Certificate Report

Version 1.0

29 June 2022

CSA_CC_21007

For

u.trust Anchor 4.49.0

From

Utimaco IS GmbH

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorising Nation under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	29 June 2022	For release

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the u.trust Anchor version 4.49.0 and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS).

The TOE is a general purpose HSM designed as a protected cryptographic module provided in form of a PCI express plug-in card for high security applications. It provides secure cryptographic services such as signing and verification of data (ECDSA, RSA), encryption or decryption (for various cryptographic algorithms like AES and RSA), hashing, on-board random number generation and secure key generation, key storage and further key management functions in a tamper-protected environment.

The TOE comprises the following:

Hardware

- The u.trust Anchor HSM hardware provided in form of a PCI Express (PCIe) plug-in card, integrated in the chassis

Firmware

- The u.trust Anchor platform firmware COSMOS: including boot loader, Linux kernel, container management firmware and Global Administration service firmware (GLAD)
- cHSM (containerized HSM) firmware which is provided by COSMOS in cHSM firmware templates which can be loaded into containers

The evaluation of the TOE has been carried out by SGS Brightsight, an approved CC test laboratory, at the assurance level CC EAL 4, augmented by ALC_FLR.3 & AVA_VAN.5, and completed on 29 June 2022.

The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The Security Target [1] forms the basis for this certification and it was developed based on the certified Protection Profile (PP) EN 419 221-5: 2018 Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Modules for Trust Services, version 1.0 [2], by applying some adaptions to the PP and therefore not claiming strict conformance to it.

The Security Functional Requirements (SFRs) relevant for the TOE are outlined in Chapter 7 of the Security Target [1].

The assets to be protected by the TOE have been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of

Assumptions, Threats and Organisation Policies. These are outlined in Chapter 4 of the Security Target [1].

Please note that for the need of publication, a public version of the Security Target [3] has been created and verified.

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Contents

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [4] [5] [6];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [7]; and
- SCCS scheme publications [8] [9] [10]

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR. Hence, the certification for this TOE is covered partially by the CCRA for the components up to EAL2.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (https://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated.

The Certificate is valid till **28 June 2027**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [10]. Potential users should check the SCCS website (www.csa.gov.sg/programmes/csa-cc-product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is: u.trust Anchor 4.49.0.

The following list contains an overview of all deliverables associated to the TOE:

- Hardware, the version number is given below
- Software, pre-installed on the hardware, version numbers see below
- Guidance documents for the Global Administrator and for users of a cHSM of the u.trust Anchor, delivered as electronic files.

The table of TOE deliverables can therefore be described as follows:

Type	Name	Exact reference	Delivery Mode
Hardware	LAN server chassis: CryptoServer LAN (19-inch network appliance)	Version 7.03.0.3	Per Courier
	Hardware Security Module: Hardware P/N CSAR-7.3.0.3-PCIe-CC (PCIe security module)		
Software	Operational Image (glados-utrust-anchor-bundle-csar73s-1.20.1.raucb) - binary image in form of a RAUC bundle (*.raucb format)	Version 1.22.5	pre-installed on TOE hardware and per web download
	Recovery Image (glados-recovery-bundle-csar73s-1.20.1.raucb) - binary image in form of a RAUC bundle (*.raucb format)	Version 1.22.5	pre-installed on TOE hardware
	Sensory Controller	Version 3.02.0.8	pre-installed on TOE hardware
Guidance Documents	u.trust Anchor PCIe CC - Operating Manual (PDF)	2021-0084, Version 1.0.4	per web download via Utimaco Portal
	u.trust Anchor LAN V5 CC - Operating Manual (PDF)	2021-0069, version 1.0.7	
	u.trust Anchor CC - Administration Manual (PDF; Administration Manual for Global Administration)	2021-0078, version 1.0.7	
	u.trust Anchor CC - Containerized Hardware Security Module (cHSM) - Administration Manual (PDF; Administration Manual for cHSM)	2021-0077, version 1.0.9	
	u.trust Anchor CC - Containerized Hardware Security Module (cHSM) - User Manual (PDF; User Manual for cHSM)	2021-0076, version 1.1.3	
	u.trust Anchor CC - Global Admin Management Tool (gladm) - Reference Manual (PDF)	2021-0074, version 1.1.3	
	u.trust Anchor CC - csadm Manual (PDF)	2021-0075, version 1.0.3	

Table 1: Deliverables of the TOE

The guide for receipt and acceptance of the abovementioned TOE is described in Chapter 4 of [11].

