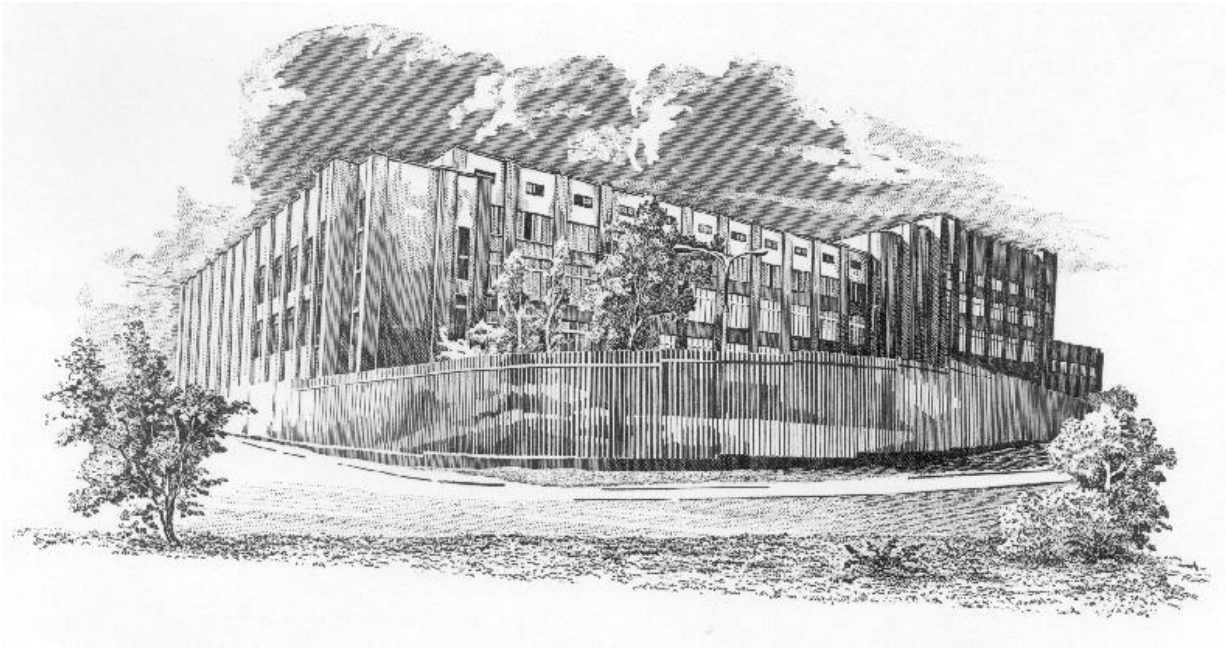
PWPW
POLSKA WYTWÓRNIA
PAPIERÓW WARTOŚCIOWYCH



SmartApp SIGN 2.2

Security Target

This page is intentionally left blank.

Table of contents

List of tables

List of figures

1 Introduction

The aim of this document is to describe the Security Target for SmartApp SIGN 2.2 which is a secure signature creation device (SSCD) with key generation according to prEN 14169-2:2009, which constitutes the protection profile [PP_SSCD-KG]. Moreover SmartApp SIGN 2.2 may provide a trusted channel to secure communication with a signature creation application (SCA) and a certificate generation application (CGA).

The SmartApp SIGN 2.2 applet (SSCD application) is implemented on the NXP JCOP operating system.

1.1 References

1.1.1 Security Target reference

ST title	SmartApp SIGN 2.2: Security Target
ST author	Polska Wytwórnia Papierów Wartościowych S.A.
ST version (date)	2.2.18.0 (2011-12-19)
Evaluation body	TÜV Informationstechnik GmbH (TÜViT)
Certification body	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Evaluation assurance level	EAL4 augmented with AVA_VAN.5 and ALC_DVS.2

1.1.2 Target of evaluation reference

TOE name	SmartApp SIGN
TOE developer	Polska Wytwórnia Papierów Wartościowych S.A.
TOE version	2.2
TOE Identification	PWPW SmartApp SIGN 2.2
TOE platform	NXP J2A080 v2.4.1 Revision 3
Certification ID	BSI-DSZ-CC-0694

1.2 Intended usage

The TOE is intended for advanced electronic signatures creation and fulfills requirements specified in [Directive] and other relevant documents.

1.3 Target of evaluation

1.3.1 Overview

SmartApp SIGN 2.2 is a multifunctional smartcard product implementing a secure signature creation device as described in [PP_SSCD-KG] that can generate a signing key (signature creation data, SCD) and operates to create electronic signatures with the generated key. SmartApp SIGN 2.2 extends [PP_SSCD-KG] with a trusted channel secure communication with a signature creation application and a certificate generation application.

The PWPW SmartApp SIGN 2.2 comprises of

- the platform (NXP J2A080 v2.4.1 Revision 3), which consist of the integrated circuit (NXP P5CC080 V0B), the operating system (JCOP 2.4.1 Revision 3) and the cryptographic library,
- the applet containing the SSCD functionality (SmartApp SIGN 2.2),
- the associated guidance documentation (AGD_PRE.1, AGD_OPE.1).

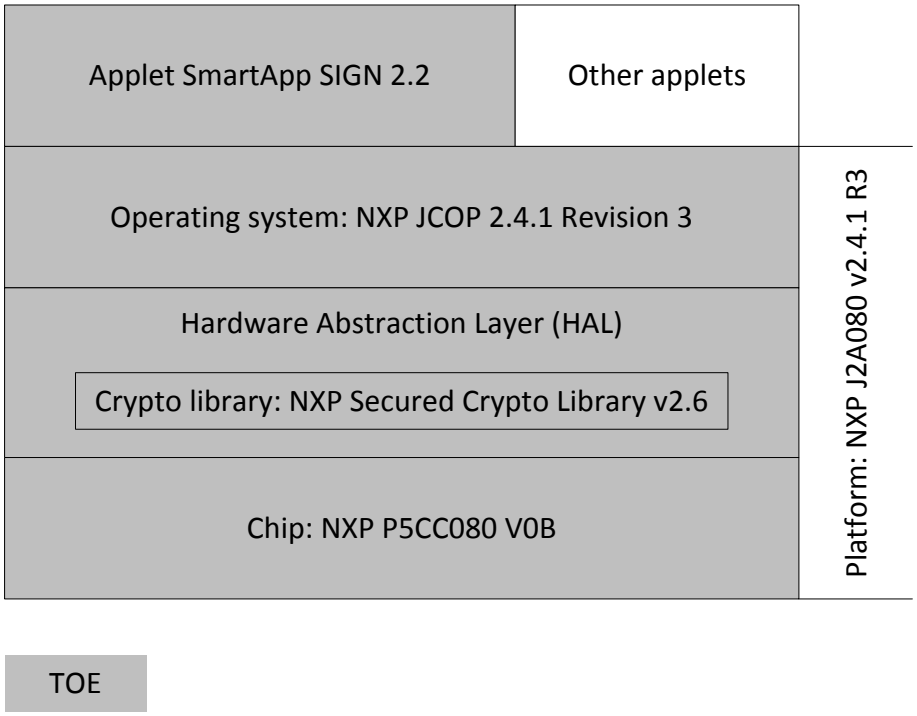
The integrated circuit is certified according to the Common Criteria for evaluation assurance level 5+ (BSI-DSZ-CC-0410-2007-MA-07).

The cryptographic library is certified according to the Common Criteria for evaluation assurance level 5+ (BSI-DSZ-CC-0709-2010).

The platform is certified according to the Common Criteria for evaluation assurance level 5+ (BSI-DSZ-CC-0674-2010).

The following Figure 1.1 shows the TOE scope.

Figure 1.1: Target of evaluation limits



The main functionalities of SmartApp SIGN 2.2 cover following areas:

- cryptographic key generation and secure management;
- secure signature generation with secure management of data to be signed;
- identification and authentication of trusted users and applications;
- data storage and protection from modification or disclosures, as needed;
- secure exchange of sensitive data between the TOE and a trusted applications;
- secure exchange of sensitive data between the TOE and a trusted human interface device.

The security functionality of the TOE will be externally available to the user by APDU commands according to the access conditions specified by the appropriate policies considering the life cycle state, user role and security state.

1.3.2 Security features

The following overview shows the security features of the composite TOE.

1.3.2.1 Authentication mechanisms

Authentication mechanisms are differentiated by the user roles Signatory (end user) and Administrator.

Authentication of the Signatory by a PIN mechanism.

Authentication of the Administrator using the appropriate keys written to the TOE by the SSCD provisioning service provider during SSCD preparation.

1.3.2.2 Cryptographic functions support

RSA key generation with specified cryptographic key sizes of 2048 bits (provided by JCOP).

Elliptic curve key generation with specified elliptic curve named NIST P-256 (provided by the cryptographic library).

Destruction of cryptographic keys by physically overwriting the keys by a special JavaCard method.

Digital signature generation using ECDSA algorithm with cryptographic key sizes of 256 bits (provided by the cryptographic library).

Digital signature generation using RSA algorithm with cryptographic key sizes of 2048 bit (provided by JCOP).

Random number generation according to class K3, SOF-high, of AIS 20 [AIS20] provided by JCOP.

All cryptographic functionality is provided by the platform, i.e. either by the cryptographic library (BSI-DSZ-CC-0608-2010) or by the operating system (BSI-DSZ-CC-0674-2010).

1.3.2.3 Protection against interference, logical tampering and bypass

The JCOP platform protects the TOE against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms.

The JCOP platform will provide protection against physical attack and perform self tests as described in [ST_JCOP].

Security domains are supported by the JavaCard platform used by the TOE underlying platform JCOP v. 2.4.1 revision 3.

The SmartApp SIGN 2.2 applet uses secure values and redundant storage mechanism as a measure to protect sensitive data as well as duplicated condition checks for flow control security.

Dedicated counter is used to limit the number of potential attacks and block the applet.

1.3.2.4 Access control / Storage and protection of data

Security attribute based access control. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification.

Keys: SmartApp SIGN 2.2 only stores keys in Java Card specified Key structures, which are protected by JCOP platform.

1.3.2.5 Trusted channel

Secure messaging in ENC_MAC mode (as specified by ICAO) with external applications as CGA and SCA.

PACE with NIST P-256 used to establish session keys for secure messaging. 3DES, ECDH and SHA-1 necessary for PACE implementation are provided by the platform.

3DES (112 bit keys) for en-/decryption (CBC) and (MAC) generation and verification (as specified by ICAO), all provided by the platform and used for secure messaging.

1.3.2.6 Security and life cycle management

Preparation including Personalization of the TOE is performed using the commands available in the preparation phase.

Communication between the TOE and external applications as CGA and SCA can be restricted to the use of secure messaging.

The test features of the JCOP platform are protected by ways described in JCOP platform.

The JCOP platform protects the TOE against malfunctions that are caused by exposure to operating conditions.

The cryptographic keys stored on TOE are protected from disclosure.

1.3.3 TOE description and use

The TOE comprises of

- the platform (NXP J2A080 v2.4.1 Revision 3), which consist of the integrated circuit (NXP P5CC080 V0B), the operating system (JCOP 2.4.1 Revision 3) and the cryptographic library,
- the applet containing the SSCD functionality (SmartApp SIGN 2.2),
- the associated guidance documentation (AGD_PRE.1, AGD_OPE.1).

Figure 1.2 presents a functional overview of the TOE in its distinct operational environments:

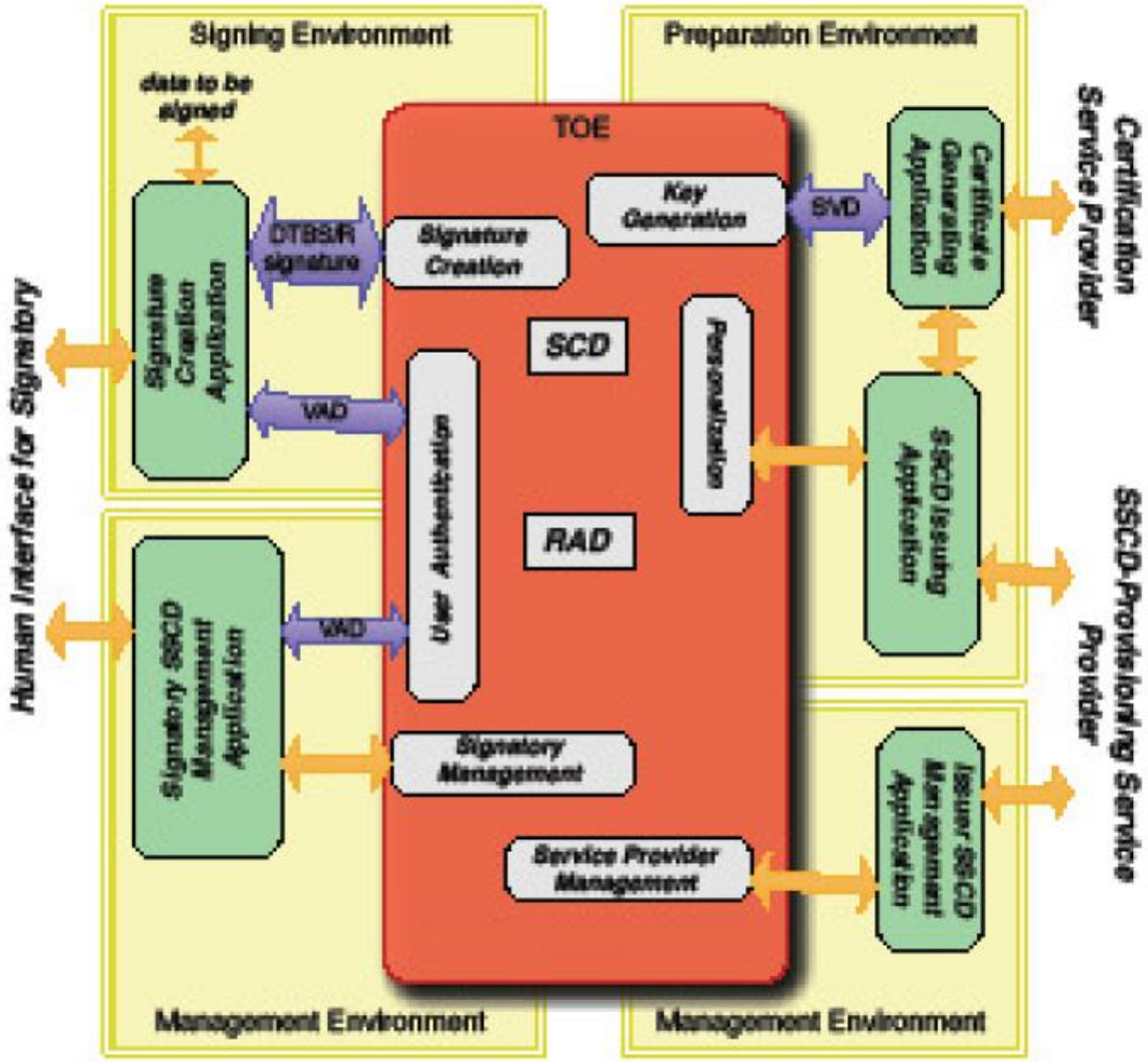
(i) The signing environment where it interacts with a signer through a signature creation application (SCA) to sign data after authenticating the signer as its signatory. The signature creation application provides a unique representation of data to be signed (DTBS/R) as input to the TOE signature creation function and obtains the resulting digital signature. Optionally, the TOE and the SCA may communicate through a trusted channel to ensure the integrity of the DTBS/R.

