BS EN 419251-1:2013

BSI Standards Publication

Security requirements for device for authentication

Part 1: Protection profile for core functionality

raising standards worldwide™

National foreword

This British Standard is the UK implementation of EN 419251-1:2013.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2013.

ISBN 978 0 580 74076 3

ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2013.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419251-1

March 2013

ICS 35.240.15

English Version

Security requirements for device for authentication - Part 1: Protection profile for core functionality

Profils de protection pour dispositif d'authentification - Partie 1: Dispositif avec import de clés

Sicherheitsanforderungen für Geräte zur Authentisierung - Teil 1: Schutzprofil für Kernfunktionalitäten

This European Standard was approved by CEN on 7 December 2012.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 419251-1:2013: E

Contents

Page

Figures

Tables

Foreword

This document (EN 419251-1:2013) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2013, and conflicting national standards shall be withdrawn at the latest by September 2013.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

EN 419251 contains the following parts:

— EN 419251-1, *Security requirements for device for authentication — Part 1: Protection profile for core functionality* (the present document);

— EN 419251-2, *Security requirements for device for authentication — Part 2: Protection profile for extension for trusted channel to certificate generation application*;

— EN 419251-3, *Security requirements for device for authentication — Part 3: Additional functionality for security targets*.

The present document was submitted to the Enquiry under the reference prEN 16248-1.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

1 Scope

This European Standard is a Protection Profile that defines the security requirements for an authentication device.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10181-2:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework*

ISO/IEC 15408-1:2009[1)], *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2[1)], *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3[1)], *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

3 Conformance

3.1 CC Conformance Claim

This Protection Profile (PP) is CC Part 2 extended and CC Part 3 conformant and written according to ISO/IEC 15408-1, -2, -3 and ISO/IEC 18045.

3.2 PP Claim

This PP does not claim conformance to any other Protection Profile.

3.3 Package Claim

The evaluation assurance level for this PP is EAL4-augmented with the assurance components AVA_VAN.5 and ALC_DVS.2.

3.4 Conformance Rationale

Since this PP is not claiming conformance to any other protection profile, no rationale is necessary here.

3.5 Conformance Statement

The conformance required by this PP is the demonstrable-PP conformance. This would facilitate conformance claim to both the PP “Authentication device” and other PPs for Security Target (ST) authors.

---

1) ISO/IEC 15408-1, -2 and -3 respectively correspond to *Common Criteria for Information Technology Security Evaluation*, Parts 1, 2 and 3.

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

4.1
Authentication Protocol sensitive data
data used in the process of authentication of the TOE by the external entity

Note 1 to entry: These data are linked to the Authentication private key, e.g. Authentication Certificate or APuK.

Note 2 to entry: Authentication Protocol sensitive data may be empty if the environment is trusted, and the holder public key known to the system.

4.2
Certificate
electronic attestation, which links the APuK to a person and confirms the identity of that person (as defined in the Directive [8], Article 2, Clause 9)

4.3
Certificate Info
information associated with an Authentication key pair that consists of either:

— a signer's public key certificate; or

— one or more hash values of a signer's public key certificate together the identifier of the hash function used to compute these hash values, and some information which allows the signer to disambiguate between several signers certificates

4.4
Configuration
set of groups

Note 1 to entry: Each configuration corresponds to one PP. It has its own rationale. See [2].

4.5
Group
set Assets, threats, objectives, and Requirements, addressing a specific function

Note 1 to entry: See [2].

4.6
Holder
legitimate holder of the authentication device

Note 1 to entry: See 9.2 for more details.

4.7
Issuer
user of the authentication device during personalisation

Note 1 to entry: See 9.2 for more details.

4.8
Protection Profile
PP
implementation-independent statement of security needs for a TOE

[SOURCE: ISO/IEC 15408-1:2009, Clause 4 "Terms and definitions", modified — in ISO/IEC 15408-1, the protection profile refers to a TOE type instead of a TOE in this document]

4.9
PP collection
document defining groups and configurations

4.10
Reference Authentication Data
usually called RAD, data stored inside the TOE and used as a reference to which the VAD will be compared

Note 1 to entry: This RAD can be biometrics data, a PIN, or a symmetric key. It can also be a combination of these factors. The RAD is not an Asset, it is TSF data.

4.11
Trusted channel
means by which a TSF and a remote trusted IT product can communicate with necessary confidence

[SOURCE: ISO/IEC 15408-1:2009, Clause 4 "Terms and definitions"]

4.12
Trusted Environment
environment that ensures the protection of sensitive data transfers between the TOE and a remote trusted IT product (resp. a user)

Note 1 to entry: A trusted (or untrusted) environment relates to the whole communication channel between the TOE and the remote trusted IT product (resp. the user).

4.13
Untrusted Environment
environment that does not ensure the protection of sensitive data transfers between the TOE and a remote trusted IT product (resp. a user)

Note 1 to entry: An untrusted (or trusted) environment relates to the whole communication channel between the TOE and the remote trusted IT product (resp. the user).

4.14
User
current User of the TOE

Note 1 to entry: The User can be the Issuer or the Holder.

4.15
Verifier
entity which is or represents the entity requiring an authenticated identity

Note 1 to entry: A verifier includes the functions necessary for engaging in authentication exchanges.

[SOURCE: ISO/IEC 10181-2:1996, modified — the full sentence at the end of the definition in the ISO/IEC has been turned into the present Note 1 to entry]

4.16
Verification Authentication Data
usually called VAD, data entered into the TOE and checked against the RAD as a means of authentication

Note 1 to entry: As the RAD, the VAD is not an Asset, it is TSF data.

5 Symbols and abbreviations

APSD	Authentication Protocol Sensitive Data
APrK	Authentication Private Key
APuK	Authentication Public Key
CA	Certificate Authority
CC	Common Criteria
OBKG	On-Board Key Generation
PIN	Personal Identification Number
PC	Personal Computer
PP	Protection Profile
RAD	Reference Authentication Data
SSCD	Secure Signature Creation Device
ST	Security Target
TOE	Target of Evaluation
VAD	Verification Authentication Data

6 Overview of the target of evaluation

6.1 TOE Type

The aimed objective is to define security requirements that an authentication device shall conform to in the perspective of a security evaluation. The Target of Evaluation (TOE [2)]) considered in this PP corresponds to a hardware device (such as, for example, a smart card or USB token) allowing its legitimate holder to authenticate himself when accessing an on-line service or to guarantee the origin authentication of data sent by the User to a distant agent [3)].

This PP has been constructed such as to make it possible for an ST writer to claim conformance to both this PP and the PP-SSCD [3], [4], [5], [6], [7] and easily merge these PPs into one ST.

6.2 TOE Usage

In order to connect to an on-line service with restricted access or send data whose origin should be authenticated, the Holder shall use his personal authentication device. The service provided by the device requires the prior input of authentication data by the Holder on a terminal device (as specified in 6.5). The authentication service included in the TOE relies solely on public-key cryptography mechanisms to allow the Holder to authenticate himself and access to the on-line service with restricted access or to enable the origin authentication of data sent by the Holder.

Note that authentication devices implementing shared key (i.e., symmetric-key) mechanisms for authentication purposes are therefore not considered in this PP.

6.3 Security Features of the TOE

The primary functionality of the TOE is to enable the Holder to authenticate himself in order to access an on-line service or guarantee the origin authentication of data sent by the Holder to a distant agent.

---

2) In the document the terms authentication device, device and TOE are equivalent.

3) He is a physical person that receives some authenticated data from the users.

To implement such services, a chain of trust shall be created between the TOE and the on-line restricted-access service or the agent in charge of authenticating the origin of data sent by the Holder. This trust chain is created in two phases:

— Authentication of the Holder by the TOE,

— Authentication of the TOE by the verifier on behalf of the Holder.

Part 3 of this European Standard splits the Authentication security features in 14 different groups that can be combined in different configurations according to the TOE described by the PP. See [2] for more details on the groups and configurations.

This PP corresponds to the minimum configuration. The APrK is loaded into the card in a secure environment. It is not generated on card. It comprises the following groups: Core, KeyImp, Trusted PersoAppli, Trusted AuthAppli, and Trusted Verifier.

— Core group

  Core group applies to all Configurations. It contains the basic security features for all Authentication devices.

— KeyImp group

  KeyImp group contains the security features directly linked to the import of the Authentication Private Key into the card.

— Trusted PersoAppli group

  Trusted PersoAppli group contains the security features directly linked to the transfer of sensitive data between the Personalisation application and the TOE, when these transfers take place in a protected environment, i.e. when potential attacks are countered by the environment.

— Trusted AuthAppli group

  Trusted AuthAppli group contains the security features directly linked to the transfer of sensitive data between the Authentication application and the TOE, when these transfers take place in a protected environment, i.e. when potential attacks are countered by the environment.

— Trusted Verifier group

  Trusted Verifier group contains the security features directly linked to the transfer of sensitive data between the Verifier and the TOE, when these transfers take place in a protected environment, i.e. when potential attacks are countered by the environment.

  This PP does not rely on the TOE to establish a trusted channel with the Verifier. This PP expects, but does not require, that the Authentication application establishes a trusted channel with the Verifier, using for instance SSL.

6.4 Examples of applications

6.4.1 E-government

The E-government applications can be services allowing a holder to access personal data ex: remaining points on the holder driving license, Tax declaration, and so on.

Such an application can be reached from PC at home. The Authentication application runs on the PC. The PC has to be properly protected against viruses and it shall be protected by a strong password so that the card holder can reasonably rely on his PC and Authentication application.

Communication between Authentication application and the TOE can then be regarded as secure for:

— Holder authentication;

— Acceptance of authentication of the TOE with the Authentication key pair.

The E-government application may get the certificate from the PKI. But the certificate can also be stored in the TOE.

The TOE can be provided to the holder with the Authentication Private key imported during Personalisation.

6.4.2 Multiple applications

e-administration for tax payment requiring signature + e-commerce only requiring authentication.

The e-administration and the e-commerce center may get the certificate from the PKI. But they may also rely on the authentication protocol to securely provide the public key, for example within a signed certificate.

Communication between Authentication application and the TOE may be regarded as secure for:

— Holder authentication;

— Selection of online server;

— Selection of a specific Authentication key pair;

— Acceptance of authentication of the TOE.

6.5 Required non-TOE Hardware and Software

The authentication device requires the services provided by a terminal device to enable the Holder to input his authentication data. Typically, this terminal device (e.g., a PINPad terminal) ensures the protection of authentication data input in confidentiality and integrity and its secure transfer to the TOE. The general features of this terminal along with the method employed to enable the input of authentication data are considered out of the TOE scope.

