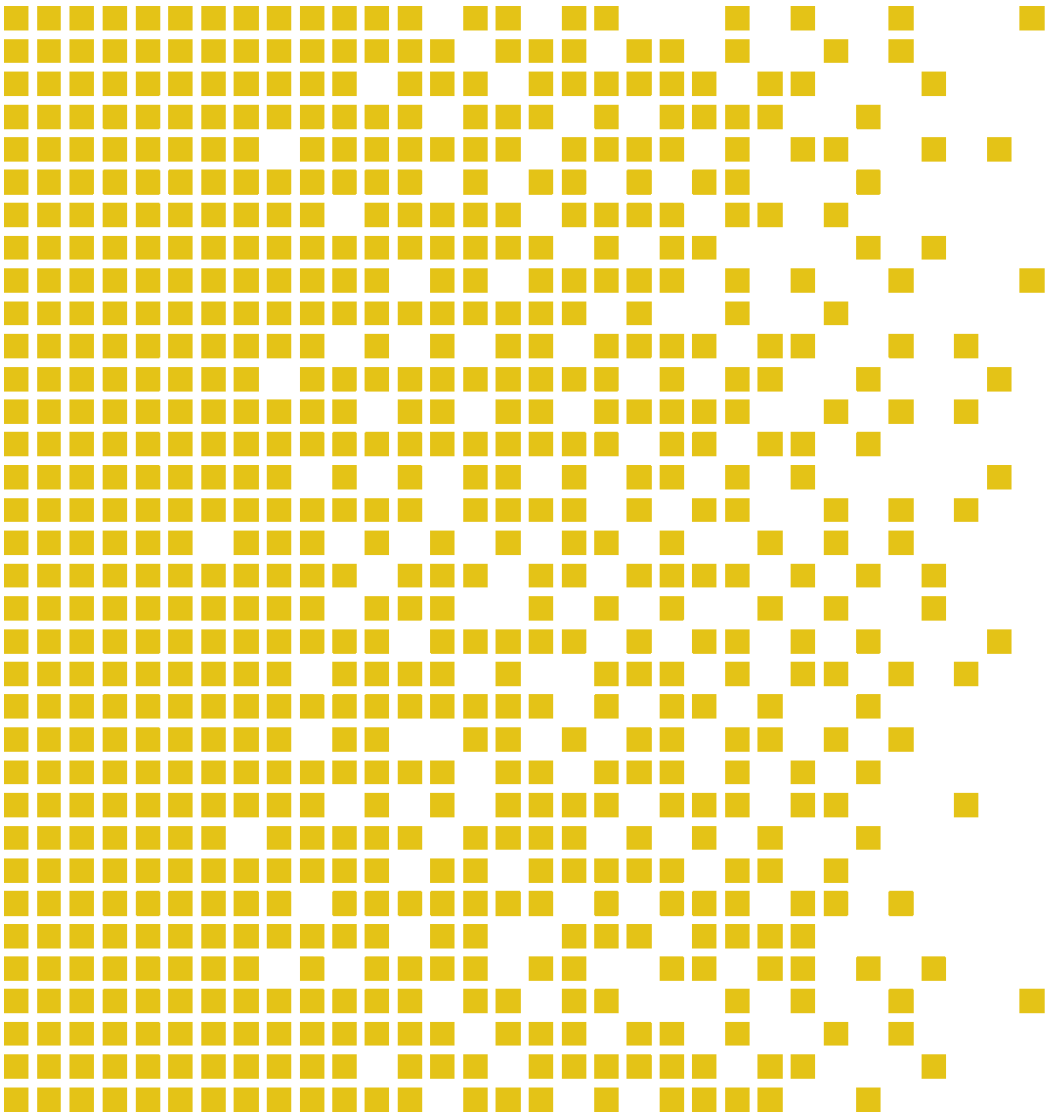
SERTIT-056 CR Certification Report

Issue 1.0 22 August 2014

TNP ECC2 CPU Card version 1.0



SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. *

* Mutual Recognition under the CC recognition arrangement applies to EAL4.

