Certification Report

Version 1.0

18 June 2019

CSA_CC_18001

for

CryptoServer Se-Series Gen2 CP5

From

Utimaco IS GmbH

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorizing Nation, under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	18 June 2019	Release

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

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 is designed as a protected cryptographic module provided in form of a PCIe (PCI express) plug-in card for high security applications.

The CryptoServer Se-Series Gen2 CP5 has undergone the CC certification procedure under the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components (refer to Chapter 3 for details):

- Hardware – four models; Se12, Se52, Se500, Se1500.
- Software – installed firmware modules
- Guidance documents – operating manuals, user manuals, interface specifications.

The evaluation of the TOE was carried out by Brightsight B.V., an approved CC test laboratory, at the assurance level CC EAL4 augmented with AVA_VAN.5. The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The Security Target [1] is the basis for this certification and is based on the certified Protection Profile for Cryptographic Modules for Trust Services [2].

Please note that for the need of publication, a public version of the Security Target [3] has been created and verified.

The Security Assurance Requirements (SARs) are based entirely on the assurance components defined in Part 3 of the Common Criteria [4]. The TOE meets the assurance requirements stated in the Protection Profile.

The Security Functional Requirements (SFRs) relevant for the TOE are outlined in Chapter 5 of the Security Target [1]. The Security Target claims conformance to CC Part 2 [5], and meets the security requirements stated in the Protection Profile.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats, and Organisation Policies. These are outlined in Chapter 4 of the Security Target [1].

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Table of Contents

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 [6] [5] [4];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 4 [7]; and
- SCCS scheme publications [8] [9] [10]

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (https://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **17 Jun 2024**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [10]. Potential users should check the SCCS website (www.csa.gov.sg/programmes/csa-cc-product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is:

CryptoServer CP5 Se12 5.0.0.0, CryptoServer CP5 Se52 5.0.0.0, CryptoServer CP5 Se500 5.0.0.0, CryptoServer CP5 Se1500 5.0.0.0

The following table identifies the TOE deliverables:

TOE Deliverable	Type/Form, Name	Exact Reference
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
	and CryptoServer CP5 firmware package consisting of the following firmware modules:	
	ADM (.msc and .sys) (Module Administration)	3.0.25.4
	AES (.msc and .sys) (AES Cryptography)	1.4.1.4
	ASN1 (.msc and .sys) (Decoding and Encoding ASN.1)	1.0.3.4
	CXI (.msc) (Cryptographic Services eXternal Interface)	2.2.3.4
	CMDS (.msc and .sys) (Command Scheduler)	3.6.0.8
	DB (.msc and .sys) (Database Management)	1.3.2.0
	ECA (.msc and .sys) (Elliptic Curve Arithmetic)	1.1.10.2
	ECDSA (.msc and .sys) (ECDSA Cryptography)	1.1.11.0
	EXAR (.msc and .sys) (Driver for Crypto Accelerator)	2.1.1.4
	HASH (.msc and .sys) (Hashing Algorithms)	1.0.11.1
	HCE (.msc and .sys) (Generic Internal Interface for Crypto Accelerator)	2.2.2.3
	LNA (.msc and .sys) (Long Number Arithmetic)	1.2.3.4
	MBK (.msc) (Master Backup Key Management)	2.2.7.3
	POST (.msc and .sys) (Power-On Self-Tests)	1.0.0.1
	SMOS (.msc and .sys) (Security Module Operating System)	5.5.9.2
	UTIL (.msc and .sys) (Utilities for RTC and RNG)	3.0.5.0
	VDES (.msc and .sys) (DES Cryptography)	1.0.9.2
	VRSA (.msc and .sys) (RSA Cryptography)	1.3.4.65
Guidance Documents	*Operating Manual in two variants (delivery variant PCIe/LAN):*	
	CryptoServer Se-Series Gen2 CP5 PCIe Operating Manual	2017-0006-en, version 1.0.12
	CryptoServer Se-Series Gen2 CP5 LAN Operating Manual	2017-0005-en, version 1.0.11
	User Manual:	
	CryptoServer Se-Series Gen2 CP5 Administration Manual	2017-0008, version 1.0.6
	Interface Specifications:	
	Firmware Module CXI for CryptoServer CP5 – Interface Specification	2017-0010, version 1.0.2
	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 1.9.5

Table 1: Deliverables of the TOE

The guide for receipt and acceptance of the above mentioned TOE are described in the set of guidance documents [11] [12] [13].

