Certification Report

u.trust Anchor 4.49.0

Sponsor and developer: ***Utimaco IS GmbH***
Germanusstr. 4
52080 Aachen
Germany

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0533229-CR**

Report version: **1**

Project number: **0533229**

Author(s): **Wim Ton**

Date: **01 Sep. 2022**

Number of pages: **15**

Number of appendices: **0**

Head Office:
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 Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

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 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, 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 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

The 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, including hardware boxes. 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 4.49.0. The developer of the u.trust Anchor 4.49.0 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 is a general purpose HSM whose primary purpose is to provide secure cryptographic services such as signing and verification of data, encryption or decryption, MAC calculation, key derivation and key agreement, hashing, on-board random number generation and secure key generation, internal as well as external protected key storage and further key management functions in a tamper-protected environment. It can be used with the cryptographic standard APIs: PKCS#11, JCE, OpenSSL, CSP/CNG and EKM. Furthermore, the TOE provides a secure software update mechanism.

The TOE can run up to 31 containerized HSMs in parallel, where each cHSM can be used independently from any other cHSM on the same hardware device.

Each cHSM has visibility only of the resource set (data, keys, configuration) that appears to be entirely its own.

A separate container is used by the Global Administrator to create, delete, configure and backup the cHSM containers.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 27-07-2022 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 security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the **u.trust Anchor 4.49.0**, 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 4.49.0** 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 (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).

TÜV Rheinland Nederland 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 4.49.0** from Utimaco IS GmbH located in **Aachen, Germany**.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	CSAR-7.3.0.3-PCIe-CC	7.3.0.3
Software	Operational Image (glados-utrust-anchor-bundle-csar73s-1.22.5.raucb)	1.22.5
Software	Recovery Image (glados-recovery-csar73s-1.22.5.raucb)	1.22.5
Software	Sensory Controller firmware	3.02.0.8

To ensure secure usage a set of guidance documents is provided, together with the **u.trust Anchor 4.49.0**. For details, see section 2.5 “Documentation” of this report.

2.1.1 Lifecycle

The TOE is delivered in the state “FACTORY DEFAULT”. The “Global Administrator” changes the lifecycle to “INITIALIZED” by replacing the initial administration key.
For a detailed and precise description of the TOE lifecycle, see the *[AGD-Global-Admin]*, Chapter 3.3.

2.2 Security Policy

The following cryptographic primitives are supported and included within the TSF:

- 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, signature verification, and key (un)wrapping
- DH and ECDH key agreement
- Generation, import, and export of keys for the above algorithms
- SHA-2, SHA-3 and HMAC for hashing, pseudo random function and MAC calculation
- Generation of random numbers.

The TSF also provide:

- Access control to all data (including keys).
- Security Audit Data Generation
- A trusted path between the TOE and the client application.
- Integrity checks on the stored data
- Physical protection of the TOEs internal components
- Self-tests
- Secure software update
- Secure backup of the TOE data.
- A unique serial number.

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 5.2 of the *[ST]*.

2.3.2 Clarification of scope

The *[ST]* was developed based on the *[EN419221-5]* PP, but does not claim it. The *[ST]* incorporates the OE.ENV from the PP, which is summarized below.

The environment for the TOE:

- protects against loss or theft of the TOE,
- deters and detects physical tampering,
- protects against attacks based on emanations of the TOE,
- protects against unauthorised software and configuration changes on the TOE and the hardware appliance in which it is contained.

(“OE.Env Protected operating environment”).

