Reference: 2017-18-INF-3170-v1
Target: Público
Date: 20.07.2020

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

CERTIFICATION REPORT

Dossier #	**2017-18**
TOE	**CELES-c001 Machine Readable Electronic Document ICAO Application - EAC-PACE-AA, version 1 (CELES-c001_1)**
Applicant	**30-70825259-6 - Eurowitcel S.A.**
References	

[EXT-3382] Certification Request

[EXT-5894] Update of Certification Request

[EXT-5972] Evaluation Technical Report

Certification report of the product CELES-c001 Machine Readable Electronic Document ICAO Application - EAC-PACE-AA, version 1 (CELES-c001_1), as requested in [EXT-3382] and [EXT-5894], and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-5972] 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 ICAO Application - EAC-PACE-AA, version 1 (CELES-c001_1).

The TOE is the integrated circuit chip of a machine readable e-Document programmed according to the Logical Data Structure (LDS) [ICAO-9303-10] and providing the Extended Access Control (EAC) according to ICAO Doc 9303 7th edition Part 11 [ICAO-9303-11].

Developer/manufacturer: HIDGlobal S.p.A.

Sponsor: Eurowitcel S.A..

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Protection Profiles: BSI-CC-PP-0056-V2-2012, Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), version 1.3.2, December 2012.

BSI-CC-PP-0068-V2-2011-MA-01, Common Criteria Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), version 1.01, July 2014.

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 ICAO Application - EAC-PACE-AA, version 1 (CELES-c001_1), a positive resolution is proposed.

TOE SUMMARY

The TOE is the integrated circuit chip of a machine readable e-Document programmed according to the Logical Data Structure (LDS) [ICAO-9303-10] and providing the Extended Access Control (EAC) according to ICAO Doc 9303 7th edition Part 11 [ICAO-9303-11].

The TOE is composed of:

- the circuitry of the dual-interface e-Document's chip Infineon M7892 G12,
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the smart card operating system CELES-c001,
- an ICAO application compliant with ICAO Doc 9303,
- a SSCD application compliant with European Parliament Directive 1999/93/EC (this application is not in the scope of this ST),
- the associated guidance documentation.

On account of its composite nature, the TOE evaluation builds on the evaluation of the integrated circuit

The TOE supports wired communication, through the IC contacts exposed to the outside, as well as wireless communication through an antenna connected to the IC. Both the TOE and the antenna are embedded in a paper or plastic substrate that provides mechanical support and protection.

Once personalized with the data of the legitimate holder and with security data, the e-Document can be inspected by authorized agents.

SECURITY ASSURANCE REQUIREMENTS

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

Security functional requirement	Title
FAU_SAS.1	Audit storage
FCS_CKM.1/CPS	Cryptographic key generation – Generation of CPS session Keys for Prepersonalization and Personalization by the TOE
FCS_CKM.1/DH_PACE	Cryptographic key generation – Diffie-Hellman for PACE session keys
FCS_CKM.1/CA	Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys
FCS_CKM.4	Cryptographic key destruction – e-Document
FCS_COP.1/AUTH	Cryptographic operation – Authentication
FCS_COP.1/AA_SIGN	Cryptographic operation – Signature for Active Authentication
FCS_COP.1/PACE_ENC	Cryptographic operation – Encryption/Decryption AES/Triple-DES for PACE protocol
FCS_COP.1/PACE_MAC	Cryptographic operation – MAC for PACE protocol
FCS_COP.1/CA_ENC	Cryptographic operation – Symmetric Encryption/Decryption for CA protocol
FCS_COP.1/CA_MAC	Cryptographic operation – MAC for CA protocol

