Certification Report

CryptoServer Se-Series Gen2 CP5, versions:

CryptoServer CP5 Se12 5.1.2.0,
CryptoServer CP5 Se52 5.1.2.0,
CryptoServer CP5 Se500 5.1.2.0,
CryptoServer CP5 Se1500 5.1.2.0

Sponsor and developer: ***Utimaco IS GmbH***
Germanusstr. 4
52080 Aachen
Germany

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-2300142-02-CR**
Report version:	**1**
Project number:	**NSCIB-2300142-02**
Author(s):	**Haico Haak**
Date:	**26 May 2025**
Number of pages:	**15**
Number of appendices:	**0**

CONTENTS

Foreword **3**

Recognition of the Certificate **4**

International recognition 4
European recognition 4

1 Executive Summary **5**

2 Certification Results **7**

2.1 Identification of Target of Evaluation 7
2.2 Security Policy 8
2.3 Assumptions and Clarification of Scope 8
2.3.1 Assumptions 8
2.3.2 Clarification of scope 8
2.4 Architectural Information 9
2.5 Documentation 10
2.6 IT Product Testing 11
2.6.1 Testing approach and depth 11
2.6.2 Independent penetration testing 11
2.6.3 Test configuration 11
2.6.4 Test results 12
2.7 Reused Evaluation Results 12
2.8 Evaluated Configuration 12
2.9 Evaluation Results 12
2.10 Comments/Recommendations 12

3 Security Target **14**

4 Definitions **14**

5 Bibliography **15**

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 CryptoServer Se-Series Gen2 CP5. The developer of the CryptoServer Se-Series Gen2 CP5 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 as a QSCD in accordance with [EU-REG] where the electronic signature/seal creation data is held in an entirely but not necessarily exclusively user-managed environment. Moreover, the CryptoServer CP5 is suitable for use by trust service providers (TSP) supporting electronic signature and electronic sealing operations, certificate issuance and revocation, time stamp operations, and authentication services.

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 19 December 2018 (CC-19-222073). The TOE was again evaluated by SGS Brightsight B.V and certified under the accreditation of TrustCB on 5 December 2023. The current evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 26 May 2025 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 bug fixes, updates of guidance document references, lifecycle updates, and the resulting updates in the Security Target.

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 CryptoServer Se-Series Gen2 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 CryptoServer Se-Series Gen2 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.

Note: The security target *[ST]* refers to the “CryptoServer Se-Series Gen2 CP5” as the collection of the 4 versions “CryptoServer CP5 Se12 5.1.2.0, CryptoServer CP5 Se52 5.1.2.0, CryptoServer CP5 Se500 5.1.2.0, CryptoServer CP5 Se1500 5.1.2.0”.

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.

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

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 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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the CryptoServer Se-Series Gen2 CP5 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	SW Boot Loader	5.01.4.0
	FPGA	5.01.0.8
	Sensory Controller	2.00.0.31
	and 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)	
	asn1.msc:	1.0.3.8
	asn1.sys:	1.0.3.4
	CMDS (.msc and .sys) (Command Scheduler)	
	cmds.msc:	3.6.0.13
	cmds.sys:	3.6.0.11
	CXI (.msc) (Cryptographic Services eXternal Interface)	2.2.3.7
	CXIAL (.msc) (CXI Abstraction Layer)	1.0.0.1
	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)	
	smos.msc:	5.6.6.1
	smos.sys:	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 Se-Series Gen2 CP5. For details, see section 2.5 “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 key generation, 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. For detailed information on the security objectives that must be fulfilled by the TOE environment, see 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.

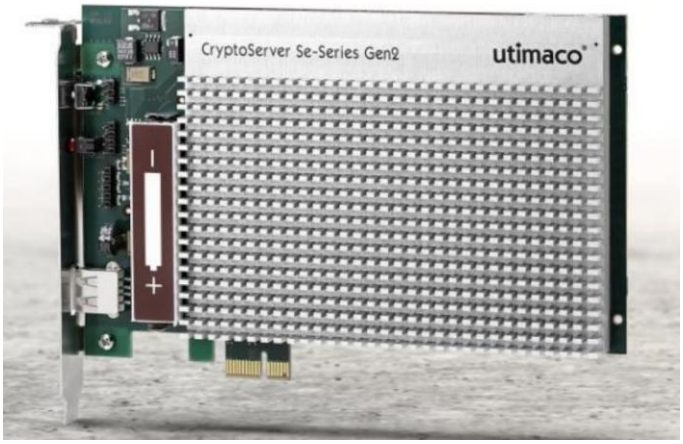
Note that EN 419221-5 Protection Profile [EN419221-5] claims the environment for the TOE protects against loss or theft of the TOE, deters and detects physical tampering, protects against attacks based on emanations of the TOE, and protects against unauthorised software and configuration changes on the 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 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 two variants (PCIe/LAN v5):*	
	CryptoServer Se-Series Gen2 CP5 PCIe Operating Manual	2017-0006-en, version 1.2.0
	CryptoServer Se-Series Gen2 CP5 LAN V5 Operating Manual	2018-0011-en, version 1.2.0
	User Manual:	
	CryptoServer Se-Series Gen2 CP5 Administration Manual	2017-0008, version 2.3.0
	Interface Specifications:	
	CryptoServer - Firmware Module CXI for CryptoServer CP5 – Interface Specification	2017-0010, version 1.0.4
	CryptoServer - Firmware Module ADM - Interface Specification - ADM Version ≥ 3.0.0.0	2009-0010, version 1.7.6
	CryptoServer - Firmware Module CMDS for CryptoServer CP5 - Interface Specification -	2023-0022, version 1.0.1
	CryptoServer – Firmware Module MBK – Interface Specification	2003-0006, version 1.10.1
	CryptoServer Se-Series Gen2 CP5 - SAM Developer Guide	2018-0013, version 1.1.6
Internal SAM Developer Documentation (only delivered to developers of an internal SAM)	*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 2.7.1
	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
	CryptoServer – Firmware Module ASN1 – Interface Specification	2002-0006, version 1.2.4