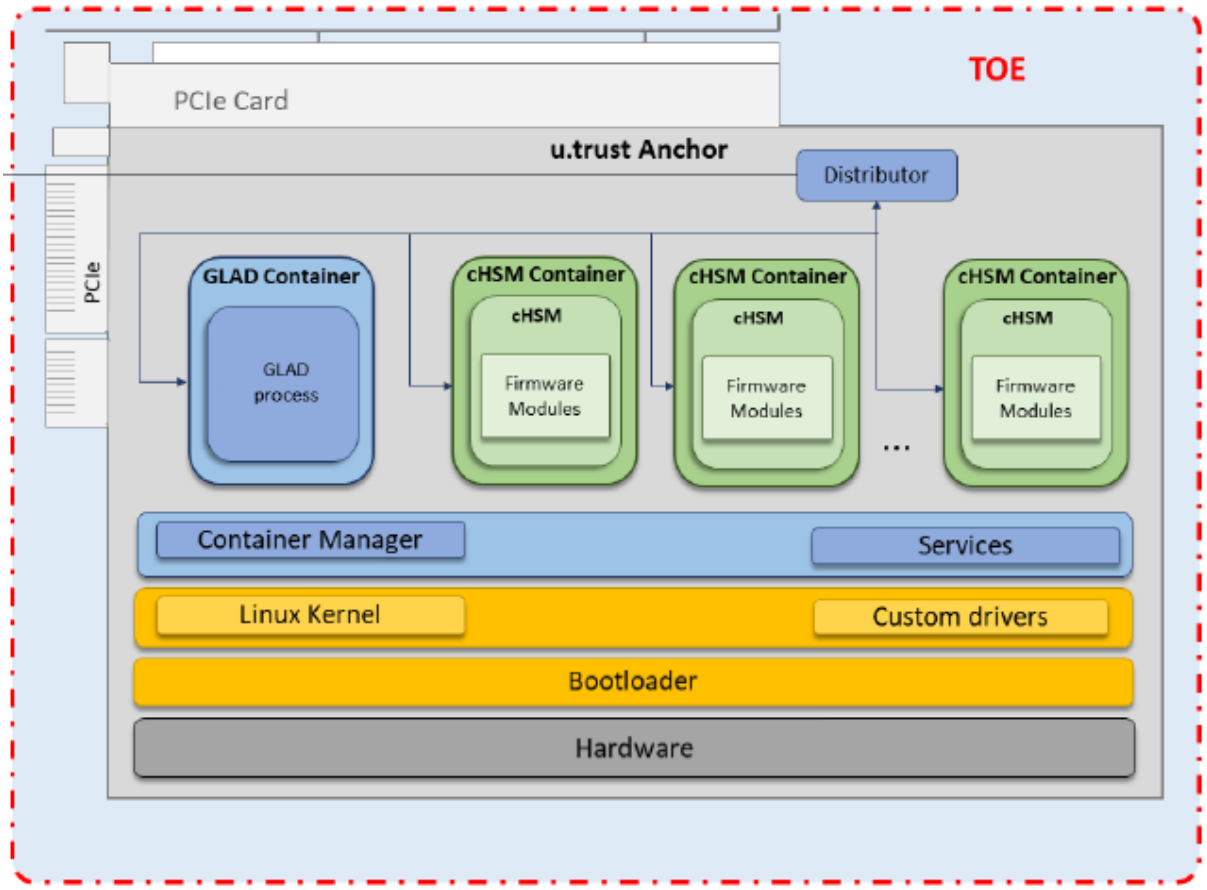
Thus, the environment in which the TOE is used must ensure the above protection.

Any threats violating these objectives for the environment are not considered.

2.4 Architectural Information

The following drawing gives an overview of the TOEs architecture:

The GLAD (Global Administrator) container is used to create and configure the cHSM containers.



The bespoke Linux kernel is compiled with the minimum features necessary to allow the platform to function, and including security components such as mandatory access control, resource control and other sandboxing techniques.

The uBoot bootloader checks the main image for errors before proceeding with the boot process.

The custom drivers and services as part of the platform firmware image enable communication, for example, with the random number generator and the cryptographic accelerators hardware.

The TOE hardware includes a multi-core ARM processor, 2 GBs of dynamic RAM, a non-volatile RAM (NV-RAM), a flash memory as secondary storage, a cryptographic accelerator with support for RSA and ECC operations, a soft cryptographic accelerator IP block in the FPGA used for acceleration of certain ECC curve operations, a real time clock, and a noise source as a physical random number generator (RNG).

A separate “Sensory Controller” monitors the temperature, the state of the tamper detection wire, and the power supplies of the various components.

A specialized “Dallas” chip provides a unique serial number.

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,	v1.0.4
u.trust Anchor LAN V5 CC - Operating Manual	V1.0.7
u.trust Anchor CC - Administration Manual (Administration Manual for	v1.0.7

Global Administration),	
u.trust Anchor CC - Containerized Hardware Security Module (cHSM) - Administration Manual (Administration Manual for cHSM)	v1.0.9
u.trust Anchor CC Containerized Hardware Security Module (cHSM) - User Manual (User Manual for cHSM)	v1.1.3
u.trust Anchor CC - Global Admin Management Tool (gladm) - Reference Manual	v1.1.3
u.trust Anchor CC - csadm Manual	v1.0.3

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 evaluator witnessed selected tests for the administrative interfaces and the cryptographic functionality at the developer's premises.