FCS_COP.1/SIG_VER	Cryptographic operation – Signature verification by e-Document
FCS_RND.1	Quality metrics for random numbers
FIA_AFL.1/Pre-pers	Authentication failure handling in Step 5 “Pre-personalization”
FIAL_AFL.1/Pers	Authentication failure handling in Step 6 “Personalization”
FIA_AFL.1/PACE	Authentication failure handling – PACE authentication using non-blocking authorization data
FIA_UID.1/PACE	Timing of identification
FIA_UAU.1/PACE	Timing of authentication
FIA_UAU.4/PACE	Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE
FIA_UAU.5/PACE	Multiple authentication mechanisms
FIA_UAU.6/PACE	Re-authenticating – Re-authenticating of Terminal by the TOE
FIA_UAU.6/EAC/CAV1	Re-authenticating – Re-authenticating of Terminal by the TOE after Chip Authentication version 1
FIA_UAU.6/EAC/CAM	Re-authenticating – Re-authenticating of Terminal by the TOE after PACE-CAM
FIA_API.1/CAV1	Authentication Proof of Identity by Chip Authentication version 1
FIA_API.1/CAM	Authentication Proof of Identity by PACE with Chip Authentication Mapping
FIA_API.1/AA	Authentication Proof of Identity by Active Authentication
FDP_ACC.1/TRM	Subset access control
FDP_ACF.1/TRM	Security attribute based access control – Terminal Access
FDP_RIP.1	Subset residual information protection
FDP_UCT.1/TRM	Basic data exchange confidentiality – e-Document
FDP_UIT.1/TRM	Data exchange integrity
FTP_ITC.1/PACE	Inter-TSF trusted channel after PACE or Chip Authentication
FTP_ITC.1/CPS	Inter-TSF trusted channel after CPS Authentication
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1/PACE	Security roles
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FMT_MTD.1/INI_ENA	Management of TSF data – Writing of Initialization Data and Pre-personalization Data
FMT_MTD.1/INI_DIS	Management of TSF data – Reading and Using Initialization and Pre-personalization Data
FMT_MTD.1/CVCA_INI	Management of TSF data – Initialization of CVCA

	Certificate and Current Date
FMT_MTD.1/CVCA_UPD	Management of TSF data – Country Verifying Certification Authority
FMT_MTD.1/DATE	Management of TSF data – Current date
FMT_MTD.1/CAPK	Management of TSF data – Chip Authentication Private Key
FMT_MTD.1/KEY_READ	Management of TSF data – Key Read
FMT_MTD.1/PA	Management of TSF data – Personalization Agent
FMT_MTD.1/AAPK	Management of TSF data – Active Authentication Private Key
FMT_MTD.3	Secure TSF data
FPT_EMS.1	TOE Emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_TST.1	TSF testing
FPT_PHP.3	Resistance to physical attack

IDENTIFICATION

Product: CELES-c001 Machine Readable Electronic Document ICAO Application - EAC-PACE-AA, version 1 (CELES-c001_1)

Security Target: Security Target for CELES-c001 Machine Readable Electronic Document - ICAO Application - EAC-PACE-AA, Version 1.9. 2020-03-06. TCAE160034.

Protection Profiles: BSI-CC-PP-0056-V2-2012, Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), version 1.3.2, December 2012.

BSI-CC-PP-0068-V2-2011-MA-01, Common Criteria Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), version 1.01, July 2014.

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 ICAO Application - EAC-PACE-AA, 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.Manufact

Manufacturing of the e-Document's chip

The IC Initialization Data are written by the IC Manufacturer to identify the IC uniquely, to set the initial configuration, to create the Master File, and to provide the key for the authentication of the Pre-personalization Agent.

The Pre-personalization Agent writes the Pre-Personalization Data which contains at least the Personalization key, the Chip Authentication public key (EF.DG14) and the Active Authentication public key (EF.DG.15).

The Pre-personalization Agent is an agent authorized by the Issuing State or Organization only

P.Pre-Operationa

Pre-operational handling of the e-Document

1. The e-Document Issuer issues the e-Document and approves it using the terminals complying with all applicable laws and regulations.
2. The e-Document Issuer guarantees correctness of the user data (amongst other of those, concerning the e-Document holder) and of the TSF-data permanently stored in the TOE.
3. The e-Document Issuer uses only such TOE's technical components (IC) which enable traceability of the e-Documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. section 1.5 above.
4. If the e-Document Issuer authorizes a Pre-personalization Agent or a Personalization Agent to personalize the e-Document for e-Document holders, the e-Document Issuer has to ensure that the Pre-personalization Agent and the Personalization Agent act in accordance with the e-Document Issuer's policy

P.Card_PKI

PKI for Passive Authentication (issuing branch)

Application Note 23 The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

1. The e-Document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the e-Document. For this aim, he runs a Country Signing Certification Authority (CSCA). The eDocument Issuer shall publish the CSCA Certificate (CCSCA).

