Version 2018-1

Certification Report

ID-ONE Cosmo V9 Essential version 3 (Cosmo V9)

Sponsor and developer: ***Idemia***
Défense Ouest - 420 rue d'Estienne d'Orves
92700 Colombes
France

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-200833-CR**
Report version:	**1**
Project number:	**200833**
Author(s):	**Wouter Slegers**
Date:	**11 December 2018**
Number of pages:	**13**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-18-200833**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Idemia** **Défense Ouest - 420 rue d'Estienne d'Orves, 92700 Colombes, France**
Product and assurance level	**ID-ONE Cosmo V9 Essential version 3 (Cosmo V9)** Assurance Package: ▪ EAL5 augmented with AVA_VAN.5 and ALC_DVS.2 Protection Profile Conformance: ▪ Java Card Protection Profile – Open Configuration, Version 3.0, May 2012 Published by Oracle, Inc. registered under the reference ANSSI-PP-2010/03-M01
Project number	**200833**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL7

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodolcgy for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity	Date of 1st issue : **14-12-2018** Certificate expiry : **14-12-2023**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

CONTENTS:

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the ID-ONE Cosmo V9 Essential version 3 (Cosmo V9). The developer of the ID-ONE Cosmo V9 Essential version 3 (Cosmo V9) is Idemia located in Colombes, France 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 TOE is a composite TOE, consisting of a Java Card smart card operating system and an underlying platform, which is a secure micro controller. The TOE provides Java Card 3.0.5 functionality with post-issuance applet loading, card content management and secure channel features as specified in Global Platform 2.3 including SCP03. Cryptographic functionality includes AES, DES, Triple-DES (3DES), RSA, RSA-CRT, RSA key-generation, and SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms, HMAC, ECC over GF(p) for signature generation and verification (ECDSA), ECC over GF(P) key generation, ECDH, random number generation according to CTR_DRBG from SP800-90, and CRC16 and CRC32.

Note that a MoC library is included in the TOE, but as there are no security claims on this library, the biometric functionality has not been assessed, only the self-protection of the TSF.

Note that CIPURSE functionality is included in the TOE, but as there are no security claims on this functionality, the CIPURSE functionality has not been assessed, only the self-protection of the TSF.

Note that MIFARE functionality from the underlying hardware is included in the TOE, but as there are no security claims on this functionality, it has not been assessed, only the self-protection of the TSF.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 11 December 2018 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ID-ONE Cosmo V9 Essential version 3 (Cosmo V9), 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 ID-ONE Cosmo V9 Essential version 3 (Cosmo V9) are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that the TOE meets the EAL5 augmented (EAL5(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and 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]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the ID-ONE Cosmo V9 Essential version 3 (Cosmo V9) from Idemia located in Colombes, France.

The TOE is comprised of the following main components:

Type	Name	Version	Form of delivery
Hardware	SLC32GDL400G3 SLC32GDA400G3 SLC32GDA348G3 SLC32GDL348G3	IFX_CCI_000005	Based on [HW-ST] Section 2.2.5: · in form of complete modules · with or without inlay mounting · with or without inlay antenna mounting · in form of plain wafers · in any IC case (for example TSSOP28, VQFN32, VQFN40, CCS-modules, etc.) · in no IC case or package, simply as bare dies · or in whatever type of package The form of delivery does not affect the TOE security and it can be delivered in any type, as long as the processes applied and sites involved have been subject of the appropriate audit.
	SLC32PDL400	IFX_CCI_000008 IFX_CCI_000014	
	software library		
	HSL	V01.22.4346-SLCx2_C65.lib	
	MCS (Mifare lib)	V02.03.3446	
	ID-ONE COSMO V9 ESSENTIAL	SAAAR 089233	

To ensure secure usage a set of guidance documents is provided together with the ID-ONE Cosmo V9 Essential version 3 (Cosmo V9). Details can be found in section ”Documentation” of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST-lite]*, chapter 1.8.

2.2 Security Policy

The TOE is a composite TOE, consisting of a Java Card smart card operating system and an underlying platform, which is a secure micro controller. The TOE provides Java Card 3.0.5 functionality with post-issuance applet loading, card content management and secure channel features as specified in Global Platform 2.3 including SCP03. Cryptographic functionality includes AES, DES, Triple-DES (3DES), RSA, RSA-CRT, RSA key-generation, and SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms, HMAC, ECC over GF(p) for signature generation and verification (ECDSA), ECC over GF(P) key generation, ECDH, random number generation according to CTR_DRBG from SP800-90, and CRC16 and CRC32.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 5.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Note that a MoC library is included in the TOE, but as there are no security claims on this library, the biometric functionality has not been assessed, only the self-protection of the TSF.

Note that CIPURSE functionality is included in the TOE, but as there are no security claims on this functionality, the CIPURSE functionality has not been assessed, only the self-protection of the TSF.

