Certification Report

ID-One CNS v2

Sponsor and developer:	***IDEMIA*** **2 Place Samuel de Champlain** **92 400 Courbevoie** **France**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-200270-CR**
Report version:	**1**
Project number:	**200270**
Author(s):	**Denise Cater**
Date:	**16 April 2019**
Number of pages:	**13**
Number of appendices:	**0**

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

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-19-200270

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer
IDEMIA

2 Place Samuel de Champlain, 92 400 Courbevoie, France

Product and assurance level
ID-One CNS v2

Assurance Package:

- EAL4 augmented with ALC_DVS.2 and AVA_VAN.5

Protection Profile Conformance

- EN 419211-2:2013, V2.0.1
- EN 419211-3:2013, V1.0.2
- EN 419211-4:2013, V1.0.1
- EN 419211-5:2013, V1.0.1
- EN 419211-6:2013, V1.0.4

Project number
200270

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)

The Designated Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 declares that:

- the IT product identified in this certificate is a Qualified Signature/Seal Creation Device (QSCD) where data is held in an entirely but not necessarily exclusively user-managed environment.
- The IT product meets the requirements laid down in Annex II of Regulation (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.
- Conformity of the IT product with the requirements of Annex II of [1] has been certified with an evaluation process that fulfils the requirements of Article 30(3.(a)) and the standards listed in the Annex of COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016."

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to 7

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology 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 : **17-04-2019**
Certificate expiry : **17-04-2024**

PRODUCTS
RvA C078
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

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

CONTENTS:

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.

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.

eIDAS-Regulation

TÜV Rheinland Nederland BV, operating the Netherlands Scheme for Certification in the Area of IT Security (NSCIB), has been notified as a Designated Certification Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014, *[EU-REG]*.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the ID-One CNS v2. The developer of the ID-One CNS v2 is IDEMIA located in Courbevoie, 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 Smart Card Integrated Circuit with Embedded Software serving as CNS application (Carta Nazionale dei Servizi) according to [CNS-SPEC], which provides QSCD (Qualified Signature Creation Device) functionality in accordance to *[EU-REG]* and conforms to the EN 419 211 Parts 2-6 (Signature Protection Profiles *[PP-SSCD-P2]*, *[PP-SSCD-P3]*, *[PP-SSCD-P4]*, *[PP-SSCD-P5]* and *[PP-SSCD-P6]* as reported in *[CR-SSCD-P2]*, *[CR-SSCD-P3]*, *[CR-SSCD-P4]*, *[CR-SSCD-P5]* and *[CR-SSCD-P6]*).

The TOE provides the following features:

- generation of the SCD and the correspondent SVD,
- importation of the SCD and, optionally, the correspondent SVD
- export the SVD for certification through a trusted channel to the CGA,
- prove the identity as QSCD to external entities
  optionally, receive and store certificate info,
- switch the TOE from a non-operational state to an operational state, and
- if in an operational state, create digital signatures for data
- identification and authentication of trusted users and applications,
- data storage and protection from modification or disclosures, as needed,
- secure exchange of sensitive data between the TOE and trusted applications,
- secure exchange of sensitive data between the TOE and a trusted human interface device.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 15 April 2019 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 CNS v2, 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 CNS v2 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 EAL4 augmented (EAL4(+)) 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 meets the requirements laid down in Annex II of Regulation (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014, *[EU-REG]*. The product will be listed on the NSCIB Certified Products list and will be notified to the European Commission (eIDAS). 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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the ID-One CNS v2 from IDEMIA located in Courbevoie, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SLC32GDL400G3 SLC32GDA400G3 SLC32GDA348G3 SLC32GDL348G3	IFX_CCI_000005
	SLC32PDL400	IFX_CCI_000008 IFX_CCI_000014
	Software Library - HSL	V01.22.4346-SLCx2_C65.lib
	Software Library - MCS (Mifare lib)	V02.03.3446
	Java Card Platform - ID-ONE COSMO V9 ESSENTIAL	SAAAAR 089233
Software	ID-One CNS v2	Code version “20 33 81” Internal version “00 00 01 09”

To ensure secure usage a set of guidance documents is provided together with the ID-One CNS v2. Details can be found in section ”*Documentation*” of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 3

2.2 Security Policy

The TOE is a composite TOE, consisting of a CNS applet (Idemia ID-One CNS v2 Java Card applet), a Java Card smart card operating system (Idemia ID-One COSMO V9 Essential Java Card platform) and an underlying platform (Infineon secure IC IFX_CCI_000005, IFX_CCI_000008 and IFX_CCI_000014). The TOE is a Smart Card Integrated Circuit with Embedded Software serving as CNS application, which provides QSCD functionality in accordance to *[EU-REG]*.

