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

REF: 2016-32-INF-2110 v2	Created by: CERT11
Target: Público	Revised by: CALIDAD
Date: 10.12.2018	Approved by: TECNICO

CERTIFICATION REPORT

File: 2016-32 SOMA SSCD

Applicant: HID Global / Arjo Systems

References:

[EXT-3094] Certification request of SOMA SSCD

[EXT-3605] Evaluation Technical Report of SOMA SSCD.

[EXT-4413] Maintenance Request

[IAR] SOMA-c007 Machine Readable Electronic Document. Impact Analysis Report for Maintenance of Certificate CCN-CC-018/2017, version 1.0. 07/09/2018.

The product documentation referenced in the above documents.

Certification report of the product SOMA-c007 Machine Readable Electronic Document SSCD Application (SOMA-c007_2) version 2, as requested in [EXT-3094] dated 13/06/2017, and evaluated by the laboratory Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-3605] received on 20/09/2017.

This certification report has been reviewed according to maintenance request [EXT-4413] and [IAR]. The requested changes were considered as minor and therefore an addendum to this certificate and a maintenance report [INF-2615] have been issued. The resistance to attacks has not been re-assessed in the course of the maintenance process.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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

The TOE is a combination of hardware and software configured to securely create, use, and manage Signature Creation Data (SCD). The SSCD (Secure Signature Creation Device) protects the SCD during its whole life cycle as to be used in a signature creation process solely by its Signatory. The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature. The TOE provides the following functions:

1. to generate Signature Creation Data (SCD) and the corresponding Signature Verification Data (SVD),

2. to export the SVD for certification to the CGA (Certification Generation Application) over a trusted channel,

3. to prove the identity as SSCD to external entities,

4. to, optionally, receive and store certificate info,

5. to switch the SSCD from a non-operational state to an operational state, and

6. if in an operational state, to create digital signatures for data with the following steps:

   a. select an SCD if multiple are present in the SSCD,

   b. authenticate the Signatory and determine its intent to sign,

   c. receive data to be signed or a unique representation thereof (DTBS/R) from the SCA over a trusted channel,

   d. apply an appropriate cryptographic signature creation function to the DTBS/R using the selected SCD.

The TOE is prepared for the Signatory’s use by:

1. generating at least one SCD/SVD pair, and

2. personalizing for the Signatory by storing in the TOE:

   a. the Signatory’s Reference Authentication Data (RAD),

   b. optionally, certificate info for at least one SCD in the TOE.

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: [PP0059] CEN: Protection profiles for secure signature creation device, Part 2: Device with Key Generation, version 2.0.1, ref. BSI-CC-PP-**0059**-2009-MA-01, January 2012.

[PP0071] CEN: Protection profiles for secure signature creation device, Part 4: Extension for device with key generation and trusted communication with certificate generation application, version 1.0.1, ref. BSI-CC-PP-**0071**-2012, November 2012

[PP0072] CEN: Protection profiles for secure signature creation device, Part 5: Extension for device with key generation and trusted communication with signature creation application, version 1.0.1, ref. BSI-CC-PP-**0072**-2012, November 2012

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 SSCD Application (SOMA-c007_2) version 2, a positive resolution is proposed.

TOE SUMMARY

The physical TOE is comprised of the following parts:

• dual-interface chip equipped with IC Dedicated Software;

• smart card operating system SOMA-c007;

• a Secure Signature Creation Device (SSCD) application compliant with European Parliament Directive 1999/93/EC [EC99-93];

• guidance documentation about the initialization of the TOE and the preparation and use of the SSCD application, 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 Users (Signatory, Administrator) [AGDOPE].

The SSCD application of the TOE supports the same SSCD life cycle phases, i.e. SSCD preparation and SSCD operational use, as well as the same SSCD roles, i.e. Administrator and Signatory, as those defined in the PPs [PP0059] [PP0071] [PP0072].