Contents

1 Certification Statement

Taiwan Name Plate Co. Ltd. TNP ECC2 CPU Card is a a dual interface CPU smartcard that implements electronic purse functionality for online or offline low value transaction in Easy Card Corporation payment system. It is mainly used for the Taipei Metro System and in convenience stores.

TNP ECC2 CPU Card version 1.0 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality when running on the platforms specified in Annex A.

Author	Kvassnes, Kjartan Jæger Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Øystein Hole Head of SERTIT
Date approved	22 August 2014

2 Abbreviations

APDU	Application Protocol Data Unit
API	Application Programming Interface
ATR	Answer to reset
ATS	Answer to select
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CM	Configuration Management
CRC	Cyclic Redundancy Check
DEMA	Differential Electro Magnetic Analysis
DES	Data Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
ECC	Easy Card Corporation
ECC2	2nd Generation ECC card / the TOE
EEPROM	Electrically Erasable Programmable Read Only Memory
EOR	Evaluation Observation Report
EP	Electronic purse
EM	Electronic Money
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
HO-DEMA	High-Order Differential Electro Magnetic Analysis
HO-DPA	High-Order Differential Power Analysis
IFX	A security level named by Infineon (highest security level)
NVM	Non-Volatile Memory
OS1	A security level named by Infineon (medium-high security level)
OS2	A security level named by Infineon (low security level)

OTP	One Time Programmable
POC	Point of Contact
QP	Qualified Participant
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman Public Key Encryption
SEMA	Simple Electro Magnetic Analysis
SERTIT	Norwegian Certification Authority for IT Security
SPA	Simple Power Analysis
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Taiwan Name Plate Co., Ltd. (TNP) TNP ECC2 CPU Card Security Target, version 1.0.1.

[2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 9.0, 02 April 2013.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] Evaluation Technical Report Common Criteria EAL4+ Evaluation of TNP ECC2 CPU Card v1.0, version 1.1, 28 March 2014.

[8] TNP ECC2 CPU Card Security Guidance version 1.0.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of TNP ECC2 CPU Card version 1.0 to the Sponsor, Taiwan Name Plate Co. Ltd., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was TNP ECC2 CPU Card version 1.0.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Taiwan Name Plate Co. Ltd.

The TOE is an anonymous Electronic Purse (EP) smartcard application running on the Infineon M7794 A12 (BSI-DSZ-CC-0883-2013) IC to the implementation of ECC EP functionalities. The Infineon M7794 A12 smartcard was certified conformant to PP0035. The firmware is installed on the NVM of the chip

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.4.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The assurance incorporated predefined evaluation assurance level EAL4 augmented by ALC_DVS.2 and AVA_VAN.5. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are detailed in the ST[1], chapter 3.6.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional requirements and security functions to

elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

- **T.COUNTERFEITING_DEBIT**

  Counterfeiting of a debit operation in order to debit the EP with an EM greater or lesser than the actual transaction that leads to unauthorized EM creation or loss.

- **T.COUNTERFEITING_CREDIT**

  Counterfeiting of a credit transaction in order to credit the EP without any financial counterpart that leads to unauthorized EM creation or loss.

- **T.COUNTERFEITING_UPDATE**

  Counterfeiting of a parameters update transaction in order to change the keys values or the static counters values.

- **T.DISCLOSURE_KEYS**

  Unauthorized access to the secret keys.

- **T.INTEG_CODE**

  Unauthorized modification of the TOE code: an attacker modifies the code in order to bypass the security policy of the EP.

- **T.INTEG_LOG**

  Unauthorized modification of transaction log: an attacker modifies the value of the last transaction log stored in the EP in order to input a known key.

- **T.INTEG_KEYS**

  Unauthorized modification of stored keys: an attacker modifies the value of the secret keys and associated attributes stored in the EP that leads to unauthorized EM modification.

- **T.INTEG_EM**

  Unauthorized modification of stored EM: An attacker modifies the amount of EM stored in the EP in order to increase or decrease the amount.