(ii) The preparation environment, where it interacts with a certification service provider through a certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with signature creation data (SCD) the TOE has generated. Optionally, the TOE may export the SVD through a trusted channel allowing the CGA to check the authenticity of the SVD. The preparation environment interacts further with the TOE to personalize it with the initial value of the reference authentication data (RAD).

(iii) The management environments where it interacts with the user or an SSCD provisioning service provider to perform management operations, e.g. for the signatory to reset a blocked RAD. A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing.

The signing environment, the management environment and the preparation environment are secure and protect data exchanged with the TOE.

Figure 1.2: Principal SSCD functions and operational environments



The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. The TOE provides interface (APDU) to SCA to select an SCD for use in the signature creation function of the SSCD and a mechanism to identify appropriate SCD[1]. SCA shall provide an interface to the signer to select an SCD for use in the signature creation function of the SSCD. The TOE protects the confidentiality of the SCD and restricts its use in signature creation to its signatory. The digital signature created with the TOE is a qualified electronic signature as defined in [Directive] if the certificate for the SVD is a qualified certificate (Annex I of [Directive]). Determining the state of the certificate as qualified is beyond the scope of this document.

The signature creation application shall protect the integrity of the input it provides to the TOE signature creation function as being consistent with the user data authorized for signing by the signatory. The SCA shall provide a signing function input which consist of computed hash value (DTBS/R) and identifier of used algorithm (OID).

[1] The TOE provides a set of elementary files for each SCD. This set allows to store information according to SCA needs. The stored information usually includes but is not limited to SCD identified and corresponding public key certificate.

The TOE stores signatory reference authentication data to authenticate a user as its signatory. The RAD is a PIN. The TOE protects the confidentiality and integrity of the RAD. The TOE receives the VAD from the signature creation application. The signature creation application protects the confidentiality of this data.

A certification service provider and a SSCD provisioning service provider interact with the TOE in the secure preparation environment to perform any preparation function of the TOE required before control of the TOE is given to the legitimate user. These functions include but are not limited to:
(i) initializing the RAD,
(ii) generating a key pair.

The TOE is a SSCD on a smart card. A smart card terminal shall be deployed that provides the required secure environment to handle a request for signatory authorization. A signature can be obtained on a document prepared by a signature creation application component running on personal computer connected to the card terminal. The signature creation application, after presenting the document to the user and after obtaining the authorization PIN initiates the digital signature creation function of the smart card through the terminal.

1.3.3.1 Target of evaluation

The TOE is a combination of hardware and software configured to securely create, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole life cycle as to be used in a signature creation process solely by its signatory.

The TOE provides the following functions:
(i) to generate signature creation data (SCD) and the correspondent signature verification data (SVD),
(ii) to export the SVD for certification,
(iii) to, optionally, receive and store certificate info,
(iv) to switch the TOE from a non-operational state to an operational state, and
(v) if in an operational state, to create digital signatures for data with the following steps:
- select an SCD,
- authenticate the signatory and determine its intent to sign,
- receive a unique representation of data to be signed (DTBS/R) and apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R.

The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the digital signature.

The TOE is prepared for the signatory's use by
(i) generating at least one SCD/SVD pair, and
(ii) personalizing for the signatory by storing in the TOE:
- the signatory’s reference authentication data (RAD)
- optionally, certificate info for at least one SCD in the TOE.

After preparation the SCD shall be in a non-operational state. Upon receiving a TOE the signatory shall verify its non-operational state and change the SCD state to operational.

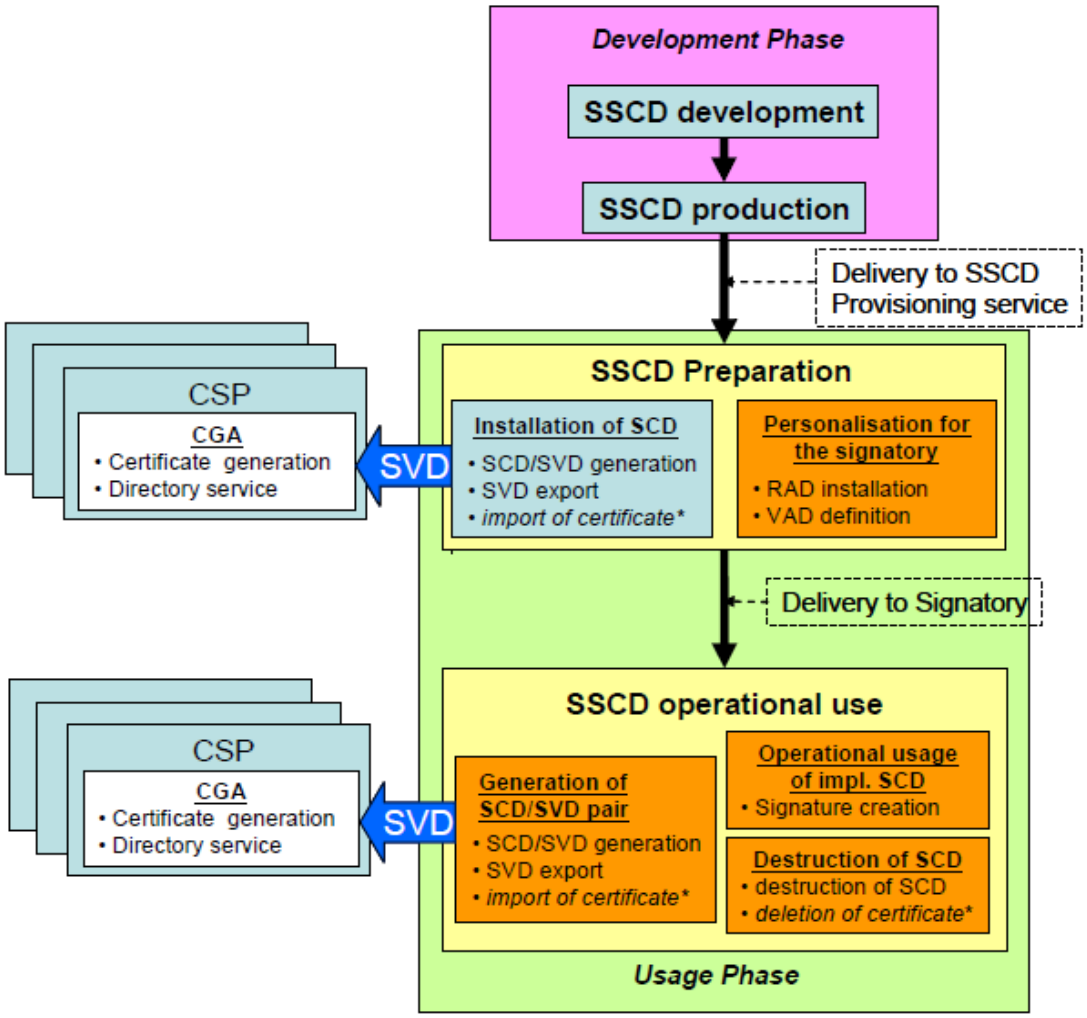
After preparation the intended, legitimate user should be informed of the signatory’s verification authentication data (VAD) required for use of the TOE in signing. As the VAD is a password or PIN, providing this information shall protect the confidentiality of the corresponding RAD.

If continued use of an SCD is no longer required the TOE will disable an SCD it holds, e.g. by erasing it from memory.

1.3.4 Life cycle

The TOE life cycle in Figure 1.3 distinguishes stages for development production, preparation and operational use. The development and production of the TOE (cf. CC part 1, para.139) together constitute the development phase of the TOE. The development phase is subject of CC evaluation according to the assurance life cycle (ALC) class. The development phase ends with the delivery of the TOE to an SSCD provisioning service provider. The functional integrity of the TOE shall be protected in delivering it to an SSCD provisioning service provider.

Figure 1.3: TOE life cycle



The TOE operational use stage begins when the signatory performs the TOE operation to enable it for use in signing operations. Enabling the TOE for signing requires at least one key stored in its memory. The TOE life cycle ends when all keys stored in it have been rendered permanently unusable. Rendering a key in the SSCD unusable shall include deletion of any stored corresponding certificate info.

1.3.4.1 Stage 1: SSCD development

SSCD development consists of two stages:
- Stage 1a: IC embedded software development – it covers activities of the IC Embedded Software Developer,
- Stage 1b: IC development – it covers activities of the IC Developer.

The IC Embedded Software Developer is in charge of:
(i) smartcard embedded software development including the development of Java Card applets,
(ii) specification of IC pre-personalization requirements, though the actual data for IC pre-personalization come from stages 2b, 3a, 3b.

The IC Developer:
(i) designs the IC,
(ii) develops IC Dedicated Software,
(iii) provides information, software or tools to the IC Embedded Software Developer,
(iv) receives the smartcard embedded software from the developer, through trusted delivery and verification procedures.

From the IC design, IC Dedicated Software and Smartcard Embedded Software, the IC Developer constructs the smartcard IC database, necessary for the IC photo mask fabrication.

Remark 1:
Stage 1a corresponds to the Phase 1 of the platform life cycle.

Remark 2:
Stage 1b corresponds to the Phase 2 of the platform life cycle.

1.3.4.2 Stage 2: SSCD production

SSCD production consists of two stages:
- Stage 2a: IC manufacturing – it covers activities of the IC Mask Manufacturer and IC Manufacturer,
- Stage 2b: IC packaging – it covers activities of the IC Packaging Manufacturer.

The IC Mask Manufacturer generates the masks for the IC manufacturing based upon an output from the smartcard IC database.

The IC Manufacturer is responsible for producing the IC through three main steps:
(i) IC manufacturing,
(ii) IC testing,
(iii) IC pre-personalization.

The IC Packaging Manufacturer is responsible for IC packaging and testing.

At the end of Stage 2 the TOE is finished.

Remark 1:
Applets which shall be present in the ROM need to be added to the ROM in the Stage 2a.

Remark 2:
Stage 2a corresponds to the Phase 3 of the platform life cycle.

Remark 3:
Stage 2b corresponds to the Phase 4 of the platform life cycle.

1.3.4.3 Stage 3: SSCD preparation

An SSCD provisioning service provider having accepted it from a manufacturer prepares the TOE for use and delivers it to its legitimate user. The preparation phase ends when the legitimate user of the TOE, having received it from an SSCD provisioning service enables an SCD it holds for use in signing.

During preparation of the TOE, as specified above, an SSCD provisioning service provider performs the following tasks:
(i) finishes the product, i.e. creates the instance of the SmartApp SIGN 2.2 applet,
(ii) obtains information on the intended recipient of the device as required for the preparation process and for identification as a legitimate user of the TOE;
(iii) generates a PIN and store this data as RAD in the TOE;
(iv) prepares information about the VAD for delivery to the legitimate user;
(v) optionally, activates a trusted channel functionality;
(vi) generates a certificate for at least one SCD either by:
- the TOE generating an SCD/SVD pair and obtaining a certificate for the SVD exported from the TOE, or
- initializing security functionalities in the TOE for protected export of the SVD and obtaining a certificate for the SVD after receiving a protected request from the TOE;

(vii) optionally, presents certificate info to the SSCD;
(viii) delivers the TOE and the accompanying VAD info to the legitimate user.

The SVD certification task of an SSCD provisioning service provider may support a centralized, pre-issuing key generation process, with at least one key generated and certified, before delivery to the legitimate user. Alternatively, or additionally, that task may support key generation by the signatory after delivery and outside the secure preparation environment. The TOE supports both key generation processes, for example with a first key generated centrally and additional keys generated by the signatory in the operational use stage. The signatory shall generate his RSA keys in a secure environment[2].