The TOE claims compliancy to EN 419 211 Parts 2-6 (Signature Protection Profiles *[PP-SSCD-P2]*, *[PP-SSCD-P3]*, *[PP-SSCD-P4]*, *[PP-SSCD-P5]* and *[PP-SSCD-P6]*), and it can be used as (depending on its configuration during personalization as described in *[UG]*:

- Config#1 claiming conformance to EN 419 211-2/3/4/5/6.
- Config#2 claiming conformance to EN 419 211-2/3/4. This configuration does not support the trusted channel between the TOE and the SCA.
- Config#3 claiming conformance to EN 419 211-2/3. This configuration does not support the trusted channel between: (i) the TOE and the SCA; (ii) the TOE and the CGA.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

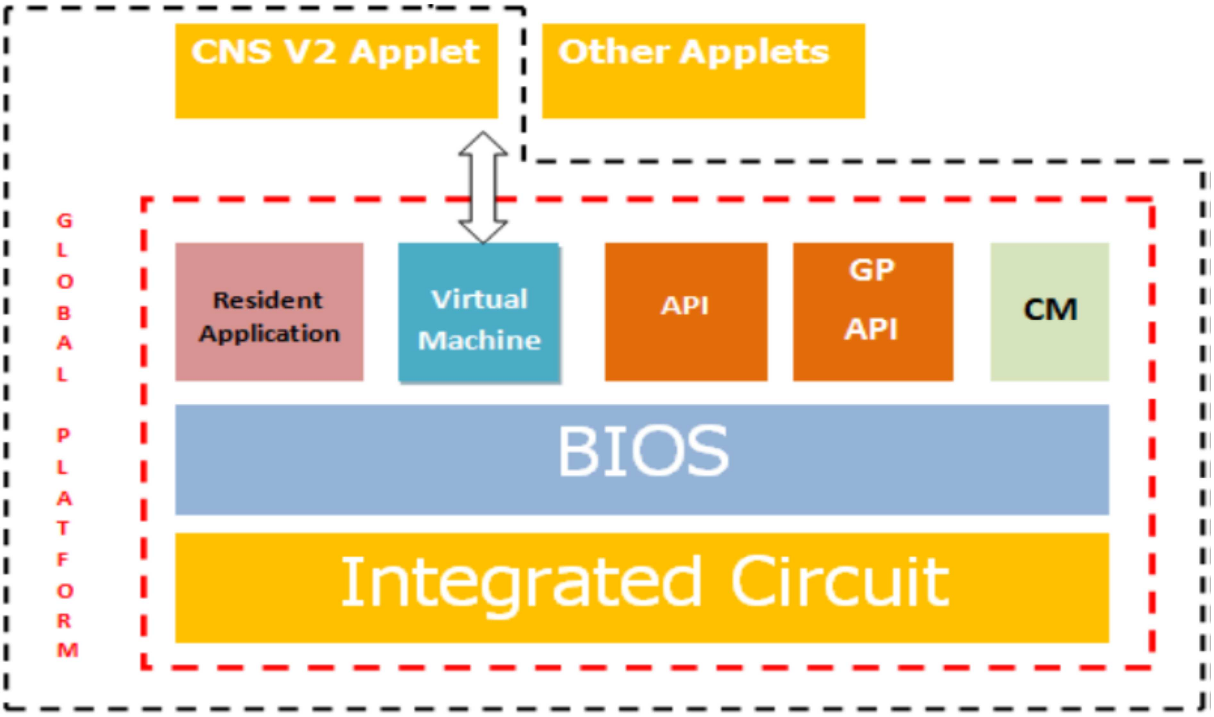
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 5.5 of the *[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.

2.4 Architectural Information

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



2.5 Documentation

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

Identifier	Version
FQR 220 1342 – SPHYNX – AGD_PRE	Issue 4
FQR 220 1343 – SPHYNX – AGD_OPE	Issue 4
FQR 220 1401 – ID-One CNS V2 Java Applet - User Guide	Issue 5
FQR 110 8797 – ID-One COSMO V9 Essential Pre-Perso Guide	Ed5
FQR 110 8823 – ID-One COSMO V9 Essential Reference Guide	Ed5
FQR 110 8794 – Applet Security Recommendations	Ed4
FQR 110 8798 – ID-One COSMO V9 Essential Application Loading Protection Guidance	Ed1
FQR 110 8921 – Secure acceptance and delivery of sensitive elements	Ed1
FQR 110 8827 – Java Card API on ID-One Cosmo V9 platform	Ed1

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 devised a test suite to test the operational behaviour of the TOE, which performs exhaustive testing in order to validate all the functionality of the CNS applet through the TSFI. The mapping of this test suite also demonstrates how the subsystem behaviour and the interactions between subsystems are demonstrated by the test suite.

The evaluator selected a small sample of tests to verify the correctness of the developer testing. The test witnessing activities were performed on site.

For the testing performed by the evaluators, the developer has provided samples. The evaluator devised and executed a set of tests aiming to verify the access conditions (including access to PIN-related objects) and secure messaging configuration of the file system.

2.6.2 Independent Penetration Testing

The independent penetration test plan has been designed based on the evaluator's white box vulnerability analysis, in compliance with the attack methodology [JIL-AM] for products claiming resistance to attackers with high attack potential (AVA_VAN.5) and the composite evaluation methodology [JIL-COMP].

The vulnerability analysis has followed the two main steps of the method described in [AIS34]:

- Examine sources publicly available.
- Conduct a methodical analysis of TOE evidence including the platform ETR for composition [HW-ETRfC] and the implementation representation.