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
FCS: Cryptographic Support	FCS_COP.1
FDP: User Data Protection	FDP_ACC.1/SCD/SVD_Generation FDP_ACF.1/SCD/SVD_Generation FDP_ACC.1/SVD_Transfer FDP_ACF.1/SVD_Transfer FDP_ACC.1/Signature creation FDP_ACF.1/Signature creation FDP_RIP.1 FDP_SDI.2/Persistent FDP_SDI.2/DTBS FDP_DAU.2/SVD FDP_UIT.1/DTBS
FIA: Identification and Authentication	FIA_UID.1 FIA_UAU.1 FIA_AFL.1/Signatory FIA_AFL.1/Admin FIA_AFL.1/Init FIA_AFL.1/Pre-pers FIA_AFL.1/Pers FIA_API.1
FMT: Security Management	FMT_SMR.1/SSCD FMT_SMR.1/Init FMT_SMR.1/Pre-pers FMT_SMR.1/Pers FMT_SMF.1 FMT_MOF.1 FMT_MSA.1/Admin FMT_MSA.1/Signatory FMT_MSA.2 FMT_MSA.3

	FMT_MSA.4 FMT_MTD.1/Admin FMT_MTD.1/Signatory FMT_MTD.1/Init FMT_MTD.1/Pre-pers FMT_MTD.1/Pers FMT_LIM.1 FMT_LIM.2
FPT: Protection of the Security Functions	FPT_EMS.1 FPT_FLS.1 FPT_PHP.1 FPT_PHP.3 FPT_TST.1 FTP_ITC.1/SVD FTP_ITC.1/VAD FTP_ITC.1/DTBS FTP_ITC.1/Init FTP_ITC.1/Pre-pers FTP_ITC.1/Pers

IDENTIFICATION

Product: SOMA-c007 Machine Readable Electronic Document SSCD Application (SOMA-c007_2) version 2

Security Target: SOMA-c007 Machine Readable Electronic Document - Security Target SSCD Application, version 1.9, 07/09/2018.

Protection Profiles: [PP0059] CEN: Protection profiles for secure signature creation device, Part 2: Device with Key Generation, version 2.0.1, ref. BSI-CC-PP-0059-2009-MA-01, January 2012.

[PP0071] CEN: Protection profiles for secure signature creation device, Part 4: Extension for device with key generation and trusted communication with certificate generation application, version 1.0.1, ref. BSI-CC-PP-0071-2012, November 2012

[PP0072] CEN: Protection profiles for secure signature creation device, Part 5: Extension for device with key generation and trusted communication with signature creation application, version 1.0.1, ref. BSI-CC-PP-0072-2012, November 2012

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 SSCD Application (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.CSP_QCert. Qualified certificates

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate ([EC99-93], article 2, clause 9, and Annex I) for the SVD generated by the SSCD. The certificates contain at least the name of the Signatory and the SVD matching the SCD implemented in the TOE under sole control of the Signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

P.QSign. Qualified electronic signatures

The Signatory uses a Signature Creation System to sign data with an advanced electronic signature ([EC99-93], article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to [EC99-93], Annex I). The DTBS are presented to the Signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature with an SCD implemented in the SSCD that the Signatory maintains under their sole control, and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

P.Sigy_SSCD. TOE as Secure Signature Creation Device

The TOE meets the requirements for an SSCD laid down in [EC99-93], Annex III. This implies that the SCD is used for digital signature creation under sole control of the Signatory and the SCD can practically occur only once.

P.Sig_Non-Repud. Non-repudiation of signatures

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

P.Manufact. Manufacturing of the e-Document

The IC Manufacturer writes IC initialization data in step 3, IC manufacturing, of TOE life cycle, including the key for the authentication of the Initialization Agent.

The Initialization Agent writes TOE initialization data in step 5, initialization, of TOE life cycle, including the key for the authentication of the Pre-personalization Agent.

The Pre-personalization Agent writes pre-personalization data in step 6, pre-personalization, of TOE life cycle, including the key for the authentication of the Personalization Agent.

Both the Initialization Agent and the Pre-personalization Agent act on behalf of the SSCD provisioning service.

P.Personalization. Personalization of the e-Document

The Personalization Agent writes personalization data in step 7, personalization, of TOE life cycle, including the credentials for the authentication of the Administrator and the PACE key for the authentication of the Signatory.