The TOE may provide a trusted channel to the CGA protecting the integrity of the SVD. This functionality may be activated during TOE preparation by the SSCD provisioning service.

Data required for inclusion in the SVD certificate at least includes (Annex II of [Directive]):
(i) the SVD;
(ii) the name of the signatory either
- a legal name, or
- a pseudonym together with an indication of this fact.

Before initiating the actual certificate signature the certificate generating application verifies the SVD received from the TOE by:
(i) establishing the sender as genuine SSCD,
(ii) establishing the integrity of the SVD to be certified as sent by the originating SSCD,
(iii) establishing that the originating SSCD has been personalized for the legitimate user,
(iv) establishing correspondence between SCD and SVD, and
(v) an assertion that the signing algorithm and key size for the SVD are approved and appropriate for the type of certificate.

The proof of correspondence between an SCD stored in the TOE and an SVD is implicit in the security mechanisms applied by the CGA.

[2] Secure environment for RSA key generation is defined in [AGD_OPE].

Prior to generating the certificate the certification service provider shall assert the identity of the signatory specified in the certification request as the legitimate user of the TOE.

SSCD preparation consist of three stages:
(i) Stage 3a: Composite product integration – it covers product finishing process,
(ii) Stage 3b: Personalization – it covers RAD storage and VAD delivery processes,
(iii) Stage 3c: SCD initialization – it covers generating SCD/SVD pair and export of SVD.

Remark 1:
The IC contains in its ROM the following applets:
- SmartApp SIGN 2.2 providing the SSCD functionality,
- SmartApp CRYPTO 1.6 providing cryptographic functionalities other than SSCD,
- SmartApp ID 2.2 providing a general purpose file system.

All these applets have been developed by PWPW S.A.

Remark 2:
During Stage 3: SSCD preparation, creation of SmartApp SIGN 2.2 applet instance is mandatory. This stage may also include the following additional activities:
- loading additional applets into the IC EEPROM,
- creating instances of additional applets.

Loading of additional applets and creation of their instances can be done only by PWPW S.A. within the secure environment of PWPW S.A. These additional applets will be tested before loading and they verifiably will not interfere with the SmartApp SIGN 2.2 applet.

The instances of additional applets, SmartApp CRYPTO 1.6 and SmartApp ID 2.2 are out of the scope of this certification and should not be used together with SmartApp SIGN 2.2.

Remark 3:
Stage 3a corresponds to the Phase 5 of the platform life cycle.

Remark 4:
Stage 3b corresponds to the Phase 6 of the platform life cycle.

Remark 5:
Stage 3c corresponds to the Phase 6 of the platform life cycle.

1.3.4.4 Stage 4: SSCD operational use

In this lifecycle stage the signatory can use the TOE to create advanced electronic signatures.

The signatory can also interact with the SSCD to perform management tasks, e.g. unblock a RAD value or use counter if the password/PIN in the reference data has been lost or blocked. Such management tasks require a secure environment.

The signatory can render an SCD in the TOE permanently unusable. Rendering the last SCD in the TOE permanently unusable ends the life of the TOE as SSCD.

The TOE support functions to generate additional signing keys and other functions necessary to securely obtain certificates for these new keys.

Remark:
Stage 4 corresponds to the Phase 7 of the platform life cycle.

2 Conformance claims

2.1 Common Criteria conformance claims

This security target claims to be conformant to the Common Criteria version 3.1, which comprises of:

(i) Common Criteria for Information Technology Security Evaluation (CC), V3.1, Part 1: Introduction and general model, Revision 3, July 2009.

(ii) Common Criteria for Information Technology Security Evaluation (CC), V3.1, Part 2: Security functional components, Revision 3, July 2009.

(iii) Common Criteria for Information Technology Security Evaluation (CC), V3.1, Part 3: Security assurance components, Revision 3, July 2009.

(iv) Common Methodology for Information Technology Security Evaluation (CEM), V3.1, Revision 3, July 2009,

as follows:

- Part 2 extended with
  - FIA_API Authentication proof of identity
  - FPT_EMSEC TOE emanation
  - FCS_RND Quality metric for random numbers
- Part 3 conformant

2.2 Protection profile claim

This security target claims conformance to the Common Criteria Protection Profile for Secure Signature Creation Device – Part 2: Device with key generation, BSI-CC-PP-0059, version 1.03 [PP_SSCD-KG].

The protection profile has been extended with provisions on trusted communication with certificate generation application and signature creation application. These provisions are taken from drafts of relevant protection profiles.

2.3 Package claim

This security target is package conformant to evaluation assurance level 4 augmented with ALC_DVS.2 and AVA_VAN.5.

2.4 Conformance rationale

This ST is claimed to be conformant to the above mentioned PP [PP_SSCD-KG]. A detailed justification is given in the following by

- describing some single aspects which are main issues of PP conformance, and
- describing differences between the ST and the PP.

2.4.1 Main aspects

- The TOE description in section 1.3 is based on the TOE overview of [PP_SSCD-KG, 5.4] and has only been added by product specific details.
- All definitions of the security problem definition in [PP_SSCD-KG, 3] have been included in the ST exactly in the same wording of the PP.
- All definitions of the security objectives in [PP_SSCD-KG, 8] have been included exactly in the same wording as the PP.

- The part of extended components definition of [PP_SSCD-KG, 4] has been included in the ST exactly in the same wording as the PP.
- All SFRs for the TOE from the [PP_SSCD-KG, 10.1] have been included in the ST exactly in the same wording as the PP.
- All text from introduction, TOE overview, TOE description has been taken from the PP and has been only added by product specific details.
- The security assurance requirements (SARs) are originally taken from SARs of CC 3.1 Part 3 according to the package conformance EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5. The addition of ALC_DVS.2 exceeds the augmentation defined by the PP.
- The structure of the ST is taken from the PP added by the section 7 (TOE summary specification) and section 8 (Statement of Compatibility concerning Composite Security Target).

2.4.2 Differences between ST and PP

The ST adds objectives and SFR's to those of the PP.

2.4.2.1 Security Objectives

The ST includes following additional security objectives for the TOE concerning trusted communication with certificate generation application and the signature creation application:

- *OT.TOE_SSCD_Auth: Authentication proof as SSCD*
- *OT.TOE_TC_SVD_Exp: TOE trusted channel for SVD export*
- *OT.TOE_TC_VAD_Imp: Trusted channel of TOE for VAD import*
- *OT.TOE_TC_DTBS_Imp: Trusted channel of TOE for DTBS import*

These additional objectives are provided because the TOE shall support a trusted channel for the authentication proof as SSCD, for the SVD export, the VAD import, and the DTBS/R import. The possibility of this additional functionality is allowed by the PP.

According to this functionality the following security objectives for the operational environment are included:

- *OE.CGA_SSCD_Auth: Preinitialisation of the TOE for SSCD authentication*
- *OE.CGA_TC_SVD_Imp: CGA trusted channel for SVD import*
- *OE.HID_TC_VAD_Exp: Trusted channel of HID for VAD export*
- *OE.SCA_TC_DTBS_Exp: Trusted channel of SCA for DTBS export*

2.4.2.2 Security Functional Requirements

All additional SFRs cover the above mentioned objectives concerning secure messaging functionality:

- *FIA_API.1: Authentication proof of identity*
- *FTP_ITC.1/SVD: Inter-TSF trusted channel*
- *FIA_UAU.1: Timing of authentication*
- *FDP_UIT.1/DTBS: Data exchange integrity*
- *FTP_ITC.1/VAD: Inter-TSF trusted channel – TC human interface device*
- *FTP_ITC.1/DTBS: Inter-TSF trusted channel – signature creation application*

2.5 Conformance statement

PP Conformant – The TOE meets the protection Profile [PP_SSCD-KG].

3 Security problem definition

3.1 General

3.1.1 Assets and objects

SCD

Private key used to perform a digital signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained.

SVD

Public key linked to the SCD and used to perform digital signature verification. The integrity of the SVD when it is exported must be maintained.

DTBS and DTBS/R

Set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the digital signature must be maintained.

Signature creation function

Function of the TOE to create digital signature for the DTBS/R with the SCD.

3.1.2 User and subjects acting for users

S.User

End user of the TOE who can be identified as Administrator or Signatory. In the TOE the subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

S.Admin

User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions. In the TOE the subject S.Admin is acting in the role R.Admin for this user after successful authentication as Administrator.

S.Sigy

User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents. In the TOE the subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as Signatory.

3.1.3 Threat agent

Attacker

Human or process acting on his behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the digital signature. An attacker has a high attack potential and knows no secret.

3.2 Threats

3.2.1 Threats from protection profile

T.SCD_Divulg: Storing, copying, and releasing of the 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: Derive the 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 the 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 the signature verification data

An attacker presents a forged SVD 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 a digital signature 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 the signatory intended to sign.

T.Sig_Forgery: Forgery of the electronic signature

Without use of the SCD an attacker forges data with associated digital signature and the verification of the digital signature by the SVD does not detect the forgery. 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.

3.2.2 Additional threats

None

3.3 Organizational security policies

3.3.1 Organizational security policies from protection profile

P.CSP_QCert: Qualified certificate

The CSP uses a trustworthy CGA to create a qualified certificate or non-qualified certificate ([Directive], Annex I of [Directive]) 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 ([Directive]), which is a qualified electronic signature if it is based on a valid qualified certificate (Annex I of [Directive])[3]. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the digital signature created with a SCD implemented in the SSCD that the signatory maintain under his 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 Annex III of [Directive]. This implies 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 his unrevoked certificate.

3.3.2 Additional organizational security policies

None

3.4 Assumptions

3.4.1 Assumptions from protection profile

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 creates and sends the DTBS/R of the data the signatory wishes to sign in a form appropriate for signing by the TOE.

3.4.2 Additional assumptions

None

[3] It is a non-qualified advanced electronic signature if it is based on a non-qualified certificate for the SVD.

4 Security objectives

4.1 Security objectives for the target of evaluation

4.1.1 Security objectives from protection profile

OT.Lifecycle_Security: Lifecycle security

The TOE shall detect flaws during the initialization, personalization and operational usage. The TOE shall provide functionality to securely destroy the SCD.

Application note:
The TOE allows storing more than one SCD. The SCD regeneration is not possible, i.e. in order to replace the existing SCD with a new one, the signatory (or the administrator) needs to destroy the existing SCD and then start the SCD generation. The signatory can destroy the SCD stored in the SSCD e.g. after expiration of the (qualified) certificate for the corresponding SVD.

OT.SCD/SVD_Gen: SCD/SVD generation

The TOE provides security features to ensure that authorized users only invoke the generation of the SCD and the SVD.

OT.SCD_Unique: Uniqueness of the signature creation data

The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation can practically occur only once and cannot be reconstructed from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible.

OT.SCD_SVD_Corresp: Correspondence between SVD and SCD

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating a digital signature creation with the SCD.

OT.SCD_Secrecy: Secrecy of the signature creation data

The secrecy of an SCD (used for signature creation) is reasonably assured against attacks with a high attack potential.

Application note:
The TOE keeps the confidentiality of the SCD at all times in particular during SCD/SVD generation, SCD signing operation, storage and by destruction.

OT.Sig_Secure: Cryptographic security of the digital signature

The TOE creates digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the digital signatures or any other data exported from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

OT.Sigy_SigF: Signature creation function for the legitimate signatory only

The TOE provides the digital signature creation function for the legitimate signatory only and protects the SCD against the use of others to create a digital signature. The TOE shall resist attacks with high attack potential.

OT.DTBS_Integrity_TOE: DTBS/R integrity inside the TOE

The TOE must not alter the DTBS/R This objective does not conflict with a signature creation process where the TOE applies a cryptographic hash function on the DTBS/R to prepare for signature creation algorithm.

OT.EMSEC_Design: Provide physical emanation security

Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.

OT.Tamper_ID: Tamper detection

The TOE provides system features that detect physical tampering of its components, and uses those features to limit security breaches.

OT.Tamper_Resistance: Tamper resistance

The TOE prevents or resists physical tampering with specified system devices and components.

4.1.2 Additional security objectives for the TOE concerning trusted communication with certificate generation application

OT.TOE_SSCD_Auth: Authentication proof as SSCD

The TOE shall hold unique identity and authentication data as SSCD and provide security mechanisms to identify and to authenticate themselves as SSCD.

OT.TOE_TC_SVD_Exp: TOE trusted channel for SVD export

The TOE shall provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA. The TOE shall enable the CGA to detect alteration of the SVD exported by the TOE.

4.1.3 Additional security objectives for the TOE concerning trusted communication with signature creation application

OT.TOE_TC_VAD_Imp: Trusted channel of TOE for VAD import

The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed.

OT.TOE_TC_DTBS_Imp: Trusted channel of TOE for DTBS import

The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS representation received from the SCA. The TOE must not generate digital signatures with the SCD for altered DTBS.

4.2 Security objectives for the operational environment

4.2.1 Security objectives from protection profile

OE.SVD_Auth: Authenticity of the SVD

The operational environment ensures the integrity of the SVD exported by the TOE to the CGA. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP.

OE.CGA_QCert: Generation of qualified certificates

The CGA creates a qualified certificate that includes, inter alias:
(i) the name of the signatory controlling the TOE,
(ii) the SVD matching the SCD stored in the TOE and controlled by the signatory,
(iii) the advanced signature of the CSP.

The CGA confirms with the created certificate that the SCD corresponding to the SVD is stored in a SSCD.

