BS EN 419251-1:2013

BSI Standards Publication

Security requirements for device for authentication

Part 1: Protection profile for core functionality

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

raising standards worldwide™

Full document details: BS EN 419251-1:2013

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.

© The British Standards Institution 2013.
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

Documents
Document Sharing Hub

Full document details: BS EN 419251-1:2013

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

© 2013 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

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

Documents
Document Sharing Hub

Full document details: BS EN 419251-1:2013

Contents

Page

Foreword 5

1 Scope 6

2 Normative references 6

3 Conformance 6
3.1 CC Conformance Claim 6
3.2 PP Claim 6
3.3 Package Claim 6
3.4 Conformance Rationale 6
3.5 Conformance Statement 6

4 Terms and definitions 7

5 Symbols and abbreviations 9

6 Overview of the target of evaluation 9
6.1 TOE Type 9
6.2 TOE Usage 9
6.3 Security Features of the TOE 9
6.4 Examples of applications 10
6.4.1 E-government 10
6.4.2 Multiple applications 11
6.5 Required non-TOE Hardware and Software 11
6.6 Protection Profile Usage 11

7 TOE Environment 12
7.1 Overall view 12
7.2 Personalisation application 13
7.2.1 General 13
7.2.2 Functionalities 13
7.2.3 Communication 13
7.3 Authentication application 14
7.3.1 General 14
7.3.2 Functionalities 14
7.3.3 Communication 14
7.4 Verifier 15
7.4.1 Functionalities 15
7.4.2 Communication 15
7.5 Key Generator 15
7.5.1 Functionalities 15
7.5.2 Communication 15
7.6 Certification Authority — Functionalities 15

8 Life Cycle 16
8.1 Overview 16
8.2 Pre-Personalisation phase 17
8.3 Personalisation phase 18
8.3.1 General 18
8.3.2 Personalisation application 18
8.4 Usage phase — Authentication application 18
8.4.1 General 18
8.4.2 Verifier 19

9 Security problem definition 19

Documents
Document Sharing Hub

Full document details: BS EN 419251-1:2013

9.1 Assets 19
9.1.1 General 19
9.1.2 Assets protected by the TOE 19
9.1.3 Sensitive assets of the TOE 19
9.2 Users 20
9.3 Threats 21
9.4 Organisational security policies 22
9.4.1 Provided services 22
9.4.2 Other services 22
9.5 Assumptions 23

10 Security objectives 24
10.1 General 24
10.2 Security objectives for the TOE 24
10.2.1 Provided service 24
10.2.2 Authentication to the TOE 24
10.2.3 TOE management 24
10.3 Security objectives for the operational environment 25
10.4 Rationale for Security objectives 26

11 Extended component definition 30

12 Security requirements 30
12.1 General 30
12.2 Introduction 31
12.2.1 Subjects Objects and security attributes 31
12.2.2 Operations 31
12.3 Security functional requirements 32
12.3.1 General 32
12.3.2 Core 32
12.3.3 KeyImp 40
12.4 Security assurance requirements 43
12.5 SFR / Security objectives 43
12.6 SFR Dependencies 46
12.7 Rationale for the Assurance Requirements 48
12.7.1 EAL.4 methodically designed, tested, and reviewed 48
12.7.2 AVA_VAN.5 Advanced methodical vulnerability analysis 48
12.7.3 ALC_DVS.2 Sufficiency of security measures 48

Bibliography 49

Index 50

Figures

Figure 1 — TOE Security Features 12
Figure 2 — Personalisation application environment 13
Figure 3 — Authentication application environment 14
Figure 4 — TOE Life Cycle 16

Tables

Table 1 — Protection of sensitive data 24
Table 2 — Security objectives vs problem definition rationale 27
Table 3 — Security attributes 31
Table 4 — Core security attributes 35
Table 5 — Core operations 35
Table 6 — Core security attributes - Operation 36

AVA Documents
Document Sharing Hub

Full document details: BS EN 419251-1:2013

Table 7 — Core security attributes - Initial value....37
Table 8 — Core security attributes – updates....38
Table 9 — TSF data – Updates....38
Table 10 — KeyImp security attributes....40
Table 11 — KeyImp security attributes - operations....41
Table 12 — KeyImp security attributes – update authorised roles....42
Table 13 — KeyImp security attributes – Update values....43
Table 14 — SFR vs Security objectives retionale....44
Table 15 — SFR dependencies....46

Documents
Document Sharing Hub
Full document details: BS EN 419251-1:2013

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.

Documents
Document Sharing Hub
Full document details: BS EN 419251-1:2013

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.

