Certification Report

u.trust Anchor 4.49.1

Sponsor and developer:	***Utimaco IS GmbH*** **Germanusstraße 4** **52080 Aachen,** **Germany**
Evaluation facility:	***Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2400107-01-CR**
Report version:	**1**
Project number:	NSCIB-**2400107-01**
Author(s):	**Alireza Rohani, Haico Haak**
Date:	**21 April 2025**
Number of pages:	**11**
Number of appendices:	**0**

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, TrustCB 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 TrustCB 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 TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence 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, TrustCB 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, 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

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the u.trust Anchor 4.49.1. The developer of the u.trust Anchor 4.49.1 is Utimaco IS GmbH located in Aachen, Germany and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE u.trust Anchor is a new generation version of a traditional hardware security module (HSM), comprising all of the traditional hardware security features normally applicable to such a device - but additionally introducing the concept of containerized HSMs (cHSMs) within the protected boundary of the hardware HSM (the TOE).

The TOE was previously evaluated by SGS Brightsight B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 01 September 2022 (NSCIB-CC-0533229). The current evaluation of the TOE has also been conducted by Brightsight B.V. and was completed on 21 April 2025 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 major changes from previous evaluations are:

Utimaco has introduced a wildcard at the end of the hardware identifier to make it version 7.03.0.3.x to allow for similar component replacement under minor version number x. The exact value of x is defined in section 2.1 of this report.

The certification took into account that the security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the u.trust Anchor 4.49.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the u.trust Anchor 4.49.1 are advised to verify that their own environment is consistent with the 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 product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.3 (Systematic flaw remediation) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the u.trust Anchor 4.49.1 from Utimaco IS GmbH located in Aachen, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	The TOE hardware is provided in form of a PCIe plug-in card Hardware P/N CSAR-7.3.0.3.x-PCIe-CC (PCIe security module)	7.03.0.3.x, with x representing the BOM identifier (see below)
Software	Operational Image (glados-utrust-anchor-1.22.5.raucb)	1.22.5
	Recovery Image (glados-recovery-1.22.5.raucb)	1.22.5
	Sensory Controller	3.02.0.8

HW BOM identifier ABCDEFGHIJKLMNOPQ-RSTUVWXYZ is constructed from 26 digits as follows (each digit A,B,C…can take between 2 and 4 possible values):

Section of HW BOM identifier	Section of HW BOM identifier
AB (digit 1-2)	Defines variant of deployed main processor
CD (digit 3-4)	Defines variant of deployed Microcontroller for Alarm Sensory
EFGHIJ (digit 5-10)	Defines variant of deployed Memory EMMCFLASH
KLMNOPQ (digit 11-17)	Defines variant of deployed Memory DDR4
RSTUVWX (digit 18-24)	Defines variant of deployed QSPI Flash
YZ (digit 25-26)	Defines variant of deployed SRAM

To ensure secure usage a set of guidance documents is provided, together with the u.trust Anchor 4.49.1. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The u.trust Anchor implements the following cryptographic algorithms:

- AES in various modes for encryption, decryption, CMAC and GMAC calculation, key (un)wrapping and Secure Messaging
- TDES in various modes for encryption and decryption
- ECDSA and EdDSA with key size >= 224 bit on dedicated elliptic curves for signature generation and signature verification
- RSA with key size >= 2048 bit and <= 16,384 bit for signature generation and signature verification and key (un)wrapping
- SHA-2, SHA-3 and HMAC for hashing, pseudo random function and MAC calculation

Furthermore the u.trust Anchor implements functionality for key establishment:

- AES key generation

- TDES key generation
- Generation of generic secret keys, e. g. for HMAC algorithm
- Elliptic curve cryptography (ECC) key generation, e. g. for ECDSA, EdDSA and ECDH
- RSA key generation
- DSA domain parameter generation and DH key generation
- Diffie-Hellman and EC Diffie-Hellman Key Agreement
- Key Derivation

For random number generation and generation of all cryptographic keys, challenges and nonces, the u.trust Anchor implements a hybrid deterministic random number generator that relies on an implemented hardware random noise generator and fulfills the requirements of [AIS 20/31].

