require a CM system and CM documentation.

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.

ALC_CMC.5.3C requires that 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 requires a unique identification of all configuration items by the CM system.

ALC_CMC.5.6C requires the CM system to support the production of the intended TOE by automated means.

ALC_CMC.5.7C requires the CM system to ensure that the person responsible for accepting a configuration items into CM is not the person who developed it.

ALC_CMC.5.8C requires the CM system to identify the configuration items that comprise the TSF.

ALC_CMC.5.9C requires the CM system to support the audit of all changes to the intended TOE by automated means, including the originator, data and time in the audit trail.

ALC_CMC.5.10C requires the CM system to provide and automated means to identify all other configuration items that are affected by the changes of a given configuration item.

ALC_CMC.5.11C requires the CM system to be able to identify the version of the implementation representation from the intended TOE is generated.

ALC_CMC.5.12C requires that the CM documentation shall include a CM plan.

ALC_CMC.5.13C and ALC_CMC.5.14C requires that the CM plan describe how CM system is used for the development of the product and how new configuration items are accepted into the system.

ALC_CMC.5.15C requires the CM Plan to demonstrate that all configuration items are being maintained. Together with ALC_CMC.5.16C the CM plan shall demonstrate how CM System is being operated in accordance with the CM plan documentation that includes a CM plan.

ALC_CMS.5.1D requires the developer to provide a configuration list for the intended TOE.

ALC_CMS.5.1C requires the configuration list to include the evaluation evidence for the fulfilment of the SARs and related information.

ALC_CMS.5.2C requires the configuration list to uniquely identify the configuration items.

ALC_CMS.5.3C requires that for each TSF relevant configuration item, the configuration list shall indicate the developer the item.

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 intended TOE.

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

O.CM.CHANGE.CONTROL

ALC_CMC.5.5C 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.5.7C requires the CM system to ensure that the person responsible for accepting a configuration items into CM is not the person who developed it.

ALC_CMC.5.8C requires the CM system to identify the configuration items that comprise the TSF.

ALC_CMC.5.9C requires the CM system to support the audit of all changes to the intended TOE by automated means, including the originator, data and time in the audit trail.

ALC_CMC.5.10C requires the CM system to provide and automated means to identify all other configuration items that are affected by the changes of a given configuration item.

ALC_CMC.5.11C requires the CM system to be able to identify the version of the implementation representation from the intended TOE is generated.

ALC_CMC.5.12C requires that the CM documentation shall include a CM plan.

ALC_CMC.5.13C and ALC_CMC.5.14C require that the CM plan describe how CM system is used for the development of the product and how new configuration items are accepted into the 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 intended TOE.

Thereby this objective is suitable to meet the Security Assurance Requirement

O.CM.LABEL

ALC_CMC.5.1D requires the developer to use a CM system.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.3C by identifying uniquely the configuration items and ALC_CMS.5.3C the owner of them (developer).

ALC_CMC.5.4.C requires a unique identification of all configuration items by the CM system.

ALC_CMS.5.1.D requires the developer to provide a configuration list for the intended TOE.

ALC_CMS.5.1.C requires the configuration list to include the evaluation evidence for the fulfilment of the SARs and related information.

ALC_CMS.5.2.C requires the configuration list to uniquely identify the configuration items.

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 intended TOE.

The objective meets the set of Security Assurance Requirements.

O.CM.RECEPTION.CONTROL

ALC_DVS.2.1C provides sufficient security measures control in order to keep confidentiality of the intended TOE, and ALC_DVS.2.2C justifies these measures. Furthermore, the integrity of the TOE is required under ALC_CMC.5.2C by uniquely identifying the items.

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

O.DATA.TRANSFER

ALC_DVS.2.1C requires that all information considered sensitive will be manipulated and transferred under proper security controls, and ALC_DVS.2.2C justifies these measures

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

O.INSTALL

Integrity of the devices used in order to manage, develop or test any critical or sensitive data is required under ALC_DVS.2.1C, and ALC_DVS.2.2C justifies these measures as appropriate for the asset(s) in question.

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

O.INTERNAL.MONITOR

Internal audits are performed periodically. This is required under ALC_DVS.2.1C, and ALC_DVS.2.2C justifies this measure.

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 required to be controlled under strict conditions. This is required by ALC_DVS.2.1C, and ALC_DVS.2.2C justifies these measures as appropriate for the asset(s) in question.

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.2.1C, and ALC_DVS.2.2C justifies these measures.

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

O.LOGICAL.OPERATION

ALC_DVS.2.1C requires sufficient logical security measures to keep integrity and confidentiality of the assets in the devices, and ALC_DVS.2.2C justifies these measures.

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

O.PASSWD

The DSD describes in the detail the security related topics for logical security as required by ALC_DVS.2.1C in relation to logical access to the assets. Those are protected by different stopping layers only accessible by proper password check controls. These measures are justified by ALC_DVS.2.2C.

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

O.PERIMETERS

ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the intended TOE, and ALC_DVS.2.2C justifies these measures.

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 required under ALC_DVS.2.1C, and ALC_DVS.2.2C justifies these measures.

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

O.RIP

This objective is covered by the asset management described in the internal policies. Also, any material that could be stolen will be tracked by the company with as described in ALC_DVS.2.1C in order to assess the physical and logical security implemented in the site, and ALC_DVS.2.2C justifies these measures.

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_DVS2.1C. 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. ALC_DVS.2.2C justifies these measures. Therefore this objective is suitable to meet the Security Assurance Requirement.

O.STAFF.ENGAGEMENT

ALC_DVS.2.1C requires the description of personnel security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment. ALC_DVS.2.2C justifies these measures. Therefore the objective fulfils this combination of Security Assurance Requirements.

O.VISITORS

ALC_DVS.2.1C requires that all visitors are being monitored all the time in order to mitigate any threat related with the development activities performed in the Bristol CC Design Centre. This is covered by the internal policies such that every visitor must be chaperoned when they enter a restricted zone. ALC_DVS.2.2C justifies these measures. Therefore this objective is suitable to meet the Security Assurance Requirement.

8.4 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.

TABLE 8 MAPPING FOR ALC_CMC.5

TABLE 9 MAPPING FOR ALC_CMS.5

TABLE 10 MAPPING FOR ALC_DVS.2

TABLE 11 MAPPING FOR ALC_LCD.1

9 References

External

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

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

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

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

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

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