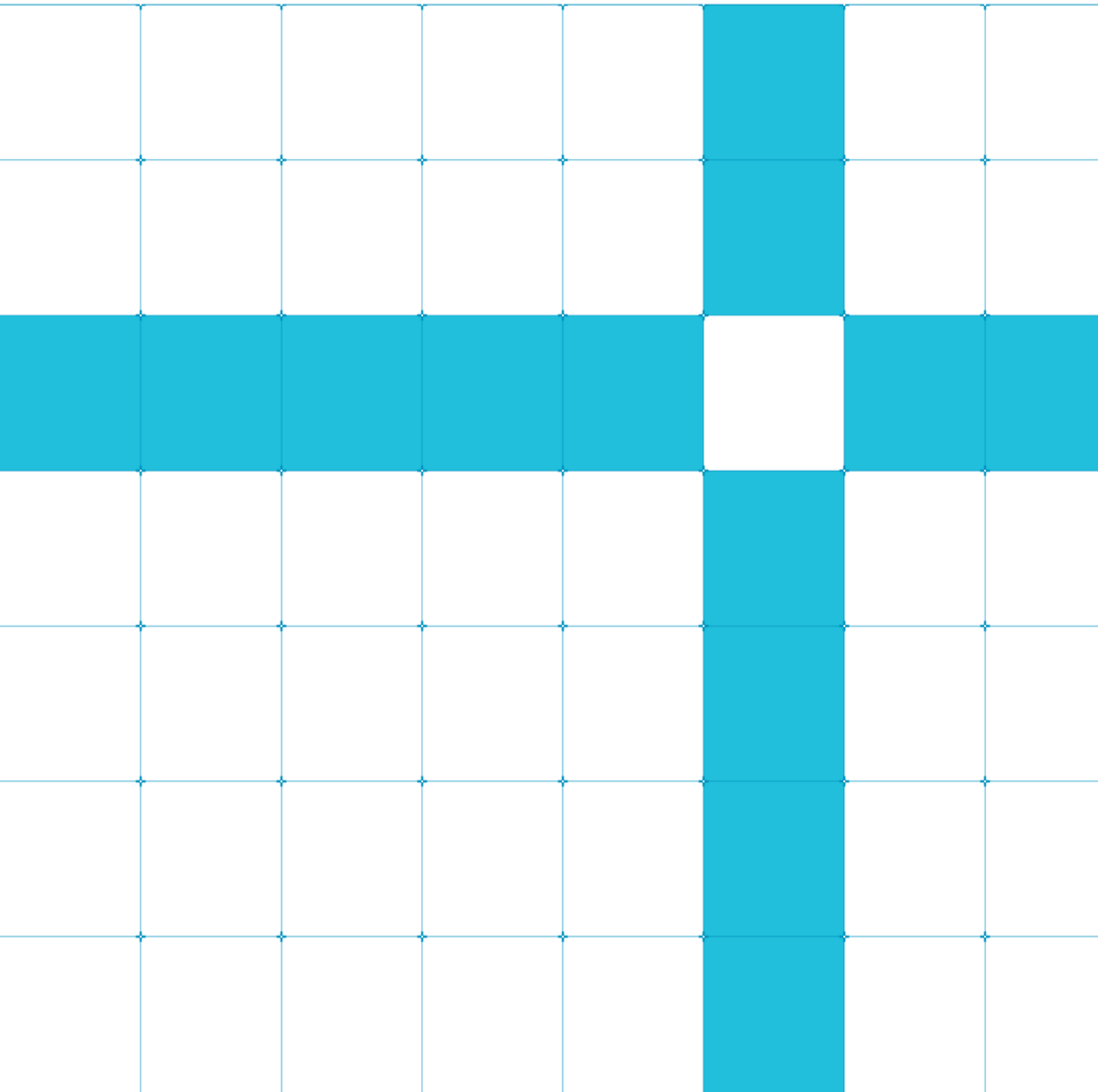
Arm Public Site Security Target
Sophia Antipolis

Version 2.0



Arm Site Security Target

Sophia Antipolis

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.

Release Information

Document History

Version	Date	Confidentiality	Change
1.0	14 January 2020	Non-Confidential	First Release
2.0	20 July 2022	Non-Confidential	Second release

Non-Confidential Proprietary Notice

This document is protected by copyright and other related rights and the practice or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm. **No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.**

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether implementations infringe any third party patents.

THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document consists solely of commercial items. You shall be responsible for ensuring that any use, duplication or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word "partner" in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

If any of the provisions contained in these terms conflict with any of the provisions of any click through or signed written agreement covering this document with Arm, then the click through or signed written agreement prevails over and supersedes the conflicting provisions of these terms. This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of the Agreement shall prevail.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. Please follow Arm's trademark usage guidelines at **http://www.arm.com/company/policies/trademarks**.

Copyright © 2019-2021 Arm Limited or its affiliates. All rights reserved.

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

LES-PRE-20349

Confidentiality Status

This document is Non-Confidential. The right to use, copy and disclose this document may be subject to license restrictions in accordance with the terms of the agreement entered into by Arm and the party that Arm delivered this document to.

Unrestricted Access is an Arm internal classification.

Product Status

The information in this document is Final, that is for a developed product.

