MINISTERIO DE PRESIDENCIA Y PARA LAS AATT
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF: 2016-31-INF-2102 v1	Created by: CERT11
Target: Público	Revised by: CALIDAD
Date: 10.10.2017	Approved by: TECNICO

CERTIFICATION REPORT

File: 2016-31 SOMA EAC

Applicant: HID Global / Arjo Systems

References:

[EXT-3093] Certification request of SOMA EAC

[EXT-3604] Evaluation Technical Report of SOMA EAC.

The product documentation referenced in the above documents.

Certification report of the product SOMA-c007 Machine Readable Electronic Document EAC-PACE-AA (SOMA-c007_2) version 2, as requested in [EXT-3093] dated 13/06/2016, and evaluated by the laboratory Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-3604] received on 20/09/2017.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product SOMA-c007 Machine Readable Electronic Document EAC-PACE-AA (SOMA-c007_2) version 2.

The TOE is an electronic document representing a contactless/contact smart card programmed according to the “Password Authenticated Connection Establishment” mechanism described in the ICAO Doc 9303 7th edition 2015 Part 11 [ICAO11], which means among other things compliance to the Logical Data Structure (LDS) defined in [ICAO10], and additionally providing the Extended Access Control according to the ICAO Doc 9303-11 [ICAO11] and BSI TR-03110 [TR-03110-1][TR-03110-3] and also compliance with Active Authentication according to ICAO Doc 9303-11 [ICAO11].

The communication between terminal and chip shall be protected by PACE using Standard Inspection Procedure with PACE [PP0068].

Developer/manufacturer: HID Global / Arjo Systems.

Sponsor: HID Global / Arjo Systems.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Applus Laboratories.

Protection Profiles: [PP0056] Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, Version 1.3.2, 5th December 2012, BSI-CC-PP-0056-V2-2012.

[PP0068] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22nd July 2014, BSI-CC-PP-0068-V2-2011-MA-01.

Evaluation Level: Common Criteria v3.1 R4 EAL5 + ALC_DVS.2 and AVA_VAN.5

Evaluation end date: 20 September 2017.

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 and AVA_VAN.5, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product SOMA-c007 Machine Readable Electronic Document EAC-PACE-AA (SOMA-c007_2) version 2, a positive resolution is proposed.

TOE SUMMARY

The physical TOE is comprised of the following parts:

• the integrated circuit chip (microcontroller) programmed with the operating system and with the ICAO application (Embedded Software).

• the guidance documentation, composed by:

o the Initialization Guidance for the Initialization Agent [AGDINI].

o the Pre-personalization guidance for the Pre-personalization Agent [AGDPRE],

o the Personalization Guidance for the Personalization Agent [AGDPERS], and

o The Operational User Guidance for the User (Inspection System) [AGDOPE].

The Embedded Software of the TOE comprises the following software components stored in the non-volatile memory units of the microcontroller:

• operating system

• file system

• e-Document applications

• security data objects

The ICAO defines the baseline required security methods Passive Authentication and the following optional advanced security methods:

• Basic Access Control to the logical e-Document,

• Active Authentication of the e-Document's chip,

• Extended Access Control to and the Data Encryption of sensitive biometrics as an optional security measure in the ICAO Doc 9303-11 [ICAO11] and

• Password Authenticated Connection Establishment [ICAO11].

The Passive Authentication and the Data Encryption are performed completely and independently of the TOE by the TOE environment.

The TOE addresses the protection of the logical e-Document:

i. in integrity by write-only-once access control and by physical means and

ii. in confidentiality by the Extended Access Control Mechanism.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL5 and the evidences required by the additional component ALC_DVS.2 and AVA_VAN.5, according to Common Criteria v3.1 R4.