Note that MIFARE functionality from the underlying hardware is included in the TOE, but as there are no security claims on this functionality, it has not been assessed, only the self-protection of the TSF.

2.4 Architectural Information

The logical architecture, originating from the Security Target *[ST],* of the TOE can be depicted as follows:

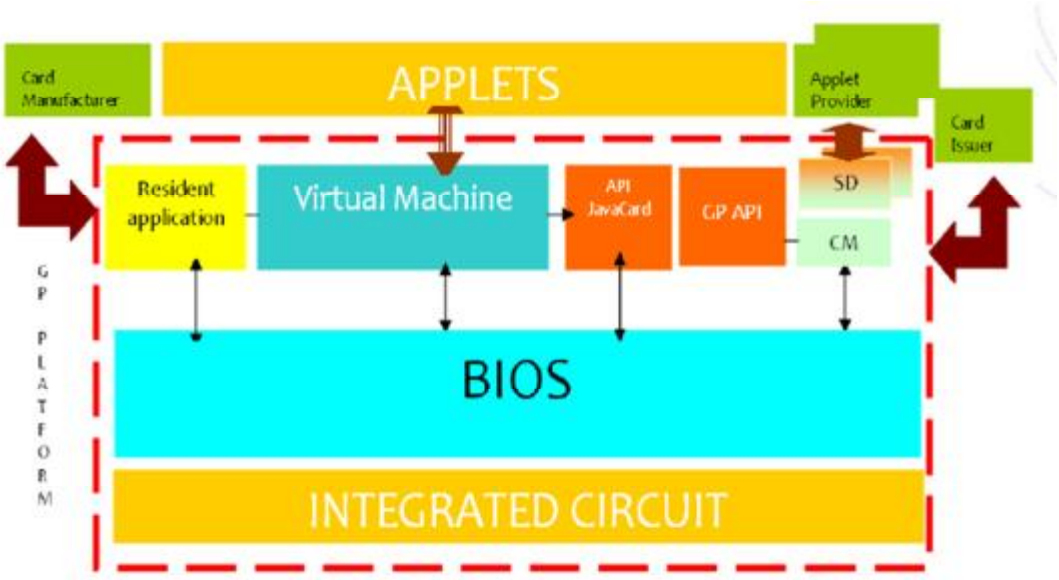

Figure 1. Logical architecture of the TOE.

2.5 Documentation

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

Name	Version	Date	Form of delivery
ID-ONE COSMO V9 ESSENTIAL Security Recommendations	4	29/10/2018	Electronic document (PDF)
ID-ONE COSMO V9 ESSENTIAL Reference Guide	5	22/10/2018	Electronic document (PDF)
Java Card API on ID-One Cosmo V9 platform	1	03/05/2018	Electronic document (html)
ID-ONE COSMO V9 ESSENTIAL Pre-Perso Guide	5	22/10/2018	Electronic document (PDF)

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Name	Version	Date	Form of delivery
ID-ONE COSMO V9 ESSENTIAL Application Loading Protection Guidance	2	24/09/2018	Electronic document (PDF)
Secure acceptance and delivery of sensitive elements	1	24/09/2018	Electronic document (PDF)

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 extensive testing on functional specification, subsystem and SFR-enforcing module level. 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.

The underlying hardware test results are extendable to composite evaluations, as the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

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 small number of test cases designed by the evaluator.

The evaluators have verified a selection of the developer tests during test witnessing, as well reproduced a small number of test cases designed by the evaluator.

2.6.2 Independent Penetration Testing

The reference for attack techniques against smart card-based devices such as the TOE must be protected against is the document named *Attack Methods for Smart Cards* and referenced as [JIL-AM]. The susceptibility of the TOE to these attacks has been analysed in a white box investigation conforming to AVA_VAN.5. The penetration tests are devised after performing the Evaluator Vulnerability Analysis. This approach has followed the following steps:

1. *Inventory of required resistance*
   This step uses the JIL attack list as described in *[JIL-AM]* as a reference for completeness and studies the ST claims to decide which attacks in the JIL attack list apply for the TOE.
2. *Validation of security functionalities*
   This step identifies the implemented security functionalities and performs tests to verify implementation and to validate proper functioning (ATE).
3. *Vulnerability analysis*
   This step first gives an overview against which attacks the implemented security functionalities are meant to provide protection. Secondly, in this step the design of the implemented security functionalities is studied. Thirdly, an analysis is performed to determine whether the design contains vulnerabilities against the attacks of step 1 (AVA).
4. *Analysis of input from other evaluation activities*
   This step first analyses the input from other CC-evaluation classes expressed as possible vulnerabilities. Secondly, the evaluators made an analysis of the TOE in its intended environment to check whether the developer vulnerability analysis provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance (AVA).
5. *Design assurance evaluation*
   This step analyses the results from an attack perspective as defined in step 1. Based on this design analysis the evaluators determine whether the design provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance (AVA).
6. *Penetration testing*
   This step performs the penetration tests identified in step 4 and step 5 (AVA).

