Reference: 2017-19-INF-3171-v1
Target: Público
Date: 20.07.2020

Created by: CERT11
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2017-19**
TOE	**CELES-c001 Machine Readable Electronic Document SSCD Application, version 1 (CELES-c001_1)**
Applicant	**30-70825259-6 - Eurowitcel S.A.**
References	
	[EXT-3383] Certification Request
	[EXT-5895] Update of Certification Request
	[EXT-5973] Evaluation Technical Report

Certification report of the product CELES-c001 Machine Readable Electronic Document SSCD Application, version 1 (CELES-c001_1), as requested in [EXT-3393] and [EXT-5895], and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-5973] received on 09/06/2020.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product CELES-c001 Machine Readable Electronic Document SSCD Application, version 1 (CELES-c001_1).

The Target Of Evaluation (TOE) is the integrated circuit chip Infineon M7892 G12 equipped with operating system CELES-c001 and with e-Document applications, namely an International Civil Aviation Organization (ICAO) application compliant with ICAO Doc 9303, and a Secure Signature Creation Device (SSCD) application compliant with European Parliament Directive 1999/93/EC. The SSCD application can optionally be configured as a PKCS #15 application.

Developer/manufacturer: HIDGlobal S.p.A.

Sponsor: Eurowitcel S.A.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Protection Profiles: Protection profiles for secure signature creation device – Part 2: Device with key generation, v2.0.1, January 2012, BSI-CC-PP-0059-2009-MA-01.

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, November 2012, BSI-CC-PP-0071-2012.

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, November 2012, BSI-CC-PP-0072-2012.

Evaluation Level: Common Criteria for Information Technology Security Evaluation version 3.1 revision 5 - EAL5+ALC_DVS.2+AVA_VAN.5.

Evaluation end date: 09/06/2020

Expiration Date[1]: 11/07/2025

All the assurance components required by the evaluation level EAL5 (augmented with ALC_DVS.2 and AVA_VAN.5) have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL5+ALC_DVS.2+AVA_VAN.5, as defined by the Common Criteria for Information Technology Security Evaluation version 3.1 revision 5 and the Common Methodology for Information Technology Security Evaluation version 3.1 revision 5.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

Considering the obtained evidences during the instruction of the certification request of the product CELES-c001 Machine Readable Electronic Document SSCD Application, version 1 (CELES-c001_1), a positive resolution is proposed.

TOE SUMMARY

The Target Of Evaluation (TOE) is the integrated circuit chip Infineon M7892 G12 equipped with operating system CELES-c001 and with e-Document applications, namely an International Civil Aviation Organization (ICAO) application compliant with ICAO Doc 9303, and a Secure Signature Creation Device (SSCD) application compliant with European Parliament Directive 1999/93/EC. The SSCD application can optionally be configured as a PKCS #15 application.

The TOE is composed of:

- dual-interface chip Infineon M7892 G12 equipped with IC Dedicated Software (cf. Appendix A for more details);
- smart card operating system CELES-c001;
- a Secure Signature Creation Device (SSCD) application compliant with European Parliament Directive 1999/93/EC;
- guidance documentation in PDF format about the preparation and use of the SSCD application, composed by:
    - the Pre-personalization Guidance ,
    - the Personalization Guidance,
    - the Operational User Guidance.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL5+ALC_DVS.2+AVA_VAN.5and the evidences required by the additional component xxxxx, according to Common Criteria for Information Technology Security Evaluation version 3.1 revision 5 - EAL5+ALC_DVS.2+AVA_VAN.5.

