Version 2020-2

Certification Report

CELES-c002 Machine Readable Electronic Document, eIDAS QSCD Application, version 1

Sponsor:	***Eurowitcel S.A.*** **Camino Parque Centenario 2222, (B1894JBB),** **Villa Elisa, La Plata,** **Buenos Aires,** **Argentina**
Developer:	***HID Global*** **viale Remo De Feo, 1** **80022 Arzano (NA),** **Italy**
Evaluation facility:	***UL*** **Unit 2 Horizon, Wade Road, Kingsland Business Park** **Basingstoke, Hampshire, RG24 8AH** **United Kingdom**
Report number:	**NSCIB-CC-0245771-CR**
Report version:	**1**
Project number:	**0245771**
Author(s):	**Denise Cater**
Date:	**02 November 2020**
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

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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the CELES-c002 Machine Readable Electronic Document, eIDAS QSCD Application, version 1. The developer of the CELES-c002 Machine Readable Electronic Document, eIDAS QSCD Application, version 1 is HID Global located in Arzano, Italy. The sponsor of the evaluation and certification was Eurowitcel S.A. located in Buenos Aires, Argentina. 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 product made up of the "eIDAS QSCD Application" and native Smart Card operating system "CELES-c002" in composition with the already certified "NXP N7121" integrated circuit.

The TOE provides an eIDAS Qualified Signature Creation Device (QSCD) application compliant with the eIDAS Regulation (EU) No 910/2014 of the European Parliament and of the Council and in accordance with the Commission Implementing Decision (EU) 2016/650.

The TOE is delivered in phase 2 of its life-cycle to the Card manufacturer as a microcontroller module which is ready to be embedded into a Smart Card or document booklet with the antenna and substrate, which are outside the physical boundaries of the TOE.

The TOE has been evaluated by UL located in Hampshire, UK. The evaluation was completed on 02 November 2020 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 CELES-c002 Machine Readable Electronic Document, eIDAS QSCD Application, version 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 CELES-c002 Machine Readable Electronic Document, eIDAS QSCD Application, version 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 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]* and the Dutch Conformity Assessment Process *[DCAP]* 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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the CELES-c002 Machine Readable Electronic Document, eIDAS QSCD Application, version 1 from HID Global located in Arzano, Italy.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NXP N7121 IC (Certification ID: BSI-DSZ-CC-1040-2019)	Hardware release B1
	• IC Dedicated Test Software	Release 9.2.3
	• IC Dedicated Support Software including:	Release 9.2.3
	○ Flashloader OS	Release 1.2.5
	○ Communication Library	Release 6.0.0
	○ CRC Library	Release 1.1.8
	○ Memory Library	Release 1.2.3
	○ Flash Loader Library	Release 3.6.0
	○ System Mode OS	Release 13.2.3
	○ Crypto Library	Release 0.7.6
Software	CELES-c002_1	Version 1

To ensure secure usage a set of guidance documents is provided together with the CELES-c002 Machine Readable Electronic Document, eIDAS QSCD Application, version 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 2.3.

2.2 Security Policy

The TOE is a contact or contactless based integrated circuit chip comprised of all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature and deciphered data. The TOE is delivered to the Card manufacturer in Phase 2 as a microcontroller module which is ready to be embedded into a Smart Card or document booklet with the antenna and substrate, which are outside the physical boundaries of the TOE.

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 also that the PPs claim the environment for the TOE protects against loss or theft of the TOE, deters and detects physical tampering, protects against attacks based on emanations of the TOE, and protects against unauthorised software and configuration changes on the TOE and the hardware appliance it is contained in ("OE.Env Protected operating environment").