Web Address

http://www.arm.com

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Contents

1 About this document 6
1.1. Scope 6
1.2. Intended audience 6
1.3. References 6
1.4. Terminology 7
1.5. Terms and Abbreviations 7

2 Introduction 8
2.1. SST reference 8
2.2. Site reference 8
2.3. Site description 8
2.3.1 Physical scope 8
2.3.2 Logical scope 8

3 Conformance claim 9

4 Security Problem Definition 10
4.1. Assets 10
4.2. Threats 10
4.3. Organizational Security Policies 11
4.4. Assumptions 12

5 Security objectives 13
5.1. Security objectives rationale 15
5.1.1 Mapping of security objectives 16

6 Extended assurance components definition 17

7 Security assurance requirements 18
7.1. Application notes and refinements 18
7.1.1 CM capabilities (ALC_CMC.5) 18
7.1.2 CM Scope (ALC_CMS.5) 18
7.1.3 Delivery Procedures (ALC_DEL.1) 18
7.1.4 Development Security (ALC_DVS.2) 19
7.1.5 Flaw remediation (ALC_FLR.1) 19
7.1.6 Lifecycle definition (ALC_LCD.1) 19
7.2. Security requirements rationale 19
7.2.1 Dependencies 19
7.2.2 Mapping 20

8 Site summary specification 26

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

8.1. Preconditions required by the site 26
8.2. Services of the site 26
8.3. Objectives rationale 27
8.4. Security Assurance Requirements rationale 28
8.4.1 CM capabilities (ALC_CMC.5) 28
8.4.2 CM scope (ALC_CMS.5) 29
8.4.3 Delivery (ALC_DEL.1) 30
8.4.4 Development security (ALC_DVS.2) 30
8.4.5 Basic flaw remediation (ALC_FLR.1) 30
8.4.6 Lifecycle definition (ALC_LCD.1) 30
8.5. Assurance measure rationale 30
8.6. Mapping of the evaluation documentation 34

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

1 About this document

1.1. Scope

This document is the Site Security Target (SST) of the Arm Sophia Antipolis site. This document is based on the Eurosmart *Site Security Target Template* [1] with adaptions such that it fits the site (that is, a development site with no production).

1.2. Intended audience

This document describes the site security of the development environment at the Arm Sophia Antipolis site. It is primarily written for the user of the site

1.3. References

This document refers to the following publications.

Reference	Title
[1]	*Site Security Target Template*, *Version 1.0,* published by Eurosmart, Eurosmart, 21.06.2009
[2]	*Security IC Platform Protection Profile with Augmentation Packages*, Version 1.0, Eurosmart, 13.01.2014
[3]	*Common Criteria for Information Technology Security Evaluations, Part 1: Introduction and General Model,* Version 3.1, Revision 5, Common Criteria, April 2017
[4]	*Common Criteria for Information Technology Security Evaluation, Part3: Security Assurance Requirements*, Version 3.1, Revision 5, Common Criteria, April 2017
[5]	*Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology*, Version 3.1, Revision 5, Common Criteria, April 2017
[6]	*Supporting Document Guidance, Site Certification*, Version 1.0, Revision 1, CCDB-2007-11-001, Common Criteria, October 2007
[7]	*Arm Sophia Antipolis Lifecycle Support, version 2.0*, 2022
[8]	*IS01 - SEC: SecurCore MSSR Security Policy Manual, Supporting DSD Documentation, 01/07/2022*

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

1.4. Terminology

This document uses the term *client* with the following definition:

Client The site providing the SST may operate as a subcontractor of the TOE manufacturer. The term *client* is used here to define this business connection. It is used instead of customer since the terms *customer* and *consumer* are reserved in CC. In this document, the terms *customer* and *consumer* are only used in the sense of the CC.

1.5. Terms and Abbreviations

This document uses the following terms and abbreviations.

Term	Meaning
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
IC	Integrated Circuit
IP	Intellectual Property
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SPD	Security Problem Definition
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

2 Introduction

2.1. SST reference

The SST is identified and referenced as follows:

Title	Arm Public Site Security Target Sophia Antipolis
Version	2.0
Reference	PJDOC-466751330-14447
Issue date	20 July 2022
Product type	Security IC
EAL level	EAL6+ assurance components

2.2. Site reference

The site is identified and referenced as follows:

Company	Arm
Name of the site	Arm Sophia Antipolis
Location	738 Avenue de Roumanille 06410 Biot - Sophia Antipolis, France.

2.3. Site description

The Arm Sophia Antipolis site performs activities related to the development of secure ICs. Within the development area, only members of the development team are entitled to access sensitive information, including source code and confidential documentation. To enforce such access restriction, a combination of physical, procedural, personnel, and logical measures have been installed.

2.3.1 Physical scope

The Arm Sophia Antipolis site comprises two 2-floor buildings names “Art” and “Science’’. The following areas are in the scope of the SST:

- Room A0R05: Secure room in Art building where intended TOE development occurs.
- Four patch rooms where TOE-related assets are transmitted. They are located in::
  - Room G052A: Patch Room located in Art Building, Ground Floor
  - Room 1024: Patch room located in Art Building, Upper Floor
  - Room G058: Patch Room located in Science Building, Ground Floor
  - Room 1048: Patch Room located in Science Building, Upper Floor. The local infrastructure such as CCTV is located in this room as well.

2.3.2 Logical scope

The Arm Sophia Antipolis site belongs to the general IP group, in the CPU subgroup. The site in scope here is dedicated to secure core IP development. The activities of the site cover the lifecycle phase IC Development (Phase 2) as defined in *Security IC*

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Platform Protection Profile with Augmentation Packages, Version 1.0, Eurosmart, 13.01.2014 [2]. Supporting services are provided within the same building, such as physical site security, local IT management, HR related services, and facilities management.

