Reference: 2017-62-INF-3233-v1
Target: Público
Date: 14.10.2020

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

CERTIFICATION REPORT

Dossier #	**2017-62**
TOE	**SOMA-c018 Machine Readable Electronic Document - Basic Access Control version 2 (SOMA-c018_2)**
Applicant	**IT12845840151 - HID Global**

References

[EXT-3669] Certification Request

[EXT-6119] Evaluation Technical Report

Certification report of the product SOMA-c018 Machine Readable Electronic Document - Basic Access Control version 2 (SOMA-c018_2), as requested in [EXT-3669], and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-6119] received on 24/07/2020.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product SOMA-c018 Machine Readable Electronic Document - Basic Access Control version 2 (SOMA-c018_2).

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 Basic Access Control (BAC) according to ICAO Doc 9303 7th edition Part 11 [ICAO-9303-11].

Developer/manufacturer: HID Global

Sponsor: HID Global.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Protection Profile: BSI-CC-PP-0055.

Evaluation Level: Common Criteria version 3.1 R5 – EAL4 + ALC_DVS.2.

Evaluation end date: 11/08/2020.

Expiration Date[1]: 13/10/2025

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 for Information Technology Security Evaluation Version 3.1, R5 and the Common Methodology for Information Technology Security Evaluation Version 3.1, R5.

Considering the obtained evidences during the instruction of the certification request of the product SOMA-c018 Machine Readable Electronic Document - Basic Access Control version 2 (SOMA-c018_2), a positive resolution is proposed.

[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.

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 Basic Access Control (BAC) according to ICAO Doc 9303 7th edition Part 11 [ICAO-9303-11].

The TOE is composed of:

- the circuitry of the e-Document's chip Samsung S3D350A (rev2) (see Appendix A),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the smart card operating system SOMA-c018 version 2 (SOMA-c018_2),
- an ICAO application compliant with ICAO Doc 9303,
- 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 eDocument can be inspected by authorized agents.

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 for Information Technology Security Evaluation Version 3.1, R5.

Security assurance requirements	Titles
Class ADV: Development	
ADV_ARC.1	Architectural design
ADV_FSP.4	Functional specification
ADV_IMP.1	Implementation representation
ADV_TDS.3	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.4	CM scope
ALC_DEL.1	Delivery
ALC_DVS.2	Development security
ALC_LCS.1	Life-cycle definition
ALC_TAT.1	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.1	Depth
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing
Class AVA: Vulnerability analysis	
AVA_VAN.3	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, R5:

Security functional requirement	Title
FAU_SAS.1	Audit storage
FCS_CKM.1/BAC	Cryptographic key generation – Generation of Document Basic Access Key by the TOE
FCS_CKM.1/CPS	Cryptographic key generation – Generation of CPS session Keys for Pre-personalization and Personalization by the TOE
FCS_CKM.1/GIM	Generation of the Initialization Key by the TOE
FCS_CKM.4	Cryptographic key destruction – e-Document
FCS_COP.1/AUTH	Cryptographic operation – Authentication
FCS_COP.1/ENC	Cryptographic operation – Encryption/Decryption Triple DES
FCS_COP.1/MAC	Cryptographic operation – Retail MAC
FCS_COP.1/SHA	Cryptographic operation – Hash for Key Derivation
FCS_RND.1	Quality metrics for random numbers
FDP_ACC.1	Subset access control – Basic Access Control

FDP_ACF.1	Basic security attribute based access control – Basic Access Control
FDP_UCT.1	Basic data exchange confidentiality – e-Document
FDP_UIT.1	Data exchange integrity – e-Document
FIA_AFL.1/Init	Authentication failure handling in Step 5 Initialization
FIA_AFL.1/Pre-pers	Authentication failure handling in Step 6 "Pre-personalization"
FIA_AFL.1/Pers	Authentication failure handling in Step 7 "Personalization"
FIA_AFL.1/BAC	Authentication failure handling in Step 8 "Operational Use"
FIA_UAU.1	Timing of authentication
FIA_UAU.4	Single-use authentication mechanisms – Single-use authentication of the Terminal by the TOE
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.6	Re-authenticating – Re-authenticating of Terminal by the TOE
FIA_UID.1	Timing of identification
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FMT_MTD.1/INI_DIS	Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data
FMT_MTD.1/INI_ENA	Management of TSF data – Writing of Initialization Data and Pre-personalization Data
FMT_MTD.1/KEY_READ/BAC	Management of TSF data – BAC keys and Personalization keys Read
FMT_MTD.1/KEY_READ/Init	Management of TSF data – Initialization key Read
FMT_MTD.1/KEY_READ/Pre-pers	Management of TSF data – Pre-personalization key Read
FMT_MTD.1/KEY_WRITE	Management of TSF data – Key Write
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_EMSEC.1	TOE emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.3	Resistance to physical attack
FPT_TST.1	TSF testing

IDENTIFICATION

Product: SOMA-c018 Machine Readable Electronic Document - Basic Access Control version 2 (SOMA-c018_2)

Security Target: Security Target for SOMA-c018 Machine Readable Electronic Document - Basic Access Control, Version 1.15. 2019-08-13.