It should be however noted that the level of security of the whole operational system including the TOE depends on the security level of the TOE operational environment. In particular, an authenticated terminal device for the input and transfer of the Holder authentication data could be required in usage environments considered as untrusted.

6.6 Protection Profile Usage

The requirements present in this PP define the minimum security rules an ST of an authentication device shall conform to but are in no way exhaustive. It remains indeed possible to add functionalities or also refer to another PP. However, any modifications to this PP are restricted by the rules defined by the conformance as set forth in Clause 3.

In other respects, this PP aims at ensuring compatibility with PP-SSCD [3], [4], [5], [6], [7], in order to define complementary security requirements for products offering both authentication and signature services.

7 TOE Environment

7.1 Overall view

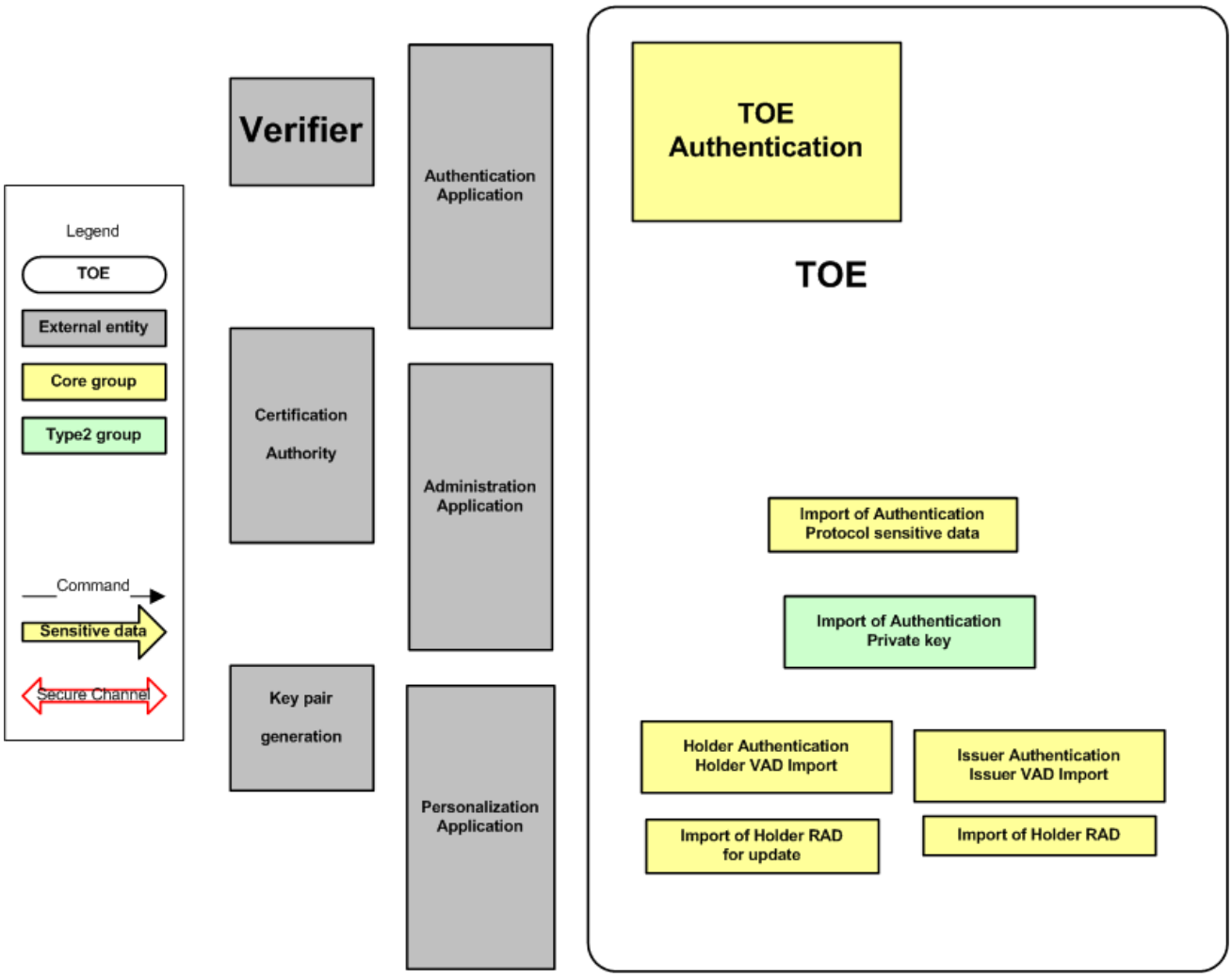

Figure 1 — TOE Security Features

Figure 1 shows all the security features of the TOE, in the Personnalisation and Usage environments.

The legend explains how different colors identity the security features of the different groups: Core and KeyImp. Further details on groups can be found in [2].

7.2 Personalisation application

7.2.1 General

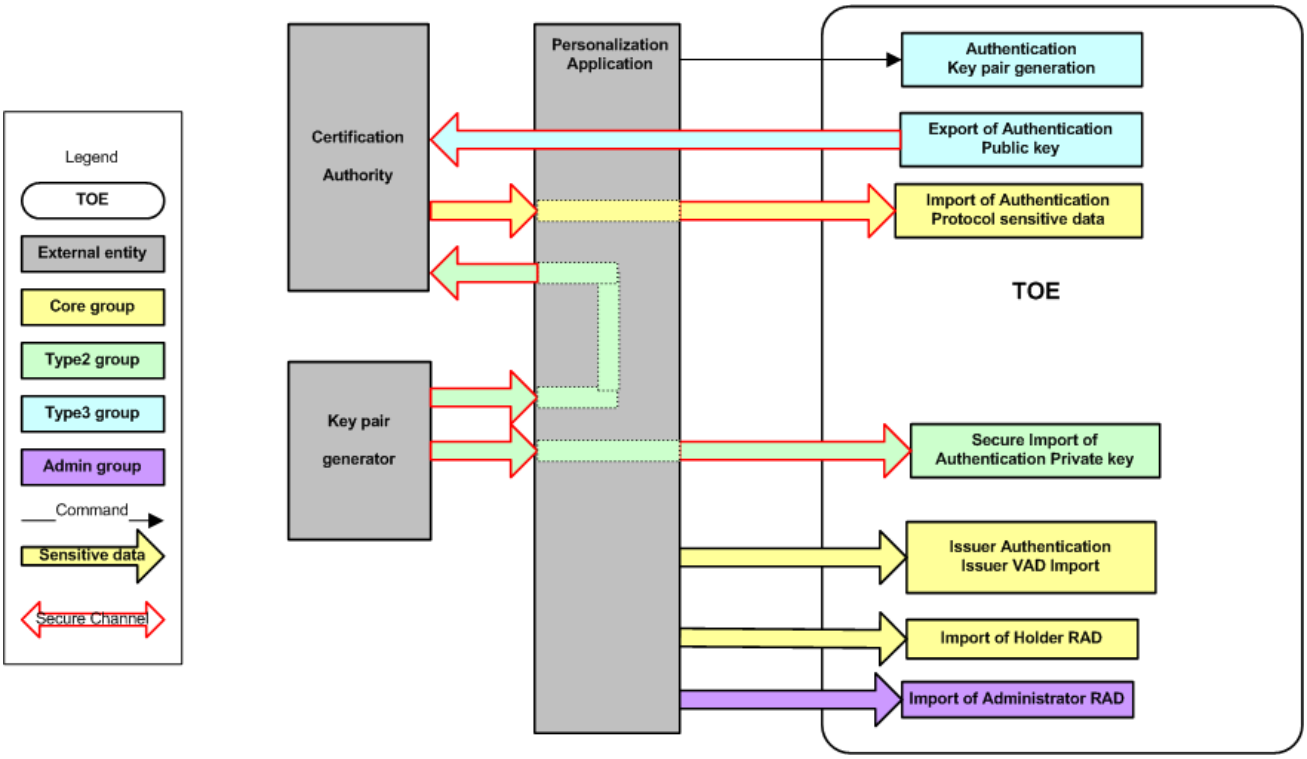

Figure 2 — Personalisation application environment

7.2.2 Functionalities

The Personalisation application interfaces the TOE at the Personalisation facility. These operations take place before the issuance of the TOE.

This application initialises all data specific to the end user. These data can include:

— APrK

— User RAD

If the TOE generates the APrK, the application retrieves the APuK and sends it to the CA that will generate the certificate.

If the TOE imports the APrK, the application retrieves the APuK and sends it to the TOE. The application also ensures that the APuK is securely - protected in integrity - sent from the key pair generator to the CA that generates the certificate.

7.2.3 Communication

As the environment is trusted, Transfer of sensitive data is protected by the environment.

However, as APrK is of special special sensitivity, a "Trusted channel" is always required to load it.

7.3 Authentication application

7.3.1 General

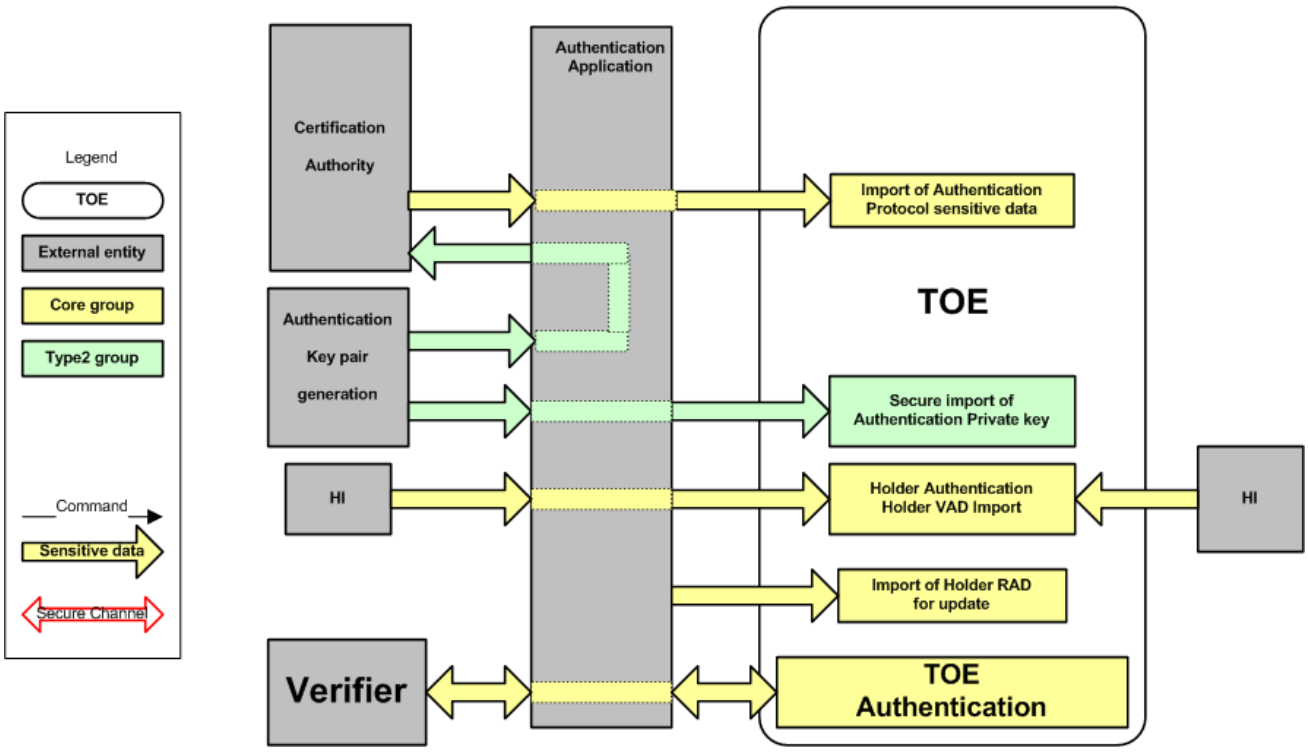

Figure 3 — Authentication application environment

7.3.2 Functionalities

The Authentication application interfaces the TOE when the holder needs to be authenticated by the Verifier. It can run on several devices:

— a PC at home to access online services (e-administration, e-commerce…).

