REF: 2016-30-INF-2094 v1	Created by: CERT11
Target: Público	Revised by: CALIDAD
Date: 10.10.2017	Approved by: TECNICO

CERTIFICATION REPORT

File: 2016-30 SOMA BAC

Applicant: HID Global / Arjo Systems

References:

[EXT-3092] Certification request of SOMA BAC

[EXT-3603] Evaluation Technical Report of SOMA BAC.

The product documentation referenced in the above documents.

Certification report of the product SOMA-c007 Machine Readable Electronic Document Basic Access Control (SOMA-c007_2) version 2, as requested in [EXT-3092] dated 13/06/2016, and evaluated by the laboratory Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-3603] 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 Basic Access Control (SOMA-c007_2) version 2.

The TOE meets the security objectives and requirements for the contact or contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security method Basic Access Control in the ‘ICAO Doc 9303’ [ICAO]. It provides the security level of EAL4 augmented with ALC_DVS.2.

The TOE is "the integrated circuit chip of machine readable electronic documents programmed according to the Logical Data Structure (LDS) [ICAO10] and providing the Basic Access Control (BAC) according to ICAO Doc 9303 7th edition Part 11 [ICAO11]", compatible with the expected TOE type described in the [PP0055].

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 Profile: Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application", Basic Access Control, Version 1.10, 25th March 2009, BSI-CCPP-0055. [PP0055].

Evaluation Level: Common Criteria v3.1 R4 EAL4 + ALC_DVS.2.

Evaluation end date: 20 September 2017.

All the assurance components required by the evaluation level EAL4 (augmented with ALC_DVS.2) 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 EAL4 + ALC_DVS.2, 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 Basic Access Control (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 [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 Basic Access Control Mechanism.

This TOE does not address the Active Authentication and the Extended Access Control as optional security mechanisms.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional component ALC_DVS.2, according to Common Criteria v3.1 R4.

Class	**Family/Component**
ADV Development	ADV_ARC.1 Security architecture description ADV_FSP.4 Complete functional specification ADV_IMP.1 Implementation representation of the TSF ADV_TDS.3 Basic 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.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures *ALC_DVS.2 Sufficiency of security measures* ALC_LCD.1 Developer defined life-cycle model ALC_TAT.1 Well-defined development tools
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.1 Testing: basic design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
AVA Vulnerability Assessment	AVA_VAN.3 Focused 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/BAC FCS_CKM.1/CPS FCS_CKM.1/GIM FCS_CKM.4 FCS_COP.1/SHA FCS_COP.1/ENC FCS_COP.1/AUTH

	FCS_COP.1/MAC FCS_RND.1
FIA: Identification and Authentication	FIA_UID.1 FIA_UAU.1 FIA_UAU.4 FIA_UAU.5 FIA_UAU.6 FIA_AFL.1/Init FIA_AFL.1/Pre-pers FIA_AFL.1/Pers FIA_AFL.1/BAC
FDP: User Data Protection	FDP_ACC.1 FDP_ACF.1 FDP_UCT.1 FDP_UIT.1
FMT: Security Management	FMT_SMF.1 FMT_SMR.1 FMT_LIM.1 FMT_LIM.2 FMT_MTD.1/INI_ENA FMT_MTD.1/INI_DIS FMT_MTD.1/KEY_READ/BAC FMT_MTD.1/KEY_READ/Init FMT_MTD.1/KEY_READ/Pre-pers FMT_MTD.1/KEY_WRITE
FPT: Protection of the Security Functions	FPT_EMSEC.1 FPT_FLS.1 FPT_PHP.3 FPT_TST.1

IDENTIFICATION

Product: SOMA-c007 Machine Readable Electronic Document Basic Access Control (SOMA-c007_2) version 2

Security Target: Security Target SOMA-c007 Machine Readable Electronic Document - ICAO Application - Basic Access Control. Version 1.9

Protection Profile: Common Criteria Protection Profile Machine Readable Travel Documents with “ICAO Application”, Basic Access Control. Version 1.10, 25th March 2009. BSI-CC-PP-0055 [PP0055]

Evaluation Level: Common Criteria v3.1 R4 EAL4 + ALC_DVS.2.

SECURITY POLICIES

The use of the product SOMA-c007 Machine Readable Electronic Document Basic Access Control (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.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.

P.Personal_Data Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the e-Document's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)[1] and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the e-Document's chip are personal data of the e-Document holder. These data groups are intended to be used only with agreement of the e-Document holder by inspection systems to which the e-Document is presented. The e-Document's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ICAO11].