See 8.2 Services of the site for more information on the services provided.

3 Conformance claim

This SST is conformant with Common Criteria Version 3.1:

- *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017* [3].
- *Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, 5, April 2017* [4].

For the evaluation, the following methodology will be used:

- *Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1, 5, April 2017* [5].
- *Supporting Document, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007* [6].

This SST is CC Part 3 conformant.

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

- ALC_CMC.5.
- ALC_CMS.5.
- ALC_DEL.1.
- ALC_DVS.2.
- ALC_FLR.1.
- ALC_LCD.1.

The chosen assurance components are derived from the assurance level EAL6+ of the *Life-cycle Support* assurance class. The augmentation is related to ALC_FLR.1. For the assessment of the security measures, attackers with a high attack potential are assumed. Therefore, this site supports potentially augmented product evaluations up to EAL6.

[1] Because the tools and techniques used are defined upfront by the client (see the A.Project-Setup assumption in 4.4 Assumptions), the site does not contribute to ALC_TAT and does not have any negative impact to it. Therefore, the site does not claim conformance to ALC_TAT.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

4 Security Problem Definition

The SPD comprises security problems derived from threats against the assets handled by the site.

4.1. Assets

The following assets are handled at the Arm Sophia Antipolis site:

Asset	Description
Development data	The site has access to (and optionally copies) electronic development data (specifications, guidance documentation, source code, etc.) related to developed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected.
Development systems	To perform its development activities, the site uses a combination of hardware and software, including tools (for example compilers) to transform source code (and potentially the libraries that come with these tools) into binaries. The integrity of these tools (running on remote development computers) must be protected.
IT infrastructure	To perform its development activities, the site is connected to an external provider that safeguards the development data and a significant part of the development systems. The combination of hardware and software used to allow the development systems access the assets is considered both from this site and the external provider. The integrity of this infrastructure must be protected.
Physical security objects	The site has physical security objects (printed documents, media used to store development data, etc.) related to developed TOEs. Both the integrity and the confidentiality of these must be protected.
Finished product	The site handles delivery of the intended TOE to be used by the customer. Both the integrity and the confidentiality must be protected.

Table 1 Assets handled at the site

4.2. Threats

The following threats are handled at the Arm Sophia Antipolis site:

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Threat	Description
T.Smart.Theft	An attacker tries to access sensitive areas of the site for manipulation or theft of assets. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered.
T.Rugged.Theft	An attacker with specialized equipment for burglary, who may be paid to perform the attack, tries to access sensitive areas and manipulate or steal assets.
T.Computer-Net	A possibly paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to (1) development data with the intention to violate confidentiality and possibly integrity or (2) development computers with the intention to modify the development process at the site.
T.Unauthorised-Staff	Employees or subcontractors not authorized to get access to assets violating the confidentiality and possibly the integrity of products.
T.Staff.Collusion	An attacker tries to get access to assets by getting support from one employee through extortion or bribery.
T.Attack-Transport	An attacker might try to get development data and finished products during the internal shipment and/or the external delivery. The target is to compromise confidential information or violate the integrity of the products during the stated internal shipment and/or the external delivery process to allow a modification or the retrieval of confidential information.

Table 2 Threats handled at the site

4.3. Organizational Security Policies

The following policies are handled at the Arm Sophia Antipolis site:

Policy	Description
P.Config-Items	The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of items that are created, generated, developed or used at the site as well as the received and transferred and/or provided items.
P.Config-Control	The procedures for setting up the development process for a new product as well as the procedure that allows changes of the initial setup for a current product shall only be applied by authorized personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes.
P.Config-Process	The services and/or processes provided by the site are controlled in the configuration management plan. This comprises tools used for the development of the product, the management of flaws and optimization of the process flow as well as the documentation that describes the services and/or processes provided by the site.
P.Transfer-Data	Any sensitive configuration items (e.g. development data, finished products, etc.) are encrypted to ensure confidentiality and integrity of the data.
P.Lifecyle-Doc	The site follows the life cycle documentation that describes: (1) Description of configuration management systems and their usage; (2) A configuration items list; (3) Site security; (4) The development process; (5) The development tools; (6) Flaw remediation process; (7) Delivery procedure.

Table 3 Policies handled at the site

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

4.4. Assumptions

The following assumptions are handled at the Arm Sophia Antipolis site:

Assumption	Description
A.Inherit-secure-IT	The local IT equipment (for example workstations) is connected to a secure remote IT-infrastructure through a secure (encrypted) network connection. The local workstations, the remote secure IT-infrastructure and the secure connection to it satisfy all relevant ALC requirements and are provided and managed by arm. The workstations are configured such that any assets are contained within encrypted containers.
A.Remote.Services	The facilities required to safeguard the remote IT-infrastructure and to establish a secure link to the development site have all the necessary security measures to provide a secure environment. The IT infrastructure is remotely managed. This approach allows to provide 24/7 support.
A.Trusted-personnel	Arm staff from other locations and external parties providing services to this site are trustworthy. External parties are bound to agreements in accordance to the site's requirements.
A.Secure-destruct	Physical security objects are securely destroyed in order to prevent information leakage.
A.Project-Setup	The site participates in the development of products. For each product the site and the client agree on the following items: • The activities to be performed by the site. • The specifications of the input for the site including tools. • The acceptance of the results by the client. • The used configuration management methods and tools. • The delivery details of any security relevant item.