— a specific device to identify and authenticate a card holder (police control…).

The TOE may contain several Authentication keys. It may also contain Signature keys. Therefore the Authentication application shall ensure a clear and secure human interface to prevent any confusion, when selecting the Verifier and the authentication key.

The VAD can also be entered via a separate Human Interface.

7.3.3 Communication

The Authentication application is in a trusted environment.

The TOE and the Authentication application exchange the following sensitive data:

— Import of Holder VAD for authentication;

— Import of Holder RAD for update;

— Request for authentication from a specific Verifier.

7.4 Verifier

7.4.1 Functionalities

The Verifier wants to authenticate the card holder.

The holder activates an “authentication application” on the PC.

The “authentication application” selects an online server (e-administration, e-commerce…), that request authentication and the authentication key.

According to the verifier selected by the holder, the “authentication application” shall allow the authentication protocol to be initiated with the selected Authentication key and the corresponding Authentication Protocol sensitive data.

If several different authentication keys are simultaneously present on the card, the holder has to select one according to the Verifier he intends to be authenticated by. The IT environment, mainly the Authentication application helps the holder to securely select the correct authentication key. It is up to the IT environment to indicate the link between the selected authentication key and the Certificate of the corresponding key. For this purpose, and to allow mobility, it may be useful to store the Certificate or Certificate Info on the card by this is not mandatory.

7.4.2 Communication

Communication between the TOE and the verifier is the authentication protocol.

This PP does not cover the data exchanges that may take place after this authentication.

This authentication may take place in an untrusted environment. Therefore the TOE has to counter the threats identified in ISO/IEC 10181-2 as relay and replay attacks, via the authentication protocol.

7.5 Key Generator

7.5.1 Functionalities

The Key Generator generates a public key pair. The private key is securely transmitted to the TOE.

The environment shall make sure that the public key is securely transmitted to the CA for the generation of the certificate.

7.5.2 Communication

Communication between the Key generator and the TOE shall be secured.

During the personalisation phase, which takes place in a trusted environment, this communication can be split in two phases:

— Transfer from the Key Generator to the Personalisation application, then

— Transfer from the Personalisation application to the TOE.

7.6 Certification Authority — Functionalities

The certification authority generates a Certificate, based on the public key it receives.

As the key is generated off TOE, the Environment shall ensure that the public key is securely transferred to the CA.

The public key shall be transferred with the correct identity data to make sure that no false certificate can be produced. The CA shall prevent the generation of certificates with wrong identity. A possible mean is the “Proof Of Possession” mechanism.

The certificate may then be sent to the card. It can prevent some attacks on authentication protocols.

8 Life Cycle

8.1 Overview

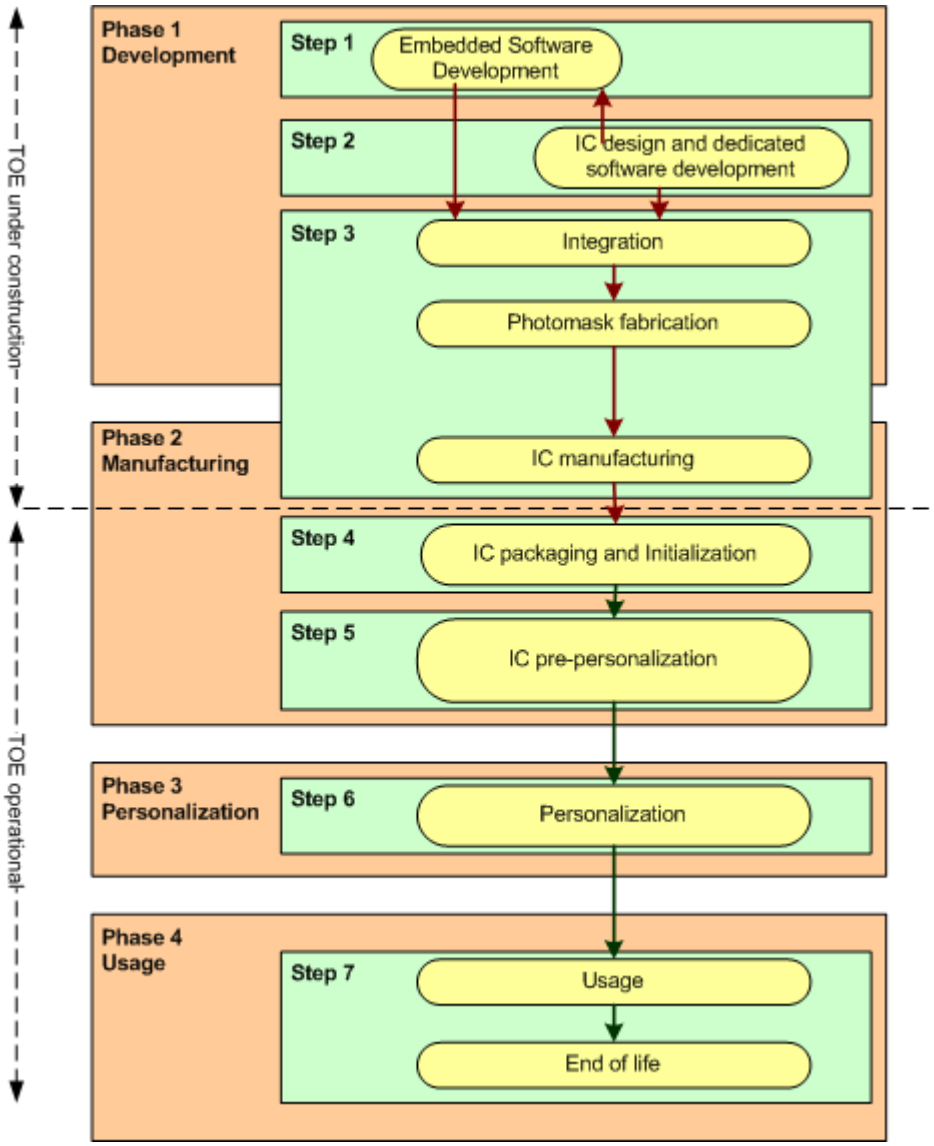

Figure 4 — TOE Life Cycle

This figure represents two views of the life-cycle:

a) An “end-user” view made of four phases, focusing on the following main logical phases:

   1) Development phase: IC design, and embedded software development;

2) Manufacturing phase: from IC manufacturing to card or token manufacturing, including patch loading, application creation and pre-personalisation;

3) Personalisation phase: loading of all data related to the TOE holder;

4) Operational use phase: TOE used by its legitimate holder to authenticate himself to a Verifier.

b) A business view made of seven steps, focusing more on the different trades and actors involved in smartcard business. For example, the company in charge of IC manufacturing may be different from the one in charge of IC packaging, as well as from the one in charge of packaging, initialisation, pre-personalisation, not considering all other actors involved in this phase: antenna supplier, booklet supplier. The definition of the content of each step and the associated supply chain vary from one provider to another and the picture is just indicative.

Referring to the life-cycle, the **evaluated product** is the product that comes out of the IC manufacturing, test and possible pre-personalisation operations (**step 3**).

At this step, the product shall already be self-protected before delivery to step 4 and all steps after. This means that if a patch is to be loaded on the product to fix a security flaw, this operation has to be performed during the IC manufacturing step, i.e. in an environment that is under control of the evaluation and assessed through assurance class of Common Criteria related to the development environment (ALC).

The following options are also important to keep in mind:

— creation of the application;

— applet instantiation for a JavaCard;

— loading of the *pre-personalisation data* in the chip.

These operations may or may not be performed within the IC manufacturer secure premises covered by the evaluation scope, depending on the business organisation for the TOE production. They may even be performed during the personalisation phase (step 6) under the control of the issuing state.

However, if they are not performed within the IC manufacturer secure premises, the procedures to perform these operations have to be well defined, and successfully evaluated through assurance tasks of Common Criteria related to guidance analysis (class AGD).

More generally, all steps that come after step 3 are to be covered by guidance (secure delivery, secure handling, etc.).

The ST writer can choose to include step 4 and also step 5 inside the perimeter of the evaluation. In this case the premises where these operations take place will be covered by ALC, not AGD and sensitive operations such as the loading of patches invoving Security Functions can be done in the included steps.

8.2 Pre-Personalisation phase

Pre-Personalisation is the final phase under the control of the Smart card manufacturer.

Application initialisation

During Pre-personalisation, the Smartcard manufacturer initialises the application.

Import of Issuer RAD

The manufacturer imports the Issuer RAD that will be used in the next phase to authenticate the Issuer.

8.3 Personalisation phase

8.3.1 General

The Personalisation phase is under the control of the Issuer.

8.3.2 Personalisation application

Issuer authentication

The Issuer authenticates himself to the TOE using a RAD.

Import of Holder RAD

This function is mandatory in Personalisation.

This function initialises the RAD.

When biometrics is used, this operation requires the holder.

Import of Authentication Protocol sensitive data

This function is optional as these data may be empty.

It is only necessary if APrK / APuK key pair is generated on TOE during Personalisation. In this case the TOE shall import the APSD, if not null, after the CA has generated the certificate.

