Version 2020-3

Certification Report

ID-One™ CNS V2 on Cosmo V9.1

Sponsor and developer:	***IDEMIA*** **2 place Samuel de Champlain** **92400 Courbevoie** **France**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0286907-CR**
Report version:	**1**
Project number:	**0286907**
Author(s):	**Denise Cater**
Date:	**16 February 2021**
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

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™ CNS V2 on Cosmo V9.1. The developer of the ID-One™ CNS V2 on Cosmo V9.1 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 claiming conformance to the SSCD Protection Profiles [EN419211-2], [EN419211-3], [EN419211-4], [EN419211-5] and [EN419211-6].

The TOE is a composite product consisting of:

- The Idemia ID-One™ CNS V2 Java Card applet
- The Idemia ID-One™ COSMO V9.1 Java Card platform
- The Infineon secure IC IFX_CCI_000005

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 10 February 2021 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]*.

Although this was a new evaluation, the TOE has been previously evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified with the reference CC-19-200270 on 16 April 2019, as reported *[CR-200270]*. This new evaluation was performed as a result of an updated platform used in the composite TOE. The security evaluation re-used the evaluation results of previously performed evaluations. A full, up to date vulnerability analysis has been made, as well as renewed testing.

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 on Cosmo V9.1, 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 on Cosmo V9.1 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 provides 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 and *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]* (Parts I, II and III).

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™ CNS V2 on Cosmo V9.1 from IDEMIA located in Courbevoie, France.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SLC32GDL400G3 SLC32GDA400G3	IFX_CCI_000005
	Java Card Platform - ID-ONE COSMO V9.1	SAAAAR 092914
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 on Cosmo V9.1. Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 4.

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 V9.1 Java Card platform) and an underlying platform (Infineon secure IC IFX_CCI_000005). 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 [EN419211-2], [EN419211-3], [EN419211-4], [EN419211-5] and [EN419211-6]), 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 6.5 of the *[ST]*.

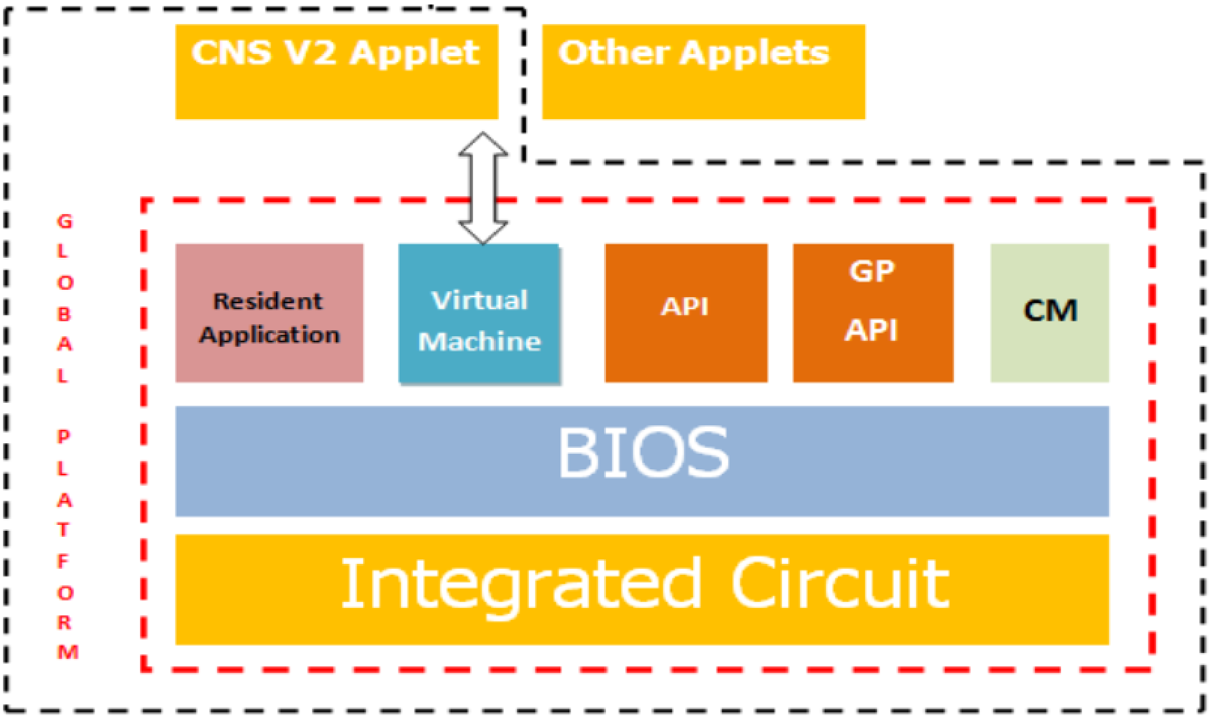
2.3.2 Clarification of scope

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

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

2.4 Architectural Information

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



The TOE provides the following features:

- generation of the SCD and the correspondent SVD,
- importation of the SCD and, optionally, the correspondent signature verification data (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 with the following steps:
    - select an SCD if multiple are present in the QSCD,
    - receive DTBS or a unique representation thereof DTBS/R through a trusted channel
- with SCA,
    - authenticate the signatory and determine its intent to sign,
    - apply an appropriate cryptographic signature creation function using the selected SCD
- to the DTBS/R
    - 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.