Security assurance requirements	Titles
Class ADV: Development	
ADV_ARC.1	Architectural design
ADV_FSP.5	Functional specification
ADV_IMP.1	Implementation representation
ADV_INT.2	Internals
ADV_TDS.4	TOE design
Class AGD: Guidance documents	
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative user guidance
Class ALC: Life-cycle support	
ALC_CMC.4	CM capabilities

ALC_CMS.5	CM scope
ALC_DEL.1	Delivery
ALC_DVS.2	Development security
ALC_LCS.1	Life-cycle definition
ALC_TAT.2	Tools and techniques
Class ASE: Security Target evaluation	
ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST introduction
ASE_OBJ.2	Security objectives
ASE_SPD.1	Security problem definition
ASE_TSS.1	TOE summary specification
Class ATE: Tests	
ATE_COV.2	Coverage
ATE_DPT.3	Depth
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing
Class AVA: Vulnerability analysis	
AVA_VAN.5	Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria for Information Technology Security Evaluation version 3.1 revision 5 - EAL5+ALC_DVS.2+AVA_VAN.5:

Security functional requirement	Title
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction – e-Document
FCS_COP.1	Cryptographic operation
FDP_ACC.1/SCD/SVD_Generation	Subset access control – SCD/SVD generation
FDP_ACF.1/SCD/SVD_Generation	Security attribute based access control – SCD/SVD generation
FDP_ACF.1/SVD_Transfer	Security attribute based access control – SVD transfer
FDP_ACC.1/Signature creation	Subset access control – Signature creation
FDP_ACF.1/Signature creation	Security attribute based access control – Signature creation
FDP_RIP.1	Subset residual information protection
FDP_SDI.2/Persistent	Stored data integrity monitoring and action – Persistent data
FDP_SDI.2/DTBS	Stored data integrity monitoring and action – DTBS
FDP_DAU.2/SVD	Data authentication with identity of guarantor

FDP_UIT.1/DTBS	Data exchange integrity
FIA_UID.1	Timing of identification
FIA_UAU.1	Timing of authentication
FIA_AFL.1/Signatory	Authentication failure handling
FIA_AFL.1/Admin	Authentication failure handling
FIA_AFL.1/Pre-pers	Authentication failure handling
FIA_AFL.1/Pers	Authentication failure handling
FIA_API.1	Authentication proof of identity
FMT_SMR.1/SSCD	Security roles
FMT_SMR.1/Pre-pers	Security roles
FMT_SMR.1/Pers	Security roles
FMT_SMF.1	Specification of management functions
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1/Admin	Management of security attributes – Administrator
FMT_MSA.1/Signatory	Management of security attributes – Signatory
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MSA.4	Security attribute value inheritance
FMT_MTD.1/Admin	Management of TSF data – Administrator
FMT_MTD.1/Signatory	Management of TSF data – Signatory
FMT_MTD.1/Pre-pers	Management of TSF data – Pre-personalization Agent
FMT_MTD.1/Pers	Management of TSF data – Personalization Agent
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FPT_EMS.1	TOE emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.3	Resistance to physical attack
FPT_TST.1	TSF testing
FTP_ITC.1/SVD	Inter-TSF trusted channel – SVD
FTP_ITC.1/VAD	Inter-TSF trusted channel – VAD
FTP_ITC.1/DTBS	Inter-TSF trusted channel – DTBS
FTP_ITC.1/Pre-pers	Inter-TSF trusted channel – Pre-personalization data
FTP_ITC.1/Pers	Inter-TSF trusted channel – Personalization data

IDENTIFICATION

Product: CELES-c001 Machine Readable Electronic Document SSCD Application, version 1 (CELES-c001_1)

Security Target: Security Target for CELES-c001 Machine Readable Electronic Document - SSCD Application, Version 1.8. 2020-03-06. TCAE160035.

Protection Profiles: Protection profiles for secure signature creation device – Part 2: Device with key generation, v2.0.1, January 2012, BSI-CC-PP-0059-2009-MA-01.

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, November 2012, BSI-CC-PP-0071-2012.

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, November 2012, BSI-CC-PP-0072-2012

Evaluation Level: Common Criteria for Information Technology Security Evaluation version 3.1 revision 5 - EAL5+ALC_DVS.2+AVA_VAN.5.

SECURITY POLICIES

The use of the product CELES-c001 Machine Readable Electronic Document SSCD Application, version 1 (CELES-c001_1) shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target. In short, it establishes the need of implementing organisational policies related to the following aspects.