Additional identification information relevant to this Certification procedure as follows:

TOE	u.trust Anchor 4.49.0
Security Target	u.trust Anchor - Security Target for u.trust Anchor v1.0.1
Developer	Utimaco IS GmbH
Sponsor	Utimaco IS GmbH
Evaluation Facility	SGS Brightsight
Completion Date of Evaluation	29 June 2022
Certification Body	Cyber Security Agency of Singapore (CSA)
Certification ID	CSA-CC- 21007
Certificate Validity	5 years from date of issuance

Table 2: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

The TOE implements policies pertaining to the following security functional classes:

- Cryptographic Support
- Identification and Authentication
- User Data Protection
- Trusted Path/Channels
- Protection of the TSF
- Security Management
- Security Audit

Specific details concerning the abovementioned security policies can be found in Chapter 7 of the Security Target [1].

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target [1] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

Assumptions	Description
A.ExternalData Protection of data outside TOE control	Where copies of data protected by the TOE are managed outside of the TOE, client applications and other entities must provide appropriate protection for that data to a level required by the application context and the risks in the deployment environment. In particular, any backups of the TOE and its data are maintained in a way that ensures appropriate controls over making backups, storing backup data, and using backup data to restore an operational TOE. The number of sets of backup data does not exceed the minimum needed to ensure continuity of the TSP service. The ability to restore a TOE to an operational state from backup data requires at least dual person control (i.e. the participation and approval of more than one authenticated administrator).
A.Env Protected operating environment	The TOE operates in a protected environment that limits physical access to the TOE to authorised Administrators. The TOE software and hardware environment (including client applications) installed is maintained by Administrators in a secure state that mitigates against the specific risks applicable to the deployment environment.
A.DataContext Appropriate use of TOE functions	Any client application using the cryptographic functions of the TOE will ensure that the correct data are supplied in a secure manner (including any relevant requirements for authenticity, integrity and confidentiality). For example, when creating a digital signature over a DTBS the client application will ensure that the correct (authentic, unmodified) DTBS/R is supplied to the TOE, and will correctly and securely manage the signature received from the TOE; and when certifying a public key the client application will ensure that necessary checks are made to prove possession of the corresponding private key. The client application may make use of appropriate secure channels provided by the TOE to support these security requirements. Where required by the risks in the operational environment a suitable entity (possibly the

	client application) performs a check of the signature returned from the TOE, to confirm that it relates to the correct DTBS. Client applications are also responsible for any required logging of the uses made of the TOE services, such as signing (or sealing) events. Similar requirements apply in local use cases where no client application need be involved, but in which the TOE and its user data (such as keys used for signatures) need to be configured in ways that will support the need for security requirements such as sole control of signing keys. Appropriate procedures are defined for the initial creation of data and continuing operation of the TOE according to the specific risks applicable to the deployment environment and the ways in which the TOE is used.
A.UAuth Authentication of application users	Any client application using the cryptographic services of the TOE will correctly and securely gather identification and authentication/authorisation data from its users and securely transfer it to the TOE (protecting the confidentiality of the authentication/authorisation data as required) when required to authorise the use of TOE assets and services.
A.AuditSupport Audit data review	The audit trail generated by the TOE will be collected, maintained and reviewed by a System Auditor according to a defined audit procedure for the specific system.
A.AppSupport Application security support	Procedures to ensure the ongoing security of client applications and their data will be defined and followed in the environment, and reflected in use of the appropriate TOE cryptographic functions and parameters, and appropriate management and administration actions on the TOE. This includes, for example, any relevant policies on algorithms, key generation methods, key lengths, key access, key import/export, key usage limitations, key activation, cryptoperiods and key renewal, and key/certificate revocation.

Table 3: Assumptions

Details can be found in section 4.5 of the Security Target [1].

5.2 Clarification of Scope

The scope of evaluation is limited to the claims made in the Security Target [1].

5.3 Evaluated Configuration

The TOE is a general purpose Hardware Security Module, designed as a protected cryptographic module provided in form of a PCI express plug-in card for high security applications. Additionally, the TOE introduces the concept of containerized HSMs (cHSMs) within the protected boundary of the hardware HSM.

