Certification Report

Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0

Sponsor and developer:	***Cryptomathic A/S*** **Aaboulevarden 22** **DK-8000 Aarhus C** **Denmark**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2300116-01-CR**
Report version:	**1**
Project number:	NSCIB-**2300116-01**
Author(s):	**Haico Haak**
Date:	**30 April 2024**
Number of pages:	**12**
Number of appendices:	**0**

Digitally signed by Grițcan Dorin
Date: 2024.09.23 23:57:31 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

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 Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0. The developer of the Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0 is Cryptomathic A/S located in Aarhus, Denmark 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 trustworthy system that offers remote digital signatures as a service. It ensures that the signing key(s) of a signer user are only used under the sole control of the signer user for the intended purpose. The TOE provides a remote service from which the signer user can obtain digital signatures. The functionality and security features of the TOE are centered around protecting this operation, the signer users, and the keys used for the signature generation.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 30-04-2024 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 Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0, 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 Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0 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 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.

The TOE is stated as a Qualified Signature Creation Device and Qualified Seal Creation Device for the purposes of electronic identification and trust services as detailed by the [EU-REG]. The evaluation by SGS Brightsight included an examination of the TOE according to the eIDAS Dutch Conformity Assessment Process Version 6 0.

TrustCB B.V., as the Dutch eIDAS-Designated Body responsible in The Netherlands for the assessment of the conformity of qualified electronic signature and/or qualified electronic seal creation devices declares that the evaluation meets the conditions for eIDAS certification for listing on the EU eIDAS compiled list of Qualified Signature/Seal Creation Devices.

[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 Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0 from Cryptomathic A/S located in Aarhus, Denmark.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	One of the following: • CryptoServer CP5 Se12 • CryptoServer CP5 Se52 • CryptoServer CP5 Se500 • CryptoServer CP5 Se1500	5.1.0.0
Software	Cryptomathic Signer SAM v6.0 to be loaded onto an HSM from the Utimaco CryptoServer Se-Series Gen2 CP5, v5.1.0.0.	V6.0

To ensure secure usage a set of guidance documents is provided, together with the Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.3.5.

2.2 Security Policy

The TOE is a trustworthy system that offers remote digital signatures as a service. It ensures that the signing key(s) of a signer user are only used under the sole control of the signer user for the intended purpose. The TOE provides a remote service from which the signer user can obtain digital signatures. The functionality and security features of the TOE are centered around protecting this operation, the signer users, and the keys used for the signature generation.

The TOE has the following features:

- TOE initialization
  - The TOE provides a command for initialization and creation of initial privileged users.
- Operator management
  - Security officers can create other privileged users.
- System management
  - Security officers can handle system configuration.
- Signer user management
  - User managers can create signer users.
  - User managers can generate signing keys and Signature Validation Data (SVD) using a Cryptographic Module and assign the signing key identifier and SVD to a signer user.
- Signature operation
  - Signer users can supply a document to be signed.
  - The link between signer authentication, DTBS/R and signing key identifier is handled by the Signature Activation Data (SAD). This SAD is securely exchanged with the TOE using the Signature Activation Protocol (SAP). Within the TOE the following actions are performed:
    - The TOE verifies the integrity of the SAD.

- The TOE verifies that the SAD binds together the signer user authentication, DTBS/R(s) and signing key identifier.
- The TOE verifies the level of authentication of the signer user.
- The TOE verifies that the signing key belongs to the signer user.
- If required, the TOE verifies that a certificate has been assigned to the SVD to ensure that the signing key has been certified.
- The TOE uses authorisation data to activate the signing key within the Cryptographic Module.
- The TOE uses the Cryptographic Module to create signatures.

- An audit trail is produced of all security relevant events within the TOE. Management access to audit trail is outside the scope of the TOE.

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 4.2 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.

Note that EN 419241-2 Protection Profile claims 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, and protects against unauthorised software and configuration changes on the TOE and the hardware appliance in which it is contained (“OE.Env Protected operating environment”).

The ST follows the PP and also claims OE.Env, 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 TOE is the SAM software component and is loaded onto an HSM which is tamper protected. The HSM is installed with firmware which comprises the Cryptographic Module functionality.