All potential vulnerabilities were found to be not exploitable due to the security mechanisms of the certified Java Card platform, which rendered all the potential attack paths impractical. Additional testing to search for supported commands not defined in the user guidance was performed by the evaluators.

2.6.3 Test Configuration

Developer's testing has been performed on the TOE as defined in 2.1 (CNS applet version "20 33 81", Internal version "00 00 01 09" on Java Card platform SAAAAR 089233 (using microcontroller version SLC32GDA400G3).

Evaluator's independent and penetration testing has been performed on CNS applet version "20 33 81", Internal version "00 00 01 09" on Java Card platform SAAAAR 089233 (using microcontroller version SLC32GDA400G3).

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. The strength of the implementation of the cryptographic functionality has been assessed as part of the evaluation of the underlying Java Card Platform - ID-ONE COSMO V9 ESSENTIAL.

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).

2.7 Re-used evaluation results

Sites involved in the development and production of the hardware platform were re-used by composition.

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the software portions of the TOE (CNS applet), by use of 2 STAR and 6 site re-use reports.

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 CNS v2, as described in the identification part of this report.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references a ASE Intermediate Report and other evaluator documents.

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

Based on the above evaluation results the evaluation lab concluded the ID-One CNS v2, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profiles EN 419 211 Parts 2-6 (Protection Profiles *[PP-SSCD-P2], [PP-SSCD-P3], [PP-SSCD-P4], [PP-SSCD-P5]* and *[PP-SSCD-P6]* as reported in *[CR-SSCD2], [CR-SSCD3], [CR-SSCD4], [CR-SSCD5]* and *[CR-SSCD6]*).

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.

Not all key sizes specified in the *[ST]* 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).

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

3 Security Target

The “SPHYNX” - CNS V2 Security Target, version 0.7, FQR 550 0001 Ed1 *[ST]* is included here by reference.

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

4 Definitions

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

CGA	Certificate Generation Application
CNS	Carta Nazionale dei Servizi
DTBS	Data to be signed
DTBS/R	Data to be signed or its unique representation
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands scheme for certification in the area of IT security
PP	Protection Profile
QSCD	Qualified Signature Creation Device
SCD	Signature Creation Data
SSCD	Secure Signature Creation Device
SVD	Signature Verification Data
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

[CNS-SPEC] CNS – Carta Nazionale dei Servizi Functional Specification – Version 1.1.6 – April 2, 2011

[CR-SSCD-P2] Certification Report for Protection profiles for secure signature creation device — Part 2: Device with key Generation, CEN/TC 224, BSI-CC-PP-0059-2009-MA-02, Version 2.0.1, 30 June 2016, CC Version - 3.1 Revision 3.

[CR-SSCD-P3] Certification Report for Protection profiles for secure signature creation device – Part3: Device with key import, CEN/TC 224, BSI-CC-PP-0075-2012-MA-01, Version 1.0.2, 30 June 2016, CC Version - 3.1 Revision 3.

[CR-SSCD-P4] Certification Report for Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, CEN/TC 224, BSI-CC-PP-0071-2012-MA-01, Version 1.0.1, 30 June 2016, CC Version - 3.1 Revision 4.

[CR-SSCD-P5] Certification Report for Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, CEN/TC 224, BSI-CC-PP-0072-2012-MA-01, Version 1.0.1, 30 June 2016, CC Version - 3.1 Revision 4.

[CR-SSCD-P6] Certification Report for Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature creation application, CEN/TC 224, BSI-CC-PP-0076-2013-MA-01, Version 1.0.4, 30 June 2016, CC Version - 3.1 Revision 4.

[ETR] Evaluation Technical Report ID-One CNS v2, 19-RPT-125, Version 4.0, 15 April 2019.

[EU-REG] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 23 July 2014

[HW-CERT] Certification Report ID-ONE Cosmo V9 Essential version 3 (Cosmo V9), v1, 11 December 2018

[HW-ETRfC] Evaluation Technical Report for Composition ID-ONE COSMO V9 ESSENTIAL – EAL5+, v5.0, 10 December 2018

[HW-ST] ID-ONE COSMO V9 ESSENTIAL, Public Security Target, v3.0, 10 December 2018

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September 2017.

[PP-SSCD-P2] EN 419211-2:2013, Protection Profiles for secure signature creation device — Part 2: Device with key Generation, V2.0.1.

[PP-SSCD-P3] EN 419211-3:2013, Protection profiles for secure signature creation device – Part3: Device with key import, V1.0.2.

[PP-SSCD-P4] EN 419211-4:2013, Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, V1.0.1.

[PP-SSCD-P5] EN 419211-5:2013, Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, V1.0.1.

[PP-SSCD-P6] EN 419211-6:2013, Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature creation application, V1.0.4.

[ST] “SPHYNX” - CNS V2 Security Target, version 0.7, FQR 550 0001 Ed1.

[ST-lite] ID-One CNS V2 Public Security Target, v1.3, 15 April 2019

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

[UG] ID-One CNS V2 USER GUIDE, FQR 220 1401, Issue 5, 13 February 2019.

(This is the end of this report).