- **T.INTEG_IV_DATA**

  Unauthorized modification of stored EP identification and validity data: an attacker modifies the value of the EP identification and validity data stored in the EP in order to input another one.

- **T.INTEG_COUNTER**

  Unauthorized modification of stored static counter: an attacker modifies the value of sequence counters in order to force the EP accepting counterfeited or replayed transactions.

- **T.INTEG_EP_STAT**

  Unauthorized modification of the State Machine: an attacker modifies or deletes information that defines the current state of the EP in order, for instance, to bypass a secure state.

- **T.REPLAY_DEBIT**

  Replay of a debit: an EP is debited several times via a previous complete sequence of debit operations; it leads to unauthorized EM loss.

- **T.REPLAY_CREDIT**

  Replay of a credit transaction: an EP is loaded several times via a previous complete sequence of credit operations; it leads to unauthorized EM creation.

- **T.REPLAY_UPDATE**

  Replay of a parameters update transaction: an EP is updated several times via a previous complete sequence of parameters update operations; it leads to fraudulent changes of parameters stored in the EP (keys and static counters).

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

It is assumed that the persons manipulating the TOE in the operational environment follow the TOE guides. And he is responsible for the application of the procedures contained in the guides, and the persons involved in delivery and protection of the product have the required skills and are aware of the security issues.

4.12 IT Security Objectives

- **O.AUTH**

  The EP shall enforce mutual authentication with external devices prior any transaction.

- **O.EM**

  The EP shall prevent unauthorized creation or loss of EM.

- **O.CONF_DATA**

  The EP shall prevent unauthorized disclosure of confidential the Keys.

- **O.INTEG_DATA**

  The EP shall prevent unauthorized modification of user and TSF data.

- **O.LIMIT**

  The EP behavior shall be limited by maximum values defined in the static counters.

- **O.OPERATE**

  The EP shall ensure the continued correct operation of its security functions especially in case of abnormal transactions and unexpected interruption.

- **O.RECORD**

  The EP shall record the last transactions to support effective security management.

- **O.REPLAY**

  The EP shall detect and reject replayed transactions.

- **O.TAMPER**

  The EP shall prevent physical tampering of its security critical parts.

4.13 Non-IT Security Objectives

- **OE.DEBIT_BEFORE_CREDIT**

  Debit must always precede credit during EM payment transaction.

- **OE.MANAGEMENT_OF_SECRETS**

  The secret User or TSF data managed outside the TOE shall be protected against unauthorized disclosure and modification.

- **OE.PROTECTION_AFTER_TOE_DELIVERY**

  Procedures and controlled environment shall ensure protection of the TOE and related information after delivery. Procedures shall ensure that people involved in TOE delivery and protection have the required skills. The persons using the TOE in the operational environment shall apply the product guides (user and administrator guidance of the product, installation documentation and personalization guide).

- **OE.TOE_USAGE**

  The EM issuer shall communicate to the Purse holder the rules dealing with the use of the EP. Especially it must inform the user that he must keep EP the same way he does for a real purse,

  The Purse holder shall enforce these rules.

- **OE.TIME**

  The terminal shall provide reliable time stamp to the TOE

4.14 Security Functional Requirements

The TOE security functional requirements are described in the ST[1], chapter 5.1.

4.15 Security Function Policy

The TOE is a dual interface CPU smartcard that implements EP (electronic purse) functionality for online or offline low value transaction in Easy Card Corporation (ECC) payment system. It is mainly used for the Taipei Metro System and in convenience stores.

The usage scenario of the EP is as below:

- Credit Purse transaction: the purse holder gives funds to the ECC Company (online transaction) or the merchant (offline transaction) who loads the EP with an equivalent amount of Electronic Money (EM),
- Debit Purse transaction: the purse holder asks the merchant for a service and transfers (offline) EM from his EP to the merchant.