OE.SSCD_Prov_Service Authentic: SSCD provided by SSCD Provisioning Service

The SSCD provisioning service handles authentic devices that implement the TOE to be prepared for the legitimate user as signatory personalizes and delivers the TOE as SSCD to the signatory.

OE.HID_VAD: Protection of the VAD

If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface.

OE.DTBS_Intend: SCA sends data intended to be signed

The Signatory uses trustworthy SCA that:
(i) creates 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,
(ii) sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
(iii) attaches the signature produced by the TOE to the data or provides it separately.

OE.DTBS_Protect: SCA protects the data intended to be signed

The operational environment ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE.

OE.Signatory: Security obligation of the Signatory

The Signatory checks that the SCD stored in the SSCD received from SSCD provisioning service is in nonoperational state. The Signatory keeps his or her VAD confidential.

4.2.2 Additional security objectives for the operational environment concerning trusted communication with certificate generation application

OE.CGA_SSCD_Auth: Preinitialisation of the TOE for SSCD authentication

The CSP shall check by means of the CGA whether the device presented by the applicant for the (qualified) certificate examples holds unique identification as SSCD and is able to prove this identity.

OE.CGA_TC_SVD_Imp: CGA trusted channel for SVD import

The CGA shall detect alteration of the SVD imported from the TOE. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the (qualified) certificate.

4.2.3 Additional security objectives for the operational environment concerning trusted communication with signature creation application

OE.HID_TC_VAD_Exp: Trusted channel of HID 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.

OE.SCA_TC_DTBS_Exp: Trusted channel of SCA 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-representation cannot be altered undetected in transit between the SCA and the TOE.

4.3 Security objectives rationale

Security objectives specified in this Security Targets cover:
(i) core functionality of SSCD,
(ii) trusted communication with certificate generation application,
(iii) trusted communication with signature creation application.

Security objectives concerning the core functionality are taken from the protection profile [PP_SSCD-KG]) – their rationale is given in 4.3.1.

Rationale for security objectives concerning trusted communication with certificate generation application is given in 4.3.2.

Rationale for security objectives concerning trusted communication with signature creation application is given in 4.3.3.

4.3.1 Security objectives from protection profile

All threats described in this Security Target are coming from the protection profile. This Security Target introduces no new threats, no new OSPs and no new assumptions. Therefore the security objective rationale given in the protection profile remains in force.

4.3.2 Additional security objectives concerning trusted communication with certificate generation application

Security objectives coverage

Table 4.1: Security problem definition to security objectives mapping (CGA)

Threats, policies and assumptions / Security objectives	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OE.CGA_SSCD_Auth	OE.CGA_TC_SVD_Imp
T.SVD_Forgery		**X**		**(X)**[4]
P.Qsign	**X**		**(X)**[5]	

Security objectives sufficiency

T.SVD_Forgery (Forgery of the signature verification data) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by OT.TOE_TC_SVD_Exp, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by OE.CGA_TC_SVD_Imp, which provides verification of SVD authenticity by the CGA.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with qualified electronic signatures. P.QSign is additionally addressed by OT.TOE_SSCD_Auth and OE.CGA_SSCD_Auth. According OT.TOE_SSCD_Auth the TOE will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD based on theses pre-initialization to prove this identity as SSCD to the CGA. The OE.CGA_SSCD_Auth ensures that the CSP checks the proof of the device presented of the applicant that it is a SSCD.

[4] This additional OE does not mitigate the part of T.SVD_Forgery already mapped by security objectives of the TOE in the PP, but the part of T.SVD_Forgery already mapped by OE.SVD_Auth:" The operational environment ensures the integrity of the SVD exported by the TOE to the CGA...." from the PP.

[5] This additional OE does not satisfy the part of P.QSign already mapped by security objectives of the TOE in the PP, but the part of P.QSign already mapped by OE.CGA_QCert:" The CGA generates a qualified certificate that includes..." from the PP.

4.3.3 Additional security objectives concerning trusted communication with signature creation application

Security objectives coverage

Table 4.2: Security problem definition to security objectives mapping (SCA)

Threats, policies and assumptions / Security objectives	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_imp	OE.HID_TC_VAD_Exp	OE.SCA TC DTBS Exp
T.DTBS_Forgery		**X**		**(X)**[6]
T.SigF_Misuse	**X**	**X**	**(X)**[7]	**(X)**[8]

Security objectives sufficiency

T.DTBS_Forgery (Forgery of the DTBS representation) addresses the threat arising from modifications of the DTBS representation sent to the TOE for signing. The threat T.DTBS_Forgery is additionally addressed by the security objectives OT.TOE_TC_DTBS_imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS), which ensure that the DTBS representation is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE.

T.SigF_Misuse (Misuse of the signature-creation function of the TOE) addresses the threat of misuse of the TOE signature creation function by others than the signatory by creating a SDO for data the signatory has not decided to sign. This threat is additionally addressed by OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD), OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD), OT.TOE_TC_DTBS_imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS).

[6] This additional OE does not mitigate the part of T.SVD_Forgery already mapped by security objectives of the TOE in the PP, but the part of T.SVD_Forgery already mapped by the OE.DTBS_Protect: “The operational environment ensures that the DTBS/R cannot be altered...” from the PP.

[7] This additional OE does not mitigate the part of T.SigF_Misuse already mapped by security objectives of the TOE in the PP, but the part of T.SigF_Misuse already mapped by the OE.HID_VAD: “...this device will ensure confidentiality and integrity of the VAD...” from the PP.

[8] This additional OE does not mitigate the part of T.SigF_Misuse already mapped by security objectives of the TOE in the PP, but the part of T.SigF_Misuse already mapped by the OE.DTBS_Protect: “The operational environment ensures that the DTBS/R cannot be altered...” from the PP.

5 Extended component definition

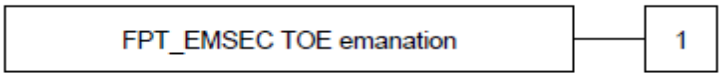
5.1 Definition of the family FPT_EMSEC

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMSEC belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation. The definition of the family FPT_EMSEC is taken from [PP_SSCD3].

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling



FPT_EMSEC.1 (TOE emanation) has two constituents:

(i) FPT_EMSEC.1.1 (Limit of emissions) requires to not emit intelligible emissions enabling access to TSF data or user data,

(ii) FPT_EMSEC.1.2 (Interface emanation) requires not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions identified that must be auditable if FAU_GEN (Security audit data generation) is included in a protection profile or security target.

FPT_EMSEC.1: TOE emanation

Hierarchical to: No other components.

Dependencies: No other components.

FPT_EMSEC.1.1
The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FPT_EMSEC.1.2
The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

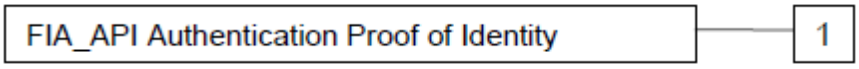
5.2 Definition of the Family FIA_API

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

Family behavior

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component leveling



FIA_API.1 (Authentication proof of identity) has only one constituent.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1 Authentication proof of identity

Hierarchical to: No other components.

Dependencies: No other components.

FIA_API.1.1
The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or role].

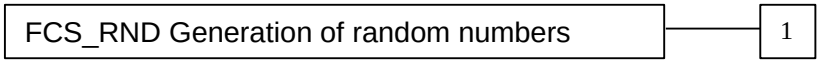
5.3 Definition of the Family FCS_RND

FCS_RND: Generation of random numbers

Family behavior

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component leveling:



FCS_RND.1
Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1
The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].

6 Security requirements

This section defines the functional requirements for the TOE and the assurance requirements for the TOE.

6.1 Security functional requirements

The permitted operations (assignment, iteration, selection and refinement) of the SFR are printed in underlined format.

6.1.1 Security functional requirements from protection profile

6.1.1.1 Class FCS: Cryptographic support

6.1.1.1.1 FCS_CKM.1: Cryptographic key generation

FCS_CKM.1.1/ECDSA

The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm NXP ECC key generation algorithm and specified cryptographic key sizes of 256 bits that meet the following: [ISO_15946-1].

Application note:
The following elliptic curve is used: NIST P-256.

FCS_CKM.1.1/RSA

The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm JCOP RSA key generation algorithm and specified cryptographic key sizes of 2048 bits that meet the following: [none].

6.1.1.1.2 FCS_CKM.4: Cryptographic key destruction

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys with zeros that meets the following: none.

6.1.1.1.3 FCS_COP.1: Cryptographic operation

FCS_COP.1.1/ECDSA

The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes of 256 bits that meet the following: [Signature Creation: ANSI_X9.62-2005, Public key cryptography for the financial services Industry: The elliptic curve digital signature algorithm (ECDSA), ANSI, 2005-11-16, section 7.3].

Application note:
The following elliptic curve is used: NIST P-256.

FCS_COP.1.1/RSA

The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes of 2048 bits that meet the following: [Signature Creation: PKCS#1 v1.5: RSA Encryption Standard, RSA Laboratories, 1993-11-01, section 10.1].

FCS_COP.1.1/PACE

The TSF shall perform secure messaging – session key agreement in accordance with a specified cryptographic algorithm PACE and cryptographic key sizes of 256 bits that meet the following: [Diffie-Hellman Key Exchange: ISO 11770-3, Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques, ISO, 2008, section 8.4] and [Session Keys Derivation with PACE: ICAO Technical Report: Machine Readable Travel Documents – Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, 2010-11-11, section 2.3].

Application note:
The following elliptic curve is used: NIST P-256.

FCS_COP.1.1/TDES

The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key sizes of 112 bits that meet the following: [Triple-DES encryption: ISO 11568-2: Banking – Key Management (Retail) – Part 2: Key Management Techniques for Symmetric Ciphers, ISO, 2005b, section 4.2], [Padding: ISO_9797-1, Information technology – Security techniques – Message Authentication – Part 1: Mechanisms using a block cipher, ISO, 1999, padding method 2, section 6.1.2] and [Triple-DES modes of operation: Doc9303-1: Machine Readable Travel Documents – Part 1: Machine Readable Passports – Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability, ICAO, 2006 section A5.4.1].

FCS_COP.1.1/MAC

The TSF shall perform secure messaging – 8 byte MAC generation and verification in accordance with a specified cryptographic algorithm ISO/IEC 9797-1 MAC algorithm 3 with block cipher DES, zero IV (8 bytes) and ISO/IEC 9791-1 padding method 2 and cryptographic key size of 112 bits that meet the following: [MAC generation ISO_9797-1, Information technology – Security techniques – Message Authentication – Part 1: Mechanisms using a block cipher, ISO, 1999, MAC algorithm 3, section 7.3], [Padding: ISO_9797-1, Information technology – Security techniques – Message Authentication – Part 1: Mechanisms using a block cipher, ISO, 1999, padding method 2, section 6.1.2] and [Triple-DES modes of operation: Doc9303-1: Machine Readable Travel Documents – Part 1: Machine Readable Passports – Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability, ICAO, 2006, section A5.4.2].

6.1.1.1.4 FCS_RND.1: Quality metric for random numbers

FCS_RND.1.1

The TSF shall perform random number generation in accordance with a specified cryptographic algorithm class K3 and cryptographic key size none that meet the following: [AIS20].

6.1.1.2 Class FDP: User data protection

The security attributes and related status for the subjects and objects are given in the Table 6.1.

Table 6.1: Security attributes and related status

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin – S.User acts as S.Admin R.Sigy – S.User acts as S.Sigy
S.User	SCD / SVD management	authorized, not authorized
SCD	SCD operational	no, yes
SCD	SCD identifier	arbitrary value
SVD	This Security Target does not define security attributes for SVD.	This Security Target does not define security attributes for SVD.

6.1.1.2.1 FDP_ACC.1: Subset access control

SCD/SVD generation SFP

FDP_ACC.1.1/SCD/SVD generation SFP

The TSF shall enforce the SCD/SVD generation SFP on:
(i) subjects: S.User,
(ii) objects: SCD, SVD,
(iii) operations: generation of SCD/SVD pair.

SVD transfer SFP

FDP_ACC.1.1/SVD transfer SFP

The TSF shall enforce the SVD transfer SFP on:
(i) subjects: S.User,
(ii) objects: SVD,
(iii) operations: export.

Signature creation SFP

FDP_ACC.1.1/Signature creation SFP

The TSF shall enforce the signature creation SFP on:
(i) subjects: S.User,
(ii) objects: DTBS/R, SCD,
(iii) operations: signature creation.

6.1.1.2.2 FDP_ACF.1: Security attribute based access control

SCD/SVD generation SFP

FDP_ACF.1.1/SCD/SVD generation SFP

The TSF shall enforce the SCD/SVD generation SFP to objects based on the following: S.User is associated with the security attribute "SCD/SVD management".

FDP_ACF.1.2/SCD/SVD generation SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute "SCD/SVD management" set to "authorized" is allowed to generate SCD/SVD pair.

FDP_ACF.1.3/SCD/SVD generation SFP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/SCD/SVD generation SFP

The TSF shall explicitly deny access of subjects to objects based on the rule: S.User with the security attribute "SCD/SVD management" set to "not authorized" is not allowed to generate SCD/SVD pair.

SVD transfer SFP

FDP_ACF.1.1/SVD transfer SFP

The TSF shall enforce the SVD transfer SFP to objects based on the following:
(i) the S.User is associated with the security attribute "Role",
(ii) the SVD.

FDP_ACF.1.2/SVD transfer SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Admin and R.Sigy are allowed to export SVD.