Import of Authentication private key.

This function is not necessarily used in Personalisation.

The TOE can also be issued without APrK.

8.4 Usage phase — Authentication application

8.4.1 General

The Authentication application interfaces the TOE to the holder.

During the usage phase, the Holder can perform the following operation on the authentication device:

Holder Authentication to the TOE,

The Holder authenticates himself to the TOE using a RAD.

When the TOE is used both for Authentication and Signature and when the RAD is a PIN, the TOE shall provide at least one PIN for Signature and one PIN for Authentication.

Import of the private key

This function is not necessarily used in Usage phase.

APrK can also be imported in Personalisation phase.

The TOE can also be issued with APrK.

Import for update of holder RAD

This function allows the holder to update his RAD. This operation is required when the Holder receives its TOE, except when RAD is biometrics. It gives the holder, exclusive control of the authentication function of the TOE.

Allow Authentication by Verifier

This function enables the Holder to accept or deny the authentication by the Verifier.

8.4.2 Verifier

Authentication by Verifier

This function allows the Verifier to authenticate the TOE and therefore its holder.

Other functions following the Authentication, such as exchange of data with the Verifier, are out of the scope of this PP.

9 Security problem definition

9.1 Assets

9.1.1 General

The description of each asset provides the type of protection required for each asset (*"Protection"* part).

RAD, VAD, Authentication Protocol sensitive data are not Assets, they are TSF data. The ST writer shall specify these TSF data.

9.1.2 Assets protected by the TOE

D.AUTHENTICATION

This asset represents the authentication function itself and all the benefits that can result from the authentication. These benefits can be:

— communication data between the authentication device and an access-restricted on-line service

— data or goods located in an access-restricted area

— rights provided in country by an ID card

9.1.3 Sensitive assets of the TOE

D. AUTHENTICATION_PRIVATE_KEY

This asset corresponds to the private key generated outside of the TOE and imported in the TOE or generated inside the TOE. The private key is associated with a public key and a public-key certificate. In addition, the private key shall remain consistent with its corresponding public key.

Protection: integrity and confidentiality.

Application notes:

This asset is used by the authentication service running on the TOE.

The TOE can contain several Authentication Keys, dedicated to different distant entities. In case of multiple Authentication Keys, the holder can be authenticated by the same RAD or by different RAD.

D.IDENTIFICATION_DATA

These data correspond to Holder identification data. These are the data to be authenticated.

These data can be present on the TOE. They are included in the certificate.

Protection: integrity and confidentiality.

9.2 Users

Issuer

During the personalisation phase of the device, the Issuer can perform the following operations:

— Authenticate himself with his own VAD.

— Import the holder RAD into the TOE.

— Import the Authentication Protocol sensitive data into the TOE.

— Import the Authentication private key into the TOE.

— Request an Authentication key pair generation inside the TOE

— Export the Authentication public key from the TOE.

The Issuer is the only person who can perform the above administration commands during the personalisation phase. During the usage phase, the issuer cannot perform import operations anymore.

Holder

Holder of the authentication device (legitimate holder). The Holder accesses by means of his authentication device an access-restricted on-line service that requires an authentication, or sends data whose origin shall be authenticated by an agent. The Holder knows the authentication data allowing him to access the authentication service in the device and unlock the associated private key (these actions can only be performed during the usage phase).

During the usage phase, the Holder can perform the following operation on the authentication device:

— Authenticate himself with his own VAD.

— Import the Authentication Protocol sensitive data into the TOE.

— Import his own RAD.

— Allow the TOE to authenticate itself to the external verifier.

The Holder cannot perform these functions during the personalisation phase.

The Holder can be a single person or a group of people. This shall be specified in the ST.

Verifier

The user “Verifier” represents either a distant device or a distant agent.

During the usage phase, the Verifier can perform the following operations:

— Authenticate the TOE, using the authentication protocol based on APrK.

— Perform other operations such as opening a trusted channel and transmitting and receiving data. These other operations are not in the scope of this PP.

9.3 Threats

Threats present in this section only target the TOE security and do not concern the services provided by the TOE since such services are considered in the security problem definition as organisational security policies environment elements. The considered threat agents are the following:

— Attackers trying to illegitimately authenticate to the on-line service and therefore have access to data or services they are not entitled.

Issuers are not considered as attackers (assumption A.ISSUER).

T.MASQUERADE_USER

An attacker illegitimately retrieves, modifies or deletes data that enable the Holder or the Issuer to authenticate himself to the TOE (i.e., RAD).

For example, an attacker may import RAD with known corresponding VAD in order to be able to use the authentication device to authenticate to an on-line service or to a distant agent.

These data can be modified when they are stored in the TOE or during their transfer to the TOE.

Threatened assets: D.AUTHENTICATION.

T.PRIV_KEY_DISCLOSURE

An attacker discloses the value of the private key in order, for instance, to illegitimately authenticate subsequently as the device holder to an on-line service or a distant agent.

The private key can be disclosed when it is stored in the TOE or during its transfer from the Key Generator to the TOE.

Threatened assets: D.AUTHENTICATION_PRIVATE_KEY.

T.PRIVATE_KEY_MODIF

An attacker modifies the value of the private key when it is stored in the TOE or during its transfer to and from the TOE.

Threatened assets: D.AUTHENTICATION_PRIVATE_KEY

T.COMM_EAVESDROP

An attacker passively eavesdrops on a legitimate communication between the authentication device and a terminal to obtain information that could be used to derive the value of sensitive information stored in the device. Such eavesdropping is conducted without the knowledge of the device holder.

Threatened assets: D.AUTHENTICATION_PRIVATE_KEY.

T.USER_TRACKING

An attacker illegitimately manages to track or identify the device holder, without the knowledge of the latter. This threat has been identified for contactless cards.

Threatened assets: D.IDENTIFICATION_DATA.

T.MASQUERADE_TOE

An attacker illegitimately retrieves, modifies or deletes data that enable the TOE to authenticate itself to the verifier (*Authentication Protocol sensitive data*).

ISO/IEC 10181-2 is the result of a study on Authentication in Open Systems. It identifies and describes the following threats:

— Replay attacks on the same verifier, see ISO/IEC 10181-2:1996, 5.8.1.1

— Replay attacks on a different verifier, see ISO/IEC 10181-2:1996, 5.8.1.2

— Relay attacks initiated by an intruder, see ISO/IEC 10181-2:1996, 5.8.2.1

— Relay attacks in which an intruder responds, see ISO/IEC 10181-2:1996, 5.8.2.2

Threatened assets: D.AUTHENTICATION.

9.4 Organisational security policies

9.4.1 Provided services

OSP.AUTHENTICATION_PROTOCOL

The TOE shall implement a public-key cryptography protocol by making use of the private key.

The authentication protocol may optionally use other data, the “Authentication Protocol sensitive data” stored on TOE, such as the public key and the certificate. This protocol shall enable the authentication device to be authenticated by the verifier.

OSP.PKI

The TOE shall be used in an environment providing a PKI that generates a certificate for the Authentication Private Key. The PKI also manages the validity of Certificates, their end of validity, their possible revocation, in such a way that the Verifier can rely on the Certificate provided by the PKI.

9.4.2 Other services

OSP.PERSO_CORE

During the personalisation phase, the issuer shall be allowed to:

— Generate on card or Import the Authentication key pair

— Import the Authentication Protocol sensitive data,

— Import the Holder RAD

OSP.CRYPTO

The cryptographic mechanisms of the TOE shall conform to the rules and recommendations defined by the relevant Certification Body.

9.5 Assumptions

A.ISSUER

It is assumed that the Issuer is non hostile and competent. He possesses the resources required for his tasks and is trained to conduct activities he is responsible for.

It is assumed that the Issuer RAD has been securely imported previously, in the pre-personalisation phase.

A.HOLDER

It is assumed that the Holder of the device (*i.e.*, the legitimate device holder) does not disclose his authentication data allowing him to authenticate to the device.

A.CERTIF_VERIF

It is assumed that the Verifier verifies the validity of the Holder certificate before considering the Holder as authenticated and granting to the service. The certificate verification includes in particular the verification that the current date belongs to the validity period of the certificate and the verification that the certificate has not been revoked.

A.CERTIF_AUTH

It is assumed that the Certification Authority issuing the certificate for the authentication service implements practices that conform to an approved certification policy.

A.COPY

It is assumed that the confidential assets of the TOE cannot be compromised by copies of such assets that may exist outside the TOE.

A.CRYPTO

The cryptographic keys generated outside the TOE and imported in the TOE are supposed to be generated in conformance to the rules and recommendations defined by the relevant Certification Body.

A.KEY_PAIR_GENERATION

When the Authentication key pair is generated outside the TOE, it is assumed that this generation is performed by an authorised person in a way that preserves the confidentiality of the private key.

10 Security objectives

10.1 General

The following sensitive data have to be protected against disclosure and/or modification when they are imported and/or exported to and from the TOE. They can be protected either by the TOE or by the environment.

Table 1 — Protection of sensitive data

Data	IT device	transfer	Protection type	Protected by
Authentication Private key	**KeyGenIT**	**Import**	**I,C**	**TOE**
Authentication Protocol sensitive data	**PersoAppli**	**Import**	**I**	**environment**
	AuthAppli	**Import**	**I**	**environment**
Issuer VAD	**PersoAppli**	**Import**	**I,C**	**environment**
Holder RAD	**HI**	**Import**	**I,C**	**environment**
	AuthAppli	**Import**	**I,C**	**environment**
	PersoAppli	**Import**	**I,C**	**environment**
Holder VAD	**HI**	**Import**	**I,C**	**environment**
	AuthAppli	**Import**	**I,C**	**environment**

10.2 Security objectives for the TOE

10.2.1 Provided service

OT.DEVICE_AUTHENTICATION

The authentication of the device (on behalf of the Holder) by the access-restricted on-line service or by the distant agent authenticating data sent by the Holder shall be ensured by the TOE. This authentication shall implement a public-key cryptographic protocol by making use of the private key stored in the TOE (and optionally of the corresponding certificate).

The TOE shall enable the import of the Authentication Protocol sensitive data, if it is not yet inside the TOE.

10.2.2 Authentication to the TOE

OT.AUTH_USER

The TOE shall provide mechanisms to authenticate the Holder and the Issuer.

Holder authentication shall use a RAD / VAD mechanism. The number of failed Holder authentication attempts shall be limited.

Before the user authenticates himself to the TOE, the TOE shall not deliver data that could enable the holder identification.