P.CSP_QCert

Qualified certificates

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate ([EP], article 2, clause 9, and Annex I) for the SVD generated by the SSCD. The certificates contain at least the name of the Signatory and the SVD matching the SCD implemented in the TOE under sole control of the Signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

P.QSign

Qualified electronic signatures

The Signatory uses a Signature Creation System to sign data with an advanced electronic signature ([EP], article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to [EP], Annex I). The DTBS are presented to the Signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature with an SCD implemented in the SSCD that the Signatory maintains under their sole control, and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

P.Sigy_SSCD

TOE as Secure Signature Creation Device

The TOE meets the requirements for an SSCD laid down in [EP], Annex III. This implies that the SCD is used for digital signature creation under sole control of the Signatory and the SCD can practically occur only once.

P.Sig_Non-Repud

Non-repudiation of signatures

The life cycle of the SSCD, the SCD, and the SVD shall be implemented in a way that the Signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

Here below are further OSPs, added in this security target to those defined in the PPs

P.Manufact

Manufacturing of the e-Document

The IC Manufacturer writes IC initialization data in step 3, IC manufacturing, of TOE life cycle, including the key for the authentication of the Pre-personalization Agent (cf. section 2.3.2).

The Pre-personalization Agent writes pre-personalization data in step 5, prepersonalization, of TOE life cycle (cf. section 2.3.2), including the key for the authentication of the Personalization Agent.

The Pre-personalization Agent acts on behalf of the SSCD provisioning service.

P.Personalization

Personalization of the e-Document by issuing State or Organization only

The Personalization Agent writes personalization data in step 6, personalization, of TOE life cycle (cf. section 2.3.3), including the credentials for the authentication of the Administrator and the PACE key for the authentication of the Signatory.

The Personalization Agent acts on behalf of the SSCD provisioning service

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

A.CGA

Trustworthy Certificate Generation Application

The CGA protects the authenticity of the Signatory's name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP

A.SCA

Trustworthy Signature Creation Application

The Signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of the data that the Signatory wishes to sign in a form appropriate for signing by the TOE.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product CELES-c001 Machine Readable Electronic Document SSCD Application, version 1 (CELES-c001_1), although the agents implementing attacks have high attack potential according to CC v3.1 R5 EAL5+ALC_DVS.2+AVA_VAN.5 assurance level and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are categorized below.

T.SCD_Divulg

Storage, copy, and release of Signature Creation Data

An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage, and use for signature creation in the TOE

T.SCD_Derive

Derivation of Signature Creation Data

An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

T.Hack_Phys

Physical attacks through TOE interfaces

An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD, and DTBS.

T.SVD_Forgery

Forgery of Signature Verification Data

An attacker forges the SVD presented by the CSP to the CGA. This results in loss of SVD integrity in the certificate of the Signatory

T.SigF_Misuse

Misuse of the signature creation function of the TOE

An attacker misuses the signature creation function of the TOE to create an SDO for data the Signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

T.DTBS_Forgery

Forgery of the DTBS/R

An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS that the Signatory intended to sign.

T.Sig_Forgery

Forgery of the electronic signature

An attacker forges an SDO, maybe using an electronic signature which has been created by the TOE, and the violation of the integrity of the SDO is not detectable by the Signatory or by third parties. The signature created by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

Here below is a further threat, added in this security target to those defined in the PPs

T.Abuse-Func

Abuse of functionality

An attacker may abuse functions of the TOE which may not be used after TOE delivery in order (i) to manipulate or disclose the user data stored in the TOE, (ii) to manipulate or disclose the TSF data stored in the TOE, or (iii) to manipulate (bypass, deactivate, or modify) the TSF.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are categorized below.

OE.SVD_Auth

Authenticity of the SVD

The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the Signatory and the SVD in the qualified certificate.

OE.CGA_QCert

Generation of qualified certificates

The CGA shall generate a qualified certificate that includes (among others):

- the name of the Signatory controlling the TOE,
- the SVD matching the SCD stored in the TOE and being under sole control of the Signatory,
- the advanced signature of the CSP

The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in the SSCD.