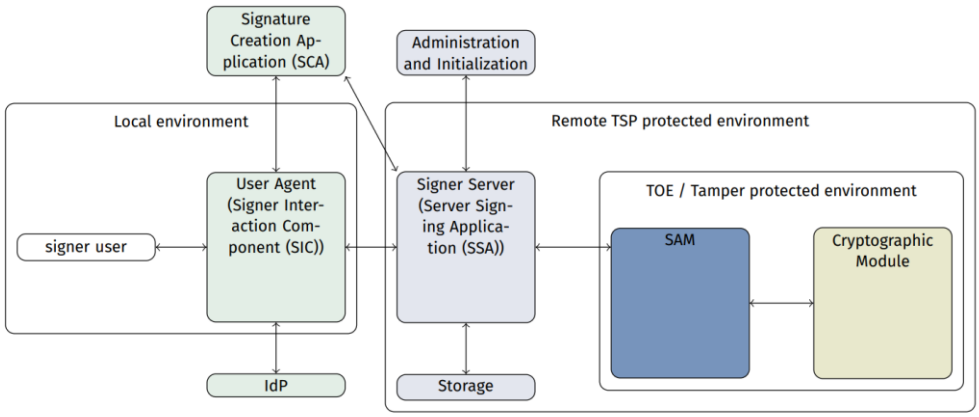

Figure 1 The TOE in its environment

2.5 Documentation

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

Identifier	Version
Guidance for implementing Server Signing Applications with Cryptomathic Signer SAM in compliance with eIDAS	revision 8e3009d265b4f4bcc0de66e47bb06fde30148664
Cryptomathic Signer SAM API 6.0	revision 15ea87c30176b9ef9b06c08cf96c6377534028e6
Cryptomathic HSM Setup and Maintenance with SCE. Utimaco CryptoServer CP5	v.1.7

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 has performed extensive testing on functional specification, subsystem and SFR-enforcing module level. The testing was largely automated using test suites. Test scripts were extensively used to verify that the functions return the expected values.

The underlying hardware test results are extendable to composite evaluations, as the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer has provided the TOE and a test environment. The evaluators have reproduced all developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

Given the restrictions imposed by the PP (which prevents any physical attack and any side channel attack that requires physical proximity to the TOE), the evaluator focused on vulnerabilities related to design/architectural flaws that would lead intended users to abuse the TOE. The methodology involves the following five steps:

1. The first step of this type of vulnerability analysis is the identification of areas of concern (as defined in [CEM] and the [CWE]).
   - The areas of concern are identified by the evaluator using the generic weaknesses enumeration database [CWE] version 3.1 as inspiration and the [CEM, Appendix B]. The CWE database is an open source publicly maintained dictionary of SW weaknesses.
   - Examples of areas of concern are Accessibility, Cryptography, and Secure Channel.
2. Collecting possible vulnerabilities from the design assessment by asking security questions inspired by generic weaknesses separately for all security implementations of the TOE.
3. Collecting possible vulnerabilities from applicable attack lists and public vulnerability search.
4. These security relevant questions are then translated into TOE-specific possible vulnerabilities in the TOE.

5. The evaluator argues whether a possible vulnerability is removed or sufficiently mitigated by the TOE implementation and/or functional testing evidence. If yes, the possible vulnerability is considered as solved, otherwise it is uniquely labelled as potential vulnerability POT_VUL_xxx. Potential vulnerabilities are then addressed in the context of further assessment, penetration tests and/or further code review.

If the assessment of a potential vulnerability leads to a penetration test (or penetration tests), they are collected in the penetration test plan.

2.6.3 Test configuration

The TOE was tested in the configuration of the Utimaco CryptoServer CP5 5.1.0.0 (CryptoServer CP5 Se1500 5.1.0.0). The [ETRfC] of the underling hardware concluded that all Utimaco CryptoServer hardware models listed in the ST are equal from a security perspective. Therefore test on one Utimaco HSM model sufficiently represent the behavior of the Cryptomathic Signer SAM software on other Utimato HSM models listed in the ST.

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.

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

Sites involved in the development and production of the hardware platform were re-used by composition.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0.

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 Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[PP]*.

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 Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0 Security Target, Revision 8e3009d265b4f4bcc0de66e47bb06fde30148664, February 23, 2024 *[ST]* is included here by reference.

4 Definitions

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

DCAP	eIDAS Dutch Conformity Assessment Process
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PKI	Public Key Infrastructure
PP	Protection Profile
QSCD	Qualified Signature/Seal Creation Device
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
[PP]	EN 419241-2:2019 Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, Version 0.16, registered under the reference ANSSI-CC-PP-2018/02-M01, 18 May 2020
[eIDAS-REP]	Assessment Reporting Sheet eIDAS, 04 April 2024, reference 24-RPT-499 v1.0
[ETR]	Evaluation Technical Report “Cryptomathic Signer SAM 6.0” – EAL4+, Version 5.0, 24 April 2024
[EU-REG]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[HW-CERT]	NSCIB-CC-2300142-01, CryptoServer CP5 Se12 5.1.0.0, CryptoServer CP5 Se52 5.1.0.0, CryptoServer CP5 Se500 5.1.0.0, CryptoServer CP5 Se1500 5.1.0.0, 05-12-2023
[HW-ST]	Security Target Lite for CryptoServer Se-Series Gen2 CP5, version 2.1.2, 21 November 2023
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	Cryptomathic Signer SAM v6.0 for Utimaco Cryptoserver CP5 v5.1.0.0 Security Target, Revision 8e3009d265b4f4bcc0de66e47bb06fde30148664, February 23, 2024

(This is the end of this report.)