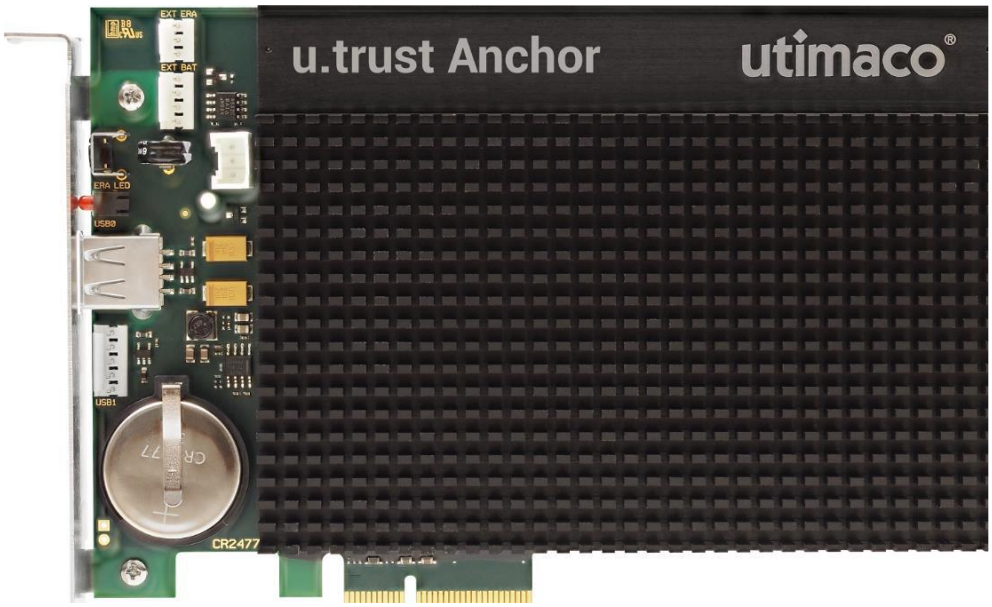

Figure 1: u.trust Anchor

Optionally and as a delivery variant, the PCIe plug-in card can be integrated into an Utimaco u.trust Anchor LAN, a 19-inch network appliance with display, control buttons and USB interfaces on the front panel, see Figure 2 below.

As any traditional HSM, u.trust Anchor 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 all cryptographic standard APIs like PKCS#11, JCE, OpenSSL, CSP/CNG and EKM.

The TOE has the following features:
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

Figure 2: u.trust Anchor LAN

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
- 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 fulfils the requirements of [AIS 20/31].

The u.trust Anchor provides the following cryptographic services:

- Functions for Initialisation:
  - Generation of RSA OAEP key establishment keys for secure import of Operator Base Secret
  - Import of wrapped Operator Base Secret
  - Generation of cHSMs with various cHSM-individual assigned system keys and certificates
  - Generation and export of user controlled Master Backup Keys
  - Import of user controlled Master Backup Keys
- Functions for Key Management (for keys in internal as well as external key store):
  - Key generation (AES keys, TDES keys, generic secret keys, ECC key pairs, RSA and DH key pairs)
  - Encrypted import & export of private & secret keys (AES, RSA)
  - Key agreement (DH, ECDH)
  - Backup and restore of keys
  - Key deletion
- Cryptographic Functions:
  - Signature generation and verification (ECDSA, EdDSA, RSA)

- Encryption and decryption (AES, TDES, RSA)
- MAC calculation & verification (AES GMAC, AES CMAC, HMAC)
- Hashing (SHA-2, SHA-3)
- Generation of random bytes

The u.trust Anchor supports the following administrative services:

- User administration (creation, deletion, change of reference authentication data (RAD))
- System time setting/display
- Export and deletion of audit data
- cHSM management (e.g. create, start, stop, delete cHSM)
- Backup ('snapshot') and restore of cHSMs

The u.trust Anchor provides appropriate countermeasures for resistance especially against the following attacks:

- Cloning of the product
- Unauthorised disclosure of confidential data (during generation, storage and processing)
- Unauthorised manipulation of data (during generation, storage and processing)
- Unauthorised usage of private and secret keys
- Derivation of information on the private key from publicly available data
- Physical and chemical attacks

Furthermore, the TOE provides a secure software update mechanism. Software revisions shall be granted security certification before their installation in the TOE.

5.4 Non-Evaluated Functionalities

All functionalities and services were evaluated as part of the evaluation. Potential users of the TOE shall follow the Guidance [1] [11] [12] carefully to configure and use the TOE.