2. The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the e-Document Issuer by strictly secure means, see [IETF_NWG_CMS]. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the e-Document Issuer, see [ST_INF].
3. A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of e-Documents.

P. Trustworthy_PKI

Trustworthiness of PKI

The CSCA shall ensure that it issues its certificates exclusively to the rightful organizations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the e-Document.

P.Terminal

Abilities and trustworthiness of terminals

The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:

1. The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by e-Document holders as defined in [IETF_NWG_CMS] [ST_INF].
2. They shall implement the terminal parts of the PACE protocol [IETF_NWG_CMS], of the Passive Authentication [IETF_NWG_CMS] and use them in this order12. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3. The related terminals need not to use any own credentials.
4. They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the eDocument [IETF_NWG_RFC] [IETF_NWG_CMS]).
5. The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current PP.

P. P.Sensitive_Data

Privacy of sensitive biometric reference data

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the e-Document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the eDocument is presented to the inspection system (Extended Inspection Systems). The issuing State or Organization authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The e-Document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication..

P.Personalization

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

The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical e-Document with respect to the e-Document holder. The personalization of the eDocument for the holder is performed by an agent authorized by the Issuing State or Organization only.

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.Passive_Auth

PKI for Passive Authentication

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical e-Document. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer:

(i) generates the Document Signer Key Pair,

(ii) hands over the Document Signer Public Key to the CA for certification,

(iii) keeps the Document Signer Private Key secret, and

(iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the e-Documents.

The CA creates the Document Signer Certificates for the Document Signer Public Keys and distributes them to the receiving States and Organizations. It is assumed that the Personalization Agent ensures that the Document Security Object contains only the hash values of the genuine user data according to [IETF_NWG_RFC].

A.Insp_Sys

Inspection Systems for global interoperability

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [IETF_NWG_CMS] and/or BAC [TR-031101-1]. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical e-Document under PACE or BAC and performs the Chip Authentication to verify the logical e-Document and establishes secure messaging. The Chip Authentication Protocol v.1 is skipped if PACECAM has previously been performed. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Justification: The assumption A.Insp_Sys does not confine the security objectives of [TR-03111], as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the EAC functionality of the TOE

A.Auth_PKI

PKI for Inspection Systems

The issuing and receiving States or Organizations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organizations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organizations. The issuing States or Organizations distribute the public keys of their Country Verifying Certification Authority to their e-Document's chip.

Justification: This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE, nor will the security objectives of [TR-03111] be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol Version 1.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product CELES-c001 Machine Readable Electronic Document ICAO Application - EAC-PACE-AA, 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.Skimming

Skimming e-Document/Capturing Card-Terminal Communication

Adverse action: An attacker imitates an inspection system trying to establish a communication to read the logical e-Document or parts of it via the contact or contactless communication channels of the TOE.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: confidentiality of logical e-Document data

Application Note 14 A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.

Application Note 15 The shared PACE password may be printed or displayed on the eDocument. Please note that if this is the case, the password does not effectively represent a secret, but nevertheless it is restricted-revealable, cf. OE.e-Document_Holder

T.Eavesdropping

Eavesdropping on the communication between the TOE and the PACE terminal

Adverse action: An attacker is listening to the communication between the e-Document and the PACE authenticated BIS-PACE in order to gain the user data transferred between the TOE and the terminal connected.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: confidentiality of logical e-Document data

Application Note 16 A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.

T. Tracing

Tracing e-Document

Adverse action: An attacker tries to gather TOE tracing data (i.e. to trace the movement of the e-Document) unambiguously identifying it directly by establishing a communication via the contact interface or remotely by establishing or listening to a communication via the contactless interface of the TOE.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: privacy of the e-Document holder.

