

Certification Report

Cryptomathic Signer SAM version 5.1 for Utimaco Cryptoserver CP5

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-2400105-01-CR**

Report version: **1**

Project number: **NSCIB-2400105-01**

Author(s): **Haico Haak**

Date: **16 October 2024**

Number of pages: **11**

Number of appendices: **0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

CONTENTS

Foreword	3
Recognition of the Certificate	4
International recognition	4
European recognition	4
1 Executive Summary	5
2 Certification Results	6
2.1 Identification of Target of Evaluation	6
2.2 Security Policy	6
2.3 Assumptions and Clarification of Scope	6
2.3.1 Assumptions	6
2.3.2 Clarification of scope	6
2.4 Architectural Information	7
2.5 Documentation	7
2.6 IT Product Testing	7
2.6.1 Testing approach and depth	7
2.6.2 Independent penetration testing	8
2.6.3 Test configuration	8
2.6.4 Test results	8
2.7 Reused Evaluation Results	8
2.8 Evaluated Configuration	9
2.9 Evaluation Results	9
2.10 Comments/Recommendations	9
3 Security Target	10
4 Definitions	10
5 Bibliography	11

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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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 version 5.1 for Utimaco Cryptoserver CP5. The developer of the Cryptomathic Signer SAM version 5.1 for Utimaco Cryptoserver CP5 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 offers remote signing using an HSM containing the Cryptographic module and which, when operated according to guidelines, provides a tamper protected environment. The TOE is the software component (SAM) loaded as a local application onto the protected environment of the HSM. It is created to be responsible for all logic performed and for making the final access decisions about whether to allow the usage of a given signing key.

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 14-05-2020 ([CC-20-159381](#)). The current evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 16 October 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 major changes from previous evaluations are a change of potting material in the HSM platform and resulting changes in documentation.

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 Cryptomathic Signer SAM version 5.1 for Utimaco Cryptoserver CP5, 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 version 5.1 for Utimaco Cryptoserver CP5 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 for the purposes of electronic identification and trust services as detailed by the [EU-REG]. The evaluation by SGS Brightsight B.V. 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 version 5.1 for Utimaco Cryptoserver CP5 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: <ul style="list-style-type: none"> • 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. 	5.1.0.0
Software	Cryptomathic Signer SAM for Utimaco	5.1

To ensure secure usage a set of guidance documents is provided, together with the Cryptomathic Signer SAM version 5.1 for Utimaco Cryptoserver CP5. 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 enables authenticated users to create digital signatures. Thanks to secure protocols, the protection of a tamper evident environment, and the strict administration procedures enforced by the trust service providers operating the service, it is possible to provide an electronic signature service to key owners.

The TOE offers remote signing using an HSM containing the Cryptographic module and which, when operated according to guidelines, provides a tamper protected environment. The TOE is the software component (SAM) loaded as a local application onto the protected environment of the HSM. It is created to be responsible for all logic performed and for making the final access decisions about whether to allow the usage of a given signing key.

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 [EN419241-2] 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.