5.5 Non-TOE components

The following hardware and software which do not belong to the TOE is required for the operating environment and is always delivered together with the TOE:

Additional deliverables	Type	Description
PIN pad (smartcard reader with keypad)	HW/SW	Utimaco cyberJack one
10 smartcards (for administrative purposes)	HW/SW	Java Card with NXP Chip and JCOP operating system

Table 4: Non-TOE Components

The TOE is delivered in two different variants:

- u.trust Anchor PCIe (PCIe plug-in card)
- u.trust Anchor LAN (network-attached appliance)

The delivery of u.trust Anchor PCIe comes only with the **product bundle**.

The delivery of u.trust Anchor LAN, has the u.trust Anchor PCIe card delivered in the **CSLAN**, as well as with **cable**s and the **product bundle**.

The items are elaborated here:

- **CSLAN**: CryptoServer LAN (19-inch network appliance with two redundant power supplies) (non-TOE hardware, delivered together with TOE hardware per courier)
- **Cable**: 2 x power supply cable (delivered with TOE)
- **Product bundle**: The product bundle containing the following firmware, software and data (available per web download via Utimaco Portal):
    - The u.trust Anchor driver (for Linux) (non-TOE software)
    - Various cryptographic APIs (non-TOE software, to be used on host)
    - The documentation of the cryptographic APIs in PDF format (non-TOE documentation)
    - The installation files of various administration tools and key management tools (non-TOE software, to be used on host)
    - Further guidance documents, e. g. for all administration tools (non-TOE documentation)
    - The keyfile with the authentication key for the default Global Administrator (initial authentication key) of the u.trust Anchor (non-TOE data)

6 Architecture Design Information

As described in the Security Target, the high-level logical architecture of the TOE can be depicted as follows:

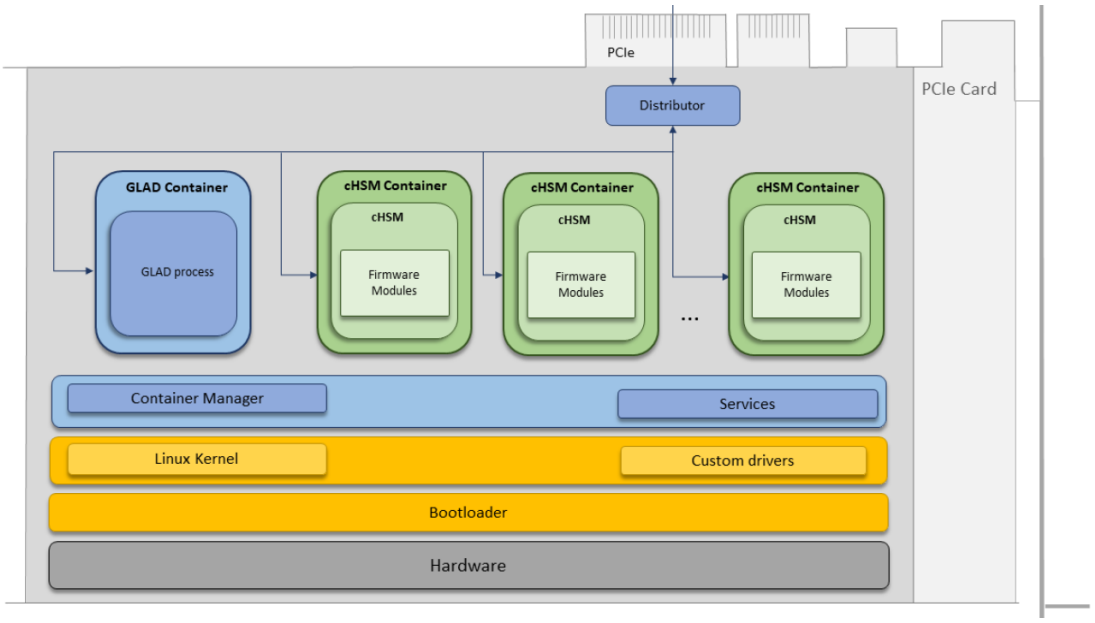

Figure 1 - Logical Architecture of the TOE

The u.trust Anchor platform firmware constitutes a limited operational environment. Loaded cHSM firmware cannot be modified and must pass a firmware integrity test on every cHSM start-up.

The u.trust Anchor platform firmware is responsible for the segregation of processes running on different containers: A process running in a container cannot detect, access or modify data belonging to a process running in a different container, or the base operating system.

The containers are isolated from each other and the base operating system by a multi-layered set of technologies (comprising namespaces, mandatory access control and resource controls), allowing multiple cHSM instances to run on a single system without interference.