OE.DTBS_Intend

SCA sends data intended to be signed

The Signatory shall use a trustworthy SCA that:

- generates the DTBS/R of the data that has been presented as DTBS and which the Signatory intends to sign in a form which is appropriate for signing by the TOE,
- sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R ,by the TOE,
- attaches the signature produced by the TOE to the data or provides it separately.

OE.Signatory

Security obligation of the Signatory

The Signatory shall check that the SCD stored in the SSCD received from the SSCD provisioning service is in non-operational state. The Signatory shall keep their VAD confidential.

Here below are the security objectives for the operational environment defined in PP Part 4.

OE.Dev_Prov_Service

Security obligation of the Signatory

The SSCD provisioning service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, personalizes the TOE for the legitimate user as Signatory,

links the identity of the TOE as SSCD with the identity of the legitimate user, and delivers the TOE to the Signatory.

Application Note 6 This objective replaces OE.SSCD_Prov_Service from PP Part 2 [PP-0059], which is possible as it does not imply any additional requirement for the operational environment when compared with OE.SSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.SSCD_Prov_Service).

OE.CGA_SSCD_Auth

Preparation of the TOE for SSCD authentication

The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as SSCD, successfully proved this identity as SSCD to the CGA, and whether this identity is linked to the legitimate holder of the device as applicant for the certificate.

OE.CGA_TC_SVD_Imp

CGA trusted channel for SVD import

The CGA shall detect alteration of the SVD imported from the TOE with the claimed identity of the SSCD.

Application Note 7 The developer prepares the TOE for the delivery to the customer (i.e. the SSCD provisioning service) in the development phase, not addressed by security objectives for the operational environment. The SSCD provisioning service performs initialization and personalization as TOE for the legitimate user (i.e. the device holder). If the TOE is delivered to the device holder with SCD, the TOE is an SSCD. This situation is addressed by OE.SSCD_Prov_Service except for the additional initialization of the TOE for proof as SSCD and trusted channel to the CGA. If the TOE is delivered to the device holder without SCD, the TOE will be an SSCD only after generation of the first SCD/SVD pair. Because this SCD/SVD pair generation is performed by the Signatory in the operational use stage, the TOE provides additional security functionality addressed by OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp. But this security functionality must be initialized by the SSCD provisioning service as described in OE.Dev_Prov_Service. Therefore, PP Part 4 [PP-0071] substitutes OE.SSCD_Prov_Service by OE.Dev_Prov_Service, allowing generation of the first SCD/SVD pair after delivery of the TOE to the device holder and requiring initialization of security functionality of the TOE. Nevertheless, the additional security functionality must be used by the operational environment as described in OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp. This approach does not weaken the security objectives and requirements for the TOE, but enforces more security functionalities of the TOE for additional methods of use. Therefore, it does not conflict with the CC conformance claim to PP Part 2.

OE.HID_TC_VAD_Exp

HID trusted channel for VAD export

The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed, including export to the TOE by means of a trusted channel.

Application Note 8 This security objective for the TOE is partly covering OE.HID_VAD from PP Part 2 [PP-0059]. While OE.HID_VAD in PP Part 2 requires only the operational environment to protect VAD, this PP requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore, PP Part 5 partly re-assigns the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp, and leaves only the necessary functionality by the HID

OE.SCA_TC_DTBS_Exp

SCA trusted channel for DTBS export

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS, to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