The Personalization Agent acts on behalf of the SSCD provisioning service.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

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

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

A.CGA. Trustworthy Certificate Generation Application

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

A.SCA. Trustworthy Signature Creation Application

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

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product SOMA-c007 Machine Readable Electronic Document SSCD Application (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.SCD_Divulg. Storage, copy, and release of Signature Creation Data

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

T.SCD_Derive. Derivation of Signature Creation Data

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

T.Hack_Phys. Physical attacks through TOE interfaces

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

T.SVD_Forgery. Forgery of Signature Verification Data

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

T.SigF_Misuse. Misuse of the signature creation function of the TOE

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

T.DTBS_Forgery. Forgery of the DTBS/R

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

T.Sig_Forgery. Forgery of the electronic signature

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

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

T.Abuse-Func. Abuse of functionality

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

OPERATIONAL ENVIRONMENT FUNCTIONALITY

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

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

OE.SVD_Auth. Authenticity of the SVD

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

OE.CGA_QCert. Generation of qualified certificates

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

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

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

OE.DTBS_Intend. SCA sends data intended to be signed

The Signatory shall use a trustworthy SCA that:

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

OE.Signatory. Security obligation of the Signatory

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

Here below are the security objectives for the operational environment defined in PP Part 4 [PP0071].

OE.Dev_Prov_Service. Authentic SSCD provided by the SSCD provisioning service

The SSCD provisioning service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, personalizes the TOE for the legitimate user as Signatory, links the identity of the TOE as SSCD with the identity of the legitimate user, and delivers the TOE to the Signatory.

Application Note. This objective replaces OE.SSCD_Prov_Service from PP Part 2 [PP0059], which is possible as it does not imply any additional requirement for the operational environment when compared with OE.SSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.SSCD_Prov_Service).

OE.CGA_SSCD_Auth. Preparation of the TOE for SSCD authentication

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

OE.CGA_TC_SVD_Imp. CGA trusted channel for SVD import

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

Application Note. The developer prepares the TOE for the delivery to the customer (i.e. the SSCD provisioning service) in the development phase, not addressed by security objectives for the operational environment. The SSCD provisioning service performs initialization and personalization as TOE for the legitimate user (i.e. the device holder). If the TOE is delivered to the device holder with SCD, the TOE is an SSCD. This situation is addressed by OE.SSCD_Prov_Service except for the additional initialization of the TOE for proof as SSCD and trusted channel to the CGA. If the TOE is delivered to the device holder without SCD, the TOE will be an SSCD only after generation of the first SCD/SVD pair. Because this SCD/SVD pair generation is performed by the Signatory in the operational use stage, the TOE provides additional security functionality addressed by OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp. But this security functionality must be initialized by the SSCD provisioning service as described in OE.Dev_Prov_Service. Therefore, PP Part 4 [PP0071] substitutes OE.SSCD_Prov_Service by OE.Dev_Prov_Service, allowing generation of the first SCD/SVD pair after delivery of the TOE to the device holder and requiring initialization of security functionality of the TOE. Nevertheless, the additional security functionality must be used by the operational environment as described in OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp. This approach does not weaken the security objectives and requirements for the TOE, but enforces more security functionalities of the TOE for additional methods of use. Therefore, it does not conflict with the CC conformance claim to PP Part 2 [PP0059].

Here below are the security objectives for the operational environment defined in PP Part 5 [PP0072].

OE.HID_TC_VAD_Exp. HID trusted channel for VAD export

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

Application Note. This security objective for the TOE is partly covering OE.HID_VAD from PP Part 2 [PP0059]. While OE.HID_VAD in PP Part 2 requires only the operational environment to protect VAD, this PP requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore, PP Part 5 [PP0072] partly re-assigns the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp, and leaves only the necessary functionality by the HID.

