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

Sponsor and developer:	***Utimaco IS GmbH*** **Germanusstr. 4** **52080 Aachen** **Germany**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-222073-CR**
Report version:	**1.2**
Project number:	**222073**
Author(s):	**Wouter Slegers**
Date:	**27 May 2020**
Number of pages:	**15**
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

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)
Certificate number	**CC-19-222073**

TÜV Rheinland Nederland B.V certifies:

Certificate holder and developer	**Utimaco IS GmbH** **Germanusstr. 4, 52080 Aachen, Germany**
Product and assurance level	**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** Assurance Package: ▪ EAL4 augmented with AVA_VAN.5 Protection Profile Conformance: ▪ prEN 419 221-5 Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services, v0.15, 2016-11-29, registered under the reference ANSSI-CC-PP-2016/05
Project number	**222073**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL7

The Designated Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 declares that:

- The IT product identified in this certificate is a Qualified Signature/Seal Creation Device (QSCD) where the electronic signature/seal creation data is held in an entirely but not necessarily exclusively user-managed environment.
- The IT 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.
- Conformity of the IT product with the requirements of Annex II of REGULATION has been certified with an evaluation process that fulfils the requirements of Article 30(3.(b)) of REGULATION and the Dutch Conformity Assessment Process (DCAP)."
- The IT product identified in this certificate is not a Qualified Signature/Seal Creation Device (QSCD) where a Qualified Trust Service Provider (QTSP) manages the electronic signature/seal creation data on behalf of a signatory/creator of a seal, but might be used as a component of such a QSCD in conformity with the applicable certification of that QSCD against REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity	Date of 1st issue : **19-12-2018**
	Date of 2nd issue : **14-03-2019**
	Date of 3d issue : **14-05-2020**
	Certificate expiry : **19-12-2023**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

R. Kruit, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

TÜVRheinland®
Precisely Right.

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 BV, 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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the 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. The developer of the 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 is Utimaco IS GmbH located in Aachen, Germany and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The CryptoServer CP5 is a hardware security module whose primary purpose is to provide 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 CryptoServer CP5 supports local signing/sealing and server signing in accordance with EN 419 241-1 Security Requirements and EN 419 241-2 Protection Profile for QSCD for Server Signing. Furthermore, it provides the functionality for creating protected backups of keys and for secure update of defined parts of the TOE software.

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 9 October 2018. The re-evaluation also took place by Brightsight B.V. and was completed on 10 December 2018 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 leading to a new certificate are the addition of an internal interface for SAM applications and the associated ST, firmware and guidance updates.

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 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, 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 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 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 4 *[CEM]* and the Dutch Conformity Assessment Process *[DCAP],* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 *[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 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 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 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 from Utimaco IS GmbH located in Aachen, Germany.

The TOE is comprised of the following main components:

Item	Identifier	Version
Hardware	Hardware of the TOE, PCIe security module (with/without crypto accelerator)	5.01.4.0 Se500/Se1500 (module with crypto accelerator) 5.01.4.0 Se12/Se52 (module without crypto accelerator)
Software	Boot Loader	5.01.4.0
	FPGA	5.01.0.8
	Sensory Controller	2.00.0.31
	CryptoServer CP5 firmware package consisting of the following firmware modules:	
	ADM (.msc and .sys) (Module Administration)	3.0.25.5
	AES (.msc and .sys) (AES Cryptography)	1.4.1.7
	ASN1 (.msc and .sys) (Decoding and Encoding ASN.1)	1.0.3.4
	CMDS (.msc and .sys) (Command Scheduler)	3.6.0.11
	CXI (.msc) (Cryptographic Services eXternal Interface)	2.2.3.6
	CXIAL (.msc) (CXI Abstraction Layer)	1.0.0.0
	DB (.msc and .sys) (Database Management)	1.3.2.4
	ECA (.msc and .sys) (Elliptic Curve Arithmetic)	1.1.12.4
	ECDSA (.msc and .sys) (ECDSA Cryptography)	1.1.16.2
	EXAR (.msc and .sys) (Driver for Crypto Accelerator)	2.2.1.1
	HASH (.msc and .sys) (Hashing Algorithms)	1.0.12.1
	HCE (.msc and .sys) (Generic Internal Interface for Crypto Accelerator)	2.2.2.3
	LNA (.msc and .sys) (Long Number Arithmetic)	1.2.4.4
	MBK (.msc) (Master Backup Key Management)	2.3.0.0
	POST (.msc and .sys) (Power-On Self-Tests)	1.0.0.2
	SMOS (.msc and .sys) (Security Module Operating System)	5.5.9.2
	UTIL (.msc and .sys) (Utilities for RTC and RNG)	3.0.5.3