Table 4 Assumptions handled at the site

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

5 Security objectives

The security objectives are related to physical, technical, and organizational security measures, the configuration management as well as the internal shipment and/or the external delivery.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Objective	Description
O.Physical-Access	The combination of physical partitioning between the different access control levels together with technical and organisational security measures allows a sufficient separation of employees to enforce the “need to know” principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorised people. The access control measures ensure that only registered employees can access restricted areas. Assets are handled in restricted areas only.
O.Security-Control	Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers.
O.Alarm-Response	The technical and organisational security measures ensure that an alarm is generated before an unauthorised person gets access to any asset. After the alarm is triggered the unauthorised person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack.
O.Internal-Monitor	The site performs security management meetings at least every six months. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures.
O.Maintain-Security	Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorised employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.
O.Logical-Access	The site enforces a logical separation between the internal network and the internet by a firewall. The firewall ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into a development network and an office network. Additional specific networks for production and configuration are physically separated from any internal network to enforce access control. Access to the development network and related systems is restricted to authorised employees that work in the related area or that are involved in the configuration tasks or the development systems. Every user of an IT system has its own user account and password. An authentication using user account and password is enforced by all computer systems.
O.Logical-Operation	Development computers enforce that every user authenticates using a password and has a unique user ID, and all development systems and IT infrastructure are kept up to date. The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.
O.LifeCycle-Doc	The site uses life cycle documentation that describes: (1) Description of configuration management systems and their usage; (2) A configuration items list; (3) Site security; (4) The development process; (5) The development tools; (6) Flaw remediation process; (7) Delivery procedure.
O.Config-Items	The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify configuration items and allow an assignment to the client. Also, the internal procedures and guidance are covered by the configuration management.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

O.Config-Control	The site applies a release procedure for the setup of the production process for each new product. In addition, the site has a process to classify and introduce changes for services and/or processes of released products. Minor changes are handled by the site, major changes must be acknowledged by the client. A designated team is responsible for the release of new products and for the classification and release of changes. This team comprises specialists for all aspects of the services and/or processes. The services and/or processes can be changed by authorised personnel only. Automated systems support configuration management.
O.Config-Process	The site controls its services and/or processes using a configuration management plan. The configuration management is controlled by tools and procedures for the development of the product, for the management of flaws and optimisations of the process flow as well as for the documentation that describes the services and/or processes provided by a site.
O.Staff-Engagement	All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.
O.Transfer-Data	Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorised employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected.
O.Control-Scrap	The site has measures in place to securely destruct assets (e.g. paper shredder).

Table 5 Objectives for the site

5.1. Security objectives rationale

The SST includes a security objectives rationale with two parts. The first part includes a tracing which shows how the threats and OSPs are covered by the security objectives. The second part include a justification that shows that all threats and OSPs are effectively addressed by the security objectives. The *Rationale* column under 5.1.1 Mapping of security objectives gives a brief explanation.
See 8.3 Objectives rationale for a detailed rationale.

Note:
The assumptions defined in this SST cannot be used to cover any threat or OSP of the site. They are seen as pre-conditions fulfilled either by the site providing the sensitive configuration items or by the site receiving the sensitive configuration items. Therefore, they do not contribute to the security of the site under evaluation.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

5.1.1 Mapping of security objectives

Threat and OSP	Security objective(s)	Rationale
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat.
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat.
T.Computer-Net	O.Internal-Monitor O.Logical-Access O.Logical-Operation O.Maintain-Security O.Staff-Engagement	The development network is not connected to anything that an attacker could use to set up a remote connection. Systems are properly maintained.
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Control-Scrap	Physical and logical access control prohibits access to assets. Secure destruction of scrap limits the amount of assets
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Transfer-Data O.Control-Scrap	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees limits unauthorized access to assets.
T.Attack-Transport	O.LifeCycle-Doc O.Transfer-Data	The data transfer method and the organizational measures ensure that confidentiality is preserved, and that integrity changes of delivered configuration items are detected and appropriately responded upon.
P.Config-Items	O.Config-Items	The security objective directly enforces the OSP.
P.Config-Control	O.Config-Control	The security objective directly enforces the OSP.
P.Config-Process	O.Config-Process	The security objective directly enforces the OSP.
P.Transfer-Data	O.Transfer-Data	The security objective directly enforces the OSP.
P.Lifecycle-Doc	O.Lifecycle-Doc	The security objective directly enforces the OSP.

Table 6 Threats - Security objectives rationale

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

6 Extended assurance components definition

No extended components are defined in this SST.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

7 Security assurance requirements

The Security Assurance Requirements (SARs) are chosen from the class ALC (Life-cycle support) as defined in (Common Criteria for Information Technology Security Evaluation, Part3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017):

- CM capabilities (ALC_CMC.5).
- CM scope (ALC_CMS.5).
- Delivery (ALC_DEL.1).
- Development Security (ALC_DVS.2).
- Flaw remediation (ALC_FLR.1).
- Life-cycle definition (ALC_LCD.1).

These SAR fulfil the requirements of (Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007) because hierarchically higher components are used in this SST. In addition, the minimum set of SARs is extended by SAR of the assurance components for Delivery (ALC_DEL), Flaw remediation (ALC_FLR), and Life-cycle definition (ALC_LCD.1).