Application Note 17 This threat completely covers and extends “T.Chip-ID” from BAC PP [TR-031101-1]

Application Note 18 A product using BAC (whatever the type of the inspection system is: BIS_BAC) cannot avert this threat in the context of the security policy defined in this ST

T.Forgery

Forgery of data

Adverse action: An attacker fraudulently alters the User Data or/and TSF-data stored on the e-Document or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BISPACE by means of changed e-Document holder’s related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.

Threat agent: having high attack p

Asset: integrity of the e-Document

T.Abuse-Func

Abuse of Functionality

Adverse action: An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialization and personalization in the

operational phase after delivery to the e-Document holder.This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to eDocument holder.

Threat agent: having high attack potential, being in possession of one or more eDocuments

Asset: integrity and authenticity of the e-Document, availability of the functionality of the e-Document

Application Note 19 Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.

T.Information_Leakage

Information Leakage from e-Document

Adverse action: An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the e-Document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker. Threat agent: having enhanced basic attack potential, being in possession of a legitimate e-Document Asset: confidentiality logical e-Document and TSF data

Threat agent: having high attack potential

Asset: confidentiality User Data and TSF data of the e-Document

Application Note 20 Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission, but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip) and can then be related to the specific operation being performed. Examples are Differential Electromagnetic Analysis (DEMA) and Differential Power Analysis (DPA). Moreover, the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

T.Phys_Tamper

Physical Tampering

Adverse action: An attacker may perform physical probing of the e-Document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the eDocument in order to alter (I) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the e-Document.

Threat agent: having high attack potential, being in possession of one or more legitimate e-Documents

Asset: integrity and authenticity of the e-Document, availability of the functionality of the e-Document, confidentiality of User Data and TSFdata of the e-Document

Application Note 21 Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g. authentication key of the e-Document) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the e-Document's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

T.Malfunction

Malfunction due to Environmental Stress

Adverse action: An attacker may cause a malfunction the e-Document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the e-Document outside the normal operating conditions, exploiting errors in the e-Document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent: having high attack potential, being in possession of one or more legitimate e-Documents, having information about the functional operation

Asset: integrity and authenticity of the e-Document, availability of the functionality of the e-Document, confidentiality of User Data and TSFdata of the e-Document

Application Note 22 A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals.

T.Read_Sensitive_Data

Read the sensitive biometric reference data

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the e-Document's chip. The attack T.Read_Sensitive_Data is similar to the threats T.Skimming in respect of the attack path (communication interface) and the motivation (to get data stored on the e-Document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE password) and therefore the possible attack methods. Note,

that the sensitive biometric reference data are stored only on the e-Document's chip as private sensitive personal data whereas the MRZ data and the portrait are visual readable on the physical e-Document as well.

Threat agent: having high attack potential, knowing the PACE password, being in possession of a legitimate e-Document

Asset: confidentiality of sensitive logical e-Document (i.e. biometric reference) data.

T.Counterfeit

Counterfeit of e-Document's chip

Adverse action: An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine e-Document's chip to be used as part of a counterfeit e-Document. This violates the authenticity of the eDocument's chip used for authentication of a presenter by possession of a e-Document. The attacker may generate a new data set or extract completely or partially the data from a genuine e-Document's chip and copy them on another appropriate chip to imitate this genuine eDocument's chip.

Threat agent: having high attack potential, being in possession of one or more legitimate e-Documents

Asset: authenticity of logical e-Document data

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.

e-Document Issuer as the general responsible

The e-Document Issuer as the general responsible for the global security policy related will implement the following security objectives for the TOE environment

OE.Legislative_Compliance

Issuing of the e-Document

The e-Document Issuer must issue the e-Document and approve it using the terminals complying with all applicable laws and regulations.

e-Document Issuer and CSCA: e-Document's PKI (issuing) branch

The e-Document Issuer and the related CSCA will implement the following security objectives for the TOE environment.