Class	Family/Component
ADV Development	ADV_ARC.1 Security architecture description ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_IMP.1 Implementation representation of the TSF ADV_INT.2 Well-structured internals ADV_TDS.4 Semiformal modular design
AGD Guidance Documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC Life-Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.5 Development tools CM coverage ALC_DEL.1 Delivery procedures *ALC_DVS.2 Sufficiency of security measures* ALC_LCD.1 Developer defined life-cycle model ALC_TAT.2 Compliance with implementation standards
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_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ATE Tests	ATE_COV.2 Analysis of coverage ATE_DPT.3 Testing: modular design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
AVA Vulnerability Assessment	*AVA_VAN.5 Advanced methodical vulnerability analysis*

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4:

Class	Component

FAU: Security Audit	FAU_SAS.1
FCS: Cryptographic Support	FCS_CKM.1/GIM FCS_CKM.1/CPS FCS_CKM.1/DH_PACE FCS_CKM.1/CA FCS_CKM.4 FCS_COP.1/AUTH FCS_COP.1/AA_SIGN FCS_COP.1/PACE_ENC FCS_COP.1/CA_ENC FCS_COP.1/PACE_MAC FCS_COP.1/CA_MAC FCS_COP.1/SIG_VER FCS_RND.1
FIA: Identification and Authentication	FIA_AFL.1/Init FIA_AFL.1/Pre-pers FIA_AFL.1/Pers FIA_AFL.1/PACE FIA_UID.1/PACE FIA_UAU.1/PACE FIA_UAU.4/PACE FIA_UAU.5/PACE FIA_UAU.6/PACE FIA_UAU.6/EAC/CAV1 FIA_UAU.6/EAC/CAM FIA_API.1/CAV1 FIA_API.1/CAM FIA_API.1/AA
FDP: User Data Protection	FDP_ACC.1/TRM FDP_ACF.1/TRM FDP_RIP.1 FDP_UCT.1/TRM FDP_UIT.1/TRM
FTP: Trusted Path/Channels	FTP_ITC.1/PACE FTP_ITC.1/CPS
FMT: Security Management	FMT_SMF.1 FMT_SMR.1/PACE FMT_LIM.1 FMT_LIM.2 FMT_MTD.1/INI_ENA FMT_MTD.1/INI_DIS FMT_MTD.1/KEY_READ FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK,

	FMT_MTD.1/PA, FMT_MTD.1/AAPK FMT_MTD.3
FPT: Protection of the Security Functions	FPT_EMS.1 FPT_FLS.1 FPT_PHP.3 FPT_TST.1

IDENTIFICATION

Product: SOMA-c007 Machine Readable Electronic Document EAC-PACE-AA (SOMA-c007_2) version 2

Security Target: Security Target SOMA-c007 Machine Readable Electronic Document - ICAO Application - EAC-PACE-AA version 1.10

Protection Profiles: [PP0056] Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, Version 1.3.2, 5th December 2012, BSI-CC-PP-0056-V2-2012.

[PP0068] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22nd July 2014, BSI-CC-PP-0068-V2-2011-MA-01.

Evaluation Level: Common Criteria v3.1 R4 EAL5 + ALC_DVS.2 and AVA_VAN.5

SECURITY POLICIES

The use of the product SOMA-c007 Machine Readable Electronic Document EAC-PACE-AA (SOMA-c007_2) version 2 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 Initialization Agent.

The Initialization Agent completes the configuration of the OS (TOE Initialization Data) and 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-Operational. 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 authorises an Initialization Agent, a Prepersonalization Agent or a Personalization Agent to personalise the e-Document for e-Document holders, the e-Document Issuer has to ensure that the Initialization Agent, 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: 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 e-Document 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 [ICAO11]. 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 [ICAO12].

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. Trustworthyness 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 trustworthyness 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 [ICAO11][ICAO12].

2. They shall implement the terminal parts of the PACE protocol [ICAO11], of the Passive Authentication [ICAO11] and use them in this order13. 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 e-Document, [ICAO10][ICAO11]).

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.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 e-Document 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 e-Document 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 [ICAO10].

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 [ICAO11] and/or BAC [PP0055]. 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 PACE-CAM 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.

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.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product SOMA-c007 Machine Readable Electronic Document EAC-PACE-AA (SOMA-c007_2) version 2, although the agents implementing attacks have an high attack potential according to the assurance level EAL5 + ALC_DVS.2 and AVA_VAN.5 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 in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contact or contactless interfaces 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: A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.