7.1. Application notes and refinements

The description of the site certification process (Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007) includes specific application notes. The main item is that a product that is considered as intended TOE is not available during the evaluation. Because the term *TOE* is not applicable in the SST, the associated processes for the handling of products, or *intended TOEs* are in the scope of this SST and are described in this document. These processes are subject of the evaluation of the site.

7.1.1 CM capabilities (ALC_CMC.5)

See the *Application Notes for Site Certification* section under *5.1 Application Notes for ALC_CMC* in *Supporting Document Guidance, Site Certification, Version 1.0, Revision 1* (Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007).

See the *Refinement* section under *6.2.1.4 Refinements regarding Development Security (ALC_CMC)* in *Security IC Platform Protection Profile with Augmentation Packages, Version 1.0* (Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014).

7.1.2 CM Scope (ALC_CMS.5)

See the *Application Notes for Site Certification* section under *5.2 Application Notes for ALC_CMS* in *Supporting Document Guidance, Site Certification, Version 1.0, Revision 1* (Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007).

See the *Refinement* section under *6.2.1.3 Refinements regarding Development Security (ALC_CMS)* in *Security IC Platform Protection Profile with Augmentation Packages, Version 1.0* (Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014).

7.1.3 Delivery Procedures (ALC_DEL.1)

See the *Application Notes for Site Certification* section under *5.3 Application Notes for ALC_DEL* in *Supporting Document Guidance, Site Certification, Version 1.0, Revision 1* (Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007).

See the *Refinement* section under *6.2.1.1 Refinements regarding Development Security (ALC_DEL)* in *Security IC Platform Protection Profile with Augmentation Packages, Version 1.0* (Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014).

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

7.1.4 Development Security (ALC_DVS.2)

See the *Application Notes for Site Certification* section under *5.4 Application Notes for ALC_DVS* in *Supporting Document Guidance, Site Certification, Version 1.0, Revision 1* (Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007).

See the *Refinement* section under *6.2.1.2 Refinements regarding Development Security (ALC_DVS)* in *Security IC Platform Protection Profile with Augmentation Packages, Version 1.0* (Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014).

7.1.5 Flaw remediation (ALC_FLR.1)

See the *Application Notes for Site Certification* section under *5.5 Application Notes for ALC_FLR* in *Supporting Document Guidance, Site Certification, Version 1.0, Revision 1* (Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007).

7.1.6 Lifecycle definition (ALC_LCD.1)

See the *Application Notes for Site Certification* section under *5.6 Application Notes for ALC_LCD* in *Supporting Document Guidance, Site Certification, Version 1.0, Revision 1* (Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007).

7.2. Security requirements rationale

7.2.1 Dependencies

The dependencies for the assurance requirements are as follows:

ALC_CMC.5	ALC_CMS.1, ALC_DVS.2, and ALC_LCD.1.
ALC_CMS.5	None.
ALC_DEL.1	None.
ALC_DVS.2	None.
ALC_FLR.1	None.
ALC_LCD.1	None.

Some of the dependencies are not (completely) fulfilled. ALC_LCD.1 is only partially fulfilled as the site does not represent the entire development environment. This is in-line with and further explained in *Supporting Document Guidance, Site Certification, Version 1.0, Revision 1* (Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007) under *5.1 Application Notes for ALC_CMC*.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

7.2.2 Mapping

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

SAR	Security objective(s)	Rationale
ALC_CMC.5.1C The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling.	O.Config-Items O.LifeCycle-Doc	Appropriate and consistent labelling is ensured through the application (O.Config-Items) of the CM-Plan (O.LifeCycle-Doc).
ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.	O.LifeCycle-Doc	The method used to uniquely identify the configuration items is described in the CM-Plan (O.LifeCycle-Doc)
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.LifeCycle-Doc	The adequate and appropriate acceptance procedures for configuration items are described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.	O.LifeCycle-Doc O.Config-Items	Unique identification of all CIs is realized by performing the CM activities (O.Config-Items) in accordance with the CM-Plan (O.LifeCycle-Doc)
ALC_CMC.5.5C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.LifeCycle-Doc O.Config-Control O.Config-Process O.Logical-Access	The configuration management systems (O.Config-Control) used (O.Config-Process) according to the CM-Plan (O.LifeCycle-Doc) enforces automated measures (O.Logical-Access) such that only authorized changes are made to the configuration items.
ALC_CMC.5.6C The CM system shall support the production of the intended TOE by automated means.	O.LifeCycle-Doc O.Config-Control O.Config-Process	The software on the development computers (O.Config-Control) supports automated production of products when used (O.Config-Process) in accordance with the CM-Plan (O.LifeCycle-Doc)
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.LifeCycle-Doc O.Config-Control	As described in the CM-Plan (O.LifeCycle-Doc) the activities performed (O.Config-Control) are such 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 clearly identify the configuration items that comprise the TSF.	O.LifeCycle-Doc O.Config-Items	The CM-Plan (O.LifeCycle-Doc) identifies the configuration items that comprise the TSF, supported by the configuration management system (O.Config-Items).
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.Config-Control O.LifeCycle-Doc	As described in the CM_Plan (O.LifeCycle-Doc) the configuration management systems (O.Config-Control) are configured such that an audit trail (showing originator, date and time) is automatically generated.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ALC_CMC.5.10C The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O.Config-Control O.LifeCycle-Doc O.Config-Items	As described in the CM_Plan (O.LifeCycle-Doc) the configurations management system and software installed on the development workstations and servers (O.Config-Control) provide automated means to identify all other configuration items (O.Config-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 intended TOE is generated.	O.Config-Control O.LifeCycle-Doc O.Config-Items	As described in the CM_Plan (O.LifeCycle-Doc) the configuration management system (O.Config-Control) identifies the version of the implementation representation (O.Config-Items) from which the intended TOE is generated through baselines.
ALC_CMC.5.12C The CM documentation shall include a CM plan.	O.LifeCycle-Doc O.Config-Control O.Config-Process	The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan, and is applied by O.Config-Control and O.Config-Process.
ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the intended TOE.	O.LifeCycle-Doc O.Config-Control O.Config-Process	The life cycle documentation (O.LifeCycle-Doc) describes how the CM system is used for the development of the product, and is applied by O.Config-Control and O.Config-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.LifeCycle-Doc	The acceptance procedures for modified or newly created configuration items are described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMC.5.15C The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.LifeCycle-Doc	All configuration items are listed in the CI-list (O.LifeCycle-Doc).
ALC_CMC.5.16C The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.	O.Config-Control O.LifeCycle-Doc	The CI-list (O.LifeCycle-Doc) is generated from the configuration management systems (O.Config-Control).