	VDES (.msc and .sys) (DES Cryptography)	1.0.9.4
	VRSA (.msc and .sys) (RSA Cryptography)	1.3.6.5

To ensure secure usage a set of guidance documents is provided together with the 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. Details can be found in section ”Documentation” of this report.

2.2 Security Policy

The TOE implements key import and export, generation, backup and restore, use and destruction. Keys attributes can be assigned and determine what operations an user can perform on and with a given key. Audit logs are generated for specified events.

Supported cryptographic operations include: AES, RSA, ECDSA keygeneration, encryption and decryption, RSA ECDSA signature generation and verification, HMAC, SHA-2 and SHA-3 calculations, Diffie-Hellman key agreement, KDF Key Derivation, and random number generation.

See the *[ST]* for details.

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 5.2 of the *[ST]*.

2.3.2 Clarification of scope

The TOE is intended for use in a hardware appliance. The appliance and its software are not part of the TOE scope.

Note that EN 419 221-5 Protection Profile is certified as version v0.15 and issued at European Norm as version v1.0. These versions of the Protection Profile only differ in formal and editorial aspects, version v1.0 being the sanitized version of v0.15. The two versions v1.0 and v0.15 do not differ in any of the requirements or objectives.

Note also that the PP 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”).

Following the PP application note 33 for FPT_PHP.1 and application note 34 for FPT_PHP.3, the developer’s testing in accordance to the specifically section 7.7.2 “Physical security general requirements” and section 7.7.3 “Physical security requirements by each physical security embodiment” in ISO/IEC 19790:2012 has been verified under this context OE.Env.

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.

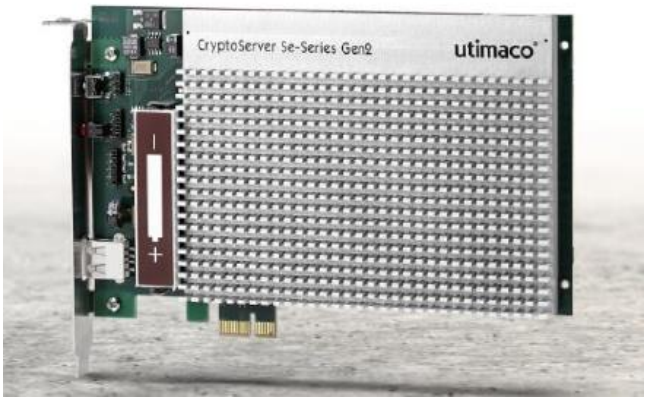
The TOE can optionally also be used for implementing a QSCD for eIDAS-compliant remote Server Signing in the sense of CEN Protection Profile EN 419 241-2, “Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing”. In this case, the customer has to develop a Signature Activation Module (SAM) module and certify it against this CEN Protection

Profile EN 419 241-2. The SAM may be either implemented as external SAM (as an application using the external interfaces of the TOE) or internal SAM (as firmware using the internal interfaces of the TOE).

The possibility of the SAM was in scope of the evaluation. The SAM itself is out of scope of this evaluation. For SAM developers see the guidance “Internal SAM developer documentation”. For composite evaluators see *[ETRfC]*.