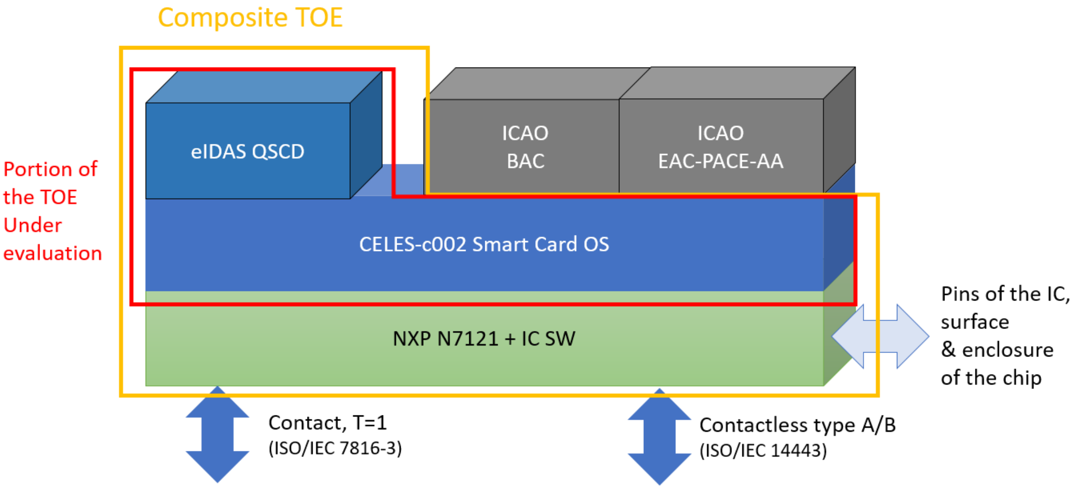
The ST follows the PPs and also claims OE.Env, thus the environment in which the TOE is used must ensure the above protection.

Any threats violating these objectives for the environment are not considered.

The CELES-c002 product consists of three separate applications. This certification addresses the TOE that contains the eIDAS QSCD Application. The additional applications noted below were evaluated concurrently with this TOE, but are addressed by separate certificates and are out of scope of this report.

- ICAO Application – BAC
- ICAO Application - EAC-PACE-AA.

2.4 Architectural Information


Composite TOE
Portion of the TOE Under evaluation
eIDAS QSCD
ICAO BAC
ICAO EAC-PACE-AA
CELES-c002 Smart Card OS
NXP N7121 + IC SW
Pins of the IC, surface & enclosure of the chip
Contact, T=1 (ISO/IEC 7816-3)
Contactless type A/B (ISO/IEC 14443)

The TOE is comprised of the following subsystems:

- Commands manager: responsible for managing application commands, managing rollback and reset, and managing access conditions.
- Security manager: responsible for authentication, secure messaging, security data management, and low-level crypto features.
- Data objects and NVM management: responsible for managing the storage of persistent data.
- Communications manager: manages the contact (T=1 ISO/IEC 7816-3) and contactless (ISO/IEC 14443) communication interface protocols, and handles errors during start-up.
- Initialization and command management: responsible for TSF secure initialization, life cycle and secure messaging status management, managing the main loop, command dispatch, and utility functions.

2.5 Documentation

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

Identifier	Version
CELES-c002 Machine Readable Electronic Document Operational User Guidance eIDAS QSCD application, TCAE190020	1.2, 2020-10-29
CELES-c002 Machine Readable Electronic Document Personalization Guidance eIDAS QSCD application, TCAE190018	1.2, 2020-10-29
CELES-c002 Machine Readable Electronic Document Pre-personalization Guidance eIDAS QSCD application, TCAE190016	1.2, 2020-10-29

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 and subsystems. The developer used a black-box testing approach. The testing coverage and depth is achieved by the black-box testing on the external interfaces. Black-box testing on the external interfaces is done using a subset of the ICAO and BSI test plans for e-passports. These are public test plans intended for testing the correct implementation of the e-passport functionality.

Since the public ICAO and BSI test plans are very comprehensive and all the TSFI's listed in the specifications are tested by them, they are the most suitable way to test the mechanisms and protocols provided by the ICAO and BSI specifications. The developer performed additional tests on the external interfaces to demonstrate those not covered by the generic BSI and ICAO test plans.

The sample of tests selected for repetition by the evaluators covered all the TSFI commands, with at least one test case per TSFI.

The evaluator augmented the testing of the interfaces used in the TOE in phases 2 and 3 (pre-personalisation and personalisation phases), which are TOE specific, by using different test parameters with the same tools as the developer.

The evaluator augmented the testing of TOE internal modules by using different inputs on a small set of interfaces with the same tools as the developer.

Some tests were performed on an earlier version of the TOE, with a subset of confirmatory test cases performed on the final version of the TOE.

2.6.2 Independent Penetration Testing

The evaluator performed a vulnerability analysis using a vulnerability-centric approach. All generic attacks to smart cards and similar devices considered in [JIL_AM] have been taken into account.