Table 7 Rationale for ALC_CMC.5

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

SAR	Security objective	Rationale
ALC_CMS.5.1C The configuration list includes the following: the intended TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the intended TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) includes a CM-Plan and a CI-List with the items required by ALC_CMS.5.1C
ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.	O.LifeCycle-Doc	The CI-List (O.LifeCycle-Doc) uniquely identifies the configurations items as described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMS.5.3C For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.	O.LifeCycle-Doc	The CI-List (O.LifeCycle-Doc) indicates the developer/subcontractor for each configuration items as described in the CM-Plan (O.LifeCycle-Doc).

Table 8 Rationale for ALC_CMS.5

SAR	Security objective(s)	Rationale
ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the intended TOE to the consumer.	O.LifeCycle-Doc O.Transfer-Data	All external deliveries are done according to O.LifeCycle-Doc supporting confidentiality and integrity (O.Transfer-Data).
ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the intended TOE to the consumer.	O.LifeCycle-Doc O.Transfer-Data	All external deliveries are done according to O.LifeCycle-Doc supporting confidentiality and integrity (O.Transfer-Data).

Table 9 Rationale for ALC_DEL.1

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

SAR	Security objective(s)	Rationale
ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment.	O.LifeCycle-Doc O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Control-Scrap O.Staff-Engagement O.Transfer-Data	The development security documentation (O.LifeCycle-Doc) describes the physical (O.Physical-Access, O.Security-Control, O.Alarm-Response), procedural (O.Internal-Monitor, O.Maintain-Security, O.Control-Scrap), personnel (O.Staff-Engagement), and other(O.Logical-Access, O.Logical-Operation) 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 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.LifeCycle-Doc	The development security documentation (O.LifeCycle-Doc) justifies the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE.

Table 10 Rationale for ALC_DVS.2

SAR	Security objective	Rationale
ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the intended TOE.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) includes a flaw remediation plan.
ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) specifies required details to identify security flaws.
ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) identifies the corrective actions for each security flaw.
ALC_FLR.1.4.C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to intended TOE users.	O.LifeCycle-Doc	The life cycle documentation (O.LifeCycle-Doc) describes the methods for users to identify and resolve security flaws.

Table 11 Rationale forALC_FLR.1

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

SAR	Security objective	Rationale
ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the intended TOE.	O.LifeCycle-Doc	The model used to develop the intended TOE is described in the life cycle documentation (O.LifeCycle-Doc).
ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the intended TOE.	O.LifeCycle-Doc	The life cycle model as described in the life cycle documentation (O.LifeCycle-Doc).

Table 12 Rationale for ALC_LCD.1

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

8 Site summary specification

8.1. Preconditions required by the site

Precondition	Assumption
IT personnel outside Sophia Antipolis provide the necessary systems engineering support to the site in order to design, implement and maintain the necessary IT infrastructure required by the development team in order to perform TOE development and testing.	A.Inherit-secure-IT
The external party provides equivalent certified facilities to provide the required environmental site security to the IT infrastructure. IT administration is handled remotely. Final access to development data is by no means granted to such groups.	A.Remote-Services
Teams based outside Sophia Antipolis are bound to the global security awareness program. External parties supporting arm are bound to agreements in accordance to the site's requirements.	A.Trusted-personnel
Physical assets are securely destroyed in a way that sensitive information can by no means be recovered.	A.Secure-destruct
The client needs to setup and maintain the used configuration management systems and provide a project specific CM plan. This includes the setup and maintenance of user accounts in the project repositories and other required configuration management tools. The client needs to agree about the configuration management methods and the usage of the configuration management tools. The configuration management methods and tools by the client ensure the correct handling of the configuration items according to Common Criteria. For each project setup, the client needs to agree on the activities to be performed by the site, the specifications of the input for the site, the provided development tools and the acceptance of the results from the site.	A.Project-Setup

Table 13 Preconditions required by the site

8.2. Services of the site

The following services and/or processes provided by Arm Sophia Antipolis are in the scope of the site evaluation process:

- IC Development and Testing
    - Secure development of the design documentation, source code and guidance documentation.
    - CM System administration and flaw remediation
    - Generation and delivery of the finished product
- Local IT infrastructure and administration
    - An appropriate environment for sensitive IT equipment employed to remotely connect to the external
    - Administration of all services with the support of IT global teams as detailed in 8.1 Preconditions required by the site.
- Supporting services
    - HR management
    - Physical security

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

- Facilities management

8.3. Objectives rationale

The following rationale provides a justification that shows that all threats and OSP are effectively addressed by the Security Objectives.