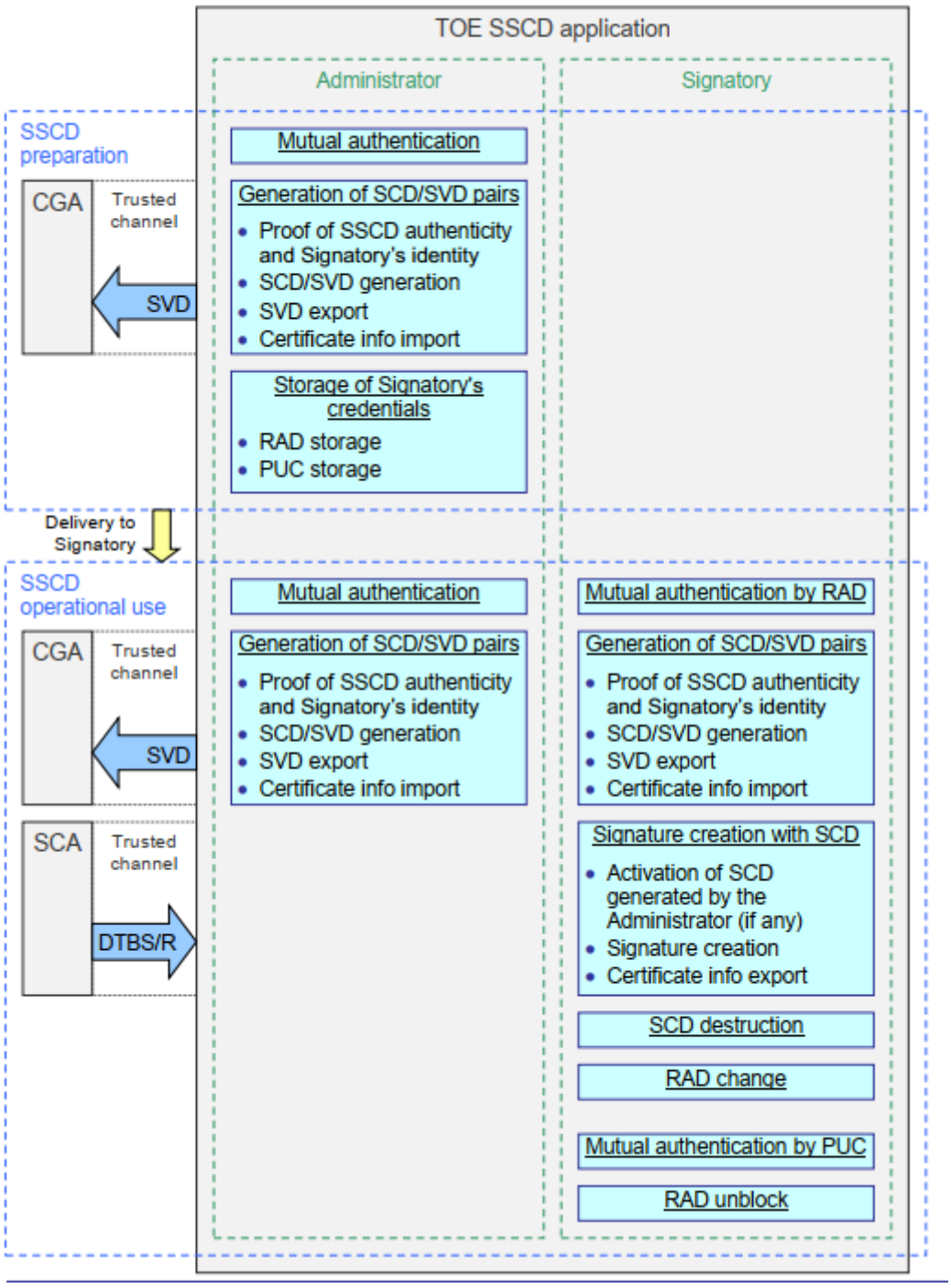
Application Note 9 This security objective for the TOE is partly covering OE.DTBS_Protect from PP Part 2 [PP-0059]. While OE.DTBS_Protect in PP Part 2 requires only the operational environment to protect DTBS, this PP requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore, PP Part 5 [PP-0072] partly re-assigns the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp, and leaves only the necessary functionality by the SCA.

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

The SSCD application of the TOE supports the same SSCD life cycle phases, i.e. SSCD preparation and SSCD operational use, as well as the same SSCD roles, i.e. Administrator and Signatory, as those defined in the PPs [PP-0059] [PP-0071] [PP-0072]. Figure 2-1 in the ST illustrates the operations supported by the SSCD application of the TOE, split according to the SSCD life cycle phases and the SSCD roles for which they are actually available.



