TÜVRheinland®
Precisely Right.

Site Security Certification Report

Arm Sophia Antipolis

Sponsor and developer: ***Arm Limited***
110 Fulbourn Road
Cambridge
England CB1 9NJ

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-SS-0031297- CR**
Report version:	**1**
Project number:	**0031297**
Author(s):	**Wouter Slegers, Hans-Gerd Albertsen**
Date:	**30 January 2020**
Number of pages:	**8**
Number of appendices:	**0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

TÜVRheinland®
Precisely Right.

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the certificate

Currently the Common Criteria Recognition Arrangement (CCRA) and SOGIS-Mutual Recognition Agreement (SOGIS-MRA) do not cover the recognition of Site Certificates. However, the evaluation process followed all the rules of these agreements and used the agreed supporting document for Site certification *[CCDB]*. Therefore, the results of this evaluation and certification procedure can be re-used by any scheme in a subsequent product evaluation and certification procedure that makes use of the certified site.

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate would indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations. As Site Certificates are not covered, these logos are not present.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the site Arm Sophia Antipolis. The operator of the site is Arm Limited located in 06560 Valbonne, France and Arm Limited located in Cambridge, England CB1 9NJ act as the sponsor of the evaluation and certification.

The evaluated site is called: Arm Sophia Antipolis.

The site is used by Arm Limited to participate in the development and testing of hardware for secure IC hardware products (Secure Code (IP core) products). To perform its activities, the site uses the Arm Limited provided remote IT-infrastructure and local IT equipment (workstations, router, VPN) and works according to the Arm Limited defined processes.

The site activities relate to Phase 2 of the seven Phases of the Lifecycle Model as defined in *[PP]*.

The site has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 30 January 2020 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the Site Security Target *[SST]*, which identifies assumptions made during the evaluation and the level of confidence (evaluation assurance level) the site is intended to satisfy for product evaluations. Users of this site certification are advised to verify that their own use of, and interaction with, the site is consistent with the Site Security Target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this site provide sufficient evidence that it meets the EAL6 assurance components ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2 at AVA_VAN.5 level, ALC_LCD.1, and ALC_FLR.1.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* and the Supporting Document Guidance CCDB-2007-11-001 Site Certification, October 2007, version 1.0, Revision 1 *[CCDB]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision **5** *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions of the Common Criteria and that the site will be listed on the NSCIB Certificates list. It should be noted that the certification results only apply to the specific site, used in the manner defined in the *[SST-Lite].*

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator and is not releasable for public review.

2 Certification Results

2.1 Identification of Site

The Target of Evaluation (TOE) for this evaluation is the site Arm Sophia Antipolis located in 06560 Valbonne, France.

2.2 Scope: Physical

This site certification considers a single 2-floor building location occupied only by Arm Limited.

The area where the relevant activities take place is limited to Secure Room (TOE development), Patch room and Server room (transmission of TOE related assets and location of local infrastructure).

2.3 Scope: Logical

This site is used for development and testing of hardware for secure integrated circuits (Secure Code (IP core) products). Testing is performed by simulation or remotely on physical objects (FPGAs) at another site. This site is covered in a different certification.

For smartcard products, these activities are related to Phase 2 of the seven Phases of the Lifecycle Model in *[PP]*.

Within those phases, the site is involved in

- ALC_DVS to control access to the assets (at AVA_VAN.5 level).
- ALC_CMC/CMS to handle the site internal documentation and TOE development related configuration items.
- ALC_LCD as part of TOE development and testing.
- ALC_DEL for secure TOE delivery
- ALC_FLR for flaw tracking and corrective actions.

2.4 Evaluation approach

The evaluation is a first evaluation, based on developer documentation.

In the evaluation all evaluator actions have been performed including a site visit. For assessment of the ALC_DVS aspects, the Minimum Site Security Requirements *[MSSR]* have been used.

2.5 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references other evaluator documents. To support re-use of the site evaluation activities a derived document *[STAR]*[3] was provided and approved. This document provides details of the site evaluation that have to be considered when this site is used in a product evaluation.

The evaluation lab concluded that the site meets the assurance requirements listed in the *[SST]* as assessed in accordance with *[CC], [CEM]* and *[CCDB]*.

2.6 Comments/Recommendations

The Site Security Target (*[SST]*) contains necessary information about the usage of the site. During a product evaluation, the evidence for the fulfillment of the Assumptions listed in the *[SST]* shall be examined by the evaluator of the product when re-using the results of this site evaluation.

[2] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator and is not releasable for public review.

[3] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

3 Site Security Target

The Arm Site Security Target Sophia Antipolis, Version 1.1, 03 October 2019 *[SST]* is included here by reference.

Please note that for the need of publication a public version *[SST-Lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MSSR	Minimum Site Security Requirements
NSCIB	Netherlands scheme for certification in the area of IT security

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.
[CCDB]	Supporting Document Guidance: CCDB-2007-11-001 Site Certification, October 2007, Version 1.0, Revision 1.
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
[ETR]	Evaluation Technical Report Site Security ARM Sophia Antipolis, 19-RPT-670, Version 2.0, 10 January 2020.
[MSSR]	Joint Interpretation Library, Minimum Site Security Requirements, Version 2.2, April 2019.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[PP]	Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, Rev 1.0, 13 January 2014.
[SST]	Arm Site Security Target Sophia Antipolis, Version 1.1, 03 October 2019.
[SST-Lite]	Arm Site Lite Security Target Sophia Antipolis, Version 1.0, 14 January 2020.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.
[STAR]	Site Technical Audit Report Arm Sophia Antipolis, 19-RPT-669, Version 2.0, 10 January 2020.

(This is the end of this report).