O.Physical-Access

The site is a closed area. The access to the building is only possible through access-controlled doors. The enabling of the alarm system and the additional external control are graduated according to the running operation at the site. This considers the manpower during working hours as well as the operational needs regarding receipt and delivery of goods. The physical, technical and organizational security measures ensure a separation of the site into three security levels. The access control ensures that only registered persons can access sensitive areas. This is supported by O.Security-Control that includes the maintenance of the access control and the control of visitors. The physical security measures are supported by O.Alarm-Response providing an alarm system.

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

O.Security-Control

The combination of security cameras and motion sensors at the main entrances and inside high security areas ensure that intrusion attempts are detected.

Thereby T.SmartTheft, T.Rugged-Theft and T.Unauthorised-Staff are addressed.

O.Alarm-Response

Alarms are notified to arm when they are triggered, and appropriate alarm handling procedures are in place.

Thereby T.SmartTheft, T.Rugged-Theft and T.Unauthorised-Staff are addressed.

O.Internal-Monitor

The established security measures of the site are regularly reviewed by security management meeting and internal audits.

Thereby T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion are addressed.

O.Maintain-Security

Access control systems are managed on site and local IT services are regularly maintained by on site personnel.

Thereby T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion are addressed.

O.Logical-Access

Access to sensitive information is only possible through a specific VLAN with appropriate network configuration to remotely access information hosted in a separate location.

Thereby T.Computer-Net and T.Unauthorised-Staff are addressed.

O.Logical-Operation

Local services and equipment are managed by the IT department in Sophia-Antipolis so that systems are kept up to date.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Thereby T.Computer-Net and T.Unauthorised-Staff are addressed.

O.LifeCycle-Doc

Dedicated documents exist for the site which describe (1) the configuration management systems and their usage; (2) A configuration items list; (3) Site security; (4) The development process; (5) The development tools; (6) Flaw remediation process; (7) Delivery procedure. The site follows the procedures and instructions of these documents.

Thereby P.Lifecycle-doc is addressed.

O.Config-Items

Gerrit (git-based system) is used as the main CM tool for sensitive TOE related information, allowing industry-standard unique identification of configuration items.

Thereby P.Config-Items is addressed.

O.Config-Control

All changes of configuration items under CM control are traceable and allow arm to univocally select the appropriate items to generate a release of the product.

Thereby P.Config-Control is addressed.

O.Config-Process

All configuration items that conform the final product are under CM control.

Thereby P.Config-Process is addressed.

O.Staff-Engagement

NDAs are signed and security awareness training is given to all employees.

Thereby T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion are addressed.

O.Transfer-Data

Product releases are handled by the PM, who is the sole responsible to encrypt and transfer releases from the secure environment to the external network.

Thereby T.Staff_Collusion, T.Attack-Transport and P.Transfer-Data are addressed.

O.Control-Scrap

Both logical and physical assets are securely destroyed.

Thereby T.Unauthorised-Staff and T.Staff-Collusion are addressed.

8.4. Security Assurance Requirements rationale

8.4.1 CM capabilities (ALC_CMC.5)

Configuration Management is described in *Arm Sophia Antipolis Lifecycle Support, version 1.0, 2019* [7].

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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.

8.4.2 CM scope (ALC_CMS.5)

Configuration Management is described in *Arm Sophia Antipolis Lifecycle Support, version 1.0, 2019* [7].

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.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

8.4.3 Delivery (ALC_DEL.1)

Delivery procedures are described in *Arm Sophia Antipolis Lifecycle Support, version 1.0, 2019* [7].

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

8.4.4 Development security (ALC_DVS.2)

Development Security is described in *Arm Sophia Antipolis Lifecycle Support, version 1.0, 2019* [7].

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.

8.4.5 Basic flaw remediation (ALC_FLR.1)

Basic flaw remediation is described in *Arm Sophia Antipolis Lifecycle Support, version 1.0, 2019* [7].

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

8.4.6 Lifecycle definition (ALC_LCD.1)

Life-cycle definition is described in *Arm Sophia Antipolis Lifecycle Support, version 1.0, 2019* [7].

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.

8.5. Assurance measure rationale

O.Physical-Access

ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Security-Control

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Alarm-Response

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Internal-Monitor

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Maintain-Security

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design, implementation and in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement. ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Logical-Access

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design, implementation and in its development environment. Thereby this objective is suitable to meet the Security Assurance Requirement. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Logical-Operation

ALC_DVS.2.1C: requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design, implementation and in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement. ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective is suitable to meet the Security Assurance Requirement. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items. Thereby this objective contributes to meet the Security Assurance Requirement.

O.LifeCycle-Doc

ALC_CMC.5.1C requires that the CM documentation show that a process is in place to ensure an appropriate and consistent labeling.

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

ALC_CMC.5.3C requires that the CM documentation justifies that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.

ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items.

ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ALC_CMC.5.6C requires that the CM system supports the production of the product by automated means.

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

ALC_CMC.5.8C requires that the CM system clearly identifies the configuration items that comprise the TSF.

ALC_CMC.5.9C requires that the CM system supports 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 requires that the CM system provides an automated means to identify all other configuration items that are affected by the change of a given configuration item.