2.6.2 Independent testing

The evaluator created the following additional test cases:

1. Verify the version of the TOE,
2. Verify that a containerized HSM instance can be identified by its UID.
3. Verify that the logs cannot be changed and/or deleted by unauthorized subjects
4. Verify that the G parameter for DSA cannot be generated with equal P and Q, or with P or Q equal to 1
5. Verify that a 192-bit key for AES-CBC cannot be used for TDES and AES-ECB
6. Verify that random data generated by the TOE passes the *[AIS 31]* test suite.

2.6.3 Independent penetration testing

The vulnerability analysis identified the following areas of concern:

1. Separation between the containers.
2. Access to syscalls.
3. Authentication bypass
4. DoS through failed attempts.
5. Access to production commands.
6. Access via the USB interface which is used for production only.
7. Access to the internal hardware components.

Tests 1 and 2 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. The test environment is described in 2.6.4.

Tests 3, 4 and 5 use the standard administrative tools, provided by the developer.

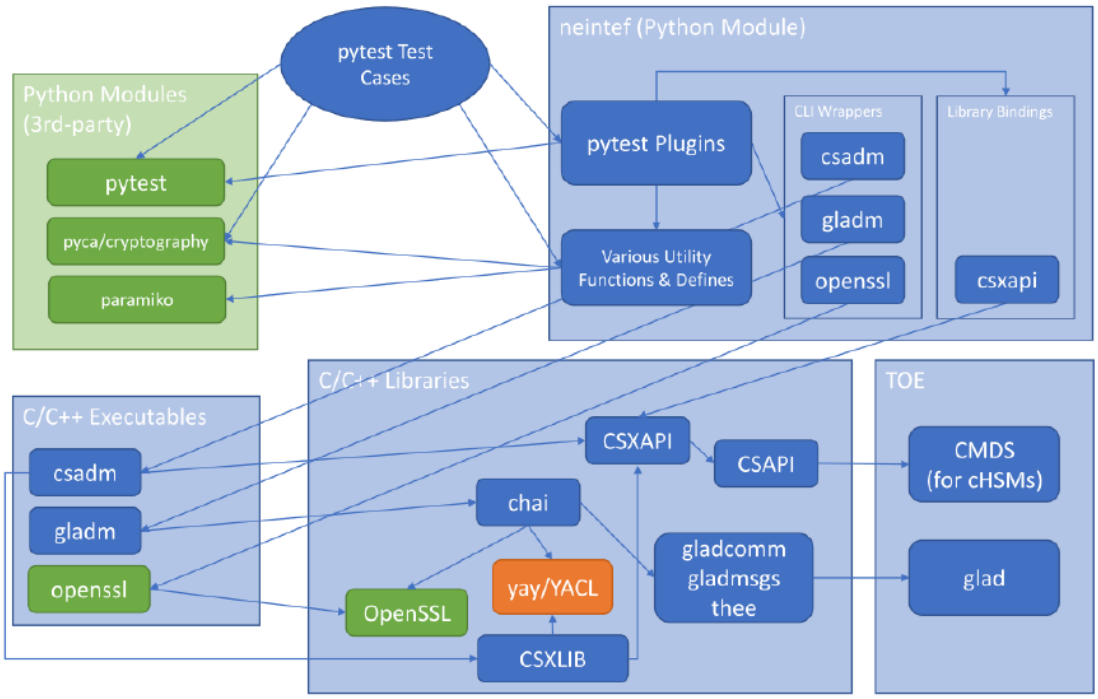
Test 6 uses USB fuzzing tools with the "Facedancer 21" hardware.

Test 7 uses a mill and a heat gun.

The total test effort expended by the evaluators was 1 week. During that test campaign, 17% of the total time was spent on fuzzing attacks, and 83% on logical tests.

2.6.4 Test configuration

The following test environment is used by the evaluator and by the developer:



The green blocks are 3rd party components:

- Operating system: CentOS 7
- Cryptographic library and utilities: OpenSSL 1.1.1g
- Python 3.8.3, along with the following modules:
  - paramiko 2.7.1 (provide SSH access for certain error state tests)
  - pyca/cryptography 2.9.2 (for additional client-side cryptography)
  - pytest 6.2.5
  - pytest-html 3.1.1 (for generating HTML test reports)
- umap version 1.03

The blue blocks outside of the TOE are TOE supporting libraries and administrative utilities provided by Utimaco.