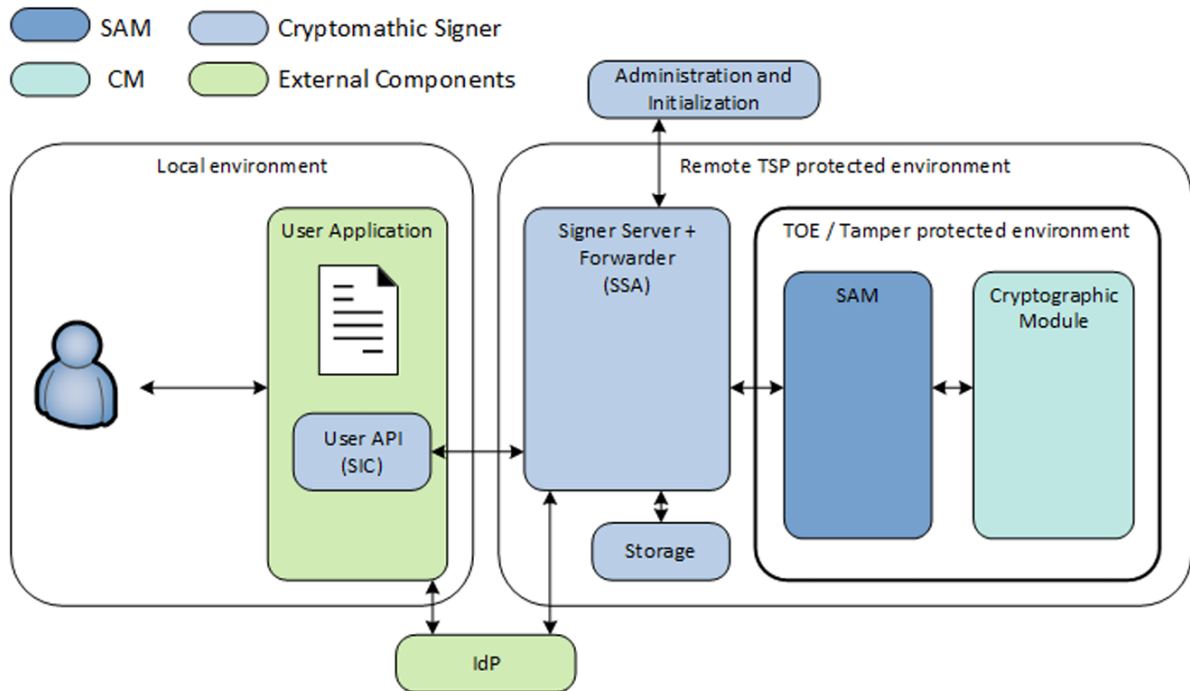


Figure 1: The TOE in its environment

2.5 Documentation

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

Identifier	Version
Cryptomathic Signer SAM CC Guidance: AGD-PRE	2.3
Cryptomathic Signer SAM CC Guidance: AGD-OPE	3.4
Cryptomathic Signer 5.1 HSM Environment Requirements	2.2
Cryptomathic Signer SAM CC Compliant Role Configuration	2.0
HSM Setup and Maintenance with SCE. Signer SAM 5.1 for Utimaco CryptoServer CP5	1.5

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

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.

2.6.2 Independent penetration testing

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 total additional test effort expended by the evaluators was 1 weeks. During that test campaign, 0% of the total time was spent on Perturbation attacks, 0% on side-channel testing, and 100% on logical tests.

This test effort excludes the test effort spent in the baseline certification and only reflects the effort applied during this recertification activity.

2.6.3 Test configuration

The TOE was tested in the configuration of the Utimaco CryptoServer Se 1500 Gen2 CP5.

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

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.

There has been extensive reuse of the ALC aspects for the sites involved in the software component of the TOE. Sites involved in the development and production of the hardware platform were reused by composition.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Cryptomathic Signer SAM version 5.1 for Utimaco Cryptoserver CP5.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the [EAR], 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 version 5.1 for Utimaco Cryptoserver CP5, 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 [EN419241-2].

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 v. 5.1 Security Target for Utimaco Cryptoserver CP5, version 5.6, 28 August 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:

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
[eIDAS-REP]	Assessment Reporting Sheet eIDAS, 24-RPT-10 v1.0, 29-August-2024
[EN419241-2]	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.
[EAR]	Evaluator Assessment of Changes Report (EAR) for Cryptomathic Signer SAM version 5.1 for Utimaco Cryptoserver CP5 – Partial ETR, Version 4.0, 15 October 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]	Utimaco 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 certificate: NSCIB-CC-2300142-01, issued, 05-12-2023
[HW-ETRFc]	ETR for Composition for CryptoServer Se-Series Gen2 CP5 EAL4+, v3.0, 5 December 2023
[HW-ST]	CryptoServer Security Target 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 v. 5.1 Security Target for Utimaco Cryptoserver CP5, version 5.6, 28 August 2024

(This is the end of this report.)