# SERTIT-093 CR Certification Report

Issue 1.0 10 February 2017

DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) Dual Interface smart card chips with HAL library, version 2.0
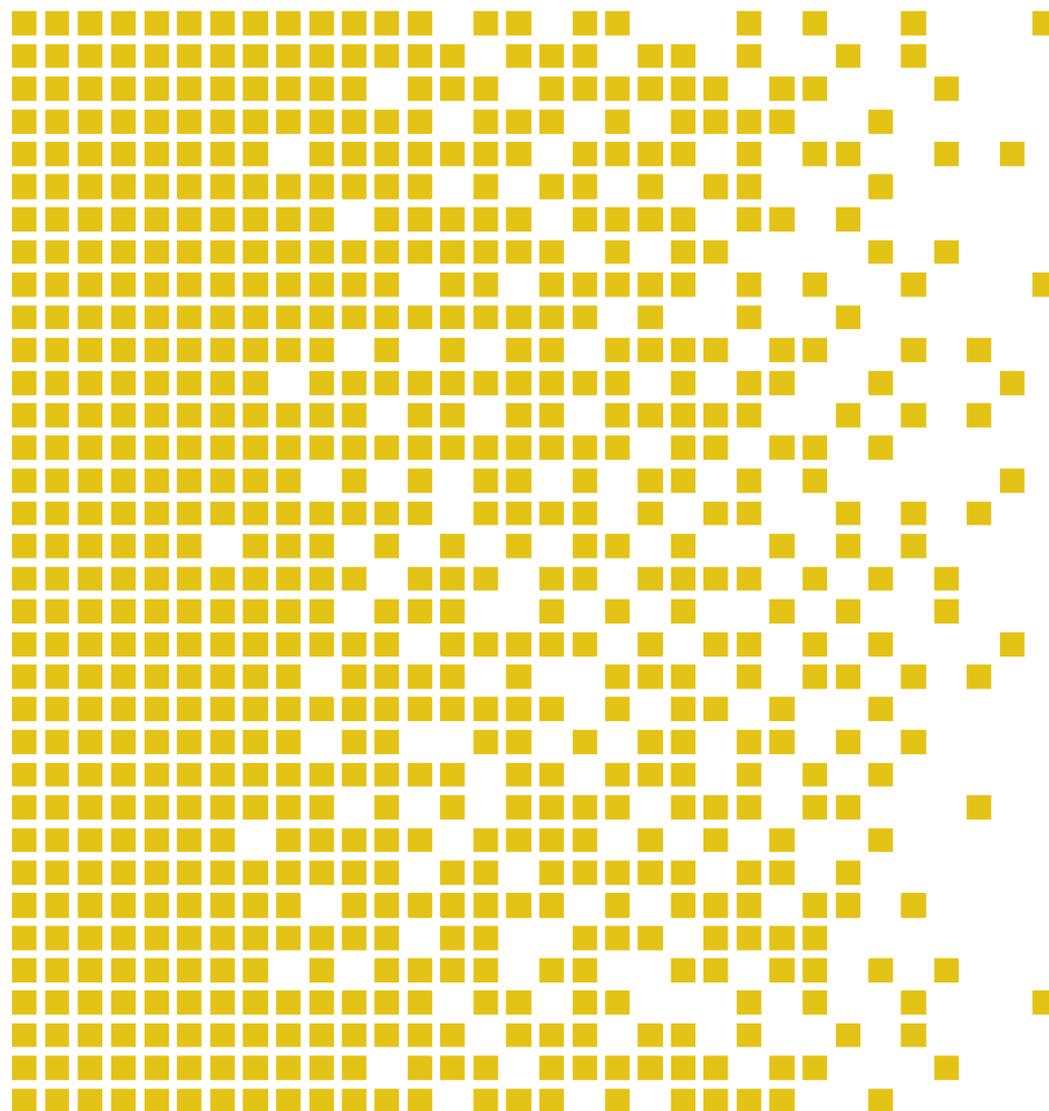
CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1 11.11.2011

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.

The recognition under CCRA is limited to cPP related assurance packages or EAL2 and ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

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

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 SOGIS MRA applies to components up to EAL4.

Contents

1   Certification Statement

Datang Microelectronics Company DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) Dual Interface smart card chips with HAL library is a high-end dual-interface secure smart card integrated circuit suitable for instance for Java Card OS, ID cards, Banking card, etc.

DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) Dual Interface smart card chips with HAL library 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 EAL 5 augmented with AVA_VAN.5 and ALC_DVS.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality in the specified environment when running on the platforms specified in Annex A. It has also met the requirements of Protection Profile BSI-CC-PP-0084-2014 V1.0.

Author	Kjartan Jæger Kvassnes
	Certifier
Quality Assurance	Arne Høye Rage
	Quality Assurance
Approved	Kristian Steinfeldt Bae
	Head of SERTIT
Date approved	10 February 2017
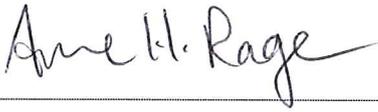
⠿⠿⠿ ⠿⠿⠿⠿⠿⠿⠿⠿ ⠿⠿⠿ ⠿⠿⠿ ⠿⠿⠿⠿⠿⠿ ⠿⠿ ⠿⠿⠿ ⠿⠿ ⠿⠿⠿ ⠿ ⠿ ⠿⠿⠿⠿⠿ ⠿ ⠿⠿⠿⠿⠿⠿⠿⠿⠿ ⠿ ⠿⠿⠿ ⠿⠿ ⠿⠿⠿

2   Abbreviations

API   Application Programming Interface

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

DEMA   Differential Electro Magnetic Analysis

DES   Data Encryption Standard

DPA   Differential Fault Analysis

EAL   Evaluation Assurance Level

EEPROM   Electrically Erasable Programmable Read Only Memory

EMFI   Electro-Magnetic Fault Injection

EOR   Evaluation Observation Report

ETR   Evaluation Technical Report

EVIT   Evaluation Facility under the Norwegian Certification Scheme for IT Security

FBBI   Forward-Body Bias Injection

IC   Integrated Circuit

OSP   Organizational Security Policy

RAM   Random Access Memory

RNG   Random Number Generator

ROM   Read Only Memory

RSA   Rivest, Shamir, Adleman Public Key Encryption

SERTIT   Norwegian Certification Authority for IT Security

SEMA   Simple Electro Magnetic Analysis

SFR   Security Functional Requirements

SPA   Simple Power Analysis

ST   Security Target

TOE   Target of Evaluation

TSF   TOE Security Functions

TSP   TOE Security Policy

⠠⠃⠗⠁⠊⠇⠇⠑ ⠞⠑⠭⠞ ⠏⠇⠁⠉⠑⠓⠕⠇⠙⠑⠗

3 References

[1] DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) Dual interface smart card chip with HAL library, version 2.0, Security Target Lite, Version 0.3, 13 December 2016.

[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 8.0, 20 August 2010.

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

[7] JIL Attack Methods for Smartcards and Similar Devices, Version 2.2, January 2013.

[8] JIL Application of Application Attack Potential to Smart Cards, Version 2.9, May 2013.

[9] AIS20/31 A proposal for Functionality classes for random number generators, Version 2.0, 18 September 2011.

[10] Evaluation Technical Report of Common Criteria EAL5+ Evaluation of DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) Dual Interface smart card chips with HAL library, version 2.0, Brightsight report 17-RPT-031 Version 2.0, 23 January 2017.

[11] DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) AGD_OPE.1 (Operational User Guidance), Version 0.1, 27 September 2016.

[12] DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) AGD_PRE.1 (Preparative Procedures), Version 0.1, 28 September 2016.

[13] Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, Version 1.0, January 2014.

4   Executive Summary

4.1   Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) Dual Interface smart card chips with HAL library to the Sponsor, Datang Microelectronics Company, 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 DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) Dual Interface smart card chips with HAL library.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Datang Microelectronics Company.

The TOE is suitable for instance to support a Java Card OS, ID cards, Banking cards, etc. It consists of:

- A dual-interface DMT-CBS-CE3D3 microcontroller, which exists in two derivatives: DMT-CBS-CE3D3/CC080 (80KB EEPROM) and DMT-CBS-CE3D3/CC048 (48KB EEPROM). The DMT-CBS-CE3D3/CC0xx provides cryptographic coprocessors for AES and TDES and a numerical coprocessor to support RSA computations. In addition, a true random number generator meeting class PTG.2 of AIS20/31 is available.
- A HAL library, which provides easy access to the hardware components for cryptographic operations, EEPROM access and retrieval of random numbers.