OE.SCA_TC_DTBS_Exp. SCA trusted channel for DTBS export

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

Application Note. This security objective for the TOE is partly covering OE.DTBS_Protect from PP Part 2 [PP0059]. While OE.DTBS_Protect in PP Part 2 requires only the operational environment to protect DTBS, this PP requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore, PP Part 5 [PP0072] partly re-assigns the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp, and leaves only the necessary functionality by the SCA.

ARCHITECTURE

LOGICAL ARCHITECTURE

The SSCD application of the TOE supports the same SSCD life cycle phases, i.e. SSCD preparation and SSCD operational use, as well as the same SSCD roles, i.e. Administrator and Signatory, as those defined in the PPs [PP0059] [PP0071] [PP0072].

The following figure illustrates the operations supported by the SSCD application of the TOE, split according to the SSCD life cycle phases and the SSCD roles for which they are actually available.

Mutual authentication

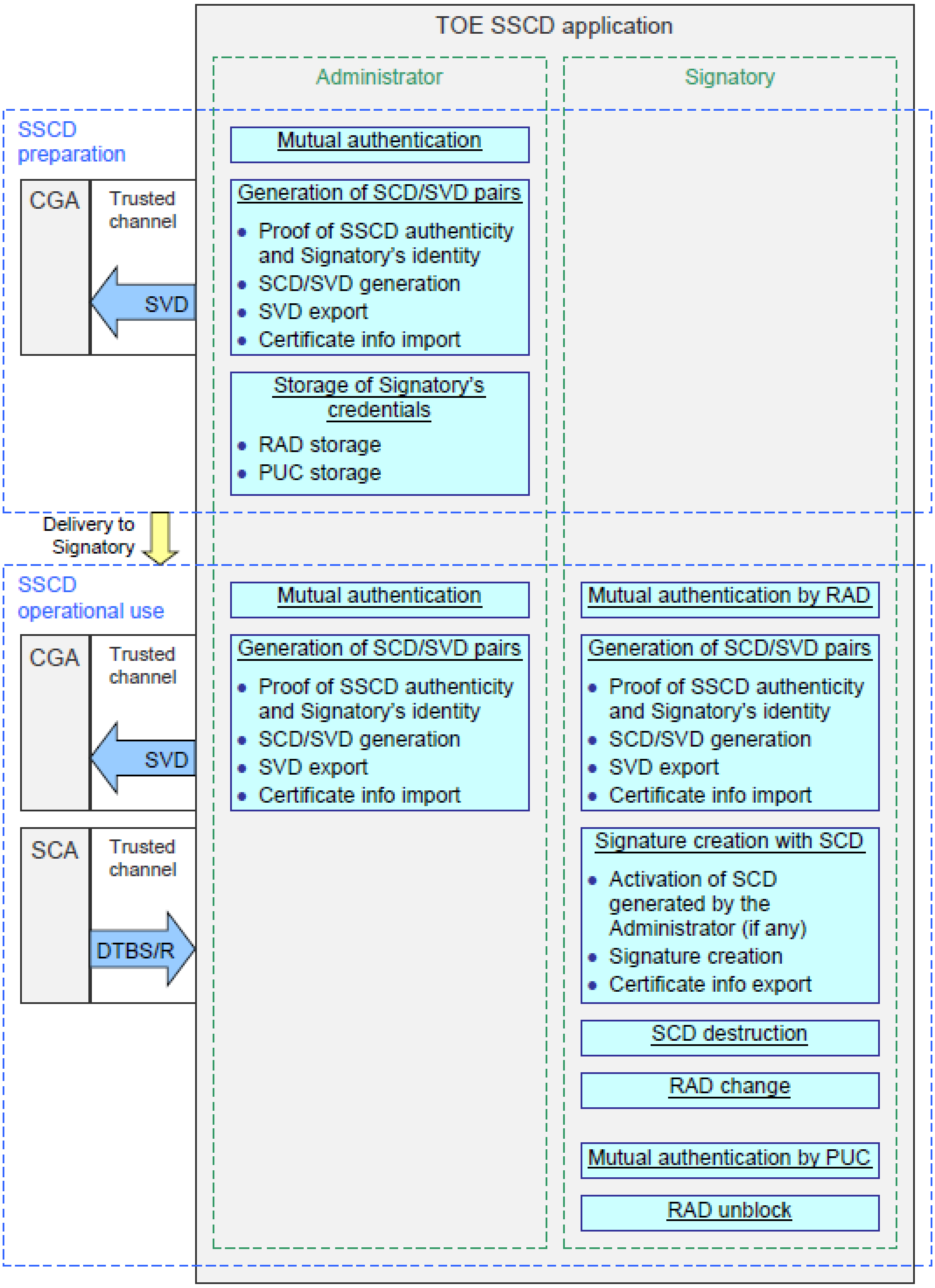
As a precondition for gaining access to further operations, both the Administrator and the Signatory must perform a mutual authentication with respect to the SSCD application. The authentication procedure is comprised of the following two steps:

1. Mutual authentication under the MF by means of a PACE authentication compliant with ICAO Doc 9303 [ICAO11];

2. External authentication under the SSCD application by means of the verification of a password over the trusted channel opened with PACE authentication.

Generation of SCD/SVD pairs

The SSCD application supports the generation of multiple SCD/SVD pairs in the SSCD preparation phase on the part of the Administrator, as well as in the SSCD operational use phase on the part of both the Administrator and the Signatory. SCD keys are activated for signature creation upon their generation just in case they are generated by the Signatory, otherwise they are not active until the Signatory explicitly activates them.



Signature creation with SCD

In accordance with IAS ECC specification [IASECC], the SSCD application supports digital signature creation with signature creation algorithm RSASSA-PKCS1-v1_5 compliant with PKCS #1 [PKCS01], hash algorithm SHA-256 compliant with FIPS PUB 180-4 [FIPS180-4], and keys of 3072 bits.

The signature creation function of the SSCD application can take all of the following types of data as input from the SCA:

- a hash value of the data to be signed;
- an intermediate hash value of a first part of the data to be signed, complemented with the remaining part of such data;
- the data to be signed themselves (provided their length is not larger than 64 bytes).

The export of public keys and certificate info to the SCA is supported as well.

PHYSICAL ARCHITECTURE

The physical TOE is comprised of the following parts:

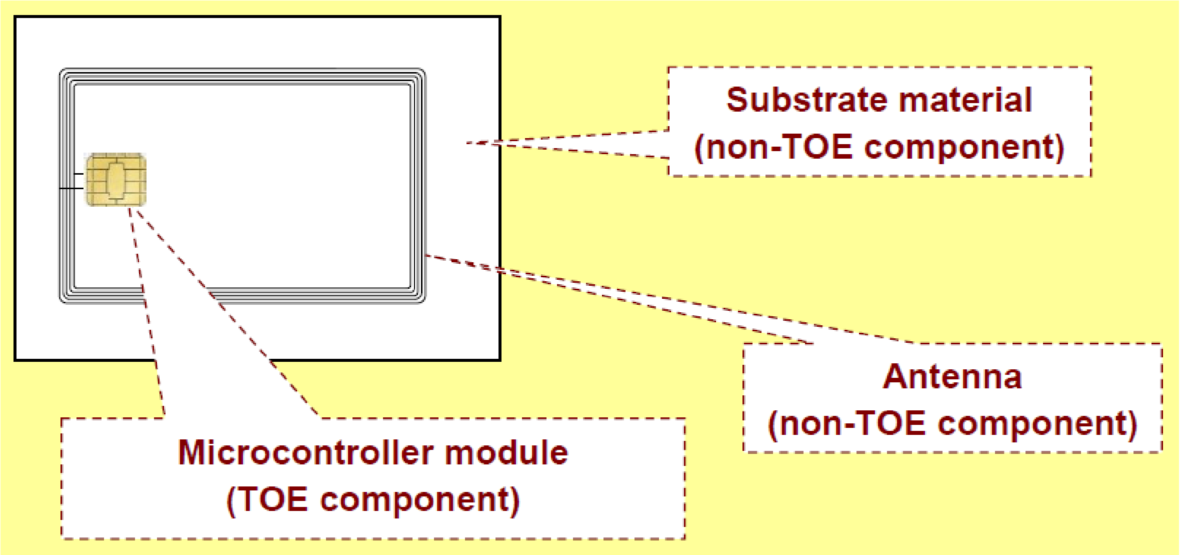
- dual-interface chip Infineon M7892 G12 equipped with IC Dedicated Software;
- smart card operating system SOMA-c007
- a Secure Signature Creation Device (SSCD) application compliant with European Parliament Directive 1999/93/EC [R20]
- the guidance documentation, composed by:
  - o the Initialization 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 Users (Signatory, Administrator) [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:

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].