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.5 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The TOE is a general purpose Hardware Security Module (HSM) based on the Utimaco u.trust Anchor platform. The TOE is a new generation version of a traditional HSM, comprising all of the traditional hardware security features normally applicable to such a device - but additionally introducing the concept of containerized HSMs (cHSMs) within the protected boundary of the hardware HSM (the TOE). As optional delivery variant, the PCIe plug-in card can be integrated into an Utimaco u.trust Anchor LAN V5, a 19-inch network appliance.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
u.trust Anchor PCIe CC - Operating Manual	2021-0084, version 1.0.4, date 2022-06-09
u.trust Anchor LAN V5 CC - Operating Manual	2021-0069, version 1.0.7, date 2022-06-09
u.trust Anchor CC - Administration Manual (Administration Manual for Global Administration)	2021-0078, version 1.0.7, date 2022-06-21
u.trust Anchor CC - Containerized Hardware Security Module (cHSM) - Administration Manual (Administration Manual for cHSM)	2021-0077, version 1.0.9, date 2022-06-07
u.trust Anchor CC - Containerized Hardware Security Module (cHSM) - User Manual (User Manual for cHSM)	2021-0076, version 1.1.3, date 2022-05-12
u.trust Anchor CC - Global Admin Management Tool (gladm) - Reference Manual	2021-0074, version 1.1.3, date 2022-06-13
u.trust Anchor CC - csadm Manual	2021-0075, version

	1.0.3, date 2022-06-07

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer provided test evidence, the following aspects of the developer testing can be mentioned:

- A python test suite is used
- The following areas are covered in testing:
- All user roles with authentication and permissions
- Secure messaging
- Logging
- Alarm and error states
- Algorithms
- Self tests
- Most tests are automated, but the following tests require manual input:
- Erase button test
- Battery removal test

Evaluator defined tests are aimed at trying some commands or combinations of commands that, based on other evaluation activities, may have unexpected results. Evaluator defined tests include TOE identification to make sure that the procedures as described in guidance can actually be followed by the user of the TOE. This includes identification of the TOE as part of the LAN V5 appliance.

2.6.2 Independent penetration testing

The total test effort expended by the evaluators in the current re-evaluation in was 2 weeks. During that test campaign, 0% of the total time was spent on physical attacks, 0% overcoming sensors and filters, 0% perturbation attacks, 0% retrieving keys with FA, 0% side-channel attacks, 0% attacks on RNG, 87% of the total time was spent on logical attacks, 13% on fuzzing attacks, and 0% application isolation penetration tests.

Two tests have been repeated from the baseline evaluation. The repeated tests are PEN_1_cHSM_Memory_Access and PEN_3_Removed_Commands.

2.6.3 Test configuration

The TOE was tested in the following configurations:

- PEN_1, PEN_2, and PEN_N1 tests are run on a modified FW image that allows calling commands that are blocked for the actual TOE, in order to check that an additional layer of protection is present. The developer provided this FW image as to allow for the testing. In all other aspects the modified FW image is identical to the actual TOE, hence the test results are representative for the TOE.
- PEN_3 up to PEN_6 and PEN_N3 tests are run on the actual TOE version. Following a detailed analysis in [EAR] the test results are considered valid for all minor hardware configurations as listed in [ST], testing on a version with replaced DDR4 memory adds assurance compared to the previous evaluation.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed. A development site has been visited as part of this evaluation

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number u.trust Anchor 4.49.1.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the u.trust Anchor 4.49.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with AVA_VAN.5 and ALC_FLR.3**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

3 Security Target

The u.trust Anchor - Security Target for u.trust Anchor, version: 1.0.4, date: 24th March 2025 *[ST]* is included here by reference.

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

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

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
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report “u.trust Anchor 4.49.1” – EAL4+, 22-RPT-254, Version 10.0, date: 14 April 2025
[EAR]	Evaluator Assessment of Changes Report (EAR) u.trust Anchor v4.49.1 – Partial ETR, 24-RPT-769, Version 6.0, date: 25 March 2025
[JIL-AAPHD]	Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.1, November 2023
[JIL-AMHD]	Attack Methods for Hardware Devices with Security Boxes, Version 3.0, February 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	u.trust Anchor - Security Target for u.trust Anchor, version: 1.0.4, date: 24th March 2025
[ST-lite]	ST Title, Unique Identifier, Issue Date u.trust Anchor - Security Target Lite for u.trust Anchor, version: 1.0.4, date: 24th March 2025
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)