Application Note. The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [ICAO11]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

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.e-Document_Manufact e-Document manufacturing on steps 4 to 7

It is assumed that appropriate functionality testing of the e-Document is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the e-Document and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft of unauthorized use).

A.e-Document_Delivery e-Document delivery during steps 4 to 7

[1] Note that EF.DG3 and EF.DG4 are only readable after successful EAC authentication not being covered by the Protection Profile.

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

• Procedures shall ensure protection of TOE material/information under delivery and storage.

• Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.

• Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

A.Pers_Agent Personalization of the e-Document's chip

The Personalization Agent ensures the correctness of:

i. the logical e-Document with respect to the e-Document holder,

ii. the Document BAC Keys,

iii. the Chip Authentication Public Key (EF.DG14)

iv. the Document Signer Public Key Certificate (is stored on the e-Document's chip).

The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys Inspection Systems for global interoperability

The Inspection System is used by a control officer of the receiving State or Organization

i. examining an e-Document presented by the user and verifying its authenticity and

ii. verifying the presenter as e-Document holder.

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 the Basic Access Control [ICAO11].

The Basic Inspection System reads the logical e-Document being under Basic Access Control and performs the Passive Authentication to verify the logical e-Document.

Application Note. According to [ICAO11] the support of Passive Authentication mechanism is mandatory whereas the Basic Access Control is optional. This ST does not address Primary Inspection Systems therefore the BAC is mandatory within this ST.

A.BAC-Keys Cryptographic quality of Basic Access Control Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [ICAO11], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

Application Note. When assessing the MRZ data resp. the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product SOMA-c007 Machine Readable Electronic Document Basic Access Control (SOMA-c007_2) version 2, although the agents implementing attacks have an enhanced-basic attack potential according to the assurance level EAL4 + ALC_DVS.2 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.Chip_ID Identification of e-Document's chip

Adverse action: An attacker trying to trace the movement of the e-Document by identifying the e-Document's chip directly by establishing a communication through the contact interface or remotely by establishing or listening to communications through the contactless communication interface.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the e-Document data page in advance.

Asset: Anonimity of user

T.Skimming Skimming the logical e-Document

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 enhanced basic attack potential, not knowing the optically readable MRZ data printed on the e-Document data page in advance.

Asset: confidentiality of logical e-Document data

T.Eavesdropping Eavesdropping to the communication between TOE and inspection system

Adverse action: An attacker is listening communication between the e-Document's chip and an inspection system to gain the logical e-Document or parts of it. The inspection system uses the MRZ data printed on the e-Document data page but the attacker does not know these data in advance.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the e-Document data page in advance.

Asset: confidentiality of logical e-Document data

T.Forgery Forgery of data on e-Document's chip

Adverse action: An attacker alters fraudulently the complete stored logical e-Document or any part of it including its security related data in order to deceive on an inspection system by means of the changed e-Document holder's identity or biometric reference data. This threat comprises several attack scenarios of e-Document forgery. The attacker may alter the biographical data on the biographical data page or section of the e-Document book or card, in the printed MRZ and in the digital MRZ to claim another identity of the presenter. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical e-Documents to create a new forged e-Document, e.g. the attacker write the digitized portrait and optional biometric reference finger data read from the logical e-Document of a holder into an other MTRD's chip leaving their digital MRZ unchanged to claim the identity of the holder this e-Document. The attacker may also copy the complete unchanged logical e-Document to another chip.

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

Asset: authenticity of logical e-Document data

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 the phase "Operational Use" in order:

i. to manipulate User Data,

ii. to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or

iii. to disclose or to manipulate TSF Data.

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

Threat agent: having enhanced basic attack potential, being in possession of a legitimate e-Document

Asset: confidentiality and authenticity of logical e-Document and TSF data, correctness of TSF

T.Information_Leakage Information Leakage from e-Document's chip

Adverse action: An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker. 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 the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

Threat agent: having enhanced basic attack potential, being in possession of a legitimate e-Document

Asset: confidentiality logical e-Document and TSF data

T.Phys_Tamper Physical Tampering

Adverse action: An attacker may perform physical probing of the e-Document's chip in order:

i.to disclose TSF Data, or

ii.to disclose/reconstruct the e-Document's chip Embedded Software.

An attacker may physically modify the e-Document's chip in order to:

i. modify security features or functions of the e-Document's chip,

ii. modify security functions of the e-Document's chip Embedded Software,

iii. modify User Data or

iv. modify TSF data.