FDP_ACF.1.3/SVD transfer SFP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/SVD transfer SFP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

Signature creation SFP

FDP_ACF.1.1/Signature creation SFP

The TSF shall enforce the signature creation SFP on:
(i) the S.User is associated with the security attribute "Role",
(ii) the SCD with the security attribute "SCD Operational".

FDP_ACF.1.2/Signature creation SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Sigy is allowed to create digital signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes".

FDP_ACF.1.3/Signature creation SFP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/Signature creation SFP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User is not allowed to create digital signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no".

6.1.1.2.3 FDP_RIP.1: Subset residual information protection

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the resource de-allocation from the following objects: SCD.

6.1.1.2.4 FDP_SDI.2: Stored data integrity monitoring and action

The following data persistently stored by TOE have the user data attribute "integrity checked persistent stored data":
(i) SCD,
(ii) SVD (if persistent stored by TOE).

The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data".

FDP_SDI.2.1/Persistent

The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors on all objects, based on the following attributes: integrity checked persistent stored data.

FDP_SDI.2.2/Persistent

Upon detection of a data integrity error, the TSF shall:
(i) prohibit the use of the altered data,
(ii) inform the S.Sigy about integrity error.

FDP_SDI.2.1/DTBS

The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors on all objects, based on the following attributes: integrity checked stored data.

FDP_SDI.2.2/DTBS

Upon detection of a data integrity error, the TSF shall:
(i) prohibit the use of the altered data,
(ii) inform the S.Sigy about integrity error.

6.1.1.3 Class FIA: Identification and authentication

6.1.1.3.1 FIA_UID.1: Timing of identification

FIA_UID.1.1

The TSF shall allow:
(i) self test according to FPT_TST.1,
(ii) none
on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF mediated actions on behalf of that user.

6.1.1.3.2 FIA_UAU.1: Timing of authentication

FIA_UAU.1.1

The TSF shall allow:
(i) self test according to FPT_TST.1,
(ii) identification of the user by means of TSF required by FIA_UID.1,
(iii) none
on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF mediated actions on behalf of that user.

6.1.1.3.3 FIA_AFL.1: Authentication failure handling

FIA_AFL.1.1

The TSF shall detect when three unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD.

6.1.1.4 Class FMT: Security management

6.1.1.4.1 FMT_SMR.1: Security roles

FMT_SMR.1.1

The TSF shall maintain the roles R.Admin and R.Sigy.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.1.1.4.2 FMT_SMF.1: Security management functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:
(i) creation and modification of RAD,
(ii) enabling the signature creation function,
(iii) modification of the security attribute SCD/SVD management, SCD operational,
(iv) change the default value of the security attribute SCD Identifier,
(v) none.

6.1.1.4.3 FMT_MOF.1: Management of security functions behavior

FMT_MOF.1.1

The TSF shall restrict the ability to enable the function signature creation to R.Sigy.

6.1.1.4.4 FMT_MSA.1: Management of security attributes

FMT_MSA.1.1/Admin

The TSF shall enforce the SCD/SVD_generation_SFP to restrict the ability to modify the security attributes SCD/SVD management to R.Admin.

FMT_MSA.1.1/Signatory

The TSF shall enforce the signature creation SFP to restrict the ability to modify the security attributes SCD operational to R.Sigy.

6.1.1.4.5 FMT_MSA.2: Secure security attributes

FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for SCD/SVD management and SCD operational.

6.1.1.4.6 FMT_MSA.3: Static attribute initialization

FMT_MSA.3.1

The TSF shall enforce the SCD/SVD generation SFP, SVD transfer SFP and signature creation SFP to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the R.Admin to specify alternative initial values to override the default values when an object or information is created.

Application note:
The TOE does not allow specifying alternative initial values at all for security reasons. Therefore even the administrator cannot specify alternative initial values.

6.1.1.4.7 FMT_MSA.4: Security attribute value inheritance

FMT_MSA.4.1

The TSF shall use the following rules to set the value of security attributes:
(i) if S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute "SCD operational" of the SCD shall be set to "no" as a single operation,
(ii) if S.Sigy successfully generates an SCD/SVD pair the security attribute "SCD operational" of the SCD shall be set to "yes" as a single operation.

6.1.1.4.8 FMT_MTD.1: Management of TSF data

FMT_MTD.1.1/Admin

The TSF shall restrict the ability to create the RAD to R.Admin.

FMT_MTD.1.1/Signatory

The TSF shall restrict the ability to modify and unblock the RAD to R.Sigy.

6.1.1.5 Class FPT: Protection of TSF

6.1.1.5.1 FPT_EMSEC.1: TOE Emanation

FPT_EMSEC.1.1

The TOE shall not emit variations in power consumption or timing during command execution in excess of non-useful information enabling access to RAD and SCD.

FPT_EMSEC.1.2

The TSF shall ensure that unauthorized users are unable to use the following interface electrical contacts to gain access to RAD and SCD.

6.1.1.5.2 FPT_FLS.1: Failure with preservation of secure state

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur:
(i) self test according to FPT_TST fails,
(ii) applet life cycle inconsistency,
(iii) card tearing (unexpected removal of the card out of the CAD) and power failure,
(iv) abortion of a transaction in an unexpected context,
(v) violation of the firewall or JCVM SFPs,
(vi) unavailability of resources,
(vii) array overflow,
(viii) other runtime errors related to applet's failure (like uncaught exceptions),
(ix) Card Manager life cycle state inconsistency audited through the life cycle checks in all administrative operations and the self test mechanism on start up,
(x) abnormal environmental conditions (frequency, voltage, temperature),
(xi) physical tampering,
(xii) EEPROM failure audited through exceptions in the read/write operations and consistency/integrity check,
(xiii) corruption of check summed objects,
(xiv) illegal access to the previously defined Java objects audited through the firewall mechanism.

6.1.1.5.3 FPT_PHP.1: Passive detection of physical attack

FPT_PHP.1.1

The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2

The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

6.1.1.5.4 FPT_PHP.3: Resistance to physical attack

FPT_PHP.3.1

The TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.

Application note:
The TOE implements appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here:
(i) assuming that there might be an attack at any time,
(ii) countermeasures are provided at any time.

6.1.1.5.5 FPT_TST.1: TSF testing

FPT_TST.1.1

The TSF shall run a suite of self tests at the conditions during initial start-up at each power on to demonstrate the correct operation of the TSF.

FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of TSF.

6.1.2 Additional security functional requirements concerning trusted communication with certificate generation application

6.1.2.1.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1/CGA

The TSF shall allow:
(i) self test according to FPT_TST.1,
(ii) identification of the user by means of TSF required by FIA_UID.1,
(iii) establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD,
(iv) none
on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/CGA

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.1.2 FIA_API.1 Authentication proof of identity

FIA_API.1.1

The TSF shall provide an authentication mechanism to prove the identity of the SSCD.

6.1.2.1.3 FTP_ITC.1/SVD Inter-TSF trusted channel

FTP_ITC.1.1/SVD

The TSF shall provide a communication channel between itself and another trusted IT product CGA that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SVD

The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3/SVD

The TSF or the CGA shall initiate communication via the trusted channel for:
(i) user authentication according to FIA_UAU.1/CGA
(ii) none.

6.1.3 Additional security functional requirements concerning trusted communication with signature creation application

6.1.3.1.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1/SCA

The TSF shall allow:
(i) self test according to FPT_TST.1,
(ii) identification of the user by means of TSF required by FIA_UID.1,
(iii) establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD,
(iv) none
on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/SCA

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.1.2 FDP_UIT.1/DTBS Data exchange integrity

FDP_UIT.1.1/DTBS

The TSF shall enforce the signature creation SFP to receive user data in a manner protected from modification and insertion errors.

FDP_UIT.1.2/DTBS
The TSF shall be able to determine on receipt of user data, whether modification and insertion has occurred.

6.1.3.1.3 FTP_ITC.1/VAD Inter-TSF trusted channel – TC human interface device

FTP_ITC.1.1/VAD

The TSF shall provide a communication channel between itself and a remote trusted IT product HID that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/VAD

The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3/VAD

The TSF or the HID shall initiate communication via the trusted channel for:
(i) user authentication according to FIA_UAU.1/SCA,
(ii) none.

6.1.3.1.4 FTP_ITC.1/DTBS Inter-TSF trusted channel – signature creation application

FTP_ITC.1.1/DTBS

The TSF shall provide a communication channel between itself and a remote trusted IT product SCA that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/DTBS

The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3/DTBS

The TSF or the SCA shall initiate communication via the trusted channel for:
(i) signature-creation,
(ii) none.

6.2 Security assurance requirements

For the evaluation assurance level 4 augmented (EAL 4+) the Table 6.2 lists the relevant assurance classes and assurance components. The selected SARs are described in [CC_Part3].

Augmentation introduced in this Security Target and not required by the protection profile is bolded.

Table 6.2: Security assurance requirements

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
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_PRE.1 Preparative procedures
AGD_OPE.1 Operational user guidance
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 lifecycle model
ALC_TAT.1 Well defined development tools
ATE: Tests
ATE_COV.2 Analysis of coverage
ATE_DPT.1 Testing: basic modular design
ATE_FUN.1 Functional testing
ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment
AVA_VAN.5 Advanced methodical vulnerability analysis

6.3 Security requirements rationale

Security requirements specified in this Security Targets cover:
(i) core functionality of SSCD,
(ii) trusted communication with certificate generation application,
(iii) trusted communication with signature creation application.

Security requirements concerning the core functionality are taken from the protection profile [PP_SSCD-KG]) – their rationale is given in 6.3.1.

Rationale for security requirements concerning trusted communication with certificate generation application is given in 6.3.2.

Rationale for security requirements concerning trusted communication with signature creation application is given in 6.3.3.

6.3.1 Security requirements coverage of SFRs from protection profile

Table 6.3: Functional requirement to TOE security objective mapping

TOE Security objectives / TOE security functional requirement	OT.Lifecycle_Securrity	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.1	**X**		**X**	**X**	**X**						
FCS_CKM.4	**X**				**X**						
FCS_COP.1	**X**					**X**					
FCS_RND.1			**X**								
FDP_ACC.1/SCD/SVD generation SFP	**X**	**X**									
FDP_ACC.1/SVD transfer SFP	**X**										
FDP_ACC.1/Signature creation SFP	**X**						**X**				
FDP_ACF.1/ SCD/SVD generation SFP	**X**	**X**									
FDP_ACF.1/SVD transfer SFP	**X**										
FDP_ACF.1/Signature creation SFP	**X**						**X**				
FDP_RIP.1					**X**		**X**				
FDP_SDI.2/Persistent				**X**	**X**	**X**					
FDP_SDI.2/DTBS							**X**	**X**			
FIA_AFL.1							**X**				
FIA_UAU.1		**X**					**X**				
FIA_UID.1		**X**					**X**				

Table 6.3 (continued)

TOE Security objectives / TOE security functional requirement	OT.Lifecycle_Securrity	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FMT_MOF.1	**X**						**X**				
FMT_MSA.1/Admin	**X**	**X**									
FMT_MSA.1/Signatory	**X**						**X**				
FMT_MSA.2	**X**	**X**					**X**				
FMT_MSA.3	**X**	**X**					**X**				
FMT_MSA.4	**X**	**X**					**X**				
FMT_MTD.1/Admin	**X**						**X**				
FMT_MTD.1/Signatory	**X**						**X**				
FMT_SMR.1	**X**						**X**				
FMT_SMF.1	**X**						**X**				
FPT_EMSEC.1					**X**				**X**		
FPT_FLS.1					**X**						
FPT_PHP.1										**X**	
FPT_PHP.3					**X**						**X**
FPT_TST.1	**X**				**X**	**X**					

TOE security requirements sufficiency

All security functional requirements and security objectives described in 6.3.1 are coming from the protection profile except the SFR FCS_RND.1, so the rationale given in the protection profile remains in force, added by the following justification of FCS_RND.1:

FCS_RND.1 contributes to OT.SCD_Unique, because a random number generator with the required qualitiy of metric used by the key generation algorithms will ensure the uniqueness of the SCD.

6.3.2 Security requirements coverage of additional SFRs concerning trusted communication with certificate generation application

Table 6.4: Functional requirements to TOE security objective mapping (CGA)

TOE security functional requirement / TOE Security objectives	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp
FDP_ACC.1/ SVD transfer SFP		**X**
FDP_ACF.1/ SVD transfer SFP		**X**
FIA_API.1	**X**	
FIA_UAU.1/CGA	**X**	
FTP_ITC.1/SVD		**X**

TOE security functional requirements sufficiency

OT.TOE_SSCD_Auth (Authentication proof as SSCD) requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD, which is directly provided by FIA_API.1 (Authentication proof of identity) and by FIA_UAU.1/CGA (Timing of identification).

OT.TOE_TC_SVD_Exp (TOE trusted channel for SVD export) requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA, which is directly provided by:

(i) the SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD transfer SFP and FDP_ACF.1/SVD transfer SFP;

(ii) FTP_ITC.1/SVD inter-TSF trusted channel, which requires the TOE to provide a trusted channel to the CGA.

6.3.3 Security requirements coverage of additional SFRs concerning trusted communication with signature creation application

Table 6.5: Functional requirements to TOE security objective mapping (SCA)

TOE security functional requirement / TOE Security objectives	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_imp
FIA_UAU.1/SCA	**X**	
FDP_UIT.1/DTBS		**X**
FTP_ITC.1/VAD	**X**	
FTP_ITC.1/DTBS		**X**

TOE security functional requirements sufficiency

OT.TOE_TC_VAD_Imp (Protection of VAD provided by SCA) is provided by FTP_ITC.1/VAD to provide and by FIA_UAU.1/SCA to establish a trusted channel to protect the VAD provided by the HID to the TOE.