Additional identification information relevant to this Certification procedure are as follow:

TOE	CryptoServer CP5 Se12 5.0.0.0, CryptoServer CP5 Se52 5.0.0.0, CryptoServer CP5 Se500 5.0.0.0, and CryptoServer CP5 Se1500 5.0.0.0
Security Target	Security Target for CryptoServer Se-Series Gen2 CP5 v1.0.0
CC Scheme	Singapore Common Criteria Scheme (SCCS)
Methodology	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Assurance Level/cPP	Strict Conformance to Protection Profile EN 419 221-5 Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services; v0.15, 2016-11-29; at EAL 4 augmented AVA_VAN.5.
Developer	Utimaco IS GmbH
Sponsor	Utimaco IS GmbH
Evaluation Facility	Brightsight B.V.
Certification Body	Cyber Security Agency of Singapore (CSA)
Certification ID	CSA_CC_18001
Certificate Validity	**18 Jun 2019** till **17 June 2024**

Table 2: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

The TOE implements policies pertaining to security functional class "User Data Protection".

Specific details concerning the above mentioned security policy can be found in Chapter 7 of the Security Target [1].

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target [1] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed below:

Usage Assumptions	Description
OE.DataContext	Any client application using the cryptographic functions of the TOE shall ensure that the correct data are supplied in a secure manner (including any relevant requirements for authenticity, integrity and confidentiality). The client application may make use of appropriate secure channels provided by the TOE to support these security requirements.
OE.Uauth	Any client application using the cryptographic services of the TOE shall correctly and securely gather identification and authentication/authorisation data from its users and securely transfer it to the TOE (protecting the confidentiality of the authentication/authorisation data as required) when required to authorise the use of TOE assets and services.

Table 3: Usage Assumptions

Environmental Assumptions	Description
OE.ExternalData	Where copies of data protected by the TOE are managed outside of the TOE, client applications and other entities shall provide appropriate protection for that data to a level required by the application context and the risks in the deployment environment.
OE.Env	The TOE shall operate in a protected environment that limits physical access to the TOE to authorised Administrators. The TOE software and hardware environment (including client applications) shall be installed and maintained by Administrators in a secure state that mitigates against the specific risks applicable to the deployment environment.
OE.AuditSupport	The audit trail generated by the TOE will be collected, maintained and reviewed by a System Auditor according to a defined audit procedure for the TSP.
OE.AppSupport	Procedures to ensure the ongoing security of client applications and their data shall be defined and followed in the environment, and reflected in use of the appropriate TOE cryptographic functions and parameters, and appropriate management and administration actions on the TOE.

Table 4: Environmental Assumptions

Details can be found in section 5.2 of the Security Target [1].

5.2 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. The scope of evaluation is limited to the claims made in the Security Target [1].

Note that EN 419 221-5 Protection Profile [2] 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.

5.3 Evaluated Configuration

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. Furthermore, it provides the functionality for creating protected backups of keys and for secure update of defined parts of the TOE software.

The evaluated configuration is as shown in Figure 1 below.

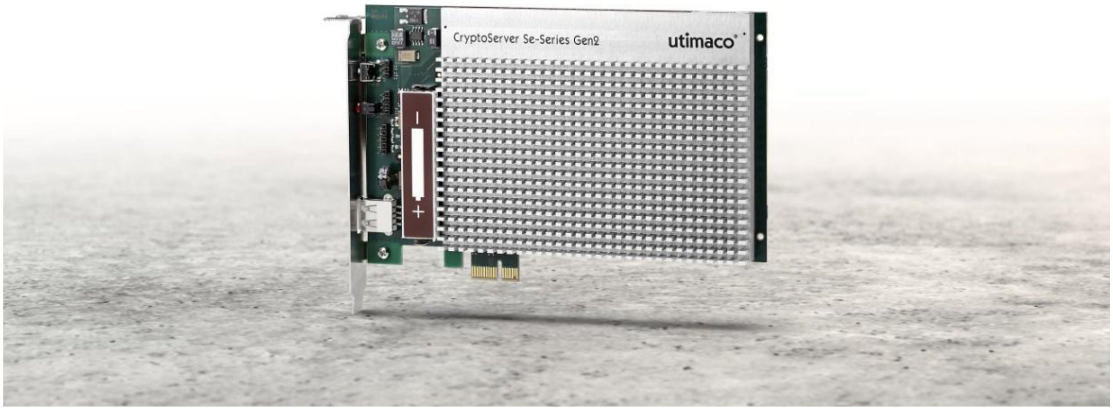

Figure 1: CryptoServer Se-Series Gen2 PCIe security module

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

Figure 2: CryptoServer Se-Series Gen2 LAN security module

The TOE is available in 4 models (Se12, Se52, Se500, and Se1500). The following table depicts the different specifications for the 4 models. There is no difference in the security architecture amongst the 4 models of the TOE.