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

2.5 Documentation

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

Identifier	Version
ID-One CNS V2 Java Applet on Cosmo V9.1 - AGD_PRE, FQR 220 1516	Ed 1
ID-One CNS V2 Java Applet on Cosmo V9.1 - AGD_OPE, FQR 220 1517	Ed 1
ID-One CNS V2 Java Applet - User Guide, FQR 220 1401	Ed 7
ID-One COSMO V9.1 Biometry Pre-Perso Guide, FQR 110 9208	Ed 8
ID-One COSMO V9.1 Biometry Reference Guide, FQR 110 9200	Ed 6
ID-One COSMO V9.1 Biometry Security Recommendations, FQR 110 9237	Ed 2
Secure acceptance and delivery of sensitive elements, FQR 110 8921	Ed 1
ID-One COSMO V9.1 Application Loading Protection Guidance, FQR 110 9238	Ed 1
FQR 110 9242 – Java Card API on ID-One Cosmo V9.1 platform	Ed 1
FQR 110 8805 – JCVM_PATCH	Ed 2

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.

During the NSCIB-CC-200270 evaluation the evaluator selected a small sample of tests to verify the correctness of the developer testing. The test witnessing activities were performed on site. The witnessing procedure was not repeated for this evaluation, because the test set-up and strategy have not changed.

For the testing performed by the evaluators, the developer has provided samples.

During both NSCIB-CC-200270 evaluation and this evaluation, the evaluator devised and executed a set of tests aiming to verify the access conditions and secure messaging configuration of the file system.

2.6.2 Independent Penetration Testing

The methodical analysis performed was conducted along the following steps during the NSCIB-CC-200270 evaluation:

- When evaluating the evidence in the classes ASE, ADV and AGD no potential vulnerabilities were identified from generating questions to the type of TOE and the specified behaviour.
- For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack oriented analysis, the protection against the attack scenarios was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of additional potential vulnerabilities. This analysis was performed according to the attack list in *[JIL-AP]*. An important source for assurance against attacks in this step is the *[JC-ETRfC]* of the underlying platform; no additional potential vulnerabilities were concluded from this.

After the first implementation representation review, the Developer decided to update the product in order to improve the security of the TOE and address some of the identified potential vulnerabilities. A

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

second implementation representation review was performed to analyse the code modifications, following the same approach as for the first review.

- All potential vulnerabilities were analysed using the knowledge gained from the two implementation representation reviews, all the evaluation classes and the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. 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. No penetration tests were defined.

2.6.3 Test Configuration

Developer's testing for this evaluation was performed on the TOE as defined in 2.1. The specific IC version used was SLC32GDA400G3.

The evaluator testing for this evaluation was performed on the TOE as defined in 2.1. The specific IC version used was SLC32GDA400G3. The TOE was tested in the following configuration:

- SSCD-2,3,4,5,6 Configuration as defined in ID-One CNS V2 Java Applet - User Guide, FQR 220 1401 Ed7, section 7.2.1.

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.

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, *[JC-ETRfC].*

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

This has been performed effectively as a re-certification using NSCIB-CC-200270 as a baseline. Documentary evaluation results of the earlier version of the TOE have been re-used, but vulnerability analysis and penetration testing has been renewed.

There has been extensive re-use of the ALC aspects for the sites involved in the software component of the TOE. 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™ CNS V2 on Cosmo V9.1, 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]*, which references an ASE Intermediate Report and other evaluator documents.

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

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

Based on the above evaluation results the evaluation lab concluded the ID-One™ CNS V2 on Cosmo V9.1, 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 *[EN419211-2], [EN419211-3], [EN419211-4], [EN419211-5]* and *[EN419211-6]*.

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 *[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", appropriate cryptographic algorithms with 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 CNS V2 on Cosmo V9.1 - Security Target, FQR 550 0043, Ed 2, 2021-02-09 *[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	Certification generation application
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 Device
SCA	Signature creation application
SVD	signature verification data
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.

[CR-200270] Certification Report ID-One CNS v2, NSCIB-CC-200270-CR, v1, dated 16 April 2019, including certificate CC-19-200270.

[ETR] Evaluation Technical Report ID-One CNS V2 on COSMO V9.1 – EAL4+, 20-RPT-1298, Version 3.0, 9 February 2021.

[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.

[JC-CERT] Rapport de certification, ANSSI-CC-2020/07, Plateforme ID-One Cosmo V9.1 masquée sur le composant IFX SLC32, Identification du matériel 092914, 31/03/2020,
including Maintenance Report: Rapport de maintenance, ANSSI-CC-2020/07-M01, Plateforme ID-One Cosmo V9.1 masquée sur le composant IFX SLC32, Identification du matériel 092914, 23/07/2020

[JC-ETRfC] ETR for composite evaluation – PYRRHA, LETI.CESTI.PYR.RTC.001, V1.1, 12/03/2020.

[JC-ST] ID-One COSMO v9.1 Public Security Target, FQR 110 9395, version 5, 10/07/2020.

[JIL-AM] Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (controlled distribution).

[JIL-AP] Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.0, July 2020.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[EN419211-2] EN 419 211-2:2013, Protection Profiles for secure signature creation device - Part 2: Device with key Generation, V2.0.1, registered under the reference BSI-CC-PP-0059-2009-MA-02, 30 June 2016.

[EN419211-3] EN 419 211-3:2013, Protection profiles for secure signature creation device - Part 3: Device with key import, V1.0.2, registered under the reference BSI-CC-PP-0075-2012-MA-01, 30 June 2016.

[EN419211-4] 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 registered under the reference BSI-CC-PP-0071-2012-MA-01, 30 June 2016.

[EN419211-5] 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 registered under the reference BSI-CC-PP-0072-2012-MA-01, 30 June 2016.

[EN419211-6] 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 registered under the reference BSI-CC-PP-0076-2013-MA-01, 30 June 2016.

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

[ST]	CNS V2 on Cosmo V9.1 - Security Target, FQR 550 0043, Ed 2, 2021-02-09.
[ST-lite]	ID-One CNS V2 on Cosmo V9.1 - Public Security Target, FQR 550 0167, Ed 1, 2021-02-09.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).

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