The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the e-Document's chip) 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 direct interaction with the e-Document's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and 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.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate e-Document

Asset: confidentiality and authenticity of logical e-Document and TSF data, correctness of TSF

T.Malfunction Malfunction due to Environmental Stress

Adverse action: An attacker may cause a malfunction of TSF or of the e-Document's chip Embedded Software by applying environmental stress in order to:

i. deactivate or modify security features or functions of the TOE or

ii. circumvent or deactivate or modify security functions of the e-Document's chip Embedded Software.

This may be achieved e.g. by operating the e-Document's chip outside the normal operating conditions, exploiting errors in the e-Document's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate e-Document

Asset: confidentiality and authenticity of logical e-Document and TSF data, correctness of TSF

OPERATIONAL ENVIRONMENT FUNCTIONALITY

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

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

OE.e-Document_Manufact Protection of the e-Document Manufacturing

Appropriate functionality testing of the TOE shall be used in step 4 to 7. During all manufacturing and test operations, security procedures shall be used through phases 4, 5, 6 and 7 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

OE.e-Document_Delivery Protection of the e-Document delivery

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

• non-disclosure of any security relevant information,

• identification of the element under delivery,

• meet confidentiality rules (confidentiality level, transmitt al form, reception acknowledgment),

• physical protection to prevent external damage,

• secure storage and handling procedures (including rejected TOE's),

• traceability of TOE during delivery including the following parameters:

o origin and shipment details,

o reception, reception acknowledgement,

o location material/information.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.

Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

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 logical 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 logical e-Document

The issuing State or Organization must ensure that the Personalization Agent acting on behalf of the issuing State or Organization

v. establish the correct identity of the holder and create biographical data for the e-Document,

vi. enroll the biometric reference data of the e-Document holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and

vii. personalize the e-Document for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

OE.Pass_Auth_Sign Authentication of logical e-Document by Signature

The issuing State or Organization must:

i. generate a cryptographic secure Country Signing CA Key Pair,

ii. ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment and

iii. distribute the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity.

The issuing State or Organization must:

i. generate a cryptographic secure Document Signing Key Pair and ensure the secrecy of the Document Signer Private Keys,

ii. sign Document Security Objects of genuine e-Document in a secure operational environment only, and

iii. distribute the Certificate of the Document Signer Public Key to receiving States and Organizations.

The digital signature in the Document Security Object relates to all data in the data groups EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO10].

OE.BAC-Keys Cryptographic quality of Basic Access Control Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [ICAO11] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

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 e-Document book or card

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 e-Document. The Basic Inspection System for global interoperability

i. includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and

ii. implements the terminal part of the Basic Access Control [ICAO11].

OE.Passive_Auth_Verif Verification by Passive Authentication

The control officer of the receiving State or Organization uses the inspection system to verify the presenter as e-Document holder. The inspection systems must have successfully verified the signature of the Document Security Objects and the integrity data elements of the logical e-Document before they are used. The Receiving States and Organizations must manage the Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

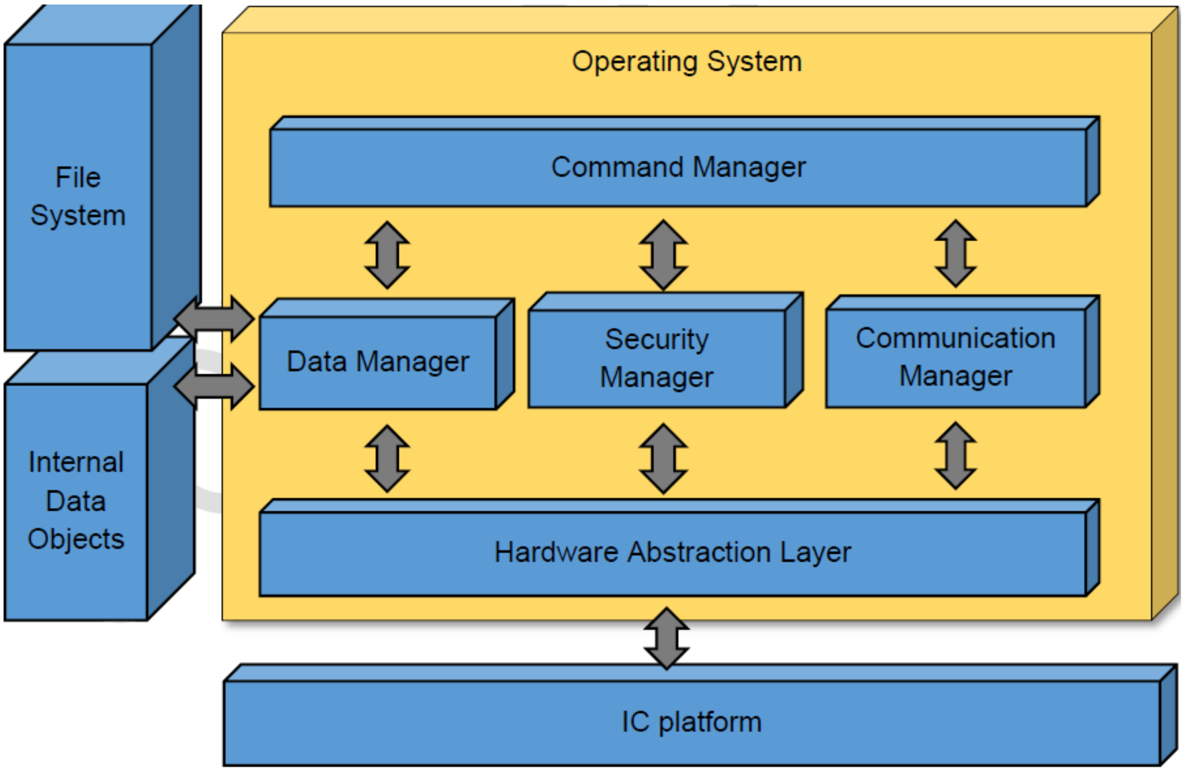
OE.Prot_Logical_e-Document Protection of data from the logical e-Document