TOE Variant	Benchmarking Performance Levels for RSA 2048	Hardware Asymmetric Crypto Accelerator
Se12 5.0.0.0	16 signings/sec	No
Se52 5.0.0.0	85 signings/sec	No
Se500 5.0.0.0	2200 signings/sec	Yes
Se1500 5.0.0.0	3400 signings/sec	Yes

Table 5: TOE Versions

The CryptoServer CP5 is a cryptographic module where at the time of delivery all hardware components of the cryptographic module, 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). Versions CryptoServer CP5 Se500 5.0.0.0 and CryptoServer CP5 Se1500 5.0.0.0 additionally contain a crypto accelerator chip (in order to provide highest performance on RSA and ECDSA operations), which is not assembled in versions CryptoServer CP5 Se12 5.0.0.0 or CryptoServer CP5 Se52 5.0.0.0.

5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities.

5.5 Non-TOE Components

The following hardware and software which do not belong to the TOE is required for the operating environment and is always delivered together with the TOE:

Additional deliverables	Type	Description	Exact reference
PIN pad (smartcard reader with keypad)	HW/SW	Utimaco cyberJack one	FW-Version V1.0
10 smartcards (for administrative purposes)	HW/SW	Java Card J2E081 - JCOP	V2.4.2. R3

Table 6: Non-TOE Components

Besides the Product CD containing relevant firmware, software, and data, depending on the delivery variant (PCIe, or LAN) non-TOE hardware such as CryptoServer LAN and power supply cables may also be delivered with the TOE.

6 Architecture Design Information

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.

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

i) Hardware: all hardware components for example CPU and memory.

ii) Boot Loader: first software started inside the security module after a reboot.

iii) Firmware Modules: all firmware modules containing all the software functionality needed after end of boot phase, like for example SMOS, CXI, CMDS and HASH.

7 Documentation

The evaluated documentation as listed in Table 1: Deliverables of the TOE

is contained in the Product CD packaged and delivered with the TOE. These documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

The developer implemented a proprietary test environment to allow interface testing of the TOE.

The Utimaco test approach covers automated and manual tests, fuzzing tests, and static code analyses. In addition, hardware tests and crypto algorithm tests are performed in the context of FIPS 140-2.

8.1.2 Test Configuration

Testing was performed on the TOE in the Se1500 (with crypto accelerator) and Se52 (without crypto accelerator), configured according to the TOE guidance document [12]. This is representative for all TOE variants, as from a security perspective, there is no difference between Se500 and Se1500 as well as no difference between Se12 and Se52.

8.1.3 Test Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the Evaluation Technical Report [14], with references to the documents containing the full details.

The test results provided by the developer covered all operational functions as described in the Security Target [1].

All test results from all tested environment showed that the expected test results are identical to the actual test results.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

The evaluator inspected a sample of the developer tests. The sample was chosen as follows:

- A diverse set of about 60 out of more than 500 automated developer tests were selected for inspection. The inspection revealed that the developer test approach is sufficient, covering both positive and negative tests.
- The inspection of static code analysis settings and results revealed that the developer test approach is sufficient, with all findings of the analysis properly justified by the developer.
- Evidences of all hardware tests performed were inspected by the evaluators and found sufficient. In particular, the test approach was reviewed by the evaluator and found sound for coverage of the physical security requirements.
- All FIPS algorithm tests, including the test vectors, were inspected and found sufficient and appropriate.

The evaluator repeated all automated developer tests on both variants of the TOE (with and without crypto accelerator) and verified the accuracy of the developer's test results. As part of the repeated tests, the evaluator also performed an independent run of the static code analysis tool (using his own defined options for the tool) on the same firmware versions tested by the developer.

The evaluator observed that all TSFIs identified by the developer were covered by several test cases except for two bootloader commands and a lower level communication protocol over PCIe interface.