Application Note: The shared PACE password may be printed or displayed on the e-Document. 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: 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: This threat completely covers and extends “T.Chip -ID” from BAC PP [PP0055].

Application Note: 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.

Application Note: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the e-Document’s chip (no Chip Authenticat ion), a threat like T.Counterfeit (counterfeiting e-Document) cannot be averted by the current TOE.

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 BIS-PACE 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 potential

Asset: integrity of the e-Document

The TOE shall avert the threat as specified below.

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 initialisation and personalization in the operational phase after delivery to the e-Document holder.

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

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

Application Note: 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 high attack potential

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

Application Note: 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 e-Document 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 TSF-data of the e-Document

Application Note: 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 TSF-data of the e-Document

Application Note: 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 (cf. [ST-BAC]) 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 e-Document'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 e-Document'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.

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.

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 [ICAO10]. The Personalization Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [ICAO10]. 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.Initialization Initialization of e-Document

The issuing State or Organization must ensure that the Initialization Agent acting on behalf of the issuing State or Organization i). Create the OS configuration data and TSF data for the e-Document, ii). initialize the e-Document together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

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 iii). Create DG14, DG15 and TSF data for the e-Document, iv). pre-personalize the e-Document together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

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 [R22]20, (iv) write the document details data,

(v) write the initial TSF data, (vi) sign the Document Security Object defined in [R23] (in the role of a DS).

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 [ICAO11]. 2). The related terminals implement the terminal parts of the PACE protocol [ICAO11], of the Passive Authentication [R23] (by verification of the signature of the Document Security Object) and use them in this order21. 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, [ICAO11]). 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.

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.

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.

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.

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.

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 and/or the Basic Access Control. 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 e- Document's chip.

OE.Prot_Logical_e-Document Protection of data from the logical e-Document

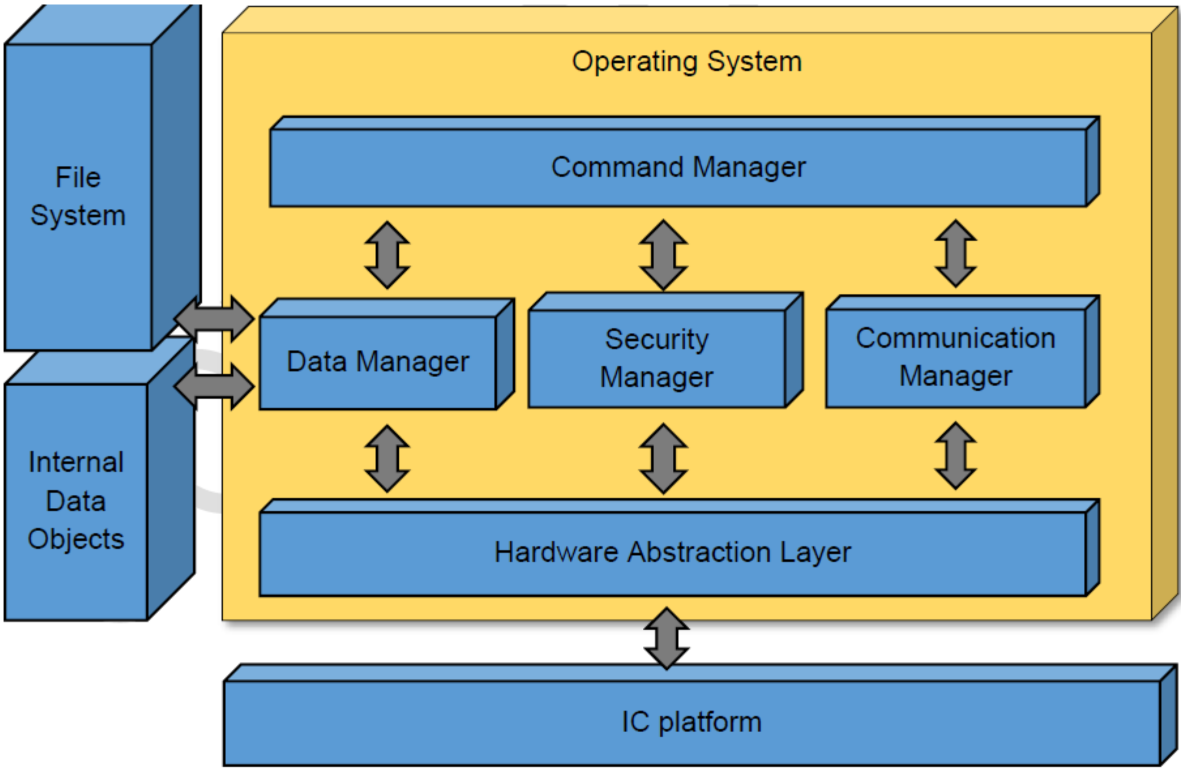
The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical e-Document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip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