OT.TOE_TC_DTBS_imp (Trusted channel for DTBS) is provided by FTP_ITC.1/DTBS to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by FDP_UIT.1/DTBS, which requires the TSF to verify the integrity of the received DTBS.

6.3.4 Dependency rationale for security functional requirements

Dependency rationale for SFRs concerning core functionality of SSCD

For all security functional requirements and security objectives coming from the protection profile the dependency rationale given in the protection profile remains in force because no dependencies have been changed or are omitted.

The additional security function requirement FCS_RND.1 (the only additional SFR, which concerns the core functionality of SSCD) has no dependencies (see Table 6.6).

Dependency rationale for additional SFRs concerning trusted communication with certificate generation application and signature creation application

Table 6.6 provides an overview how all dependencies of all security functional requirements are solved.

Table 6.6: Functional requirements dependencies

Requirement	Dependencies	Fulfilled
RND		
FCS_RND.1	No dependencies	n.a.
CGA		
FDP_ACC.1/ SVD transfer SFP	FDP_ACF.1	FDP_ACF.1/SVD transfer SFP
FDP_ACF.1/ SVD transfer SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD transfer SFP, FMT_MSA.3
FIA_API.1	No dependencies	n.a.
FIA_UAU.1/CGA	FIA_UID.1	FIA_UID.1
FTP_ITC.1/SVD	No dependencies	n.a.
SCA		
FIA_UAU.1/SCA	FIA_UID.1	FIA_UID.1
FDP_UIT.1/DTBS	No dependencies	n.a.
FTP_ITC.1/VAD	No dependencies	n.a.
FTP_ITC.1/DTBS	No dependencies	n.a.

6.3.5 Security assurance requirements rationale

Evaluation Assurance Level 4

The assurance level for this protection profile is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions.

The TOE described in this protection profile is just such a product. Augmentation results from the selection of:
(i) AVA_VAN.5 Advanced methodical vulnerability analysis,
(ii) ALC_DVS.2 Sufficiency of security measures.

AVA_VAN.5: Advanced methodical vulnerability analysis

The TOE is intended to function in a variety of signature creation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure.

The component AVA_VAN.5 has the following dependencies:
(i) ADV_ARC.1 Security architecture description,
(ii) ADV_FSP.4 Complete functional specification,
(iii) ADV_TDS.3 Basic modular design,
(iv) ADV_IMP.1 Implementation representation of the TSF,

(v) AGD_OPE.1 Operational user guidance,
(vi) AGD_PRE.1 Preparative procedures,
(vii) ATE_DPT.1 Testing: basic design.

All of these dependencies are met or exceeded in the EAL4 assurance package.

ALC_DVS.2: Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. This assurance component is a higher hierarchical component to EAL 4 (only ALC_DVS.1 is required in EAL 4). Due to the nature of the TOE, there is a need to justify the sufficiency of these procedures to protect the confidentiality and the integrity of the TOE.

ALC_DVS.2 has no dependencies.

7 Target of evaluation summary specification

As described in the TOE description (see section 1.4) the TOE provides security services which can be associated into following groups:

- Access control/Storage and protection of data
- Security and life cycle management
- Cryptographic functions support
- PACE protocol
- Secure messaging
- Identification and authentication mechanisms
- Random number generation
- Protection against interference, logical tampering and bypass

The following overview shows how these TOE Security Services (ToSS) satisfy the security functional requirements specified in section 6.1.

7.1 TOE security functionality

7.1.1 Security functional requirement to TOE security functionality mapping

All functionalities of security services are described in sections from 7.1.2 to 7.1.7. Each functionality is identified by a number, which is unique in the context of specific security service. These numbers are used in Table 7.1 to provide detailed information on SFRs coverage.

Table 7.1: Functional requirement to TOE security functionality mapping

TOE security functional requirement / **TOE Security functionality**	SF.ACCESS	SF.CRYPTO	SF.TRUST	SF.USER	SF.RANDOM	SF.PROTECTION
FCS_CKM.1		**1,2**				
FCS_CKM.4		**3**				
FCS_COP.1		**4-7**	**1,2**			
FCS_RND.1		**1,2**	**1**		**1**	
FDP_ACC.1/SCD/SVD generation SFP	**1**					
FDP_ACC.1/SVD transfer SFP	**1**					
FDP_ACC.1/Signature creation SFP	**1**					
FDP_ACF.1/ SCD/SVD generation SFP	**1**					
FDP_ACF.1/SVD transfer SFP	**1**					
FDP_ACF.1/Signature creation SFP	**1**					
FDP_RIP.1		**1-3**				

Table 7.1 (continued)

TOE security functional requirement / **TOE Security functionality**	SF.ACCESS	SF.CRYPTO	SF.TRUST	SF.USER	SF.RANDOM	SF.PROTECTION
FDP_SDI.2/Persistent	**1**					
FDP_SDI.2/DTBS	**1**					
FDP_UIT.1/DTBS			**1**			
FIA_AFL.1				**1,3**		
FIA_API.1			**1**			
FIA_UAU.1			**1**	**1,3**		
FIA_UAU.1.1/CGA			**1**			
FIA_UAU.1.1/SCA			**1**			
FIA_UID.1				**1,3**		
FMT_MOF.1	**2**					
FMT_MSA.1/Admin	**1,2**			**4**		
FMT_MSA.1/Signatory	**1,2**			**2**		
FMT_MSA.2	**2**					
FMT_MSA.3	**2**			**4**		
FMT_MSA.4	**2**					
FMT_MTD.1/Admin	**2**			**4**		
FMT_MTD.1/Signatory	**2**			**2**		
FMT_SMR.1	**1,2**			**1-4**		
FMT_SMF.1	**1,2**			**2,4**		
FPT_EMSEC.1						**1**
FPT_FLS.1						**1**
FPT_PHP.1						**1**
FPT_PHP.3						**1**
FPT_TST.1						**1**
FTP_ITC.1/DTBS			**1**			
FTP_ITC.1/SVD			**1**			
FTP_ITC.1/VAD			**1**			

7.1.2 SF.ACCESS

1. Access control/Storage and protection of data

The TOE implements the subjects, objects, security attributes and rules according to the security attribute based access control. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification. The security status represents the current state possibly achieved after completion of the answer to reset and a possible protocol and parameter selection and / or a single command or a sequence of commands possibly performing authentication procedures. The security attributes, when they exist, define which actions are allowed, and under which conditions.

2. Security and life cycle management

After the production phase the TOE goes through the preparation phase before obtaining the operational phase. The preparation phase is functionality supported by both the JCOP platform and the SmartApp SIGN 2.2 applet

The Composite product integration, the product finishing process is part of the JCOP platform TOE preparation and will be performed according to the JCOP Administrator and User Guidance and [AGD_PRE]. The personalization steps covering RAD storage and VAD delivery processes are performed according [AGD_PRE]. SCD initialization covering generation of a SCD/SVD pair and the export of SVD may be done during the preparation phase or after delivery by the Signatory.

The SmartApp SIGN 2.2 applet keeps an internal state. This state, together with the access control mechanisms force the user into a specific role for the preparation and operational phases. The phases are controlled by appropriate APDU commands.

Remark:

During TOE preparation one key pair is generated. The signatory may generate additional key pair during the "SSCD operational use" phase. To be more precise during the "Stage 3a: Composite product integration" the maximum number of key pairs is specified and appropriate number of security environments ("empty key slots") is created. During "Stage 3b: Personalization" the administrator creates separate PIN (and PUK) for each security environment. They will be used later on to authenticate the signatory. During "Stage 3c: Initialization" the administrator generates one key pair ("he fills one slot"). The other security environments are left empty. The signatory may use them to generate additional key pair during the "SSCD operational use" phase. In order to replace the existing key with a new one it is necessary to delete the existing key before invoking the new key generation.

Neither the administrator nor the signatory may create additional security environments. Their number is specified during "Stage 3a: Composite product integration" and then is fixed.

7.1.3 SF.CRYPTO

Cryptographic functions support

The SF provides following cryptographic functionality which is totally provided by the platform:

1. ECDSA cryptographic key generation with the curve NIST P-256, key size of 256 bits and NXP ECC key generation algorithm using the SF.CryptoOperation functionality of the platform for generation and verification of an SCD/SVD pair.
2. RSA key generation with key size of 2048 bits and JCOP RSA key generation algorithm using the SF.CryptoOperation functionality of the platform for generation and verification of an SCD/SVD pair.
3. Destruction of EC and RSA keys by physically overwriting the keys by method ClearKey of Java Card API [Java_API].
4. EC digital signature generation and verification with SHA-256 as hash functions and cryptographic key sizes of 256 bit according to [ANSI_X.9.62] , section 7.3 and the used curve NIST P-256.
5. RSA digital signature generation and verification with SHA-256 as hash function and cryptographic key sizes of 2048 bit according to [PKCS#1], section 10.1.
6. EC digital signature generation and verification with SSL3_SHAMD5 as hash functions and cryptographic key sizes of 256 bit according to [ANSI_X.9.62], section 7.3 and the used curve NIST P-256.
7. RSA digital signature generation and verification with SSL3_SHAMD5 as hash function and cryptographic key sizes of 2048 bit according to [PKCS#1], section 10.1.

Application note:
Digital signatures with SSL3_SHAMD5 hash function are intended only for establishing SSL connections. Qualified electronic signatures shall use SHA-256 hash function.

These cryptographic mechanisms support:
- generating a SCD/SVD pair on authenticated user request,
- physical deleting of cryptographic keys on authenticated user request,
- creating digital signatures on authenticated signatory request – hash values are calculated and sent by SCA,
- ensuring SCD/SVD correspondence.

7.1.4 SF.TRUST

1. PACE protocol

This security service establishes trusted channels to the CGA or SCA.

Trusted channel establishment is performed according to [PACE] and uses following SF.CryptoOperation functionality provided by the platform:

- encryption of the transmitted message with Triple-DES in CBC mode and cryptographic key sizes of 112 bits that meets [ISO_11568-2], section 4.2 and [ISO_9797-1], section 6.1.2 and [Doc9303-1], section A.5.4.1;
- MAC generation and verification with ISO/IEC 9797-1 MAC algorithm 3 with block cipher DES, zero IV (8 bytes) and ISO/IEC 9791-1 padding method 2 and cryptographic key size of 112 bits according to [ISO_9797-1], section 7.3 and [ISO_9797-1], section 6.1.2 and [Doc9303-1], section A.5.4.2;
- Diffie-Hellman key agreement with EC over GF(p), the curve NIST P-256 and key size of 256 bits according to [ISO_11770-3], section 8.4 and [PACE], section 2.3;
- secure hash computation with SHA-1 according to [FIPS_180-1],
- random number generation according to [AIS20] class K3 provided by SF.RANDOM.

Application note:
SHA-1 is used only to derive session keys for secure messaging. It is not used for any other purpose.

2. Secure messaging

This security service provides secure messaging for protection of the communication data as the DTBS, authentication data as the VAD or for ensuring the integrity of the SVD.

The confidentiality and integrity is obtained by using the SF.CryptoOperation functionality of the platform:

- encryption and decryption of the transmitted message with Triple-DES in CBC Mode and cryptographic key sizes of 112 bit that meets [NIST_SP800-67] and [NIST_SP800-38A]
- MAC generation and verification with ISO/IEC 9797-1 MAC algorithm 3 with block cipher DES, zero IV (8 bytes) and ISO/IEC 9791-1 padding method 2 and cryptographic key size of 112 bit according to [ISO9797-1]

The communication may be initiated by another trusted IT product (i.e. CGA, SCA) or local user.

7.1.5 SF.USER

Identification and Authentication mechanisms

Provided mechanisms are:

1. *Authentication mechanism for the signatory*

   The authentication mechanism is based on the knowledge of a PIN or a password with a minimum length of 6 characters. For each SCD separate signatory's RADs (PINs or passwords) are assigned. If 3 consecutive authentication attempts fail the according RAD (PIN or password) is blocked.

   The authentication mechanism uses the platform (the class OwnerPIN of Java Card Framework) in order to perform all PIN operations.

2. *Signatory's RAD management functionality*

   The Signatory may modify or unblock the RAD. For this aim a second RAD (RAD2) for each SCD is provided which the Signatory can use to unblock the RAD. The Signatory cannot unblock the RAD2.

3. *Authentication mechanism for the Administrator*

   The administrator authentication is based on the challenge response mechanism, relying on Triple DES in CBC mode and a key of 168 bit length, using the platform functionality

SF.CryptoOperation. The Administrator's RAD (Triple DES key) is written to the TOE during SSCD Preparation by SSCD provisioning service provider. For all SCDs the same administrator's RAD is used. If 3 or more consecutive authentication attempts fail the RAD (Triple DES key) is blocked.

4. *Administrator's RAD management functionality*

   The Administrator creates the Signatory's RAD and RAD2. He may also generate a SVD/SCD key pair.

   Only the Administrator is allowed to unblock the Signatory's RAD2.

7.1.6 SF.RANDOM

1. Random number generation

This security functionality provides random challenges using the SF.CryptoOperation functionality of the platform, e.g. for authentication mechanisms. It uses random number generation according to [AIS20] class K3.

7.1.7 SF.PROTECTION

1. Protection against interference, logical tampering and bypass

Protection against interference, logical tampering and bypass are provided mainly by the platform. Security domains are supported by the JavaCard platform used by the TOE underlying platform JCOP v. 2.4.1 R3. The JCOP platform provides protection against physical attack and performs self tests as described in [ST_JCOP]. The JCOP platform protects the TOE against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms.