Protection Profile: BSI-CC-PP-0055, Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application", Basic Access Control, version 1.10, March 2009.

Evaluation Level: Common Criteria for Information Technology Security Evaluation Version 3.1, R5 EAL4 + ALC_DVS.2.

SECURITY POLICIES

The use of the product SOMA-c018 Machine Readable Electronic Document - Basic Access Control version 2 (SOMA-c018_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 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 eDocument 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 eDocument'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)[3] and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the eDocument'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 [ICAO_P11].

Application Note 12 The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [ICAO_P11]. 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 6

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 6

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:

1. the logical e-Document with respect to the e-Document holder,
2. the Document BAC Keys,
3. the Chip Authentication Public Key (EF.DG14), and
4. the Document Signer Public Key Certificate.

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

1. examining an e-Document presented by the user and verifying its authenticity, and
2. verifying the presenter as e-Document holder.

The Basic Inspection System for global interoperability

1. includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and
2. implements the terminal part of the Basic Access Control [ICAO_P11].

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 10 According to [ICAO_P11], 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' [ICAO_P11], 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 11 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-c018 Machine Readable Electronic Document - Basic Access Control version 2 (SOMA-c018_2), although the agents implementing attacks have the attack potential enhanced-basic 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: anonymity of use

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 eDocument 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 eDocument 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 eDocument 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

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:

1. to manipulate User Data,
2. to manipulate (explore, bypass, deactivate or change) security

3. features or functions of the TOE, or
4. 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 eDocument 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:

1. to disclose TSF Data, or
2. to disclose/reconstruct the e-Document’s chip Embedded Software.

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

1. modify security features or functions of the e-Document’s chip,
2. modify security functions of the e-Document’s chip Embedded Software,
3. modify User Data, or

4. 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 eDocument'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:

1. deactivate or modify security features or functions of the TOE, or
2. circumvent or deactivate or modify security functions of the eDocument'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 6. 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, transmittal 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:
    - origin and shipment details,
    - reception, reception acknowledgement,
    - 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

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

(ii) 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 log

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

(i) establish the correct identity of the holder and create biographical data for the eDocument,

(ii) enrol 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

(iii)personalize the e-Document for the holder together with the defined physical and

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 [ICAO_P10] and [ICAO_P12].

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' 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.t

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 [ICAO_P11]

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 Object and the integrity of the 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 Basis 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

A State or Organization issues e-Documents to be used by the holder. The user presents an e-Document to the inspection system to prove his or her identity. The e-Document in context of this protection profile contains

(i) visual (eye readable) biographical data and portrait of the holder,

(ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine Readable Zone (MRZ), and

(iii)data elements on the e-Document's chip according to LDS for machine reading.

The authentication of the presenter1 is based on:

- the possession of a valid e-Document personalized for the holder with the claimed identity as given on the biographical data page and
- biometrics using the reference data stored in the e-Document chip.

The Issuing State or Organization ensures the authenticity of the data of genuine eDocuments, the receiving State or Organization trusts a genuine e-Document of an IssuingState or Organization.

The logical e-Document as data of the e-Document holder stored according to the Logical Data Structure [ICAO_P10] as specified by ICAO on the integrated circuit. It presents machine readable data including (but not limited to) personal data of the e-Document holder:

(i) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

(ii) the digitized portraits (EF.DG2),

(iii)the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[2],

(iv)the other data according to LDS (EF.DG5 to EF.DG16),

(v) the Document Security Object (SO_D),

(vi)security data objects required for product management

[2] These biometric reference data are optional according to [CC_P1]. These data are protected by means of Extended Access Control, which is out of scope of the Security Target.

Application Note 1 EF.DG15 is out of the scope of this ST as Active Authentication is not included in the TOE.