The TOE is able to:

- Store its amount of EM which defines the balance of the EP,
- Indicate the available amount of EM,
- Debit EM via Debit Purse operations,
- Credit EM via Credit Purse transactions,
- Update parameters.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[7] to SERTIT in 28 March 2014. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 4 assurance package augmented with AVA_VAN.5 and ALC_DVS.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation procedures are described in detail in the supporting documents[8].

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Developers should follow the guidance[8] for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

An independent vulnerability analysis has been performed. The vulnerability analysis presented comprises of the following steps:

- A design and implementation review on the TOE was performed to identify weaknesses in the TOE that could potentially be exploited by attackers.
- Validation tests of security features performed in ATE are taken into account for the following vulnerability analysis.
- A vulnerability analysis based on the design and implementation review results and the validation test results of security features, was performed considering the well-known attacks from the "JIL Attack Methods for Smartcards and Similar Devices".
- The ETR report [ETR_COMP] and chip security guidance [ADV SG] of the certified chip M7794 A12 (BSI-DSZ-CC-0883-2013) from the chip vendor is taking into consideration while analysing potential vulnerabilities.
- A penetration test plan is established based on the results of the vulnerability analysis.
- Practical penetration tests are performed according the penetration test plan.

The evaluators first performed general vulnerability analysis by reviewing the source code (version V170) and then identified verification test cases for AVA_VAN penetration test to check the effectiveness of the countermeasures implemented according to the hardware security guidelines.

Next, a thorough vulnerability analysis was done and identified 4 vulnerabilities which are reported to the certifier. The developer, later on, patched the TOE ECC2 firmware to fix the identified vulnerabilities and provided an updated TOE with ECC2 firmware version v0.8.0 (next version of V170). Also a potential replay attack vulnerability was identified during ATE testing. It was later on covered by [AGD] v0.9.

After reviewing the code again, the evaluator confirmed that no additional vulnerability was introduced by these changes, so the test cases already performed remain valid. The evaluators confirmed that the patch fixed the identified vulnerability, and additional verification tests were conducted.

5.6 Developer's Tests

The developer tests are performed on TOE samples that have the ECC2 firmware in NVM. The ECC2 firmware version is v0.8.0. The developer tests are performed on TOE non-personalized samples with test scripts running on the developer's test tool.

5.7 Evaluators' Tests

The evaluator approaches ATE independent testing as follows: a distinction is made between reproduction of (a sample of) developer functional tests and tests additional to the developer functional tests.

The evaluator's responsibility for performing independent testing is required by the ATE_IND class. The evaluators repeated the developer's tests with the developer's test tool and scripts by using contact smartcard reader. Then, the evaluator defined additional test cases, prompted by study of the developer documentation and test scripts. The test strategy is as shown below.

- Augmentation of developer testing for interfaces by varying parameters to more rigorously test the interface
- Performing positive and negative tests on selected Security Function or Security Mechanism
- Change the execution sequence and perform replay test
- Enumerate all possible commands (INS)

The evaluators performed the evaluator's independent tests with the developer's test tool and scripts by using contact smartcard reader. According to code review result, the evaluator confirmed that the code for processing the APDU commands from contact and contactless smartcard reader is the same. Therefore the evaluators requested the developer to perform these same logical tests (both repeating part and independent part) on the contactless smartcard reader. The evaluators witnessed the execution of the same test cases performed by the developer by using contactless smartcard reader.

The last independent test was done by Brightsight's proprietary software.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that TNP ECC2 CPU Card version 1.0 meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of TNP ECC2 CPU Card version 1.0 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

The above "Evaluation Findings" include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE is an anonymous Electronic Purse (EP) smartcard application running on the Infineon M7794 A12 (BSI-DSZ-CC-0883-2013) IC to the implementation of ECC EP functionalities. The Infineon M7794 A12 smartcard was certified conformant to [PP0035]. The firmware is installed on the NVM of the chip.

The TOE is a dual interface CPU smartcard that implements EP (electronic purse) functionality for online or offline low value transaction in Easy Card Corporation (ECC) payment system. It is mainly used for the Taipei Metro System and in convenience stores.