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

7. *Conclusions on resistance*
   This step performs a *[JIL-AM]* compliant rating on the results of the penetration tests in relation with the assurance already gained by the design analysis. Based on the ratings the evaluators draw conclusions on the resistance of the TOE against attackers possessing a high attack potential.

In total 23,5 weeks of testing effort were spent, 15,5 weeks on the cryptographic functionality, 8 weeks on the Java Card functionality.

2.6.3 Test Configuration

Testing of the TOE was performed on SLC32PDL400 and SLC32GDL400G3 hardware samples. The TOE was in the version and configuration described in the *[ST]*.

2.6.4 Testing Results

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

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e. from the current best cryptanalytic attacks published, has been taken into account.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential".

The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits 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. These activities revealed that for some cryptographic functionality the security level could be reduced from an algorithmic security level above 100 bits to a practical remaining security level lower than 100 bits. As the remaining security level still exceeds 80 bits, this is considered sufficient. So no exploitable vulnerabilities were found with the independent penetration tests.

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

2.7 Re-used evaluation results

There has been extensive re-use of the ALC aspects for the sites involved in the software component of the TOE (Oberthur Technologies sites in Colombes, Pessac, Shenzen and Vitré Cedex, as well as ID3 Technologies in Grenoble), by use of 5 site re-use report approaches. Sites involved in the development and production of the hardware platform were re-used by composition.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number ID-ONE Cosmo V9 Essential version 3 (Cosmo V9)

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

[CCDB-2007-09-01] a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that have to be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the ID-ONE Cosmo V9 Essential version 3 (Cosmo V9) to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with AVA_VAN.5** and ALC_DVS.2. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'demonstrable' conformance to the Protection Profile *[PP]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. 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.

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>

Not all key sizes specified in the Security Target have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". In order to be protected against attackers with a "high attack potential", sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

3 Security Target

The SECURITY TARGET «SCYLLA» COSMO V9 ESSENTIAL,document reference FQR 110 8779 Ed 2.0 - I1.0, dated 10 December 2018 *[ST]* is included here by reference.

4 Definitions

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

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DES	Data Encryption Standard
DFA	Differential Fault Analysis
ECB	Electronic Code Book (a block cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MOC	Match On Card
NSCIB	Netherlands scheme for certification in the area of IT security
PP	Protection Profile
RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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.
[ETR]	Evaluation Technical Report ID-ONE Cosmo V9 Essential version 3 EAL5+, document reference 18-RPT-646, version 4.0, dated 2018-12-10
[ETRfC]	Evaluation Technical Report for Composition ID-ONE COSMO V9 ESSENTIAL – EAL5+, document reference 18-RPT-647, version 5.0 dated 2018-12-10
[HW-CERT]	BSI-DSZ-CC-0945-V2-2018forInfineon smart card IC (Security Controller) IFX_CCI_000003h, 000005h, 000008h, 00000Ch,000013h, 000014h, 000015h, 00001Ch, 00001Dh,000021h, 00022Dh, design step H13 with optional libraries CCL V2.0.0002, RSA2048/4096 V2.07.003 /V2.06.003, EC V2.07.003 / V2.06.003, ToolboxV2.07.003 / V2.06.003, HSL V02.01.6634 /V01.22.4346, MCS V02.02.3389 / V02.03.3446, SCL V2.02.010 and with specific IC dedicated software from Infineon Technologies AG, compliant to security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 Assurance: Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1, certificate date 20-04-2018
[HW-ETRfC]	ETR for composite evaluation (EFC), IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 00022Dh, design step H13, Certification ID BSI-DSZ-CC-0945-V2 2.03, 04 April 2018 2.03, 04 April 2018
[HW-ST]	Public Security Target Common Criteria v3.1 – EAL6 augmented / EAL6+ IFX_CCI_000003h IFX_CCI_000005h IFX_CCI_000008h IFX_CCI_00000Ch IFX_CCI_000013h IFX_CCI_000014h IFX_CCI_000015h IFX_CCI_00001Ch IFX_CCI_00001Dh IFX_CCI_000021h IFX_CCI_000022h H13 Resistance to attackers with HIGH attack potential, With firmware and software library options: 2x FW-Identifiers, Flash Loader, 2xMCS, 2xHSL, 2xACL, SCL and CIPURSE™ CL version 0.7, 2017-11-06
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September April 2017.
[PP]	Java Card Protection Profile – Open Configuration, Version 3.0, May 2012 Published by Oracle, Inc. registered under the reference ANSSI-PP-2010/03-M01.
[ST]	SECURITY TARGET «SCYLLA» COSMO V9 ESSENTIAL,document reference FQR 110 8779 Ed 2.0 - I1.0, dated 10 December 2018
[ST-lite]	ID-ONE COSMO V9 ESSENTIAL – Public Security Target, document reference FQR 110 8959 Ed 3.0 - I1.0, dated 10 December 2018

(This is the end of this report).

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.