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.

ARCHITECTURE

LOGICAL ARCHITECTURE



This picture shows an overview of the TOE architecture. In particular:

- The Hardware Abstraction Layer acts as the interface with the IC platform;
- The Security Manager provides the cryptographic services (Triple-DES, AES, SHA, MAC), as well as the authentication mechanisms (GIM, CPS, BAC).
- The Communication Manager manages both the contact and the contactless communication with the terminal.
- The Data Manager provides services for the management of the file system and of data objects, as well as the security status associated with data objects.
- The Command Manager provides for the interpretation and execution of commands as well as the management of the security status associated with commands.
- The File System holds the LDS application, the data groups and other ISO 7816 dedicated files and elementary files.
- Internal Data Objects include the following data:

o Initialization key,

o Retry counters,

o Failure counter,

o Contact and contactless communication parameters,

o Memory size information,

o Life cycle status information,

o Command enabling bitmask,

o File system information

PHYSICAL ARCHITECTURE

The physical TOE is comprised of the following parts:

- the integrated circuit chip Infineon M7892 G12 (microcontroller) programmed with the operating system and with the ICAO application (Embedded Software).
- the guidance documentation, composed by:

o the Initialization Guidance for the Initialization Agent [AGDINI].

o the Pre-personalization guidance for the Pre-personalization Agent [AGDPRE],

o the Personalization Guidance for the Personalization Agent [AGDPERS], and

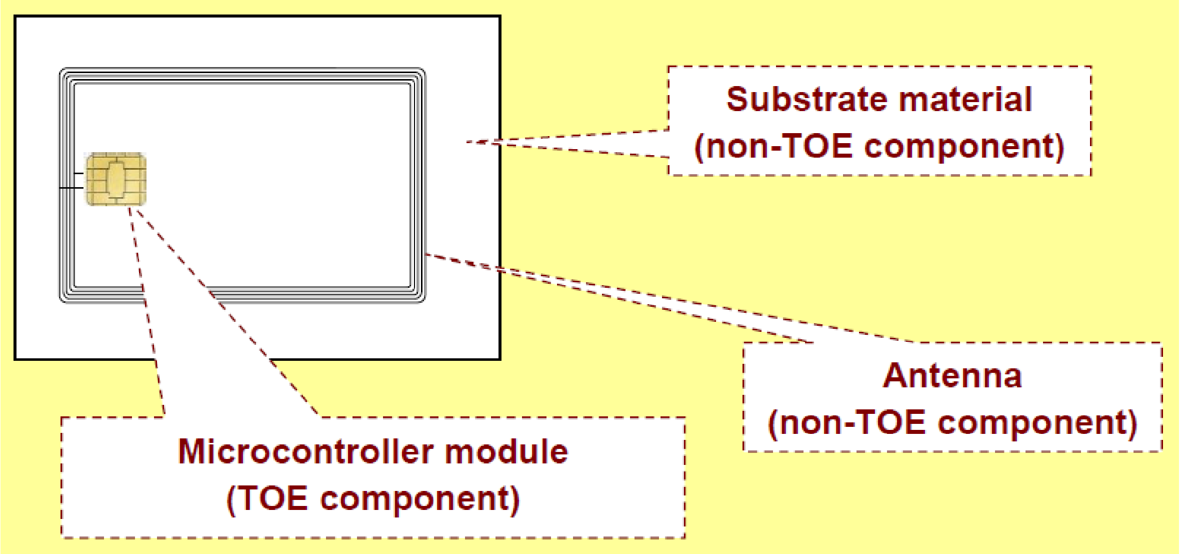
o The Operational User Guidance for the User (Inspection System) [AGDOPE].