10.2.3 TOE management

OT.PROTECTIONS

The TOE shall be able to protect any sensitive data, Assets and TSF data, against unauthorised disclosure and/or modification. This protection applies when the data are on the TOE.

OT.HOLDER_RAD

The TOE shall be able to import the Holder RAD and to replace it. Such import shall be allowed only in the following cases:

— in the personalisation phase, when the Issuer is authenticated,

— in the usage phase, when the Holder is authenticated.

OT.AUTHENTICATION_PRIVATE_KEY_IMPORT

The TOE shall be able to import the authentication private key.

The import of the private key is only allowed:

— in the personalisation phase, when the Issuer is authenticated,

— in the usage phase, when the Holder is authenticated.

The import of the private key shall be protected against disclosure and modification.

When a new key is imported, the previous key shall be deleted.

10.3 Security objectives for the operational environment

OE.ISSUER

The Issuer shall possess the resources required for his tasks and is trained to conduct activities he is responsible for.

OE.HOLDER

The Holder of the device (*i.e.*, the legitimate device holder) shall not disclose his authentication data allowing to authenticate himself to the device.

OE.CERTIF_VERIF

The access-restricted “verifier” shall verify the validity of the Holder certificate before considering the Holder as authenticated and granting to the service. The certificate verification shall include in particular:

— the verification that the current date belongs to the validity period of the certificate,

— the verification that the certificate has not been revoked.

OE.CERTIF_AUTH

The Certification Authority issuing the certificate for the authentication service shall implement practices that conform to an approved certification policy, in particular concerning:

— the verification of the certificate subject identity,

— the verification of possession of the corresponding private key by the subject,

— the certificate generation,

— the certificate issuance.

OE.COPY

The confidential sensitive data, Assets and TSF data, of the TOE shall not be compromised by copies of such data that may exist outside the TOE.

OE.CRYPTO

The cryptographic mechanisms used outside the TOE, to protect sentitive assets of the TOE shall conform to the rules and recommendations defined by the relevant Certification Body. These mechanisms include the generation of the Authentication Key Pair and the generation of the Authentication Certificate.

OE.KEY_PAIR_GENERATION

As the key pair is not generated by the TOE, the device generating the key pair used by the authentication service shall ensure the integrity and the confidentiality of APrK and the integrity of the APuK until it is transferred to the CA, protected in integrity.

OE.TRUSTED_PERSONALIZATION_APPLI

The TOE relies on its environment to protect the following data transfers:

— Authentication with Issuer_VAD – protected in integrity and confidentiality.

— Import of Holder_RAD – protected in integrity and confidentiality.

— Import of APSD – protected in integrity.

OE.TRUSTED_AUTHENTICATION_APPLI

The TOE relies on its environment to protect the following data transfers:

— Authentication with Holder_VAD – protected in integrity and confidentiality.

— Import of Holder_RAD – protected in integrity and confidentiality.

— Import of Authentication Protocol sensitive data – protected in integrity.

OE.TRUSTED_VERIFIER

The TOE relies on its environment to protect the following data transfers:

— Import of random message to be signed – protected in integrity.

— Export of Signed message – protected in integrity.

— The environment shall also protect the authentication mechanism against Replay and Relay attacks as defined in ISO/IEC 10181-2:1996, 5.8.1 and 5.8.2.

10.4 Rationale for Security objectives

Color code:

This rationale uses colors to indidicate the groups to which the threats, policies, assumptions, objectives and requirements come from.

Core group: Yellow ; KeyImp group: Green; All Trusted/Untrusted groups: Orange.

Table 2 — Security objectives vs problem definition rationale

Objectives vs Threats OSP Assumptions	OT.DEVICE_AUTHENTICATION	OT.AUTH_USER	OT.PROTECTIONS	OT.HOLDER_RAD	OT.AUTHENTICATION_PRIVATE_KEY_IMPORT	OE.ISSUER	OE.HOLDER	OE.CERTIF_VERIF	OE.CERTIF_AUTH	OE.COPY	OE.CRYPTO	OE.KEY_PAIR_GENERATION	OE.TRUSTED_PERSONALIZATION_APPLI	OE.TRUSTED_AUTHENTICATION_APPLI	OE.TRUSTED_VERIFIER
T.MASQUERADE_USER		X	X	X			X			X			X	X	
T.PRIV_KEY_DISCLOSURE		X	X		X	X				X					
T.PRIVATE_KEY_MODIF		X	X		X								X		
T.COMM_EAVESDROP					X								X	X	X
T.USER_TRACKING		X												X	X
T.MASQUERADE_TOE	X		X		X							X			X
OSP.AUTHENTICATION_PROTOCOL	X														X
OSP.PKI												X			
OSP.PERSO_CORE				X	X							X			
OSP.CRYPTO					X						X				
A.ISSUER						X									
A.HOLDER							X								
A.CERTIF_VERIF								X							
A.CERTIF_AUTH									X		X				
A.COPY										X					
A.CRYPTO											X				

T.MASQUERADE_USER addresses the threat of retrieving or modifying the holder RAD in order to illegimately access to the TOE. This threat is countered by:

OT.AUTH_USER that ensures that the user, (Issuer or Holder) will be authenticated to the TOE before sensitive operations can be performed on the TOE,

OT.PROTECTIONS that ensures the integrity and confidentiality of Issuer and holder RAD inside the TOE,

OT.HOLDER_RAD that ensures the import and update of the holder RAD,

OE.HOLDER that ensures the Holder will maintain the confidentiality of his RAD outside the TOE,

OE.COPY that ensures the confidentiality of Issuer and holder RAD outside he TOE,

OE.TRUSTED_ PERSONALIZATION_APPLI that ensures the integrity and confidentiality of the Issuer and holder RAD when they are transferred from the personalisation application to the TOE, and

OE.TRUSTED_ AUTHENTICATION_APPLI that ensures the integrity and confidentiality of the holder RAD when it is transferred from the authentication application to the TOE.

T.PRIV_KEY_DISCLOSURE addresses the threat of retrieving the Authentication Private Key in order to illegimately authenticate to the Verifier. This threat is countered by:

OT.AUTH_USER that ensures that the user, (Issuer or Holder) will be authenticated to the TOE before he can import APrK into the TOE,

OT.PROTECTIONS that ensures the confidentiality of Authentication Private Key inside the TOE,

OT.AUTHENTICATION_PRIVATE_KEY_IMPORT, that ensures the integrity and the confidentiality of the Authentication Private Key, when it is transferred to the TOE. It also ensures that only the authorised user can import the Authentication Private Key.

OE.ISSUER, that ensures the Issuer will not cause the Authentication Private Key disclosure, and

OE.COPY that ensures the confidentiality of the Authentication Private Key outside he TOE.

T.PRIVATE_KEY_MODIF addresses the threat of modifying the Authentication Private Key in order to illegimately use it and deceive the Verifier. This threat is countered by:

OT.AUTH_USER that ensures that the user, (Issuer or Holder) will be authenticated to the TOE before he can import APrK into the TOE,

OT.PROTECTIONS that ensures the integrity of the Authentication Private Key inside the TOE,

OT.AUTHENTICATION_PRIVATE_KEY_IMPORT, that ensures the integrity and the confidentiality of the Authentication Private Key, when it is transferred to the TOE. It also ensures that only the authorised user can import the Authentication Private Key, and

OE.TRUSTED_ PERSONALIZATION_APPLI that ensures the integrity and confidentiality of the Authentication Private Key when it is transferred from the administration application to the TOE.

T.COMM_EAVESDROP addresses the threat of retrieving sensitive data by eavesdropping the communication of the TOE.This threat is countered by:

OT.AUTHENTICATION_PRIVATE_KEY_IMPORT that ensures the integrity and the confidentiality of the Authentication Private Key, when it is transferred to the TOE. It also ensures that only the authorised user can import the Authentication Private Key,

OE.TRUSTED_ PERSONALIZATION_APPLI that ensures the integrity and/or confidentiality of sensitive data – Holder RAD, Authentication Protocol sensitive data - when they are transferred between the TOE and the personalisation application,

OE.TRUSTED_ AUTHENTICATION_APPLI that ensures the integrity and/or confidentiality of sensitive data – Holder RAD, Authentication Protocol sensitive data - when they are transferred between the TOE and the authentication application, and

OE.TRUSTED_VERIFIER that ensures the integrity and/or confidentiality of sensitive data – Authentication Protocol sensitive data - when they are transferred between the TOE and the Verifier.

T.USER_TRACKING addresses the threat of identifying and tracking the Holder. This threat is countered by:

OT.AUTH_USER that ensures that the user, (Issuer or Holder) will be authenticated to the TOE before sensitive operations can be performed on the TOE,

OE.TRUSTED_ AUTHENTICATION_APPLI that ensures the integrity and/or confidentiality of sensitive data – Holder RAD, Authentication Protocol sensitive data - when they are transferred between the TOE and the authentication application, and

OE.TRUSTED_VERIFIER that ensures the integrity and/or confidentiality of sensitive data – Authentication Protocol sensitive data - when they are transferred between the TOE and the Verifier.

T.MASQUERADE_TOE addresses the threat of replay and relay attacks on the Authentication protocol. This threat is countered by:

OT.DEVICE_AUTHENTICATION that ensures that authentication of the TOE using a public-key cryptographic protocol with the private key stored in the TOE,

OT.PROTECTIONS that ensures the integrity and/or confidentiality of sensitive data – Holder RAD, Authentication Protocol sensitive data - inside the TOE,

OT.AUTHENTICATION_PRIVATE_KEY_IMPORT, imports the Authentication Private Key

OE.KEY_PAIR_GENERATION that provides the cryptographic key pair used in the authentication of the TOE, and

OE.TRUSTED_VERIFIER that ensures the integrity and/or confidentiality of sensitive data – Authentication Protocol sensitive data - when they are transferred between the TOE and the Verifier.

OSP.AUTHENTICATION_PROTOCOL addresses the authentication protocol. This OSP is covered by:

OT.DEVICE_AUTHENTICATION that ensures the authentication of the TOE using a public-key protocol, and

OE.TRUSTED_VERIFIER that ensures the integrity of the Authentication Protocol sensitive data when it is transferred from the TOE to the Verifier.

OSP.PKI addresses the PKI.This OSP is covered by:

OE.KEY_PAIR_GENERATION, which ensure the correct generation of Authentication Key pairs.

OSP.PERSO_CORE addresses Issuer activities during the Personnalisation. This OSP is covered by:

OT.HOLDER_RAD that ensures the import and update of the Holder RAD,

OT.AUTHENTICATION_PRIVATE_KEY_IMPORT that allows the Issuer to import APrK in Personnalisation, and

OE.KEY_PAIR_GENERATION that provide the cryptographic key pair used in the authentication of the TOE.