2.4 Architectural Information

The CryptoServer CP5 is designed as a protected cryptographic module provided in form of a PCIe (PCI express) plug-in card (specific hardware and software product).



All hardware components of the TOE, including the Central Processing Unit, all memory chips, Real Time Clock, and hardware noise generator for random number generation, are located on a printed circuit board (PCB). These hardware components are completely covered with potting material (epoxy resin) and a heat sink. In total this is called “PCIe security module”.

To enable communication of the cryptographic module with a host, the PCIe security module offers a PCIe interface and two USB interfaces. The PCIe security module is plugged into the PCIe bus interface of the backplane.

Before delivery the PCIe security module can be optionally integrated into an Utimaco CryptoServer LAN appliance.

Regardless of the TOE variant, at a high level of abstraction, the TOE is structured into the following three subsystems:

1. Hardware: all hardware components for example CPU and memory.
2. Boot Loader: first software started inside the security module after a reboot.
3. Firmware Modules: all firmware modules containing all the software functionality needed after end of boot phase, like for example SMOS, CXI, CMDS and HASH.

2.5 Documentation

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

Item	Identifier	Version
Manuals	*Operating Manual in three variants (PCIe/LAN v4/LAN v5):*	
	CryptoServer Se-Series Gen2 CP5 PCIe Operating Manual	2017-0006-en, version 1.0.15
	CryptoServer Se-Series Gen2 CP5 LAN Operating Manual	2017-0005-en, version 1.0.13
	CryptoServer Se-Series Gen2 CP5 LAN V5 Operating Manual	2018-0011-en, version 1.0.1
	User Manual:	
	CryptoServer Se-Series Gen2 CP5 Administration Manual	2017-0008, version 2.0.2

	Interface Specifications:	
	CryptoServer - Firmware Module CXI for CryptoServer CP5 – Interface Specification	2017-0010, version 1.0.3
	CryptoServer - Firmware Module ADM - Interface Specification - ADM Version ≥ 3.0.0.0	2009-0010, version 1.7.6
	CryptoServer - Firmware Module CMDS - Interface Specification - CMDS Version ≥ 3.0.0.0	2009-0002, version 1.8.3
	CryptoServer – Firmware Module MBK – Interface Specification	2003-0006, version 1.10.1
Internal SAM Developer Documentation (only delivered to developers of an internal SAM)	CryptoServer Se-Series Gen2 CP5 - SAM Developer Guide	2018-0013, version 1.1.3
	Interface Specifications:	
	CryptoServer - Firmware Module AES - Interface Specification	2003-0008, version 1.6.1
	CryptoServer - Firmware Module CXIAL – Interface Specification	2018-0002, version 1.0.1
	CryptoServer – Firmware Module DB – Interface Specification	2002-0009, version 1.1.9
	CryptoServer – Firmware Module ECA – Interface Specification	2006-0004, version 1.3.6
	CryptoServer – Firmware Module ECDSA – Interface Specification	2006-0005, version 1.4.8
	CryptoServer – Firmware Module HASH – Interface Specification	2002-0010, version 1.6.2
	CryptoServer – Firmware Module SMOS – Interface Specification - SMOS Version ≥ 2.5.0.0	2008-0001, version 2.5.11
	CryptoServer – Firmware Module UTIL – Interface Specification - UTIL Version ≥ 3.0.0.0	2009-0012, version 1.2.5
	CryptoServer – Firmware Module VRSA – Interface Specification	2002-0019, version 1.9.4

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 testing on functional specification and subsystem level. All parameter choices have been addressed at least once. The testing was largely automated using industry standard (FIPS-140-2 CAVP) and proprietary test suites. Test scripts were extensively used to verify that the functions return the expected values. Additional fuzzing testing and code inspection are used for hard to externally verify properties.