PHYSICAL ARCHITECTURE

The TOE is comprised of the following parts:

- dual-interface chip Infineon M7892 G12 equipped with IC Dedicated Software (cf. Appendix A for more details);
- smart card operating system CELES-c001;

- a Secure Signature Creation Device (SSCD) application compliant with European Parliament Directive 1999/93/EC [EP];
- guidance documentation in PDF format about the preparation and use of the SSCD application, composed by:
    - the Pre-personalization Guidance,
    - the Personalization Guidance,
    - the Operational User Guidance.

For each guidance document, the actors involved in TOE life cycle who are the intended recipients of that document.

The TOE is distributed in accordance with the evaluated delivery procedure.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

Title	Version	User
Pre-personalization Guidance for CELES-c001 Machine Readable Electronic Document – SSCD Application	1.3	Pre-personalization Agent
Personalization Guidance for CELES-c001 Machine Readable Electronic Document – SSCD Application	1.3	Personalization Agent
Operational User Guidance for CELES-c001 Machine Readable Electronic Document – SSCD Application	1.3	Inspection System

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises. In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product CELES-c001 Machine Readable Electronic Document SSCD Application, version 1 (CELES-c001_1) it is necessary the disposition of the following software components:

Title	Information
TOE Name	CELES-c001 Machine Readable Electronic Document SSCD Application
TOE Version	1
TOE Developer	HID Global
TOE Identification	CELES-c001_1
TOE identification data	43h 45h 4Ch 45h 53h 2Dh 63h 30h 30h 31h 5Fh 31h
Evaluation sponsor	Eurowitcel S.A
IC	M7892 G12 family

The TOE is based on the secure microcontrollers of the M7892 G12 family, all equipped with RSA library v2.03.008, EC library v2.03.008, SHA-2 library v1.01, Toolbox library v2.03.008 and Symmetric Crypto Library v2.02.010. Only the RSA library v2.03.008, EC library v2.03.008 and Toolbox library v2.03.008 are used in the TOE.

The SHA-2 library v1.01 and Symmetric Crypto Library v2.02.010 are not used in the TOE.

This IC family received a Common Criteria certification at the EAL6 assurance level augmented by ALC_FLR.1 [PP-0068] [ST_INF], with certification ID BSI-DSZ-CC-0891-V3-2018.

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the evaluation is described.

EVALUATION RESULTS

The product CELES-c001 Machine Readable Electronic Document SSCD Application, version 1 (CELES-c001_1) has been evaluated against the Security Target Security Target for CELES-c001 Machine Readable Electronic Document - SSCD Application, Version 1.8. 2020-03-06. TCAE160035..

All the assurance components required by the evaluation level EAL5+ALC_DVS.2+AVA_VAN.5have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL5+ALC_DVS.2+AVA_VAN.5, as defined by the Common Criteria for Information Technology Security Evaluation version 3.1 revision 5 and the Common Methodology for Information Technology Security Evaluation version 3.1 revision 5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- The laboratory encourages the different users to use the guidance's associated to the product.
- Use the cryptographic approved algorithms depending on the functionality chosen by the user.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product CELES-c001 Machine Readable Electronic Document SSCD Application, version 1 (CELES-c001_1), a positive resolution is proposed.

The certifier strongly recommends to the TOE consumer to strictly follow the security recommendations that can be found on section DOCUMENTS of this certification report as well as to observe the operational environment requirements and assumptions defined in the applicable security target.

GLOSSARY

CCN Centro Criptológico Nacional

CNI Centro Nacional de Inteligencia

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

OC Organismo de Certificación

TOE Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- Security Target for CELES-c001 Machine Readable Electronic Document - SSCD Application, Version 1.8. 2020-03-06. TCAE160035.

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- Security Target Lite for CELES-c001 Machine Readable Electronic Document - SSCD Application, Version 1.0. 2020-03-09. TCLE160038.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.