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.

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 SSCD 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 SSCD Application (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 SSCD Application (SOMA-c007_2) version 2 has been evaluated against the Security Target "SOMA-c007 Machine Readable Electronic Document - Security Target SSCD Application, version 1.9, 07/09/2018".

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 3-1, 3-2, 3-3 and 3-4 of the ST (Changes, additions, and deletions to the threats/OSPs/security objectives/SFRs with respect to the PPs).

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product SOMA-c007 Machine Readable Electronic Document SSCD Application (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].

This certification report has been reviewed according to maintenance request [EXT-4413] and [IAR]. The requested changes were considered as minor and therefore an addendum to this certificate and a maintenance report [INF-2615] have been issued. The resistance to attacks has not been re-assessed in the course of the maintenance process.

GLOSSARY

AA	Active Authentication
BAC	Basic Access Control
BIS	Basic Inspection System
CC	Common Criteria
CCN	Centro Criptológico Nacional
CGA	Certificate Generation Application
CNI	Centro Nacional de Inteligencia
DTBS	Data To Be Signed
DTBS/R	Data To Be Signed or its unique Representation
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
PUC	Personal Unblocking Code
RAD	Reference Authentication data
RNG	Random Number Generator
SAR	Security assurance requirements
SCA	Signature Creation Application
SCD	Signature Creation Data
SCD/SVD Pair	
SFP	Security Function Policy
SFR	Security functional requirement
SSCD	Secure Signature Creation Device
ST	Security Target
SVD	Signature Verification Data
TOE	Target Of Evaluation
TSF	TOE Security Functions
VAD	Verification Authentication Data

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: - SOMA-c007 Machine Readable Electronic Document - Operational User Guidance, version 2.0a, 05/09/2018. TCAE160015.

[AGDPERS] HID Global / Arjo Systems: - SOMA-c007 Machine Readable Electronic Document - Personalization Guidance SSCD Application, version 2.0a, 05/09/2018. TCAE160014.

[AGDPRE] HID Global / Arjo Systems: Pre-personalization Guidance for SOMA-c007 Machine Readable Electronic Document – SSCD Application v2.0, ref. TCAE160013

[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.

[EC99-93] European Parliament: Directive 1999/93/EC on a Community framework for electronic signatures, December 1999

[FIPS180-4] NIST: FIPS PUB 180-4, Federal Information Processing Standards Publication, Secure Hash Standard (SHS), March 2012

[IASECC] GIXEL: European Card for e-Services and National e-ID Applications, IAS ECC, Identification Authentication Signature European Citizen Card, Technical Specifications, version 1.0.1, March 2008

[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.

[PKCS01] RSA Laboratories: PKCS #1: RSA Cryptography Standard, version 2.2, October 2012

[PP0059] CEN: Protection profiles for secure signature creation device, Part 2: Device with Key Generation, version 2.0.1, ref. BSI-CC-PP-0059-2009-MA-01, January 2012.

[PP0071] CEN: Protection profiles for secure signature creation device, Part 4: Extension for device with key generation and trusted communication with certificate generation application, version 1.0.1, ref. BSI-CC-PP-0071-2012, November 2012

[PP0072] CEN: Protection profiles for secure signature creation device, Part 5: Extension for device with key generation and trusted communication with signature creation application, version 1.0.1, ref. BSI-CC-PP-0072-2012, November 2012

[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 SSCD Application, version 1.9, 07/09/2018. TCAE160003.

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 SSCD Application Public Version, Version 1.1, 06/12/2018. TCAE160021.