OSP.CRYPTO addresses the cryptographic rules to be applied. This OSP is covered by:

OT.AUTHENTICATION_PRIVATE_KEY_IMPORT that securely imports APrK,

OE.CRYPTO. which requires cryptographic mechanisms of the TOE to conform to the rules and recommendations defined by the relevant Certification Body.

A.ISSUER assumes qualifications of the Issuer. This assumption is directly covered by:

OE.ISSUER that ensures that the Issuer is trained to conduct his activities.

A.HOLDER assumes qualifications of the Holder. This assumption is automatically covered by the objective on the environment

OE.HOLDER that ensures that the Issuer is aware he shall not disclose his own RAD.

A.CERTIF_VERIF assumes the Verifier checks the certificate.This assumption is automatically covered by the objective on the environment

OE.CERTIF_VERIF that ensures the Verifier shall check the validity of the Holder certificate.

A.CERTIF_AUTH assumes qualifications of the Certification Authority. This assumption is covered by the objectives on the environment:

OE.CERTIF_AUTH that ensures the CA shall implement practices that conform to an approved certification policy, and

OE.CRYPTO, which defines the cryptographic rules to be applied by the CA.

A.COPY assumes confidential assets are not disclosed outside the TOE. This assumption is covered by the objective on the environment:

OE.COPY that prevents the sensitive date to be compromised by copies of such data that may exist outside the TOE.

A.CRYPTO assumes that the rules and recommendations defined by the relevant Certification Body are applied for the generation of authentication keys outside the TOE. This assumption is automatically covered by the objective on the environment

OE.CRYPTO, which ensures that the generation of the Authentication Key Pair and the generation of the Authentication Certificate shall conform to the rules and recommendations defined by the relevant Certification Body.

A.KEY_PAIR_GENERATION assumes the correct generation of keys outside the TOE. This assumption is automatically covered by the objective on the environment

OE.KEY_PAIR_GENERATION, which ensures the integrity and the confidentiality of APrK and the integrity of the APuK and

OE.CRYPTO, which ensures that the generation of the Authentication Key Pair shall conform to the rules and recommendations defined by the relevant Certification Body.

11 Extended component definition

There is no SFR component in this PP that is not extracted from [CC-2].

12 Security requirements

12.1 General

This clause describes the operations and requirements that a TOE shall fulfill in order to be compliant to this PP.

The device shall implement all the following requirements/operations:

— Device authentication by the verifier (on behalf of the Holder);

— Issuer authentication;

— Holder authentication with limited authentication attempts;

— Import of the authentication protocol sensitive data;

— Import of the Holder RAD;

— Export of the authentication protocol sensitive data;

Moreover, the device shall implement the following set of requirements:

— Import of the authentication private key;

Transfers security shall be enforced by the environment. There are no SFR for that purpose.

12.2 Introduction

12.2.1 Subjects Objects and security attributes

S.command_manager

It manages commands sent to the TOE and corresponding responses from the TOE, including import/export of sensitive assets.

S.communication_manager

IT manages the communication with the on-line service or with the distant agent in order to perform the service provided by the TOE.

O.Authentication_Private_Key

This object is the authentication key used to authenticate the card to a Verifier. This object is not necessarily unique.

O.Holder_RAD

This object is the Holder RAD. If it is a PIN, it has to be modified by the holder to ensure that only he can authenticate to the TOE.

Table 3 — Security attributes

Subject	Security attribute	Possible Values	Initial Value
S.command_manager	AT.Phase	Personalisation, Usage	Personalisation
S.command_manager	AT.Authenticated_user	Issuer, Holder, None	None
S.communication_manager	AT.Authenticated_device	Verifier, None	None
O.Authentication_Private_Key	AT.Operational	Yes, No	Yes, No
O.Authentication_Private_Key	AT.Consistency_pub_key	Yes, No	No
O.Authentication_Private_Key	AT.Identifier	Arbitrary value	Null
O.Holder_RAD	AT.Holder_only	Yes, No	No
O.Holder_RAD	AT.RAD_value	Arbitrary value	Null
O.Holder_RAD	AT.RAD_retry_counter	0 to HOLDER_MAX_RETRY_COUNTER	0

12.2.2 Operations

— Calculate: This operation corresponds to the internal use of the authentication private key.

— Issuer Authentication.

— Holder authentication with limited authentication attempts.

— Import of the Authentication Protocol sensitive data: This writing operation includes the deletion of the previous Authentication Protocol sensitive data (if any).

— Import of the Holder RAD: This writing operation includes the deletion of the previous Holder RAD (if any).

— Import of the authentication private key: This writing operation includes the deletion of the previous authentication private key (if any) and the deletion of the previous Authentication Protocol sensitive data(if any).

12.3 Security functional requirements

12.3.1 General

Global refinement for crypto operations:

The cryptographic algorithms, modes of operations and protocols including random generation shall be compliant with the rules and recommendations defined in OSP.CRYPTO.

12.3.2 Core

12.3.2.1 General

This section contains the generic SFR.

12.3.2.2 Device authentication by the verifier

FCS_COP.1/Signature Cryptographic operation

Hierarchical to: No other component
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1/ Signature **The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].**

FCS_CKM.4/Priv_key Cryptographic key destruction

Hierarchical to: No other component
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

FCS_CKM.4.1/ Priv_key **The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].**

Application note:

The private key has to be overwritten when a new private key is regenerated or re-imported, for the same authentication usage

FIA_ATD.1 User attribute definition

Hierarchical to: No other component

Dependencies: No dependencies

FIA_ATD.1.1 **The TSF shall maintain the following list of security attributes belonging to individual users: [see Table 3 — Security attributes, other security attributes].**

FIA_USB.1/Device User-subject binding

Hierarchical to: No other component
Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1/ Device **The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: AT.Authenticated_device.**

FIA_USB.1.2/ Device **The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:**
Before a user binds to S.Communication_manager the TSF shall authenticate to that user.

FIA_USB.1.3/ Device **The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:**
If the device is successfully authenticated by the verifier then the value of the security attribute Authenticated_ device of S.communication_manager shall be set at "verifier".

Application note:

The authentication mechanism implemented by the TOE shall be based on a public key cryptographic algorithm that allows the verifier to prevent replay of authentication data.

12.3.2.3 User authentication

FIA_UAU.1 Timing of authentication

Hierarchical to: No other component
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 **The TSF shall allow [assignment: *list of TSF mediated actions*] 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.**

Application note:

When refining this SFR, the ST writer shall pay attention to prevent any disclosure of data that can enable the tracking of the holder, without his consent.

FIA_USB.1/User User-subject binding

Hierarchical to: No other component
Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1/User **The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: AT.Phase.**

FIA_USB.1.2/User **The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:**

- **Before a user binds to S.Communication_manager the TSF shall authenticate to that user.**

FIA_USB.1.3/User **The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:**

- **If the user provides the VAD corresponding to the Issuer RAD and if Phase[S.command_manager]=Personalization, then the value of the security attribute Authenticated_ user of S.command_manager shall be set at "Issuer".**

- **If the user provides the VAD corresponding to the Holder RAD and if Phase[S.command_manager]=Usage, then the value of the security attribute Authenticated_ user of S.command_manager shall be set at "Holder".**

FIA_AFL.1/Holder Authentication failure handling

Hierarchical to: No other component
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/ Holder **The TSF shall detect when [HOLDER_RAD_MAX_RETRY] unsuccessful authentication attempts occur related to the same user (Holder).**

FIA_AFL.1.2/ Holder **When the defined number of unsuccessful authentication attempts has been [met, surpassed], the TSF shall prevent any subsequent Holder authentication attempt.**

Application notes:

The ST writer shall define the integer HOLDER_RAD_MAX_RETRY.

“unsuccessful authentication attempts” here shall be regarded as “consecutive unsuccessful authentication attempts”.

When the RAD is blocked, there is no way to unblock it.

12.3.2.4 Access control

FDP_ACC.1/Core Subset access control

Hierarchical to: No other component
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ Core **The TSF shall enforce the Core access control SFP on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].**

Subject	Object	Operation
S.command_manager	Authentication private key	Calculate

FDP_ACF.1/Core Security attribute based access control

Hierarchical to: No other component
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/ Core **The TSF shall enforce the Core access control SFP to objects based on the following:**

Table 4 — Core security attributes

Subject/Object	Security attribute
S.command_manager	AT.Phase
S.command_manager	AT.Authenticated_user
O.Authentication_Private_Key	AT.Operational
O.Holder_RAD	AT.Holder_Only

FDP_ACF.1.2/ Core **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:**

The following operation is allowed when the rule is met:

Table 5 — Core operations

Operation	Rule
Calculate	Phase[S.command_manager]=Usage AND Authenticated_user[S.command_manager]=Holder AND Operational[O.Authentication private key]=Yes AND Holder_Only[O.Holder_RAD] =Yes

FDP_ACF.1.3/ Core **The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: None**

FDP_ACF.1.4/ Core **The TSF shall explicitly deny access of subjects to objects based on the following rules:**

The following operations are never allowed:

— Export (read) of the authentication private key

— Modification (other than the import operations) of the authentication private key and the Authentication Protocol sensitive data.