PHYSICAL ARCHITECTURE

The physical e-Document as electronic document in the form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the e-Document holder:

(i) the biographical data on the biographical data page of the e-Document booklet,

(ii) the printed data in the Machine Readable Zone (MRZ),

(iii)the printed portrait;

The TOE is comprised of the following parts:

- Integrated circuit chip Samsung S3D350A (rev2) equipped with IC Dedicated Software (cf. Appendix A for more details);
- smart card operating system SOMA-c018 version 2 (SOMA-c018_2);
- an International Civil Aviation Organization (ICAO) application compliant with ICAO Doc 9303 [ICAO_P10] [ICAO_P11] [ICAO_P12];
- guidance documentation in PDF format about the preparation and use of the ICAO application, composed by:
  - the Initialization Guidance,
  - the Pre-personalization Guidance,
  - the Personalization Guidance,
  - the Operational User Guidance.

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
Initialization Guidance	1.7	Initialization Agent
Pre-personalization Guidance	1.7	Pre-personalization Agent
Personalization Guidance	1.7	Personalization Agent
Operational User Guidance	1.7	User

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. Likewise, he has selected and repeated about 25% of the developer functional tests in the testing platform implemented in the evaluation laboratory, selecting one test for each of the most relevant functional class.

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 SOMA-c018 Machine Readable Electronic Document - Basic Access Control version 2 (SOMA-c018_2) it is necessary the disposition of the following software components:

Title	Information
TOE Name	SOMA-c018 Machine Readable Electronic Document - Basic Access Control
TOE Version	2
TOE Developer	HIDGlobal S.p.A.
TOE Identification	SOMA-c018_2
TOE identification data	53h 4Fh 4Dh 41h 2Dh 63h 30h 31h 38h 5Fh 32h
Evaluation sponsor	HIDGlobal S.p.A.
IC	S3D350A (rev2) family

The Machine Readable Electronic Document certified shall return the following string, representing the Global Reference:

- SOMA-c018_2 - (ASCII codes 53h 4Fh 4Dh 41h 2Dh 63h 30h 31h 38h 5Fh 32h)

The ASCII encoding of the TOE identifier constitutes the TOE identification data, located in the persistent memory of the chip. The identification bytes can be read by means of the GET DATA (Even INS) command as described in in section 6.3 of Pre-personalization Guidance.

The IC on which the TOE is based, constituting the platform for its composite evaluation (cf. [R30]), is the secure microcontroller S3D350A (rev2) with the AT1 Secure RSA and ECC Library version 1.03 including specific IC Dedicated Software, developed and manufactured by Samsung.

The versions of the two libraries are encoded in the ATR string returned by both the contact and contactless interfaces as follows:

- The version of the PKA library (RSA/ECC/SHA) is encoded in the third to last byte.
- The version of the True Random Number Generation Library (DTRNG) is encoded in the second to last byte.
- In both bytes, the most significant nibble identifies the version major number, and the least significant nibble identifies the version minor number.

In the ATR returned by the TOE identified, the value of the above two bytes shall be 13h 20h, thus identifying version 1.03 of the PKA library (RSA/ECC/SHA) and version 2.0 of the True Random Number Generation Library (DTRNG). Both of PKA library (RSA/ECC/SHA) version 1.03 and True Random Number Generation Library (DTRNG) version 2.0 are used in the TOE.

This IC has obtained a Common Criteria certification at Evaluation Assurance Level EAL6 augmented by ASE_TSS.2.

The current certification report of chip S3D350A (rev2) is identified in the bibliography, and is associated with the following reference code:

ANSSI-CC-2018/12

EVALUATION RESULTS

The product SOMA-c018 Machine Readable Electronic Document - Basic Access Control version 2 (SOMA-c018_2) has been evaluated against the Security Target Security Target for SOMA-c018 Machine Readable Electronic Document - Basic Access Control, Version 1.15. 2019-08-13.

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 evaluation level EAL4 + ALC_DVS.2, as defined by the Common Criteria for Information Technology Security

Evaluation Version 3.1, R5 and the Common Methodology for Information Technology Security Evaluation Version 3.1, R5.

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 Applus Laboratories, a positive resolution is proposed.

The CCN Certification Body 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.

The TOE consumer should also observe the application notes defined in the applicable security target. The recommended cryptographic algorithms and key lengths are those defined in SOGIS Agreed Cryptographic Mechanisms, version 1.1.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

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

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

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

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

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

SECURITY TARGET

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 SOMA-c018 Machine Readable Electronic Document - Basic Access Control, Version 1.15. 2019-08-13.

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 SOMA-c018 Machine Readable Electronic Document - EAC-PACE-AA, Version 1.0, 2020-07-07.

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.