The SmartApp SIGN 2.2 applet implements additional mechanisms for protection against interference, logical tampering and bypass. Sensitive data is stored redundantly and controlled before use. Important flow-control conditions are checked twice. When an integrity error is detected, the operation is aborted and the dedicated counter is incremented. The counter itself is secured by redundant storage as well and controlled before execution of each command. Detection of integrity error of the counter value or reaching the number of five detected errors causes blocking of the TOE permanently. It cannot be reverted to operational state.

8 Statement of compatibility concerning composite Security Target

8.1 Separation of the platform TSF

This section describes the separation of relevant security functionality described in the ST of the platform (JCOP v. 2.4.1, Revision 3 [ST_JCOP]) being used by this ST and others. The security functionality provided by the platform is summarized in [ST_JCOP], section 1.3.1. The following table confronts the relevant security functionality of the platform with those of the composite TOE defined in the present ST. In Table 8.1 the security functions of the platform and of this composite ST are listed with the aim of separation of the platform functionality.

Table 8.1: Separation of the platform TSF (overview)

JCOP-functionality	Usage by TOE	References /Remarks
Cryptographic algorithms and functionality:		
3DES (112 and 168 bit keys) for en-/decryption (CBC and ECB) and MAC generation and verification (Retail-MAC and CBC-MAC)	Used by the TOE for: - PACE protocol - encryption/decryption, - MAC calculation, - administrator authentication.	Section 7.1.3, 7.1.4, 7.1.5
AES (Advanced Encryption Standard) with key length of 128, 192, and 256 bit for en-/decryption (CBC and ECB)	Not used by the TOE.	-
RSA and RSA CRT (1280 up to 2048 bits keys) for en-/decryption and signature generation and verification	RSA CRT signature described in [PKCS#1]	Section 7.1.3
RSA CRT key generation (1280 up to 2048 bits keys) in a secured environment	Used by the TOE.	Section 7.1.3
SHA-1, SHA-224, and SHA-256 hash algorithm	SHA-1 used by the TOE for secure messaging key derivation [FIPS 180-1]	Section 7.1.4
EC over GF(p) for key length between 192 and 320 bits	Used by the TOE	Section 7.1.3
Random number generation according to class K3 of AIS 20 [AIS20]**.**	Used by the TOE	Section 7.1.6

Table 8.1 (continued)

JCOP-functionality	Usage by TOE	References /Remarks
Java Card 2.2.2 functionality:		
Garbage Collection fully implemented with complete memory reclamation incl. compactification	Used by the TOE	-
Support for Extended Length APDUs	Used by the TOE.	-
GlobalPlatform 2.1.1 functionality:		
CVM Management (Global PIN) fully implemented: all described APDU and API interfaces for this feature are present	Not used by the TOE	-
Secure Channel Protocol (SCP01, and SCP02) is supported	Used by the TOE.	-
Further platform functionality		
Functionality as defined in the JC PP minimal configuration (i.e. no post-issuance installation and deletion of applets, packages and objects, no RMI, no logical channels, no on-card bytecode verification)	Not used by the TOE.	-
GP Card manager functionality for pre-issuance loading and management of packages and applets.	Used by Platform and TOE during TOE preparation	The GP Card Manager is used for executing applet preparation steps specified in the Guidance documentation.

In Table 8.2 only those SFRs of the platform are designated as “relevant” or “used by this composite ST”, which required functionality is also aimed or mentioned in the SFRs of this composite ST. This limit has been chosen although further security relevant functionality of the platform is necessary for the security of the whole composite TOE but the SFRs of this composite TOE are not directly concerned.

Table 8.2: Compatibility between SFRs of the platform ST and the composite ST

JCOP-SFRs	Usage by TOE / Not used	References /Remarks
FAU Security audit		
FAU_ARP.1 Security alarms	Not directly used	-[9]
FAU_SAA.1 Potential violation analysis	Not directly used	-[4]
FAU_SAS.1/SCP Audit Data Storage	Not used	-
FCS Cryptographic support		
FCS_CKM.1 Cryptographic key generation	Used EC, RSA	Section 7.1.3
FCS_CKM.2 Cryptographic key distribution	Used for setting administrator key	Section 7.1.5
FCS_CKM.3 Cryptographic key access	Used for checking key initialization state before use	Section 7.1.3, 7.1.4, 7.1.5
FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 Used method clearKey of Java Card API [Java_API]	Section 7.1.3
FCS_COP.1 Cryptographic operation 1. FCS_COP.1/TripleDES 2. FCS_COP.1/AES 3. FCS_COP.1/RSACipher 4. FCS_COP.1/DHKeyExchange 5. FCS_COP.1/DESMAC 6. FCS_COP.1/RSASignatureISO9796 7. FCS_COP.1/RSASignaturePKCS#1 8. FCS_COP.1/ECSignature 9. FCS_COP.1/SHA-1 10. FCS_COP.1/SHA-224 11. FCS_COP.1/SHA-256 12. FCS_COP.1/TDES_MRTD 13. FCS_COP.1/MAC_MRTD	Used operations: FCS_COP.1/TripleDES FCS_COP.1/RSACipher FCS_COP.1/ECSignature FCS_COP.1/DHKeyExchange FCS_COP.1/SHA-1 FCS_COP.1/TDES_MRTD FCS_COP.1/MAC_MRTD	Section 7.1.3, 7.1.4, 7.1.5
FCS_RNG.1 Quality metric for Random Numbers	Used	Section 7.1.6
FDP User data protection		
FDP_ACC.1 Subset access control	Not used	-
FDP_ACC.2 Complete access control	Not used	-
FDP_ACF.1 Security attribute based access control	Not used	-
FDP_ETC.1 Export of user data without security attributes	Not used	-
FDP_IFC.1 Subset Information flow control	Not used	-
FDP_IFF.1 Simple security attributes	Not used	-

[9] SFR indirectly supports FPT_FLS.1.

Table 8.2 (continued)

JCOP-SFRs	Usage by TOE / Not used	References /Remarks
FDP_ITC.1 Import of user data without security attributes	Not used	-
FDP_ITT.1/SCP Basic internal transfer protection	Not directly used	-[10]
FDP_RIP.1 Subset residual information protection	Not used	-
FDP_ROL.1 Basic rollback	Not used	-
FDP_SDI.2 Stored data integrity monitoring and action	Not directly used	-[4]
FIA Identification and authentication		
FIA_AFL.1 Authentication failure handling (/PIN, /CMGR)	Not used	-
FIA_ATD.1 User attribute definition	Not used	-
FIA_UAU.1 Timing of authentication	Not used	
FIA_UAU.3 Unforgeable authentication	Not used	
FIA_UAU.4 Single use authentication mechanisms	Not used	
FIA_UID.1 Timing of identification	Not used	
FIA_UID.2 User identification before any action	Not used	
FIA_USB.1 User-subject binding	Not used	
FMT Security Management		
FMT_LIM.1 Limited capabilities	Not used	-
FMT_LIM.2 Limited availability	Not used	-
FMT_MSA.1 Management of security attrib	Not used	-
FMT_MSA.2 Secure security attributes	Not used	-
FMT_MSA.3 Static attribute initialization	Not used	-
FMT_MTD.1 Management of TSF data	Not used	-
FMT_MTD.3 Secure TSF data	Not used	
FMT_SMF.1 Specification of Management Functions	Not used	-

[10] SFR indirectly supports FPT_EMSEC.1.

Table 8.2 (continued)

JCOP-SFRs	Usage by TOE / Not used	References /Remarks
FMT_SMR.1 Security roles	Not used	-
FPR Privacy		
FPR_UNO.1 Unobservability	Not used	-
FPT Protection of the TSF		
FPT_EMSEC.1 TOE emanation	FPT_EMSEC.1	Section 6.1.1.5.1
FPT_FLS.1 Failure with preservation of secure state	FPT_FLS.1	Section 6.1.1.5.1
FPT_ITT.1/SCP	Not directly used	-[4]
FPT_PHP.1 Passive detection of physical attack	FPT_PHP.1	Matches the homophone requirement of the platform
FPT_PHP.3 Resistance to physical attack	FPT_PHP.3	Matches the homophone requirement of the platform
FPT_RCV.3 Trusted Recovery	Not directly used	-[4]
FPT_RCV.4 Trusted Recovery	Not directly used	-
FPT_TDC.1 Inter-TSF basic TSF data consistency	Not used	-
FPT_TST.1 TSF testing	FPT_TST.1	Matches the homophone requirement of the platform
FRU Resource utilization		
FRU_FLT.2 Limited fault tolerance	Not directly used	-[4]
Trusted path/channels		
FTP_ITC.1 Inter-TSF trusted channel	FTP_ITC.1	Section 6.1.2.1.3, 6.1.3.1.3, 6.1.3.1.4

As shown in Table 8.3 the security assurance requirements of the composite evaluation represent a subset of the SARs of the underlying platform.

Table 8.3: Security assurance requirements of the platform ST and composite ST

Assurance class	Assurance component JCOP platform	Compare	Assurance component Composite ST
Development	ADV_ARC.1	=	ADV_ARC.1
	ADV_FSP.5	⊃	ADV_FSP.4
	ADV_IMP.1	=	ADV_IMP.1
	ADV_TDS.4	⊃	ADV_TDS.3
	ADV_INT.2	⊃	-
Guidance documents	AGD_OPE.1	=	AGD_OPE.1
	AGD_PRE.1	=	AGD_PRE.1
Life-cycle support	ALC_CMC.4	=	ALC_CMC.4
	ALC_CMS.5	⊃	ALC_CMS.4
	ALC_DEL.1	=	ALC_DEL.1
	ALC_DVS.2	=	ALC_DVS.2
	ALC_LCD.1	=	ALC_LCD.1
	ALC_TAT.2	⊃	ALC_TAT.1
Security Target evaluation	ASE_CCL.1	=	ASE_CCL.1
	ASE_ ECD.1	=	ASE_ ECD.1
	ASE_INT.1	=	ASE_INT.1
	ASE_OBJ.2	=	ASE_OBJ.2
	ASE_REQ.2	=	ASE_REQ.2
	ASE_SPD.1	=	ASE_SPD.1
	ASE_TSS.1	=	ASE_TSS.1
Tests	ATE_COV.2	=	ATE_COV.2
	ATE_DPT.3	⊃	ATE_DPT.1
	ATE_FUN.1	=	ATE_FUN.1
	ATE_IND.2	=	ATE_IND.2
Vulnerability assessment	AVA_VAN.5	=	AVA_VAN.5

8.2 Compatibility between the composite Security Target and the platform Security Target

The following mapping in Table 8.4 demonstrates the compatibility between the composite Security Target (the document at hand) and the platform Security Target [ST_JCOP] regarding security environments, security objectives, and security requirements. There is no conflict between security environments, security objectives, and security requirements of the composite Security Target and the platform Security Target.

Table 8.4: Compatibility between platform and composite ST

JCOP Definition	Equivalent in [ST_JCOP]	Remarks
Security objectives		
Platform objectives concerning the ESW	Pendant in ST with similar aim	Remarks
O.PROTECT_DATA	OT.SCD_Secrecy, OT.Tamper_ID OT.Tamper_Resistance	No contradictions
O.SIDE_CHANNEL	OT.EMSEC_Design	No contradictions
O.OS_DECEIVE	-	No contradictions
O.IDENTIFICATION	-	No contradictions
O.FAULT_PROTECT	OT.Tamper_Resistance	No contradictions
O.PHYSICAL	OT.Tamper_Resistance	No contradictions
O.RND	Used by the Composite ST according FCS_RND.1 (OT.SCD/SVD_Gen, OT.SCD_Unique)	No contradictions
O.SID	-	No contradictions
O.OPERATE	OT.SCD_Unique	No contradictions
O.RESOURCES	-	No contradictions
O.FIREWALL	-	No contradictions
O.REALLOCATION	-	No contradictions
O.SHRD_VAR_CONFID	-	No contradictions
O.SHRD_VAR_INTEG	-	No contradictions
O.ALARM	-	No contradictions
O.CIPHER	OT.SCD_Unique OT.Sig_Secure	No contradictions
O.PIN-MNGT	-	No contradictions
O.KEY-MNGT	OT.SCD_Secrecy, OT.SCD/SVD_Gen, OT.SCD_Unique	No contradictions
O.CARD-MANAGEMENT	-	No contradictions
O.SCP.RECOVERY	-	No contradictions
O.SCP.SUPPORT	-	No contradictions
O.SCP.IC	OT.Tamper_Resistance	No contradictions

Table 8.4 (continued)

JCOP Definition	Equivalent in [ST_JCOP]	Remarks
Relevant threats of the Platform ST vs. threats of the Composite-ST.		
Threats of Platform ST	Corresponding threats of comp. ST	
T.ACCESS_DATA	T.SCD_Divulg, T.SCD_Derive T.SVD_Forgery T.DTBS_Forgery T.Sig_Forgery	No contradictions
T.OS_OPERATE	T.SigF_Misuse	No contradictions
T.OS_DECEIVE	-	No contradictions
T.LEAKAGE	-	No contradictions
T.FAULT	-	No contradictions
T.RND	-	No contradictions
T.PHYSICAL	T.Hack_Phys	No contradictions
T.CONFID-JCSCODE	-	No contradictions
T.CONFID-JCS-DATA	-	No contradictions
T.INTEG-JCSCODE	-	No contradictions
T.INTEG-JCS-DATA	-	No contradictions
T.INTEG-APPLICODE	-	No contradictions
T.CONFID-APPLI-DATA	-	No contradictions
T.INTEG-APPLICODE	-	No contradictions
T.INTEG-APPLI-DATA	T.SCD_DivulgT.SCD_Deriv T.SVD_Forgery	No contradictions
T.SID.1	-	No contradictions
T.SID.2	-	No contradictions
T.EXE-CODE.1	-	No contradictions
T.EXE-CODE.2	-	No contradictions
T.RESOURCES	-	No contradictions