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 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 properties that are hard to verify externally.

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.

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

Step 3: These security relevant questions were then translated into TOE-specific possible vulnerabilities. Note that the evaluator also used the list of publicly known crypto attacks to formulate possible vulnerabilities as well as web searches.

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 was considered as solved, otherwise it was uniquely labeled as potential vulnerability.

The potential vulnerabilities were addressed by penetration tests.

No vulnerabilities remained after these tests.

The total test effort expended by the evaluators in the original evaluation in 2018 was 2 weeks. During that test campaign, 0% of the total time was spent on physical attacks, 0% overcoming sensors and filters, 0% perturbation attacks, 0% retrieving keys with FA, 50% on side-channel attacks, 0% attacks on RNG, 50% on software attacks, and 0% application isolation penetration tests.

The total test effort expended by the evaluators in the previous re-evaluation in 2023 was 1 week. During that test campaign, 0% of the total time was spent on physical attacks, 0% overcoming sensors and filters, 0% perturbation attacks, 0% retrieving keys with FA, 0% side-channel attacks, 0% attacks on RNG, 100% on software attacks, and 0% application isolation penetration tests.

The total test effort expended by the evaluators in the current re-evaluation in 2025 was 1 week. During that test campaign, 0% of the total time was spent on physical attacks, 0% overcoming sensors and filters, 0% perturbation attacks, 0% retrieving keys with FA, 0% side-channel attacks, 0% attacks on RNG, 100% of the total time was spent on software attacks, and 0% application isolation penetration 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 versions.

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.

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.

For composite evaluations, please consult the *[ETRfC]* for details.

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.

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 "CryptoServer Se-Series Gen2 CP5" and version numbers:

- CryptoServer CP5 Se12 5.1.2.0,
- CryptoServer CP5 Se52 5.1.2.0,
- CryptoServer CP5 Se500 5.1.2.0,
- CryptoServer CP5 Se1500 5.1.2.0

See the preparative guidance for acceptance steps and verification procedures

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must 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 Se-Series Gen2 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 *[*EN419221-5*]*.

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.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.

To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The CryptoServer Security Target for CryptoServer Se-Series Gen2 CP5, version 2.2.0, 4th February 2025 *[ST]* is included here by reference.

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

4 Definitions

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

AES	Advanced Encryption Standard
DCAP	eIDAS 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
QSCD	Qualified Signature/Seal Creation Device
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SCD	Signature Creation Device
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 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[eIDAS-REP]	Assessment Reporting Sheet eIDAS, 25-RPT-571, v1.0, 17 April 2025
[EN419221-5]	EN 419 221-5:2018, Protection Profiles for TSP Cryptographic Modules – Part 5 Cryptographic Module for Trust Services, v1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020
[ETR]	Evaluation Technical Report CryptoServer Se-Series Gen2 CP5 EAL4+, 25-RPT-055, Version 4.0, 20 May 2025
[EAR]	Evaluator Assessment of Changes Report (EAR) CryptoServer Se-Series Gen2 CP5, 25-RPT-056, Version 6.0, 20 May 2025
[ETRfC]	ETR for Composition for CryptoServer Se-Series Gen2 CP5 EAL4+, 25-RPT-570, Version 3.0, 20 May 2025
[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
[JIL-AAPHD]	Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.1, November 2023
[JIL-AMHD]	Attack Methods for Hardware Devices with Security Boxes, Version 3.0, February 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	CryptoServer Security Target for CryptoServer Se-Series Gen2 CP5, version 2.2.0, 4th February 2025
[ST-lite]	CryptoServer Security Target Lite for CryptoServer Se-Series Gen2 CP5, version 2.2.0, 4th February 2025
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)