The Embedded Software of the TOE comprises the following software components stored in the non-volatile memory units of the microcontroller:

- operating system
- file system
- e-Document applications
- security data objects

The antenna and the substrate are not part of the TOE.

The following picture shows the smart card components, distinguishing between TOE components and non-TOE components.



DOCUMENTS

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

- the Initialization Guidance for the Initialization Agent [AGDINI].
- the Pre-personalization guidance for the Pre-personalization Agent [AGDPRE],
- the Personalization Guidance for the Personalization Agent [AGDPERS], and
- The Operational User Guidance for the User (Inspection System) [AGDOPE].

PRODUCT TESTING

The evaluation has been performed according to the Composite Evaluation Scheme as defined in the guides [JILCOMP] and [JILADVARC] in order to assess that the combination of the TOE with the underlying platform did not lead to any exploitable vulnerability.

This evaluation has then taken into account the evaluation results and security recommendations for the platform which is part of the evaluated composite TOE, and was already certified with certificate BSI-DSZ-CC-0891-V2.

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

During the evaluation process, each test unit has been executed to check that the declared security functionality has been identified and also to check that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using a 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 evaluation team has applied a sampling strategy and has concluded that the information is complete and coherent enough to reproduce tests and identify the functionality tested. Moreover, the evaluation team has planned and executed additional tests independently of those executed by the developer. The latter tests covered the TOE EAC, PACE and AA functionalities. The underlying RNG has been also tested.

The obtained results have been checked to be conformant to the expected results and in cases where a deviation relative to the expected results has been detected the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

PENETRATION TESTING

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment, the evaluation team has devised attack scenarios for penetration tests according to JIL supporting documents [JILAAPS] and [JILADVARC]. Within these activities all aspects of the security architecture which were not covered by functional testing have been considered.

The implementations of the requirements of the provided platform's ETR for Composition and guidance, as well as of the security mechanisms of the TOE in general have been verified by the evaluation team. An appropriate test set was devised to cover these potential vulnerabilities.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the High attack potential has been successful in the TOE's operational environment as defined in the security target when all measures required by the developer are applied.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product SOMA-c007 Machine Readable Electronic Document EAC-PACE-AA (SOMA-c007_2) version 2 it is not necessary any additional software or hardware components.

The version of the software may be retrieved by following the procedure in section 4.2 (Retrieval of TOE, product and chip information) of the "Initialization Guidance for SOMA-c007 Machine Readable Electronic Document" [AGDINI].

To identify the TOE is necessary for the initialization agent to execute the "GET DATA (Even INS)" command with P1 = 01h and P2 = 20h. APDU shall be encoded as follows:

o CLA = E0h

o INS = CAh

o P1 = 01h

o P2 = 20h

o LE = 00h

The e-Document certified under Common Criteria v.3.1 shall return **SOMA-c007_2** (ASCII codes 53h 4Fh 4Dh 41h 2Dh 63h 30h 30h 37h 5Fh 32h), representing the TOE Identification Data

EVALUATION RESULTS

The product SOMA-c007 Machine Readable Electronic Document EAC-PACE-AA (SOMA-c007_2) version 2 has been evaluated against the Security Target "Security Target SOMA-c007 Machine Readable Electronic Document - ICAO Application - EAC-PACE-AA" version 1.10

All the assurance components required by the evaluation level EAL5 + 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 mentioned evaluation level, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

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.