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 Security Target[1], Section 1.3.

4.4   Protection Profile Conformance

The Security Target[1] claims conformance to the following protection profile:

BSI-CC-PP-0084-2014 V1.0

4.5 Assurance Level

The Security Target[1] specifies the assurance requirements for the evaluation. The assurance incorporates the predefined evaluation assurance level EAL 5, augmented by AVA_VAN.5 and ALC_DVS.2. 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 Security Target[1] , Section 3.3.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats and OSP's which these objectives counter or meet and security functional requirements and security functions to elaborate the objectives. Most of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

The following SFR's are defined in the Protection Profile[13]:FCS_RNG.1, FMT_LIM.1, FMT_LIM.2, FAU_SAS.1, FDP_SDC.1.

4.8 Threats Countered

All threats that are countered are described in the Security Target[1], Section 3.2.

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 are described that are not countered.

4.11 Environmental Assumptions and Dependencies

The assumptions that apply to this TOE are described in the Security Target[1], Section 3.4.

4.12 IT Security Objectives

The security objectives that apply to this TOE are described in the Security Target[1], Section 4.1.

The security objectives for the Security IC Embedded Software are described in the Security Target[1], Section 4.2.

4.13 Non-IT Security Objectives

The security objectives for the environment are described in the Security Target[1], Section 4.3.

4.14 Security Functional Requirements

The following Security Functional Requirements are directly taken from the Protection Profile[13]. Except for FAU_SAS.1, FDP_SDC.1, FDP_SDI.2, FCS_RNG.1 and FCS_COP.1 all assignments and selections are completely defined in the Protection Profile[13].

Security functional requirement	Title
FRU_FLT.2	"Limited fault tolerance"
FPT_FLS.1	"Failure with preservation of secure state"
FMT_LIM.1	"Limited capabilities"
FMT_LIM.2	"Limited availability"
FAU_SAS.1	"Audit storage"
FPT_PHP.3	"Resistance to physical attack"
FDP_ITT.1	"Basic internal transfer protection"
FDP_IFC.1	"Subset information flow control"
FPT_ITT.1	"Basic internal TSF data transfer protection"
FDP_SDC.1	"Stored data confidentiality"
FDP_SDI.2	"Stored data integrity monitoring and action"
FCS_RNG.1[PTG.2]	"Quality metric for random numbers"
FCS_COP.1[TDES]	"Cryptographic operation - TDES"
FCS_COP.1[AES]	"Cryptographic operation - AES"
FCS_COP.1[RSA]	"Cryptographic operation - RSA"

4.15 Security Function Policy

The TOE is suitable for instance to support a Java Card OS, ID cards, Banking cards, etc.

The TOE consists of hardware and IC dedicated software. The hardware is based on a 32-bit CPU with ROM (Non-Volatile Read-Only Memory), EEPROM (Non-volatile Programmable Memory) and RAM (Volatile Memory). The hardware of the TOE also

⠀⠀

incorporates communication peripherals and cryptographic coprocessors for execution and acceleration of symmetric and asymmetric cryptographic algorithms. The IC dedicated software consists of a hardware abstraction (HAL) library that provides cryptographic services and EEPROM access support.

The TOE supports the following communication interfaces:

- ISO/IEC 7816 contact interface.
- ISO/IEC 14443 contactless interface

The TOE is delivered to a composite product manufacturer. The security IC embedded software is developed by the composite product manufacturer. The security IC embedded software is sent to Datang Microelectronics Company to be implemented in ROM and delivered back to the composite product manufacturer together with the TOE. The security IC embedded software is not part of the TOE.

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] gives 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]. Interpretations[7][8][9] are used.

SERTIT monitored the evaluation which was carried out by Brightsight B.V. as Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[10] to SERTIT on 23 January 2017. As a result 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 EAL5 assurance package augmented by AVA_VAN.5 and ALC_DVS.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete semi-formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Semiformal 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.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.2	Compliance with implementation standards
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: modular 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[10] 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 of its constituent components has been supplied, and to check that the security of the TOE has not been compromised in delivery.

The delivery procedure is described in the supporting document[12].

5.3 Installation and Guidance Documentation

Installation procedures are described in detail in the supporting document[12].