For the testing performed by the evaluators, the developer has provided samples and a test environment. The evaluators have reproduced a selection of the developer tests, as well as a 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. For this reason, the evaluator needed to find a methodical approach to scout the TOE implementation searching for such design/architectural flaws.

- **Step 1:** The first step of this type of vulnerability analysis was the identification of areas of concern (as defined in [CEM]).
  - The areas of concern were identified by the evaluator using the generic weaknesses enumeration database CWE version 3.1 (last updated April 2018) as inspiration. The CWE database is an open source publicly maintained dictionary of SW weaknesses.
  - Examples of areas of concern that were identified by the evaluator are Accessibility, Cryptography, Secure Channel.

- **Step 2:** iteratively, for each security function (and hence indirectly for each SFR), the evaluator formulates security relevant questions for each identified area of concern.

- **Step 3:** These security relevant questions were then translated into TOE-specific possible vulnerabilities (uniquely identified with **POS_VUL.xxx.yyy**). Note that the evaluator **also** uses the **list of publicly known crypto attacks to formulate possible vulnerabilities as well as web searches and cvedetails.com.**
  - The public vulnerabilities that were considered by the evaluator as one of the inputs to identify possible vulnerabilities. This included known crypto vulnerabilities, APDU/API level attacks, Spectre/Meltdown/Rowhammer and ROCA (Return of Coppersmith attack)
  - In total, on basis of TOE design and publicly available sources of information, the evaluator identified more than 120 possible vulnerabilities.
- **Step 4:** the evaluator argued whether each possible vulnerability was removed or sufficiently mitigated by the TOE implementation/environment/functional testing evidence. If yes, the possible vulnerability is considered as solved, otherwise it was uniquely labeled.
  - With this process, the evaluator identified a total of 15 potential vulnerabilities. All other possible vulnerabilities were solved.
  - The remaining potential vulnerabilities were addressed by penetration tests (a total of 6 weeks of effort) and further code review.
  - No vulnerabilities remained after these tests.

2.6.3 Test Configuration

Testing was performed on the TOE in the Se1500 (with crypto accelerator) and Se52 (without crypto accelerator) figurations. This is representative for all TOE variants.

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.

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

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Re-used evaluation results

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

One site (Utimaco IS GmbH in Aachen) has been audited as part of the original evaluation, however no STAR report has been made and hence this audit is not re-usable outside the NSCIB scheme.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number 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. See the preparative guidance for acceptance steps and verification procedures.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] 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 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, 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. Certain aspects of the TOE's security, in particular the countermeasures against physical attacks, depend on accurate conformance to the user guidance for the environment. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details with respect to the resistance against certain attacks.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself 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.

[2] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

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>.

To fend off attackers with high attack potential appropriate cryptographic algorithms with adequate key lengths must be used (references can be found in national and international documents and standards).

3 Security Target

The Security Target for CryptoServer Se-Series Gen2 CP5, CryptoServerCP5_ST_2016-0002, version 2.0.0 *[ST]* is included here by reference.

Please note that for the need of publication a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
DCAP	Dutch Conformity Assessment Process
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands scheme for certification in the area of IT security
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
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 4, September 2012.
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
[DCAP]	Dutch Conformity Assessment Process v3.0, dated 28-02-2019
[ETR]	Evaluation Technical Report Evaluation Technical Report CryptoServer Se-Series Gen2 CP5 EAL4+, 18-RPT-621, Version 3.0, 18 December 2018.
[ETRfC]	ETR for Composition of CryptoServer Se-Series Gen2 CP5 EAL4+, 18-RPT-622, version 4.0, 18 December 2018.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September 2017.
[PP]	prEN 419 221-5 Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services, v0.15, 2016-11-29, registered under the reference ANSSI-CC-PP-2016/05
[ST]	Security Target for CryptoServer Se-Series Gen2 CP5, CryptoServerCP5_ST_2016-0002, version 2.0.0.
[ST-lite]	Security Target Lite for CryptoServer Se-Series Gen2 CP5, version 2.0.0
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).