Management of the containers, including creation, deletion, start, stop, backup and restore of the containers is part of the Global Administrator role. The Global Administrator role and its authentication mechanisms are completely separate from the cHSM roles and authentication mechanisms. The Global Administrator has - by design of the operator roles - no mechanism to access unencrypted data from individual cHSMs.

The cHSM firmware is a collection of firmware components (called modules) instantiated from a cHSM template that provides the required cryptographic functionality like AES, RSA, ECC, and hashing as well as supporting functionality like key storage and communication with external devices/host applications.

7 Documentation

The evaluated documentation as listed in Table 1: Deliverables of the TOE is being provided with the product to the customer. These documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

This section contains information with regard to the developer test effort.

8.1.1 Test Approach and Depth

Referencing 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

8.1.2 Test Configuration

The network diagram in Figure 4 describes the base setup used for both developer's and evaluator's testing. This is the same configuration as stated in the ST.

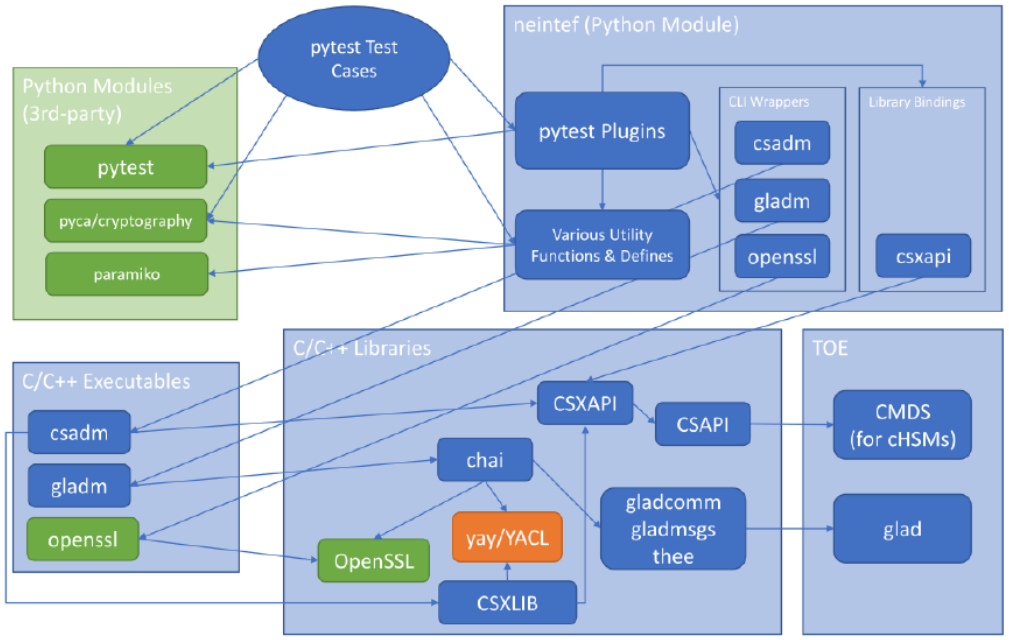

Figure 2: Developer's Test Setup

8.1.3 Test Results

Command-line administration tools csadm and gladm are installed on the test computer connected to the u.trust Anchor appliance.

Default ports 4000 to 4031 are used, whereas port 4000 refers to the gladm interface. TOE version is verified using the port 4000 command-line to send gladm -d utrustanchor system-get-info. All test results were as expected.

The developer provided an automatically generated PDF with test results that showed all tests passed.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluator analysed the developer's test coverage, test plans and procedures, expected and actual test results.

8.2.1.1 Repeated Developer's Tests

The evaluator repeated three developer's tests each from three groups of test cases, namely:

- Global Management Tests
- cHSM Management Tests
- CXI Crypto Tests

8.2.1.2 Evaluator-Defined Tests

Evaluator-defined tests are aimed at trying some commands or combinations of commands that, based on other evaluation activities, may have unexpected results. This includes trying to remove a log file in multiple ways, such as overwriting or first renaming followed by deleting, and to see that the proper behaviour is triggered once a ring buffer is overloaded.

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. The list of tests includes additional tests for:

- TOE Identification.
- cHSM Identification
- Log File Manipulation
- DSA Parameters
- AES CBC Key Function
- Entropy of Random Data

8.2.2 Test Configuration

Tests were witnessed by the evaluators on 1 June 2022 at the developer's premises in Aachen. In the witnessing session, some unexpected elements were added to ensure that actual live testing on the TOE was taking place.

The configuration of the sample was the same as during the original developer testing, which is the same as the configuration described in the ST.