Hardware components

The basic configuration elements of the TOE are the CPU, the various memory elements (EEPOM, ROM, and RAM), security function circuits SCP (symmetric coprocessor), various types of control circuits (including various types of detection circuits).

Software components

The software component of the TOE is the ECC2 firmware. The software is organized into three security levels: IFX level, OS1 level and OS2 level. The invocation of APIs between different security level can only be done through so called Branch Table. Only APIs in higher security level that registered in the Branch Table can be invoked by code in lower security level.

OS2 is the lowest security level that includes functions to process I/O data. No sensitive information is kept in this level. During system boot up, Main Subsystem invoked InitMem function of System Service Subsystem to initialize the chip and check system integrity. The Main Subsystem also implements the main execution loop that receives and sends APDU commands through I/O Subsystem and then the Hardware Subsystem to communicate with the card reader. It then dispatches APDU commands to Command Interpreter, in OS1 security level, for command processing.

The major functionality of the TOE is implemented by ECC2 and Card Manager Subsystems in OS1 security level. When an APDU command is sent from Main Subsystem, the Command Interpreter in System Service Subsystem checks the security status and interprets the APDU command and dispatch the command to corresponding ECC2 or Card Manager Subsystem. These two subsystems implemented all APDU commands of the TOE. Tool subsystem implements security mechanisms, required by the chip vendor's security guideline, to interact with hardware and Infineon Tool Subsystem. Life Cycle subsystem is used by other subsystems to maintain the lifecycle status. Mifare subsystem is only used in the ECC metro system migration phase which is not in the TOE evaluation scope.

Infineon Tool Subsystem, in IFX security level, is the software part of the certified platform (BSI-DSZ-CC-0883-2013) that provides chip identification information and security services to manage the NVM.

The Hardware Subsystem is the certified IC (BSI-DSZ-CC-0883-2013) that provides the major security functions and mechanisms to protect the TOE.

TOE Documentation

The supporting guidance documents evaluated were:

[a] TNP ECC2 CPU Card Security Guidance version 1.0.

Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".

TOE Configuration

The following configuration was used for testing:

Item	Identifier	Versions
Hardware	Infineon M7794 Integrated Circuit	A12
Software	ECC2	1.0
Manuals	TNP ECC2 CPU Card Security Guidance	1.0

The hardware part of the TOE is identified by M7794 A12. Another characteristic of the TOE are the chip identification data. These chip identification data is accessible via the Generic Chip Identification Mode (GCIM). The Generic Chip Identification Mode (GCIM) can be activated on the ISO/IEC 7816-3 and ISO/IEC 14443-3 interfaces after power-on with a dedicated signalling sequence as specified in [ADV SG].

The software (ECC2 v1.0) is identified by the return values of the following ATR or ATS commands. In the developer's CM system, ECC2 firmware is tagged as v0.8.0. After this CC certification, it will be tagged as v1.0 according to [ALC, 5.4.2] without any change in the source code. Hereafter, ECC2 firmware version 0.8.0 and version 1.0 both refer to the same TOE in this report. Both of these two tagged versions are identified by the same return values of ATR and ATS commands.

ATS: 78 80 E4 02 54 4E 05 19 00 00 00 02 20

ATR: 3B F8 11 00 00 81 71 FE 42 00 54 4E 05 19 00 00 00 02 A1

Certificate

The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunctionwith the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Product Manufacturer: Taiwan Name Plate Co. Ltd.

Product Name: TNP ECC2 CPU Card

Type of Product: Electronic Purse (EP) smartcard application

Version and Release Numbers: Version 1.0

Assurance Package: EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5

Evaluation Criteria: Common Criteria version 3.1R4 (ISO/IEC 15408)

Name of IT Security Evaluation Facility: Brightsight B.V.

Name of Certification Body: SERTIT

Certification Report Identifier: SERTIT-056 CR, issue 1.0, 22 August 2014

Certificate Identifier: SERTIT-056 C

Date Issued: 22 August 2014

Kjartan Jæger Kvassnes
Certifier

Lars Borgos
Quality Assurance

Øystein Hole
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security