The evaluator performed a public vulnerability search, including a literature review of conference proceedings, University research, relevant journals and published papers. The evaluator also considered Internet surveys and online vulnerability databases.

The evaluator then performed an independent vulnerability analysis as follows:

- The security architecture of the TOE was analysed and understood based on the security architecture document.
- The SFRs defined in [ST] were analysed and for each, a deep understanding of the SFR was gained based on all the evidence provided for ADV.
- The security guidance documentation and the ETR for composition of the underlying platform were analysed and a list of requirements that the embedded software must be compliant with were extracted.

- The code review confirmed that the elements listed in the previous bullets were implemented as described and looked for vulnerabilities in each item.

The evaluators performed two perturbation tests, with light, EMFI and FBBI for fifteen weeks and one side channel attack test for six weeks. These tests were performed on an earlier version of the TOE. Having examined the changes between the earlier version and final version of the TOE, the evaluator profiled the commands that were tested on the earlier version of the TOE and demonstrated the test results were equally applicable to the final version of the TOE.

2.6.3 Test Configuration

All developer and evaluator testing was performed on operational samples of the TOE. The only exception to this was the use of open samples during the identification phase of the side-channel testing. Some test were performed on an earlier version of the TOE, with a subset of confirmatory test cases performed on the final version of the TOE, as identified in Identification of Target of Evaluation section above.

The following test equipment and tools were used by the evaluator:

- UL Zeus test suite v4.2.0.18.
- UL DEEPLY_v0.7.9_Release_bis.
- UL Crypto Tool v1.0, including:
  - Artemis v4.2
  - Atropos v5.0
- MATLAB R2017a.

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.

2.7 Re-used evaluation results

There has been extensive re-use of the ALC aspects for the sites involved in the development of the TOE, by use of one Site Technical Audit Re-use report *[STAR]*.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number CELES-c002 Machine Readable Electronic Document, eIDAS QSCD Application, version 1.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* which references an ASE 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 CELES-c002 Machine Readable Electronic Document, eIDAS QSCD Application, version 1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 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 *[PP2]*, *[PP4]* and *[PP5]*.

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. 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.

3 Security Target

The Security Target for CELES-c002 Machine Readable Electronic Document - QSCD Application, TCAE190026, v1.2, 2020-09-17 *[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:

AA	Active Authentication
BAC	Basic Access Control
EAC	Extended Access Control
eIDAS	electronic IDentification, Authentication and trust Services
eMRTD	electronic MRTD
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MRTD	Machine Readable Travel Document
NSCIB	Netherlands Scheme for Certification in the area of IT security
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
QSCD	Qualified Signature/Seal Creation Device
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.

[CR-SSCD-PP2] 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, 30 June 2016.

[CR-SSCD-PP4] Certification Report for Protection profiles for secure signature creation device – Part3: Extension for device with key generation and trusted communication with certificate generation application, CEN/TC 224, BSI-CC-PP-0071-2012-MA-01, 30 June 2016.

[CR-SSCD-PP5] Certification Report for Protection profiles for secure signature creation device – Part5: Extension for device with key generation and trusted communication with signature creation application, CEN/TC 224, BSI-CC-PP-0072-2012-MA-01, 30 June 2016.

[ETR] CELES-c002 Machine Readable Electronic Document eIDAS QSCD Application Evaluation Technical Report, UL12665569-CELES/ETR_QSCD, Version 2.0, 2020-11-02.

[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

[HW-CERT] Certification Report BSI-DSZ-CC-1040-2019 for NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library from NXP Semiconductors Germany GmbH.

[HW-ETRfC] ETR for Composition NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (N7121) – EAL6+ according to AIS36, BSI-CC-1040, version 8.0, 31 May 2019.

[HW-ST] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library Security Target Lite, version 1.1, 31 May 2019.

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

[PP2] EN 419211-2:2013, Protection Profiles for secure signature creation device - Part 2: Device with key Generation, V2.0.1.

[PP4] 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.

[PP5] 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.

[ST] Security Target for CELES-c002 Machine Readable Electronic Document - QSCD Application, TCAE190026, v1.2, 2020-09-17.

[ST-lite] Security Target for CELES-c002 Machine Readable Electronic Document – eIDAS QSCD Application - Public Version, TCLE190029, v1.1, 2020-10-19.

[STAR]	Site Technical Audit Report HID Global S.p.A, Arzano, Italy, version 3.0, 2020-08-14.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).