The inspection system of the Receiving State or Organization ensures the confidentiality and integrity of the data read from the logical e-Document. The receiving State or Organization examining the logical e-Document being under Basic Access Control will use inspection systems which implement the terminal part of the Basci Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic 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



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,

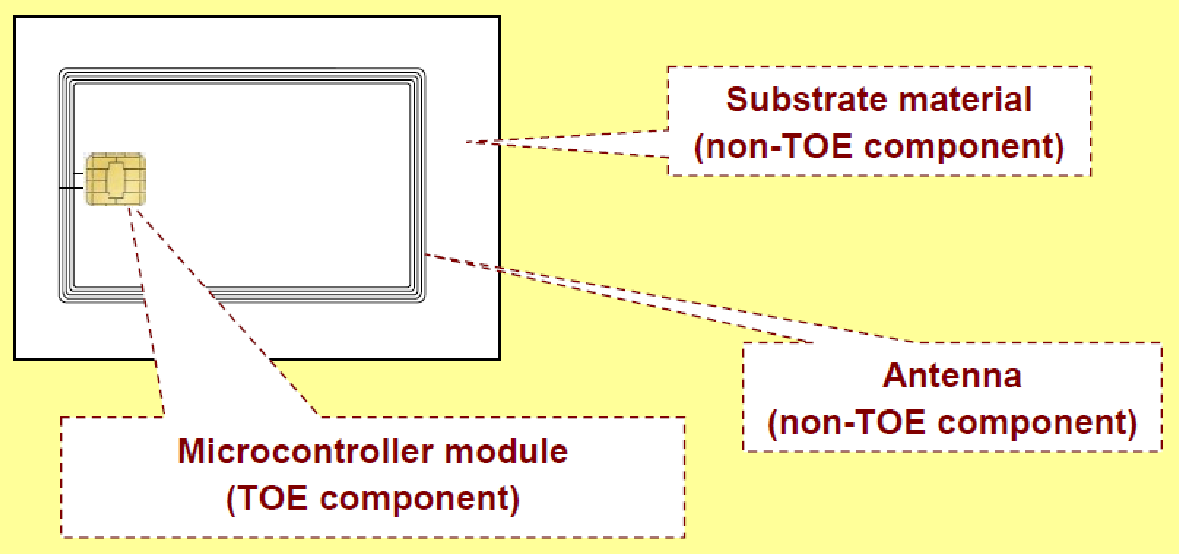
o Command enabling bitmask,

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 [AGFPERS], 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 [AGFPERS], 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 BAC 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 attack potential Enhanced-Basic 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 Basic Access Control (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 Basic Access Control (SOMA-c007_2) version 2 has been evaluated against the Security Target "Security Target SOMA-c007 Machine Readable Electronic Document - ICAO Application - Basic Access Control", version 1.9

All the assurance components required by the evaluation level EAL4 + ALC_DVS.2 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 Profile it is based on. The customer should review if those differences are bearable for his application. Those differences are collected in the tables 2-1 and 2-2 of the ST (Modified elements in the security problem definition and security objectives and SFRs iterations and refinements).

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product SOMA-c007 Machine Readable Electronic Document Basic Access Control (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
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.

[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, BSI-CCPP-0055.

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 Basic Access Control, Version 1.9, Date 2017-09-01, Reference TCAE160001.

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 Basic Access Control Public Version, Version 1.0, Date 2017-09-21, Reference TCAE160019.