OE.Passive_Auth_Sign

Authentication of e-Document by Signature

The e-Document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the e-Document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (CCSCA). Hereby authenticity and integrity of these certificates are being maintained.

A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine e-Documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [IETF_NWG_RFC]. The Personalization Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [IETF_NWG_RFC]. The CSCA must issue its certificates exclusively to the rightful organizations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on e-Document.

OE.Pre-personalization

Pre-personalization of e-Document

The issuing State or Organization must ensure that the Pre-personalization Agent acting on behalf of the issuing State or Organization

(i) create DG14, DG15 and TSF data for the e-Document,

(ii) pre-personalize the e-Document together with the defined physical and logical

OE.Personalization

Personalization of e-Document

The e-Document Issuer must ensure that the Personalization Agent acting on his behalf (i) establish the correct identity of the e-Document holder and create the biographical data for the e-Document, (ii) enrol the biometric reference data of the e-Document holder, (iii) write a subset of these data on the physical Document (optical personalization) and store them in the e-Document (electronic personalization) for the e-Document holder as defined in [IETF_NWG_RFC]19, (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [IETF_NWG_CMS] (in the role of a DS).

Terminal operator: Terminal's receiving branch

OE.Terminal

Terminal operating

The terminal operators must operate their terminals as follows:

1. The related terminals (basic inspection systems, cf. above) are used by terminal operators and by e-Document holders as defined in [IETF_NWG_CMS].
2. The related terminals implement the terminal parts of the PACE protocol [IETF_NWG_CMS], of the Passive Authentication [IETF_NWG_CMS] (by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3. The related terminals need not to use any own credentials.
4. The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication of the e-Document (determination of the authenticity of data groups stored in the e-Document, [IETF_NWG_CMS]).
5. The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

Application Note 27 OE.Terminal completely covers and extends “OE.Exam_MRTD”, “OE.Passive_Auth_Verif“ and “OE.Prot_Logical_MRTD” from BAC PP [TR-031101-1].

OE.e-Document_Holder

e-Document holder Obligations

The e-Document holder may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device who definitely act according to respective regulations and are trustworthy.

Issuing State or Organization

The issuing State or Organization will implement the following security objectives of the TOE environment.

OE.Chip_Auth_Key_e-Document

e-Document Authentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the e-Document’s Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or Organizations to verify the authenticity of the e-

Document's chip used for genuine e-Document by certification of the Chip Authentication Public Key by means of the Document Security Object. Justification: This security objective for the operational environment is needed to counter the threat T.Counterfeit, as it specifies the pre-requisite for the Chip Authentication which is one of the features of the TOE described only in this Security Target.

OE.Authoriz_Sens_Data

Authorization for Use of Sensitive Biometric Reference Data

The issuing State or Organization has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of e-Document holders to authorized receiving States or Organizations. The Country Verifying Certification Authority of the issuing State or Organization generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

Justification: This security objective for the operational environment is needed in order to handle the Threat T.Read_Sensitive_Data, the Organizational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the features of the TOE described only in this Security Target

OE.Active_Auth_Key_e-Document

e-Document Active Authentication key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the e-Document's Active Authentication Key Pair, (ii) sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and (iii) support inspection systems of receiving States or Organizations to verify the authenticity of the e-Document's chip used for genuine e-Document by certification of the Active Authentication Public Key by means of the Document Security Object.

Receiving State or Organization

The Receiving State or Organization will implement the following security objectives of the TOE environment.

OE.Exam_e-Document

Examination of the physical part of the e-Document

The inspection system of the receiving State or Organization must examine the e-Document presented by the user to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the e-Document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer

Public Key of each issuing State or Organization, and (ii) implements the terminal part of PACE [4] and/or the Basic Access Control [6]. Extended Inspection Systems perform additionally to these points the Chip Authentication as either part of PACE-CAM or as Chip Authentication Protocol Version 1 to verify the Authenticity of the presented eDocument's chip.