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Security IC Embedded Software shall follow the guidance documentation[11][12] for the TOE in order to ensure that the TOE is operated 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

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

An independent vulnerability analysis was done, consisting of the following steps:

- A design and implementation review on the TOE was done to identify weaknesses in the TOE that could potentially be exploited by attackers. A code review of the crypto library and boot code was also executed.

⠠⠙⠍⠞⠤⠉�������������������

- Validation tests of security features performed in the ATE class 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"[7]. User guidance is also taken 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.

5.6   Developer Tests

The developer tests consist of four parts:

1) *Testing on engineering samples*

   Developer tests performed on engineering samples (cards or Dual-In-Line-Package ICs)

2) *Testing on wafer*

   Developer tests performed on wafers

3) *Testing on simulation tools*

   Developer tests were done on simulation tools in the chip development environment, which were used to verify the logical functions.

4) *Testing on an emulation board*

   Developer tests were done on an emulation board (FPGA), mainly for the HAL.

5.7   Evaluator Tests

The evaluator's responsibility for independent testing is required by the ATE_IND class. Since developer's testing procedures were found to be extensive and thorough, and developer's hardware testing tools are not generally available to allow reproduction of developer test cases in the evaluator's test lab, the choice was made to perform the evaluator independent testing by witnessing of the developer's test cases, using the developer's tools, at the premises of the developer. The evaluator used a sampling strategy to select developer tests to validate the developer's test results. The sampling strategy is as follows:

- Tests on TSFI's are sampled

- Tests on Interfaces of SFR-enforcing modules are sampled

- Tests on Security Mechanisms are sampled

- All the testing methods (Wafer/Sample/Simulation/Emulator) will be sampled

In addition to this, the evaluator has defined additional test cases, prompted by study of the developer documentation. The test strategy is as shown below:

- Augmentation of developer testing for interfaces by varying parameters to more rigorously test the interface
- Supplementation of developer testing strategy, for example by applying the tests performed on engineering samples to wafer samples

The considerations that are taken during the selection of the interfaces to be tested are:

- Observation and understanding during the performance of the work units in ATE_COV, DPT and FUN
- Significance of the interfaces with respect to security

These tests are also performed using the developer's tools at the premises of the developer. The evaluator witnessed the whole process of the tests.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[10] as produced by the Evaluators, and of the conduct of the evaluation as witnessed by the Certifier, SERTIT has determined that DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) Dual Interface smart card chips with HAL library meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 5 augmented with AVA_VAN.5 and ALC_DVS.2 for the specified Common Criteria Part 2 extended functionality and Protection Profile BSI-CC-PP-0084-2014 V1.0, in the specified environment.

6.2 Recommendations

Prospective consumers of DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) Dual Interface smart card chips with HAL library 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.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 4.3 "TOE Scope   " and Chapter 5 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

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 consists of:

Type	Name	Version	Package
Hardware	DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048)	V2.0	die, module
Software	HAL	V1.0	Software library in ROM
Manual	DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) Preparative Procedures[12]	V0.1	document
	DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) Operational User Guidance[11]	V0.1	document

TOE Documentation

The supporting guidance documents evaluated were:

[a] DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) AGD_OPE.1 (Operational User Guidance), Version 0.1, 27 September 2016 [11]

[b] DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) AGD_PRE.1 (Preparative Procedures), Version 0.1, 28 September 2016 [12]

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

TOE Configuration

The TOE configuration used for testing was the same used for developer tests, this is described in Section 5.6 of this report.

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: Datang Microelectronics Technology Co., Ltd (DMT)

Product Name: DMT-CBS-CE3D3 Family (DMT-CBS-CE3D3/CC080/CC048) Dual Interface smart card chips with HAL library version 2.0

Type of Product: IC

Version and Release Numbers: 1.0

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

Evaluation Criteria: Common Criteria v. 3.1 R4

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

Name of Certification Body: SERTIT

Certification Report Identifier: SERTIT-093 CR Issue 1.0, 10 February 2017

Certificate Identifier: SERTIT-093 C

Date Issued: 10 February 2017

Kjartan Jæger Kvassnes
Certifier

Arne Høye Rage
Quality Assurance

Kristian Steinfeldt Bae
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security

CCRA recognition for components up
EAL 2 and ALC_FLR only.

SOGIS MRA recognition for
components up to EAL 4.