TÜVRheinland®
Precisely Right.

Certification Report

Cryptomathic Signer SAM version 5.1 for Utimaco Cryptoserver CP5

Sponsor and developer: ***Cryptomathic A/S***
Jargergardsgade 118
DK-8000 Aarhus C
Denmark

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-159381-CR2**
Report version:	**1**
Project number:	**159381**
Author(s):	**Wouter Slegers**
Date:	**21 April 2020**
Number of pages:	**11**
Number of appendices:	**0**

Headoffice:
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 Dutch Chamber of Commerce 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 license 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 (site) security target or protection profile, in addition to this certification report, in order 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 and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

eIDAS-Regulation

TÜV Rheinland Nederland B.V., operating the Netherlands Scheme for Certification in the Area of IT Security (NSCIB), has been notified as a Designated Certification Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 *[EU-REG]*.

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 C, 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 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.

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 15-11-2019. The re-evaluation also took place by Brightsight B.V. and was completed on 21-04-2020 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a “recertification with major changes”.

The major change is the addition of signing keys based on elliptic curve cryptography (ECC).

The security evaluation re-used 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 provides 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]* and the Dutch Conformity Assessment Process *[DCAP],* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

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 meets the requirements laid down in Annex II of Regulation (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014. The product meets the requirements defined in [EU-REG] article 29 and article 39 and thus is a QSCD in the sense of [EU-REG]. It will be listed on the NSCIB Certified Products list and will be notified to the European Commission (eIDAS). It should be noted that the certification results only apply 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 releasable 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 C, Denmark.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	One of the following: Utimaco CryptoServer CP5 Se12 Utimaco CryptoServer CP5 Se52 Utimaco CryptoServer CP5 Se500 Utimaco CryptoServer CP5 Se1500	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. Details can be found in section 2.5 of this report.

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in 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 it is contained in (“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.

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	2.0
Cryptomathic Signer SAM CC Guidance: AGD-OPE	3.2
Cryptomathic Signer 5.1 HSM Environment Requirements	2.0
Cryptomathic Signer SAM CC Compliant Role Configuration	2.0
Cryptomathic HSM Setup and Maintenance with SCE. Utimaco CryptoServer CP5	1.4

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. In this evaluation, four penetration tests were devised.

2.6.3 Test Configuration

The TOE was tested in the configuration of the Utimaco CryptoServer Se 1500 Gen2. The *[ETRfC]* of the underling hardware concluded that all Utimaco CryptoServer hardware models listed in the ST are no difference 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 Testing 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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential".

The algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5).

2.7 Re-used evaluation results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been re-used, but vulnerability analysis and penetration testing has been renewed.

There has been extensive re-use 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 re-used 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 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* which references a ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[CCDB-2007-09-01]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that have to be considered when this TOE is used as platform in a composite evaluation.

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 *[PP]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 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 need to 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. In order for the evolution of attack methods and techniques to be covered, he 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, v5.5, 12 March 2020 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms 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 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.

[CR-SSCD-PP2] Certification Report for Protection profiles for secure signature creation device — Part 2: Device with key Generation, CEN/TC 224, BSI-CC-PP-0059-2009-MA-02, Version 2.0.1, 30 June 2016.

[DCAP] Dutch Conformity Assessment Process v3.0, dated 28-02-2019.

[ETR] Evaluation Technical Report Cryptomathic Signer SAM version 5.1 for Utimaco Cryptoserver CP5, 20-RPT-245, Version 3.0, 21 April 2020.

[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] Certification Report 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, NSCIB-CC-222073-CR, version 1.1, dated 14 March 2019
Maintenance Report 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, NSCIB-CC-222073-MR, version 1.0, dated 21 April 2020.

[HW-ETRfC] ETR for Composition of CryptoServer Se-Series Gen2 CP5 EAL4+, 18-RPT-622, v6.0, 21 April 2020.

[HW-ST] CryptoServer Security Target for CryptoServer Se-Series Gen2 CP5 2.0.2, 1 April 2020.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[PP] prEN 419 241-2 Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, version 0.16.

[ST] Cryptomathic Signer SAM v. 5.1 Security Target for Utimaco Cryptoserver CP5, v5.5, 12 March 2020.

(This is the end of this report).