8.2.3 Test Results

The evaluator concluded that the repeated developer tests and the evaluator-defined tests fully tested the TOE functionalities and security behaviours. The developer's test reproduced were verified by the evaluator to conform to the expected results from the test plan.

8.3 Penetration Testing (AVA_VAN)

8.3.1 Overview

The penetration testing was performed using the test environment of the evaluation lab. The TOE was set up and configured based on the guidance document.

All configurations of the TOE being intended to be covered by the current evaluation were tested.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential HIGH was successful.

8.3.2 Test Approach and Depth

The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN.5) treating the resistance of the TOE to an attack with the HIGH attack potential.

For the vulnerability assessment, the evaluators used sources of information publicly available to identify potential vulnerabilities in the TOE. The evaluator analysed which potential vulnerabilities are not applicable to the TOE in its operational environment.

For the potential vulnerabilities being applicable to the TOE in its operational environment and, hence, which were candidates for testing applicable to the TOE in its operational environment, the evaluator devised the attack scenarios where these potential vulnerabilities could be exploited.

For each such attack scenario the evaluator firstly performed a theoretical analysis on the related attack potential. Where the attack potential was HIGH or slightly beyond HIGH, the evaluator conducted penetration tests for such attack scenarios.

Test ID	Description
PEN_1_cHSM_Memory_Access	Verifying if a cHSM can access other cHSM's memory.
PEN_2_cHSM_Syscalls	Verifying if the cHSM can bypass the protection on calling specific syscalls.
PEN_3_Removed_Commands	Verifying if all commands that should not exist in the production version are really non-existing, even if used in combination with another GLAD/RAPP command.

PEN_4_Authentication_Failure_Ring_Buffer	Verifying that the authentication failure ring buffer cannot be overloaded, such that it does prevent users brute forcing authentication.
PEN_5_Authentication_Bypassing	Some commands require a quorum of global admins to be authenticated. The objective of this test is to verify if it is possible to reach the quorum with less global admins then required or by using expired/blocked/deleted admins.
PEN_6_USB_Fuzzing	The test is aiming at verifying if the TOE processes input via USB interface properly. The USB interface is disabled for all users, however it is not completely physically disabled.

Table 5: Penetration Test Cases

In addition, the evaluator also attempted to bypass the TOE's chassis tamper detection mechanism via physical attacks and concluded that such attack scenarios are feasible but it would leave obvious tamper evidence on the outside of the TOE which would be noticeable during regular inspection. Moreover, it is important to note that the TOE is assumed to be operated in a protected environment where only authorised administrators would have physical access to the TOE.

8.3.3 Test Results

The evaluator found no exploitable vulnerability in the TOE when operated in the evaluated configuration. No residual risks were identified.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM and requirements of SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 augmented by ALC_FLR.3 and AVA_VAN.5 assurance package

This implies that the TOE satisfies the security requirements specified in the Security Target [1].

10 Obligations and recommendations for the usage of the TOE

The documents as outlined in Table 1: Deliverables of the TOE contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that not covered by the TOE shall be fulfilled by the operational environment of the TOE. In particular, the TOE relies on the physical environment of the provisioning and deployment site to prevent unauthorised physical and logical access to the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certification.

11 Acronyms

AES	Advanced Encryption Standard
CC	Common Criteria for IT Security Evaluation
CCRA	Common Criteria Recognition Arrangement
CCTL	Common Criteria Test Laboratory
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CSA	Cyber Security Agency of Singapore
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
RSA	Rivest-Shamir-Adleman
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TDES	Triple Decryption Encryption Standard
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

[1] Utimaco IS GmbH, “u.trust Anchor - Security Target for u.trust Anchor v1.0.1,” 2022.

[2] EN 419 221-5: 2018, “Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services v1.0”.

[3] Utimaco IS GmbH, “u.trust Anchor - Security Target Lite for u.trust Anchor v1.0.1”.

[4] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2017-04-001]. Version 3.1 Revision 5,” 2017.

[5] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5,” 2017.

[6] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2018-04-003] Version 3.1 Revision 5,” 2017.

[7] Common Criteria Maintenance Board (CCMB), “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5,” 2017.

[8] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 5.0,” 2018.

[9] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 5.0,” 2018.

[10] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 5.0,” 2018.

[11] Utimaco IS GmbH, “u.trust Anchor CC Manual Administrators v1.0.6”.

[12] Utimaco IS GmbH, “u.trust Anchor CC cHSM Manual Administrators v1.0.9”.

----------End of Report ----------