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other component
Dependencies: No dependencies

FDP_RIP.1.1 **The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects: Authentication private key.**

FDP_SDI.2 Stored data integrity monitoring and action

The following data persistently stored by the TOE have the user data attribute “stored sensitive data”:

— Authentication private key

— Authentication Protocol sensitive data

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring
Dependencies: No dependencies

FDP_SDI.2.1 **The TSF shall monitor user data stored within the TSC for *integrity errors* on all objects, based on the following attributes: "stored sensitive data".**

FDP_SDI.2.2 **Upon detection of a data integrity error, the TSF shall:**
prohibit the use of the altered data
inform the user about the error

FMT_MSA.1/Core Management of security attributes

Hierarchical to: No other component
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Core **The TSF shall enforce the Core access control SFP, [assignment: other *access control SFP, other information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].**

Table 6 — Core security attributes - Operation

Authorised role	Operation	Attribute	At value
Issuer	Set value of	AT.Phase [S.command_manager]	Usage
Issuer	Change default value of	AT.Identifier [Authentication_Private_Key]	Arbitrary value
Holder	Set value of	AT.Holder_Only [Holder_RAD]	Yes
Holder	Set value of	AT.Authenticated_device [S.communication_manager]	Verifier
Issuer, Holder	Modify value of	AT.Authenticated_user [S.command_manager]	Not Applicable

FMT_MSA.2 Secure security attributes

Hierarchical to: No other component
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.2.1 **The TSF shall ensure that only secure values are accepted for [see Table 3 — Security attributes, other security attributes].**

FMT_MSA.3/Core Static attribute initialization

Hierarchical to: No other component
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1/Core **The TSF shall enforce Core access control SFP, [assignment: other access control SFP, other information flow control SFP] to provide restrictive default values for security attributes that are used to enforce the SFP.**

Table 7 — Core security attributes - Initial value

Security attribute	Initial value
AT.Phase [S.command_manager]	Pre-personalisation
AT.Authenticated_ user [S.command_manager]	None
AT.Authenticated_device [S.communication_manager]	None
AT.Holder_Only [Holder_RAD]	No
AT.Operational [Authentication_Private_Key]	No
AT.Consistency_Pub_Key [Authentication_Private_Key]	No
AT.RAD_retry _counter [Holder_RAD]	0

FMT_MSA.3.2/Core **The TSF shall allow the None to specify alternative initial values to override the default values when an object or information is created.**

FMT_MSA.4/Core Security attributes value inheritance

Hierarchical to: No other component
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.4.1/Core **The TSF shall use the following rules to set the value of security attributes [assignment: *rules for setting the value of security attributes*].**

Table 8 — Core security attributes – updates

Condition	Modification	
	Set value of	*at*
Authenticated Issuer AND Issuer command to Usage phase	AT.Phase [S.command_manager]	Usage
Authenticated Issuer AND Issuer command to Usage phase AND RAD is PIN or symmetric key	AT.Holder_Only [Holder_RAD]	No
Authenticated Issuer AND Issuer command to Usage phase AND RAD is biometrics	AT.Holder_Only [Holder_RAD]	Yes
Reset of the device or end of session.	AT.Authenticated_user [S.command_manager]	None
Reset of the device or end of session.	AT.Authenticated_device	None
Authenticated Holder AND change PIN	AT.Holder_Only [Holder_RAD]	Yes
Issuer Authentication AND Phase personalisation	AT.Authenticated_user [S.command_manager]	Issuer
Holder Authentication AND Phase usage	AT.Authenticated_ user [S.command_manager]	Holder
Import Authentication Protocol sensitive data for the current Authentication Private Key	AT.Operational [Authentication_Private_Key]	Yes
Import Authentication Protocol sensitive data for the current Authentication Private Key	AT.Operational [Authentication_Private_Key]	Yes
Failed Holder Authentication	AT.RAD_retry_counter [Holder_RAD]	current RAD_retry_Counter +1
Successful Holder Authentication	AT.RAD_retry _counter [Holder_RAD]	0
Authenticated Holder AND Successful Authentication by Verifier	AT.Authenticated_device [S.communication_manager]	Verifier

Application note:

When RAD_retry _counter [Holder_RAD] reaches HOLDER_RAD_MAX_RETRY, All subsequent authentication are blocked.

FMT_MTD.1/Core Management of TSF data

Hierarchical to: No other component
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MTD.1.1/Core **The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorised identified roles].**

Table 9 — TSF data – Updates

Operation	TSF data	role
modify	**Holder_RAD**	**holder**
modify	**Authentication Protocol sensitive data**	**holder**

FMT_SMR.1/Core Security roles

Hierarchical to: No other component
Dependencies: FIA_UID.1 Timing of Authentication

FMT_SMR.1.1/Core **The TSF shall maintain the roles Issuer, Holder.**

FMT_SMR.1.2/Core **The TSF shall be able to associate users with roles.**

FMT_SMF.1/Core Specification of management functions

Hierarchical to: No other component
Dependencies: No dependencies

FMT_SMF.1.1/Core **The TSF shall be capable of performing the following management functions:**
Creation and modification of RAD,
Import of Authentication Protocol sensitive data
[assignment: list of other management functions to be provided by the TSF].

12.3.2.5 Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other component
Dependencies: No dependencies

FPT_FLS.1.1 **The TSF shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TSF*].**

FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other component
Dependencies: No dependencies

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.**

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other component
Dependencies: No dependencies

FPT_PHP.3.1 **The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: *list of TSF devices/elements*] by responding automatically such that the TSP is not violated.**

Application note:

Physical tampering includes know attacks such as SPA, DPA, SEMA, DEMA, DFA

FPT_TST.1 TSF testing

Hierarchical to: No other component

Dependencies: No dependencies

FPT_TST.1.1 **The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of the TSF. operation of [selection: [assignment: parts of TSF], the TSF].**

FPT_TST.1.2 **The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: parts of TSF], TSF data].**

FPT_TST.1.3 **The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.**

12.3.3 KeyImp

This section contains the SFR that are specific to the import of the Authentication Private Key

FDP_ACC.1/KeyImp Subset access control

Hierarchical to: No other component
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ KeyImp **The TSF shall enforce the KeyImp access control SFP on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].**

Subject	Object	Operation
Holder/Issuer	Authentication Private Key	Import of the authentication private key

FDP_ACF.1/KeyImp Security attribute based access control

Hierarchical to: No other component
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/ KeyImp **The TSF shall enforce the KeyImp access control SFP to objects based on the following:**

Table 10 — KeyImp security attributes

Subject/Object	Security attribute
S.command_manager	AT.Phase
S.command_manager	AT.Authenticated_user

FDP_ACF.1.2/ KeyImp **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:**

The following operation is allowed only when the rule is met:

Table 11 — KeyImp security attributes - operations

Operation	Rule
Import of the authentication private key	{AT.Phase[S.command_manager]=Usage AND AT.Authenticated_user[S.command_manager]=Holder} OR {AT.Phase[S.command_manager]=Personalization AND AT.Authenticated_user[S.command_manager]=Issuer}

FDP_ACF.1.3/ KeyImp **The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: None.**

FDP_ACF.1.4/ KeyImp **The TSF shall explicitly deny access of subjects to objects based on the following additional rules: None.**

FDP_ITC.2/Priv_key Import of user data with security attributes

Hierarchical to: No other component
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_ITC.2.1/Priv_key **The TSF shall enforce the KeyImp access control SFP when importing user data, controlled under the SFP, from outside of the TOE**

FDP_ITC.2.2/Priv_key **The TSF shall use the security attributes associated with the imported user**

FDP_ITC.2.3/Priv_key **The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.**

FDP_ITC.2.4/Priv_key **The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.**

FDP_ITC.2.5/Priv_key **The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].**

FDP_UCT.1/Priv_key Basic Data exchange confidentiality

Hierarchical to: No other component
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UCT.1.1/Priv_key **The TSF shall enforce the KeyImp access control SFP to be able to receive user data in a manner protected from unauthorised disclosure.**

The user considered here is the Authentication Private key.

FDP_UIT.1/Priv_key Data exchange integrity

Hierarchical to: No other component

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1/Priv_key **The TSF shall enforce the KeyImp access control SFP to be able to receive user data in a manner protected from modification, deletion, insertion, replay errors.**

FDP_UIT.1.2/Priv_key **The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, replay errors_has occurred.**

FMT_MSA.1/KeyImp Management of security attributes

Hierarchical to: No other component

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/ KeyImp **The TSF shall enforce the KeyImp access control SFP, [assignment: other *access control SFP, other information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].**

Table 12 — KeyImp security attributes – update authorised roles

Authorised role	Operation	Attribute	At value
Issuer, Holder	Set value of	AT.Operational[Authentication_Private_Key]	Yes, No
Issuer, Holder	Set value of	AT.Consistency_pub_key[Authentication_Private_Key]	Yes, No

FMT_MSA.4/KeyImp Security attributes value inheritance

Hierarchical to: No other component

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.4.1 /KeyImp **The TSF shall use the following rules to set the value of security attributes [assignment: *rules for setting the value of security attributes*].**

Table 13 — KeyImp security attributes – Update values

Condition	Modification	
	Set value of	*at*
Import Authentication private key	AT.Operational[Authentication_Private_Key]	No
Import Authentication Protocol sensitive data	AT.Operational[Authentication_Private_Key]	Yes
Import Authentication private key	AT.Consistency_pub_key[Authentication_Private_Key]	No

FTP_ITC.1/Priv_Key Inter-TSF trusted channel

Hierarchical to: No other component
Dependencies: No dependencies

FTP_ITC1.1/ Priv_Key **The TSF shall provide a communication channel between itself and another trusted IT product 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_ITC1.2/ Priv_Key **The TSF shall permit another trusted IT product to initiate communication via the trusted channel.**

FTP_ITC1.3/ Priv_Key **The TSF shall initiate communication via the trusted channel for:**

- **Import of Priv_Key**

Application note:

1. The Remote Trusted IT product is Key pair generator

12.4 Security assurance requirements

The assurance requirements associated with the EAL selected for this PP are not described below (as they are described in ISO/IEC 15408-3).

The security assurance requirement level is EAL4. The EAL is augmented with ALC_DVS.2 and AVA_VAN.5.

12.5 SFR / Security objectives

Color code:

This rationale uses colors to indidicate the groups to which the threats, policies, assumptions, objectives and requirements come from.

Core group: Yellow ; KeyImp group: Blue ; All Trusted/Untrusted groups: Orange.

Table 14 — SFR vs Security objectives retionale

Objectives vs SFR	OT.DEVICE_AUTHENTICATION	OT.AUTH_USER	OT.PROTECTIONS	OT.HOLDER_RAD	OT.AUTHENTICATION_PRIVATE_KEY_IMPORT
FCS_COP.1/Signature	X				
FCS_CKM.4/Priv_key					X
FIA_ATD.1		X			
FIA_UAU.1		X			
FIA_USB.1/User		X			
FIA_USB.1/Device	X				
FIA_AFL.1/Holder		X			
FDP_ACC.1/Core		X	X	X	
FDP_ACF.1/Core		X	X	X	
FDP_RIP.1			X		
FDP_SDI.2			X		
FMT_MSA.1/Core	X	X	X	X	
FMT_MSA.2	X	X	X	X	X
FMT_MSA.3/Core	X	X	X	X	X
FMT_MSA.4/Core	X	X	X	X	
FMT_MTD.1/Core	X			X	
FMT_SMR.1/Core		X		X	X
FMT_SMF.1/Core				X	
FPT_FLS.1		X			
FPT_PHP.1			X		
FPT_PHP.3			X		
FPT_TST.1			X		
FDP_ACC.1/KeyImp					X
FDP_ACF.1/KeyImp					X
FDP_ITC.1/Priv_key					X
FDP_UCT.1/Priv_key					X
FDP_UIT.1/Priv_key					X
FMT_MSA.1/KeyImp					X
FMT_MSA.4/KeyImp					X
FTP_ITC.1/ Priv_key					X

OT.DEVICE_AUTHENTICATION This objective ensures the authentication mechanism itself. It is is covered by

FCS_COP.1/Signature, which signs a message, received from the Verifier, using APrK, and by this means, authenticates the card to the Verifier,,

FIA_USB.1/Device that sets the AT.Authenticated_device security attribute to Verifier,

FMT_MSA.1/Core that allows only the Holder to set the AT.Authenticated_device security attribute to Verifier,

FMT_MSA.2 that ensures that only secure values are accepted for AT.Authenticated_device,

FMT_MSA.3/Core that ensures that the default values for Authenticated_ device is "None",

FMT_MSA.4/Core, which sets the rules for modifying the "Authenticated_device" security attribute, and

FMT_MTD.1/Core, which allows the Holder to modify APSD.