The evaluator decided to devise additional independent functional tests on both variants of the TOE, in order to target TSFIs that were not tested by the developer, and provide further coverage and/or an alternative approach for coverage of an SFR [14]. These include:

- Secure messaging test that decouples secure messaging and user authentication
- Further negative tests for failed authentication
- Testing of key initialisation and authorisation as two decoupled steps
- Creation of extra user
- Further tests for modification of key attributes and key backup
- Tests for malformed command frames.

8.2.2 Test Configuration

The test setup is the same as that used by the developer, as described in section 8.1.2.

8.2.3 Test Results

All of the developer's test were verified by the evaluator to conform to the expected results from the test plan. The results of the additional independent tests devised by the evaluator also conformed to the expect results.

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

The AVA_VAN.5 assurance class requires the evaluator to conduct a methodical vulnerability analysis based on publicly available source of information and based on structured examination of the evidence while performing previous evaluation activities (ASE, ADV, AGD, ATE).

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 is the identification of areas of concern (as defined in [7]).
    - The areas of concern are identified by the evaluator using the generic weaknesses enumeration database as inspiration. The CWE database is an open source publicly maintained dictionary of SW weaknesses.
    - Examples of areas of concern 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 are then translated into TOE-specific possible vulnerabilities. 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 include known crypto vulnerabilities, APDU/API level attacks, ASN.1 vulnerabilities Spectre/Meltdown, ROCA (Return of Coppersmith's attack), and Rowhammer.

The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN.5) treating the resistance of the TOE to an attack with the High attack potential.

The evaluator found no exploitable vulnerability in the TOE when operated in the evaluated configuration. No residual risks were identified.

9 Results of the Evaluation

The Evaluation Technical Report [14] was provided by the CCTL in accordance with the CC, CEM and requirements of the SCCS. The verdict PASS is confirmed for each of the claimed assurance requirement.

As a result of the evaluation, the CCTL concluded the CryptoServer CP5 Se12 5.0.0.0, CryptoServer CP5 Se52 5.0.0.0, CryptoServer CP5 Se500 5.0.0.0, CryptoServer CP5 Se1500 5.0.0.0, 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 TOE satisfies the security requirements specified in the Security Target [1].

The Security Target claims 'strict' conformance to the Protection Profile [2].

10 Obligations and recommendations for the usage of the TOE

The documents as outlined in Table 1 contain necessary information about the usage of the TOE and all security hints therein have to be considered. 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. In particular, the TOE should be deployed within a physically secure premise in accordance to the assumption listed in the Protect Profile [2] to which the TOE conforms to.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. Appropriate cryptographic algorithms with adequate key lengths must be used to fend off attackers with high attack potential.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available, the user of the TOE should request the sponsor to provide a re-certification. In the meantime, a risk assessment should be conducted to

1) determine the suitability of deploying uncertified updates and patches; or
2) to retain usage of the existing certified version and take additional measures in order to maintain system security.

11 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Test Laboratory
CSA	Cyber Security Agency of Singapore
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
LAN	Local Area Network
PCI	Peripheral Component Interconnect
PIN	Personal Identification Number
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	Trusted Service Provider

12 Bibliography

[1] Utimaco IS GmbH, “Security Target for CryptoServer Se-Series Gen2 CP5 v1.0.0”.

[2] CEN Technical Committee CEN/TC 224, “Protection Profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services v0.15”.

[3] Utimaco IS GmbH, “Security Target Lite for CryptoServer Se-Series Gen2 CP5 v1.0.0”.

[4] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2012-09-003] Version 3.1 Revision 4”.

[5] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2012-09-002], Version 3.1 Revision 4”.

[6] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2012-09-001]. Version 3.1 Revision 4”.

[7] Common Criteria Maintenance Board (CCMB), “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2012-09-004], Version 3.1 Revision 4”.

[8] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 5.0”.

[9] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 5.0”.

[10] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 5.0”.

[11] Utimaco IS GmbH, “CryptoServer Se-Series Gen2 CP5 – Administration Manual v1.0.6”.

[12] Utimaco IS GmbH, “CryptoServer Se-Series Gen2 CP5 – LAN Operating Manual v1.0.11”.

[13] Utimaco IS GmbH, “CryptoServer Se-Series Gen2 CP5 – PCIe Operating Manual v1.0.6”.

[14] Brightsight B.V., “Evaluation Technical Report CryptoServer Se-Series Gen2 CP5 EAL4+ version 3.0”.

--End of Report --