Table 8.4 (continued)

JCOP Definition	Equivalent in [ST_JCOP]	/Remarks
Assumptions (platform) significant for Composite-ST		
Assumptions of Platform ST	Relevancy for Composite-ST	
A.USE_DIAG phase 7	Significant: OE.CGA_TC_SVD_Imp, OE.HID_TC_VAD_Ex, OE.SCA_TC_DTBS_Exp	Consistent
A.USE_KEYS phase 7	Significant: A.SCA, A.CGA	Consistent
A.NO-DELETION phase 7	Guidance of the Platform-Developer for the Applet Developer has to be applied.	Consistent
A.NO-INSTALL phase 7	Guidance of the Platform-Developer for the Applet Developer has to be applied.	Consistent
A.VERIFICATION phases 1-6	Guidance of the Platform-Developer for the Applet Developer has to be applied.	Consistent
A.NATIVE	Guidance of the Platform-Developer for the Applet Developer has to be applied.	Consistent
	A.CGA A.SCA	Related to the operational phase, which is not in the focus of the platform. No contradictions
Platform security objectives for the environment and relevancy for the Composite ST		
OE of platform [ST_JCOP], section 4.2	Matching aspects in Composite-ST	Remarks
OE.USE_DIAG	Guidance of the Platform-Developer for the Applet Developer has to be applied.	Consistent
OE.USE_KEYS	Guidance of the Platform-Developer for the Applet Developer has to be applied.	Consistent
OE.NATIVE	Guidance of the Platform-Developer for the Applet Developer has to be applied.	Consistent
OE.NO-DELETION, OE.NO-INSTALL, OE.VERIFICATION	Guidance of the Platform-Developer for the Applet Developer has to be applied.	Consistent
Platform organizational security policies for the environment and relevancy for the Composite ST		
OSP of platform ST	Matching aspects in Composite-ST	Remarks
OSP.PROCESS-TOE	OT.TOE_SSCD_Auth	No contradictions

Bibliography

[Directive] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

[CC_Part1] Common Criteria for Information Technology Security Evaluation (CC), V3.1, Part 1: Introduction and general model, Revision 3, July 2009.

[CC_Part2] Common Criteria for Information Technology Security Evaluation (CC), V3.1, Part 2: Security functional components, Revision 3, July 2009.

[CC_Part3] Common Criteria for Information Technology Security Evaluation (CC), V3.1, Part 3: Security assurance components, Revision 3, July 2009.

[CC_CEM] Common Methodology for Information Technology Security Evaluation (CEM), V3.1, Revision 3, July 2009.

[PP_SSCD-KG] Common Criteria Protection profiles for Secure Signature Creation Device – Part 2: Device with key generation, version 1.03, BSI-CC-PP-0059, prEN 14169-1:2009, Dec. 2009

[PP_SSCD3] Common Criteria Protection Profile for Secure Signature Creation Device Type 3, BSI-PP-0006, version 1.05

[ST_P5Cx80] P5CD080 / P5CN080 / P5CC080 / P5CC073V0B, Security Target Lite, Rev. 1.7, 28 September 2009

[ST_CRYPTO] Crypto Library V2.6 on P5CD080V0B / P5CN080V0B / P5CC080V0B / P5CC073V0B, Security Target Lite, Rev. 2.3 – 12 November 2010

[ST_JCOP] NXP J3A080 and J2A080, Secure Smart Card Controller Revision 3, Security Target Lite, Rev. 01.02, 08.12.10

[Doc9303-1] ICAO Doc 9303: Machine Readable Travel Documents – Part 1: Machine Readable Passports – Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability, Sixth Edition, 2006

[PACE] ICAO Technical Report: Machine Readable Travel Documents – Supplemental Access Control for Machine Readable Travel Documents; Version 1.01; November 11, 2010

[ISO_9797-1] ISO/IEC 9797-1:1999: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher

[ISO_11568-2] ISO 11568-2:2005: Banking – Key Management (Retail) – Part 2: Key Management Techniques for Symmetric Ciphers

[ISO_11770-3] ISO 11770-3:2008: Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques

[ISO_15946-1] ISO 15946-1:2008: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General

[ANSI_X.9.62]	ANSI X9.62-2005: The Elliptic Curve Digital Signature Algorithm (ECDSA)
[ANSI_X.9.63]	ANSI X9.63:2001: Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography
[FIPS_180-1]	FIPS PUB 180-1: Secure Hash Standard, April 17th, 1995
[NIST_SP800-67]	NIST Special Publication 800-67 Version 1.1, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, May 2004, Revised 19 May 2008
[NIST_SP800-38A]	NIST SP 800-38A Recommendation for Block Cipher Modes of Operation, SP 800-38A 2001 ED, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, December 2001.
[PKCS#1]	PKCS#1 v1.5: RSA Encryption Standard, RSA Laboratories, 1993-11-01
[AIS20]	Anwendungshinweise und Interpretationen zum Schema, AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 1, 02.12.1999, Bundesamt für Sicherheit in der Informationstechnik
[Algorithms]	ETSI TS 102176-1 V2.0.0 (2007-11): Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
[Java_API]	Application Programming Interface, Java Card™ Platform, Version 2.2.2, March 2006, Sun Microsystems
[Java_VM]	Virtual Machine Specification, Java Card™ Platform, Version 2.2.2, March 2006, Sun Microsystems
[GP]	Global Platform, Card Specification, Version 2.1.1, March 2003
[AGD_PRE]	SmartApp SIGN 2.2: Preparative procedures, Version 2.2.11.0 (2011-09-07)
[AGD_OPE]	SmartApp SIGN 2.2: Operational user guidance, Version 2.2.16.0 (2011-09-07)

Acronyms

CAD	card acceptance device
CC	common criteria
CGA	certificate generation application
CSP	certification service provider
DPA	differential power analysis
DTBS	data to be signed
DTBS/R	data to be signed or its unique representation
EAL	evaluation assurance level
EF	elementary file
EEPROM	electrically erasable programmable read only memory
HID	human interface device
ICAO	International Civil Aviation Organization
IT	information technology
JCVM	java card virtual machine
NOS	native operating system
OID	object identifier
PIN	personal identification number
PP	protection profile
RAD	reference authentication data
RAM	random access memory
RNG	random number generation
ROM	read only memory
SAR	security assurance requirement
SCA	signature creation application
SCD	signature creation data
SCP	smart card platform
SCS	signature creation system
SDO	signed data object
SEF	security enforcing function
SF	security function
SFP	security function policy
SFR	security functional requirement
SOF	strength of function
SPA	simple power analysis

SSCD	secure signature creation device
ST	security target
SVD	signature verification data
TOE	target of evaluation
TSC	TOE scope of control
TSF	TOE security function
TSP	TOE security policy
TSFI	TSF interface
VAD	verification authentication data

Glossary

Security Evaluation terms

Application note

Optional informative part of the protection profile containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.

Common Criteria

A set of rules and procedures for evaluating the security properties of a product.

Evaluation Assurance Level

A set of assurance requirements for a product, its manufacturing process and its security evaluation specified by Common Criteria.

Protection Profile

A document specifying security requirements for a class of products that conforms in structure and content to rules specified by Common Criteria.

Security Target

A document specifying security requirements for a particular product that conforms in structure and content to rules specified by Common Criteria, which may be based on one or more Protection Profiles.

Target of Evaluation

Abstract reference in a document, such as a Protection Profile, for a particular product that meets specific security requirements.

Target of Evaluation Security Functions

Functions implemented by the TOE to meet the requirements specified for it in a Protection Profile or Security Target.

TSF data

Data created by and for the TOE, that might affect the operation of the TOE.

User data

Data created by and for the user, that does not affect the operation of the TSF.

Technical terms

Administrator

A user that performs TOE initialization, TOE personalization, or other TOE administrative functions.

Advanced electronic signature

An electronic signature which meets the following requirements:
(i) it is uniquely linked to the signatory,
(ii) it is capable of identifying the signatory,
(iii) it is created using means that the signatory can maintain under his sole control,
(iv) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Authentication data

Information used to verify the claimed identity of a user.

Certificate

An electronic attestation which links the SVD to a person and confirms the identity of that person.

Certificate info

Information associated with a SCD/SVD pair that may be stored in a secure creation device.

Certificate generation application

A collection of application elements which requests the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate.

Certification service provider

An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

Data to be signed

All electronic data to be signed (including both user message and signature attributes).

Data to be signed or its unique representation

Data received by a secure signature creation device as input in a single signature creation operation.

The DTBS/R is either:
(i) a hash-value of the data to be signed (DTBS), or
(ii) an intermediate hash-value of the first part of the DTBS and the remaining part of the DTBS, or
(iii) the DTBS.

Legitimate user

An user of a secure signature creation device who gains possession of it from an SSCD provisioning service provider and who may be authenticated by the SSCD as its signatory.

Notified body

An organizational entity designated by a member state of the European Union as responsible for accreditation and supervision of the evaluation process for products conforming to [PP_SSCD-KG] and for determining admissible algorithms and algorithm parameters.

Qualified certificate

A certificate which meets the requirements laid down in Annex I of [Directive] and is provided by a CSP who fulfils the requirements laid down in Annex II of [Directive].

Qualified electronic signature

An advanced signature that has been created with SSCD with a key certified with a qualified certificate according to [Directive], article 5, paragraph 1.

Reference authentication data

Data persistently stored by the TOE for authentication of a user as authorized for a particular role.

Secure signature creation device

Configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the [Directive].

Signatory

A person who holds a SSCD and acts either on his own behalf or on behalf of the natural or legal person or entity he represents.

Signature attributes

Additional information that is signed together with the user message.

Signature creation application

The application complementing an SSCD with a user interface with the purpose to create an electronic signature.

The signature creation application is software consisting of a collection of application components configured to:

(i) present the data to be signed (DTBS) for review by the signatory,
(ii) obtain prior to the signature process a decision by the signatory,
(iii) send a DTBS/R to the TOE if the signatory indicates by specific unambiguous input or action its intent to sign,
(iv) process the electronic signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.

Signature creation data

Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.

Signature creation system

The complete system that creates an electronic signature. The signature creation system consists of the SCA and the SSCD.

Signature verification data

Data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.

Signed data object

The electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.

SSCD provisioning service

A service to prepare and provide a SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD.

User

Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Verification authentication data

Data provided as input to a secure signature creation device for authentication by cognition or by data derived from user’s biometric characteristics.

Revision history

Version (date)	Changes
0.0.0 (2010-02-12)	Sent to BSI as annex to certification application
0.0.1 (2010-03-03)	Reworked
0.0.2 (2010-03-15)	Modified according to the new protection profile (SSCD Type 3)
	NXP comments addressed
0.0.3 (2010-03-18)	Chip type corrected
0.0.4 (2010-05-07)	Adopted according to the new protection profile (prEN 14169-2:2009)
0.0.5 (2010-05-14)	Extended with provisions on trusted communication for CGA and SCA
0.0.9 (2010-06-23)	TUV comments addressed
1.0.0 (2010-06-29)	Submitted for evaluation
1.0.1 (2010-06-29)	Editorial bug fixed
1.0.2 (2010-07-12)	Comments from Observation Report (OR V1) addressed
1.0.3 (2010-07-15)	Triple DES mode in SF.USER have been changed
1.0.4 (2010-07-16)	Editorial changes
1.0.5 (2010-07-16)	New SmartApp-SIGN version, SF.CRYPTO modified
1.0.6 (2010-08-02)	References given in FCS_COP.1.1 modified according to JCOP ST
1.0.7 (2010-08-10)	Comments from Observation Report (OR V2a) addressed
1.0.8 (2010-08-13)	Comments from Observation Report (OR V4) addressed
1.0.9 (2010-08-27)	Comments from Observation Report (OR V5) addressed
1.0.10 (2010-09-09)	Editorial bug in OE.Signatory fixed (SVD replaced with VAD)
2.2.11.0 (2011-07-12)	Document version numbering changed according to new scheme
	Mapping of SFRs to SFs in Table 7.1 corrected
	Updated bibliography references to NXP STs
	Typo corrected in 7.1.5
	Corrected reference for Crypto Library certification in 1.3.1 (BSI-DSZ-CC-0608-2010 changed to BSI-DSZ-CC-0709-2010)
	Updated logo of PWPW
2.2.12.0 (2011-07-25)	Some formatting problems resolved
2.2.13.0 (2011-09-07)	Updated bibliography entries for [PACE], [AGD_PRE] and [AGD_OPE]
	Updated reference to ICAO specification in FCS_COP.1.1/PACE
2.2.14.0 (2011-10-27)	Remarks 1 and 3 in the section 1.3.4.3 have been updated.

2.2.15.0 (2011-10-28)	Remark 1 in the section 1.3.4.3 has been updated to add information on applets developer.
2.2.17.0 (2011-11-04)	The SmartApp SIGN version given in Figure 1.1 has been corrected. In the section 1.3.4.3 Remarks 2 and 3 have been joined and reworked. The other remarks have been renumbered.
2.2.18.0 (2011-12-19)	Remark 2 in the section 1.3.4.3 has been updated to add information, that additional applets embedded in the ROM mask should not be used together with SmartApp SIGN.