2.6.5 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.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number “u.trust Anchor” 4.49.0. Administrators and assigned users can verify the correct version with the “csadm GetState” or “gladm system-get-info” commands. The device type must contain “CC”.

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 4.49.0**, 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. Certain aspects of the TOE’s security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

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**, which are out of scope as there are no security claims relating to these.

3 Security Target

The *[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
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programmers Interface
cHSM	Containerized Hardware Security Module
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CNG	Cryptography New Generation (Microsoft)
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
DMK	Device Master Key
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EKM	Extensible Key Management (SQL)
IC	Integrated Circuit
FPGA	Field Programmable Gate Array
FW	Firmware
GLAD	Global Administrator, sets up cHSM containers
JCE	Java Cryptography Extension
JIL	Joint Interpretation Library
LAN	Local Area Network
MAC	Message Authentication Code
MBK	Master Backup Key

MITM	Man-in-the-Middle
PCI	Peripheral Component Interconnect
PCIe	PCI Express, serial version of PCI
RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SM	Secure Messaging
SSL	Secure Sockets Layer
USB	Universal Serial Bus
VLAN	Virtual LAN

5 Bibliography

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

[AGD-cHSM]	u.trust Anchor CC Containerized Hardware Security Module (cHSM) Administration Manual, v1.0.9, 07 July 2022
[AGD-cHSM-User]	u.trust Anchor CC Containerized Hardware Security Module (cHSM) - User Manual (User Manual for cHSM), v1.1.3, 12 May 2022
[AGD-GLAD]	u.trust Anchor CC - Global Admin Management Tool (gladm) - Reference Manual, v1.1.3, 13 June 2022
[AGD-Global-Admin]	utrust_Anchor_CC - Administration Manual, v1.0.7, 21 June 2022
[AGD-ADM]	u.trust Anchor CC - csadm Manual, v1.0.3, 13 June 2022
[AGD-LAN-User]	u.trust Anchor LAN V5 CC - Operating Manual, v1.0.7, 11 March 2022
[AGD-PCIe-User]	u.trust Anchor PCIe CC - Operating Manual, v1.0.4, 11 March 2022
[AIS-31]	Functionality classes and evaluation methodology for deterministic/physical random number generators, v3, 15 May.2013,
[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
JIL-AAPHD]	Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.0, July 2020
[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 2.5, 28 March 2019
[EN 419 221-5]	Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services, v1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020
[ST]	u.trust Anchor - Security Target for u.trust Anchor, v1.0.1,21 June 2022
[ST-lite]	u.trust Anchor - Security Target Lite for u.trust Anchor, v1.0.1,22 June 2022
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[ETR]	Evaluation Technical Report “u.trust Anchor 4.49.0” – EAL4+, v5.0, 28 June 2022
[IR-ASE]	22-RPT-247 IR-ASE u.trust Anchor, v2.0,
[ADV PRES]	22-RPT-248 ADV EAL4+ Ultimaco presentation u.trust Anchor, v4.0, 13 June 2022

[ADV-AGD]	22-RPT-252 ADV-AGD reference document Ultimaco UTrust Anchor, v3.0, 30 May 2022
[TSFI CHECK]	22-RPT-249 External Interfaces Analysis document, v2.0, 28 April 2022
[SFR COV]	22-RPT-250 SFR coverage against TSFI and modules, v3.0, 28 April 2022
[SFR COV CRYPTO]	22-RPT-251 Crypto SFR coverage against TSFI and modules, v2.0, 28 April 2022
[ALC PRES]	22-RPT-253 ALC presentation EAL4+ Ultimaco uTrust Anchor, v4.0, 14-06-2022
[ATE AVA PRES]	22-RPT-540 ATE AVA presentation EAL4+ Ultimaco uTrust Anchor v2.0, 16 June 2022
[AVA VA]	22-RPT-541 Vulnerability Analysis u.Trust Anchor, v2.0, 16 May 2022
[ATE AVA Testplan]	22-RPT-542 ATE and AVA Test Plan u.Trust Anchor v2.0, 20 June 2022
[AVA PHYS]	22-RPT-543 Evaluation Report on Physical Protection u.trust Anchor, v2.0, 30 May 2022
[Site Audit Checklist]	22-RPT-544 Site Audit Checklist Utimaco Aachen, v2.0, 16 June 2022

(This is the end of this report.)