There are slight differences between the Security Target and the Protection Profiles it is based on. The customer should review if those differences are bearable for his application. Those differences are collected in the tables 2-3 and 2-5 of the ST (Modified/Added components and Additions, iterations and changes to SFRs).

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product SOMA-c007 Machine Readable Electronic Document EAC-PACE-AA (SOMA-c007_2) version 2, a positive resolution is proposed.

The certifier strongly recommends to the TOE consumer to strictly follow the security recommendations that can be found on guidance documents as well as to observe the operational environment requirements and assumptions defined in the applicable security target.

Some of the key lengths for some of the cryptographic mechanisms defined in the ST are considered as legacy mechanisms according to [ACM].

GLOSSARY

AA	Active Authentication
BAC	Basic Access Control
BIS	Basic Inspection System
CC	Common Criteria
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EF	Elementary File
EIS	Extended Inspection System
ETR	Evaluation Technical Report
GIS	General Inspection System
ICAO	International Civil Aviation Organization
IT	Information Technology
MRTD	Machine Readable Travel Document
OC	Organismo de Certificación
OSP	Organizational security policy
PA	Passive Authentication
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
RNG	Random Number Generator
SAR	Security assurance requirements
SFP	Security Function Policy
SFR	Security functional requirement
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functions

BIBLIOGRAPHY

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

[ACM] SOG-IS agreed cryptographic mechanisms. SOG-IS crypto working group. May 2016.

[AGDINI] HID Global / Arjo Systems: Initialization Guidance for SOMA-c007 Machine Readable Electronic Document v2.1, ref. TCAE160012

[AGDOPE] HID Global / Arjo Systems: User Guidance for SOMA-c007 Machine Readable Electronic Document ICAO Application v2.0, ref. TCAE160018

[AGDPERS] HID Global / Arjo Systems: Personalization Guidance for SOMA-c007 Machine Readable Electronic Document ICAO Application v2.0, ref. TCAE160017

[AGDPRE] HID Global / Arjo Systems: Pre-personalization Guidance for SOMA-c007 Machine Readable Electronic Document ICAO Application v2.0, ref. TCAE160016

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, Sept. 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, Sept. 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, Sept. 2012.

[CCSANIT] Common Criteria. Additional CCRA Supporting Documents. ST sanitising for publication. Document number 2006-04-004, April 2006.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, Sept. 2012.

[ICAO10] Doc 9303 Machine Readable Travel Documents, Seventh Edition, 2015, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC).

[ICAO11] Doc 9303 Machine Readable Travel Documents, Seventh Edition, 2015, Part 11: Security Mechanisms for MRTDs.

[ICAO12] Doc 9303 Machine Readable Travel Documents, Seventh Edition, 2015, Part 12: Public Key Infrastructure for MRTDs

[JILAAPS] Joint Interpretation Library. Application of Attack Potential to Smartcards, version 2.9. Jan.2013.

[JILADVARC] Joint Interpretation Library. Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices.

[JILCOMP] Joint Interpretation Library. Composite Product evaluation for Smart Cards and similar devices, version 1.4. Aug. 2015

[PP0055] Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application ", Basic Access Control, Version 1.10, 25th March 2009.

[PP0056] Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, Version 1.3.2, 5th December 2012, BSI-CC-PP-0056-V2-2012.

[PP0068] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22nd July 2014, BSI-CC-PP-0068-V2-2011-MA-01.

[ST-BAC] Security Target SOMA-c007 Machine Readable Electronic Document, Basic Access Control, Version 1.9. Ref. TCAE160001.

[TR-03110-1] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, part 1 – eMRTDs with BAC/PACEv2 and EACv1, version 2.20, 26. February 2015

[TR-03110-3] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, part 3 – Common Specifications, version 2.21, 21. December 2016

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- SOMA-c007 Machine Readable Electronic Document Security Target ICAO Application EAC-PACE-AA, Version 1.10, Date 2017-09-01, Reference TCAE160002.

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

- SOMA-c007 Machine Readable Electronic Document Security Target ICAO Application EAC-PACE-AA Public Version, Version 1.0, Date 2017-09-21, Reference TCAE160020.