Justification: This security objective for the operational environment is needed in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication as either part of PACE-CAM or as Chip Authentication protocol v.1. OE.Exam_e-Document also repeats partly the requirements from above OE.Terminal and therefore also counters T.Forgery and A.Passive_Auth. This is done because this ST introduces the Extended Inspection System, which is needed to handle the features of a e-Document with Extended Access Control.

OE.Prot_Logical_e-Document

Protection of data from the logical e-Document

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical e-Document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication.

Justification: This security objective for the operational environment is needed in order to handle the Assumption A.Insp_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication.

OE.Ext_Insp_Systems

Authorization of Extended Inspection Systems

The Document Verifier of receiving States or Organizations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical e-Document. The Extended Inspection System authenticates themselves to the e-Document's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

Justification: This security objective for the operational environment is needed in order to handle the Threat T.Read_Sensitive_Data, the Organizational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

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 CELES-c001 operating system manages all the resources of the integrated circuit that equips the e-Document, providing secure access to data and functions.

In more detail, in each life cycle phase/step, access to data and functions is restricted by means of cryptographic mechanisms as follows:

- In step 5, Pre-personalization, of phase 2, the Pre-personalization Agent must prove his/her identity by means of an authentication mechanism based on Triple-DES with 112-bit keys.
- In phase 3, Personalization, the Personalization Agent must prove his/her identity by means of an authentication mechanism based on Triple-DES with 112-bit keys.
- In phase 4, Operational use, the user must prove his entitlement to access less sensitive data, i.e. DG1, DG2, and DG5 to DG16, by means of the PACE mechanism compliant to ICAO Doc 9303-11 [IETF_NWG_CMS]. Access to sensitive data, i.e. DG3 and DG4, is allowed after the genuineness of the IC has been proven by means of the Chip Authentication mechanism defined in [IETF_NWG_CMS] and after the user has proven his/her entitlement by means of the Terminal Authentication mechanism as defined in [CC_P3].

After a successful authentication, the communication between the e-Document and the terminal is protected by the Secure Messaging mechanism defined in section 6 of the ISO 7816-4 specification International Standard 14443-3, part 3.

The integrity of the data stored under the LDS can be checked by means of the Passive Authentication mechanism defined in [IETF_NWG_CMS]. The Active Authentication mechanism defined in [IETF_NWG_CMS]may be used as an alternative technique to ascertain the genuineness of the chip. However, access to sensitive data requires the use of the Chip Authentication mechanism. Passive Authentication, PACE, Active Authentication, Chip Authentication, and EAC mechanisms are described in more detail in the following subsections.

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;
- an International Civil Aviation Organization (ICAO) application compliant with ICAO Doc 9303;
- guidance documentation in PDF format about the preparation and use of the ICAO application, composed by:

- the Pre-personalization Guidance,
- the Personalization Guidance,
- the Operational User Guidance.

Table 1-5 identifies, 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 in BSI-CCPP-0056.

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	1.3	Pre-personalization Agent TOE
Personalization Guidance	1.3	Personalization Agent
Operational User Guidance	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 ICAO Application - EAC-PACE-AA, 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 ICAO Application - EAC-PACE-AA
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 BSI-CC-PP-0056-V2-2012 [M7892], with certification ID BSI-DSZ-CC-0891-V3-2018.

Regarding the hardware components, the only requierement is that they shall support the software elements previously detailed.

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

EVALUATION RESULTS

The product CELES-c001 Machine Readable Electronic Document ICAO Application - EAC-PACE-AA, version 1 (CELES-c001_1) has been evaluated against the Security Target Security Target for CELES-c001 Machine Readable Electronic Document - ICAO Application - EAC-PACE-AA, Version 1.9. 2020-03-06. TCAE160034.

All the assurance components required by the evaluation level EAL5+ALC_DVS.2+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 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 ICAO Application - EAC-PACE-AA, 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 Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

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

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

[CEM] Common Methodology for Information Technology Security Evaluation 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 - ICAO Application - EAC-PACE-AA, Version 1.9. 2020-03-06. TCAE160034.

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 - ICAO Application - EAC-PACE-AA - Public Version, Version 1.0. 2020-03-10. TCLE160037.

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.