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

ALC_CMC.5.12C requires that the CM documentation includes a CM plan.

ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development of the TOE.

ALC_CMC.5.14C requires that the CM plan describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the CM system.

ALC_CMC.5.16C requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system.

ALC_CMS.5.1C requires that the CL includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.

ALC_CMS.5.2C requires that the CL uniquely identify the configuration items.

ALC_CMS.5.3C requires that for each configuration item, the configuration list indicates the developer/subcontractor of the item.

ALC_DEL.1.1C requires that the delivery documentation describes all procedures that are necessary to maintain security when distributing versions of the TOE to the customer.

ALC_DVS.2.1C requires that the development security documentation describes 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 requires that the development security documentation justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_FLR.1.1C requires that the flaw remediation procedures documentation describe the procedures used to track all reported security flaws in each release of the intended TOE.

ALC_FLR.1.2C requires that the flaw remediation procedures require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C requires that the flaw remediation procedures require that corrective actions be identified for each of the security flaws.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ALC_FLR.1.4C requires that the flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the TOE.

ALC_LCD.1.2C requires that the life-cycle model provides for the necessary control over the development and maintenance of the TOE. All these content elements of the mentioned SARs require dedicated content of the CM documentation and the configuration list, properties of the SM system, content of the development security documentation, content of the life-cycle documentation. The objective meets the set of Security Assurance Requirements.

O.Config-Items

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. In addition, ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items.

ALC_CMC.5.8C requires that the CM system clearly identifies the configuration items that comprise the TSF.

ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a change given to a configuration item.

ALC_CMC.5.11C requires that the version of test programs, internal procedures and processes used at the site can be identified.

The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information.

ALC_CMS.5.2C requires that the developer of each TSF relevant configuration item is indicated in the configuration list. The objective meets the set of Security Assurance Requirements.

O.Config-Control

ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items.

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

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

ALC_CMC.5.9C requires the support of audit information for all changes to the TOE by automated means including the originator, date and time.

ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a change given to a configuration item.

ALC_CMC.5.11C requires that the version of test programs, internal procedures and processes used at the site can be identified.

ALC_CMC.5.12C requires a CM documentation that includes a CM plan.

ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development (production) of the TOE.

ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan. The objective meets the set of Security Assurance Requirements.

O.Config-Process

The provision of automated measures such that only authorized changes are made to the configuration items as required by ALC_CMC.5.5C.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ALC_CMC.5.6C requires that the CM system supports the production by automated means.

ALC_CMC.5.12C requires that the CM documentation includes a CM plan.

ALC_CMC.5.13C requires that the CM plan describe how the CM system is used for the development of the TOE. The objective meets the set of Security Assurance Requirements.

O.Staff-Engagement

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

O.Transfer-Data

ALC_DVS.2.1C requires that the development security documentation describes 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.

ALC_DEL.1.1C requires that the delivery process maintains security when distributing versions of the TOE to the customer. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Control-Scrap

ALC_DVS.2.1C requires that the development security documentation describes 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. Therefore, this SAR is suitable to meet the security objective.

8.6. Mapping of the evaluation documentation

The scope of the evaluation according to the assurance class ALC comprises the processing and handling of security products and the complete documentation of the site provided for the evaluation. The specifications and descriptions provided by the client are not part of the configuration management at arm. The mapping between the internal site documentation and the Security Assurance Requirements is described in the following tables.

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

SAR	References
ALC_CMC.5.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	7 Chapter 3 in *Arm Sophia Antipolis Lifecycle Support, version 2.0*, June 2022 [7]
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 intended TOE by automated means.	
ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	
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 intended 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 intended 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 intended 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 intended 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.	

Table 14 Mapping for ALC_CMC.5

SAR	References
ALC_CMS.5.1C: The configuration list shall include the following: the intended TOE itself; 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.	7 Section 3.3.3 in Arm *Sophia Antipolis Lifecycle Support, version 2.0*, June 2022 [7]
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.	

Table 15 Mapping for ALC_CMS.5

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

SAR	References
ALC_DEL.1.1C: The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.	7 Chapter 4 in Arm *Sophia Antipolis Lifecycle Support, version 2.0*, June 2022 [7]

Table 16 Mapping for ALC_DEL.1

SAR	References
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment	8 *IS01 - SEC: SecurCore MSSR Security Policy Manual, Supporting DSD Documentation*
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.	8 *IS01 - SEC: SecurCore MSSR Security Policy Manual, Supporting DSD Documentation*

Table 17 Mapping for ALC_DVS.2

SAR	References
ALC_FLR.1.1C: The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.	7 *Chapter 5* in Arm *Sophia Antipolis Lifecycle Support, version 2.0*, June 2022 [7]
ALC_FLR.1.2C: The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.	
ALC_FLR.1.3C: The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	
ALC_FLR.1.4.C: The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.	

Table 18 Mapping for ALC_FLR.1

SAR	References
ALC_LCD.1.1C: The life cycle definition documentation shall describe the model used to develop and maintain the intended TOE.	7 Chapter 6 in Arm *Sophia Antipolis Lifecycle Support, version 2.0*, June 2022 [7]
ALC_LCD.1.2C: The life cycle model shall provide for the necessary control over the development and maintenance of the intended TOE.	

Table 19 Mapping for ALC_LCD.1

Copyright © 2020-2022 Arm Limited or its affiliates. All rights reserved.
Non-Confidential