OT.AUTH_USER This objective ensures the authentication of the holder or the issuer to the TOE. It is covered by:

FIA_ATD.1, which allows the creation of an authentication chain,

FIA_UAU.1, which ensures the authentication of the User,

FIA_USB.1/User, which binds the authenticated user to the Holder role,

FIA_AFL.1/Holder, which limis the number of authentication attemps,

FDP_ACC.1/Core and

FDP_ACF.1/Core, which only allows the access to the RAD to the subject that performs the authentication of the User to the TOE and prevents access to sensitive data by unauthorised users,

FMT_MSA.1/Core that allows only the Issuer or the Holder to modify the AT.Authenticated_user,

FMT_MSA.2 that ensures that only secure values are accepted for AT.Authenticated_user,

FMT_MSA.3/Core that ensures that the default values for AT.Authenticated_user is "None",

FMT_MSA.4/Core, which control the "AT.Authenticated_user" security attribute,

FMT_SMR.1/Core, which maintains the roles Issuer and Holder, and

FPT_FLS.1, which deals with the protection of User authentication to the TOE.

.

OT.PROTECTIONS This objective protects sensitive data on TOE against unauthorised modification and disclosure. It is covered by:

FDP_ACC.1/Core and

FDP_ACF.1/Core, which prevents access to sensitive data by unauthorised users,

FDP_RIP.1, which participate to the confidentiality of sensitive stored data,

FDP_SDI.1, which ensures with the integrity of sensitive stored data,

FMT_MSA.1/Core that restricts the modification of security attributes to authorised roles,

FMT_MSA.2 that ensures that only secure values are accepted for security attributes,

FMT_MSA.3/Core that ensures that default values for security attributes are used,

FMT_MSA.4/Core, which controls the setting of the security attributes,

FPT_PHP.1, which detects attacks against the TOE,

FPT_PHP.3, which protects the TOE against attacks, and

FPT_TST.1, which tests the physical integrity of the TOE.

OT.HOLDER_RAD controls the import of the Holder RAD. It is covered by:

FDP_ACC.1/Core and

FDP_ACF.1/Core, which define the access control rules to import, modify, and replace the Holder RAD,

FMT_MSA.1/Core that restricts the modification of the "AT.Holder_only" and "AT.Authenticated_user" security attributes to the Holder,

FMT_MSA.2 that ensures that only secure values are accepted for security attributes,

FMT_MSA.3/Core that provides "No" and "None" as default values for the "Holder_only" and "Authenticated_user" security attributes,

FMT_MSA.4/Core, which controls the setting of the "AT.Holder_only" and "AT.Authenticated_user" security attributes,

FMT_MTD.1/Core, which allows the import of the Holder RAD.

FMT_SMR.1/Core, which maintains the roles Issuer and Holder, and

FMT_SMF.1/Core, which allows the import of the Holder RAD.

OT.AUTHENTICATION_PRIVATE_KEY_IMPORT controls the import of APrK. This objective is covered by:

FCS_CKM.4/Priv_key, which controls the deletetion of APrK,

FMT_SMR.1/Core, which maintains the roles Issuer and Holder,

FDP_ACC.1/KeyImp and

FDP_ACF.1/KeyImp, which define the access control rules to import APrK,

FMT_MSA.1/KeyImp that restricts the modification of the "AT.Operational" and "AT.Consistency_pub_key" security attributes to the Holder or the Issuer,

FMT_MSA.2 that ensures that only secure values are accepted for the "AT.Operational" and "AT.Consistency_pub_key" security attributes,

FMT_MSA.3/Core that provides "No" default value for the "AT.Operational" and "AT.Consistency_pub_key"security attributes,

FMT_MSA.4/KeyImp, which control the "AT.operational" security attribute of APrK,

FDP_ITC/ Priv_key, which protects the integrity of APrK when it imported into the TOE,

FDP_UCT.1/Priv_key, which protects the confidentiality of APrK when it imported into the TOE,

FDP_UIT.1/Priv_key, which protects the integrity of APrK when it imported into the TOE, and

FTP_ITC/ Priv_key, which protect the integrity and the confidentiality of APrK when it imported into the TOE.

12.6 SFR Dependencies

Table 15 — SFR dependencies

SFR	Dependencies	Satisfied dependencies
FCS_COP.1/Signature	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FDP_ITC.1/Priv_key FCS_CKM.4/Priv_key FMT_MSA.2
FCS_CKM.4/Priv_key	[FDP_ITC.1, or FDP_ITC.2, or	FDP_ITC.1/Priv_key

SFR	Dependencies	Satisfied dependencies
	FCS_CKM.1], FMT_MSA.2	FMT_MSA.2
FIA_ATD.1	None	
FIA_UAU.1	**FIA_UID.1**	
FIA_USB.1/User	FIA_ATD.1	FIA_ATD.1
FIA_USB.1/Device	FIA_ATD.1	FIA_ATD.1
FIA_AFL.1/Holder	FIA_UAU.1	FIA_UAU.1
FDP_ACC.1/Core	FDP_ACF.1	FDP_ACF.1/Core
FDP_ACF.1/Core	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Core FMT_MSA.3/Core
FDP_RIP.1	None	
FDP_SDI.2	None	
FMT_MSA.1/Core	[FDP_ACC.1, or FDP_IFC.1l] FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Core FMT_SMR.1/Core FMT_SMF.1/Core
FMT_MSA.2	[FDP_ACC.1, or FDP_IFC.1] FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/Core FMT_MSA.1/Core FMT_SMR.1/Core
FMT_MSA.3/Core	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Core FMT_SMR.1/Core
FMT_MSA.4/Core	[FDP_ACC.1, or FDP_IFC.1l]	FDP_ACC.1/Core
FMT_MTD.1/Core	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1/Core FMT_SMF.1/Core
FMT_SMR.1/Core	**FIA_UID.1**	
FMT_SMF.1/Core	None	
FPT_FLS.1	None	
FPT_PHP.1	None	
FPT_PHP.3	None	
FPT_TST.1	**FPT_AMT.1**	
FDP_ACC.1/KeyImp	FDP_ACF.1	FDP_ACF.1/KeyImp
FDP_ACF.1/KeyImp	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/KeyImp FMT_MSA.3/Core
FDP_ITC.1/Priv_key	[FDP_ACC.1, or FDP_IFC.1], FMT_MSA.3	FDP_ACC.1/KeyImp FMT_MSA.3/Core
FDP_UCT.1/Priv_key	[FDP_ACC.1, or FDP_IFC.1], [FTP_ITC.1, or FTP_TRP.1]	FDP_ACC.1/KeyImp FTP_ITC/ Priv_key
FDP_UIT.1/Priv_key	[FDP_ACC.1, or FDP_IFC.1], [FTP_ITC.1, or FTP_TRP.1]	FDP_ACC.1/KeyImp FTP_ITC/ Priv_key
FMT_MSA.1/KeyImp	[FDP_ACC.1, or FDP_IFC.1l] FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/KeyImp FMT_SMR.1/Core FMT_SMF.1/Core
FMT_MSA.4/KeyImp	[FDP_ACC.1, or FDP_IFC.1l	FDP_ACC.1/KeyImp
FTP_ITC/ Priv_key	None	

The dependency FIA_UID.1 of FMT_SMR.1 is not supported; Identification is not required for the TOE.

The dependency FPT_AMT.1 of FPT_TST.1 is not supported. The TOE does not have an underlying abstract machine.

12.7 Rationale for the Assurance Requirements

12.7.1 EAL.4 methodically designed, tested, and reviewed

EAL4 is required for this type of TOE and product since it is intended to defend against sophisticated attacks. This evaluation assurance level allows a developer to gain maximum assurance from positive security engineering based on good practices. EAL4 represents the highest practical level of assurance expected for a commercial grade product. In order to provide a meaningful level of assurance that the TOE and its embedding product provide an adequate level of defense against such attacks, the evaluators should have access to the low level design and source code. The lowest for which such access is required is EAL4.

12.7.2 AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the definition of the TOE and of the embedding the product, the product shall resist to high attack potential. This is due to the fact that the product (Smart Card or similar device) can be placed in a hostile environment, such as electronic laboratories. This robusteness level is achieved by the assurance AVA_VAN.5 component. Independent vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication. AVA_VAN.5 has dependencies with ADV_ARC.1, ADV_FSP.1, ADV_TDS.3, ADV_IMP.1, AGD_PRE.1, AGD_OPE.1. All these dependencies are satisfied by EAL4.

12.7.3 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 and the embedding product. This assurance component is a higher hierarchical component to EAL4 (only ALC_DVS.1 is found in EAL4). Due to the nature of the TOE and embedding product, there is a need to justify the sufficiency of these procedures to protect their confidentiality and integrity. ALC_DVS.2 has no dependencies.

Bibliography

[1] EN 419251-2:2013, *Security requirements for device for authentication — Part 2: Protection profile for extension for trusted channel to certificate generation application*

[2] EN 419251-3:2013, *Security requirements for device for authentication — Part 3: Additional functionality for security targets*

[3] prEN 14169-2:2010, *Protection Profile for Secure signature creation device — Part 2: Device with key generation*

[4] prEN 14169-3:2010, *Protection profiles for secure signature creation device — Part 3: Device with key import*

[5] prEN 14169-4:2010, *Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application*

[6] prEN 14169-5:2010, *Protection profiles for secure signature creation device — Part 5: Device with key generation and trusted communication with signature-creation application*

[7] prEN 14169-6:2010, *Protection profiles for secure signature creation device — Part 6: Device with key import and trusted communication with signature-creation application*

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

Index

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

BSI is incorporated by Royal Charter. British Standards and other standardisation products are published by BSI Standards Limited.

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similary for PASs, please notify BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about British Standards is available on the BSI website at **www.bsi-group.com/standards**

Copyright

BSI

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™