Documents
Document Sharing Hub
Full document details: BS EN 419251-1:2013

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]

Documents
Document Sharing Hub
Full document details: BS EN 419251-1:2013

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.

Documents
Document Sharing Hub
Full document details: BS EN 419251-1:2013

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.

Documents
Document Sharing Hub
Full document details: BS EN 419251-1:2013

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.

Documents
Document Sharing Hub
Full document details: BS EN 419251-1:2013

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.

Documents
Document Sharing Hub
Full document details: BS EN 419251-1:2013

7 TOE Environment

7.1 Overall view

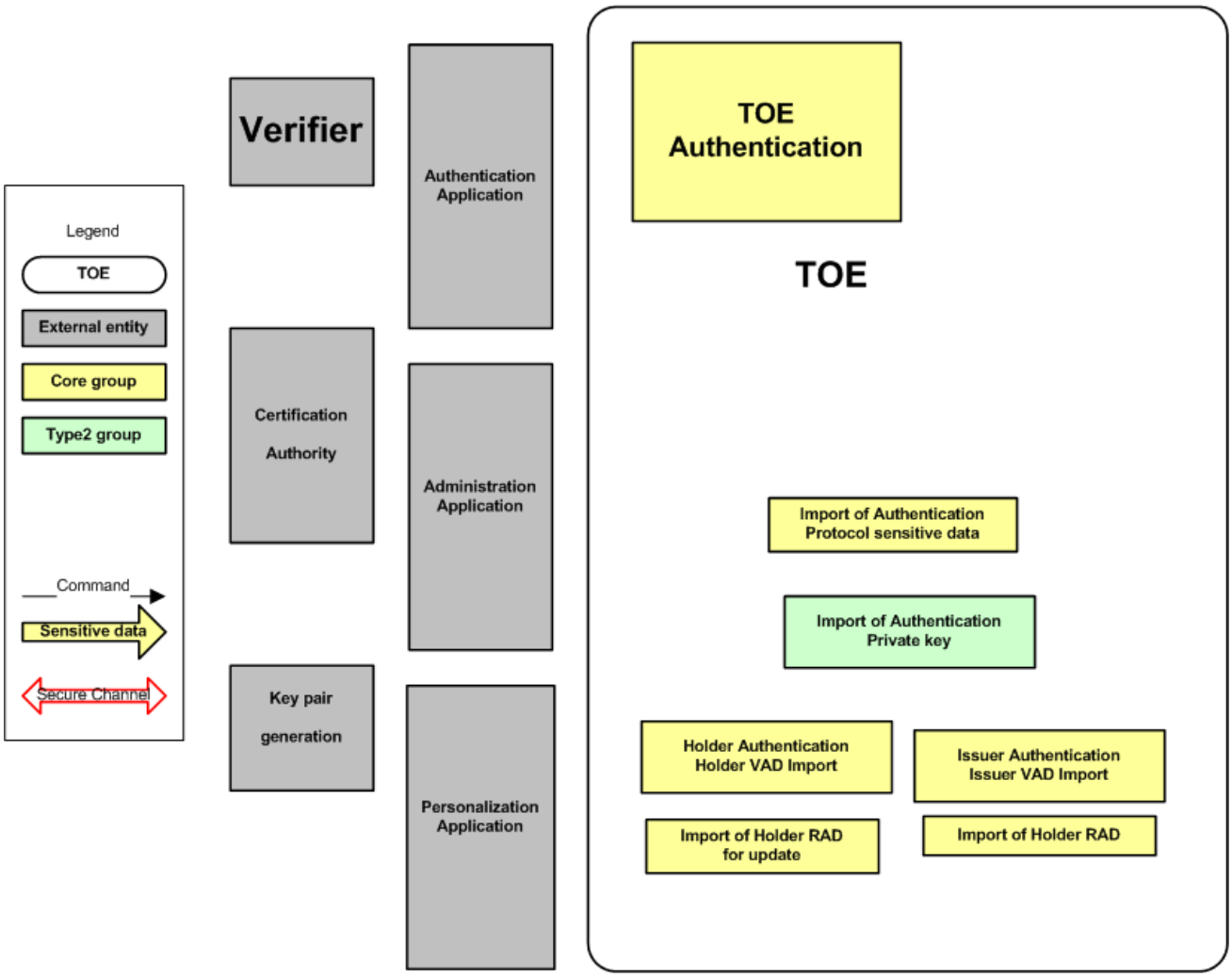

Figure 1 — TOE Security Features

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].

Documents
Document Sharing Hub
Full document details: BS EN 419251-1:2013

7.2 Personalisation application

7.2.1 General

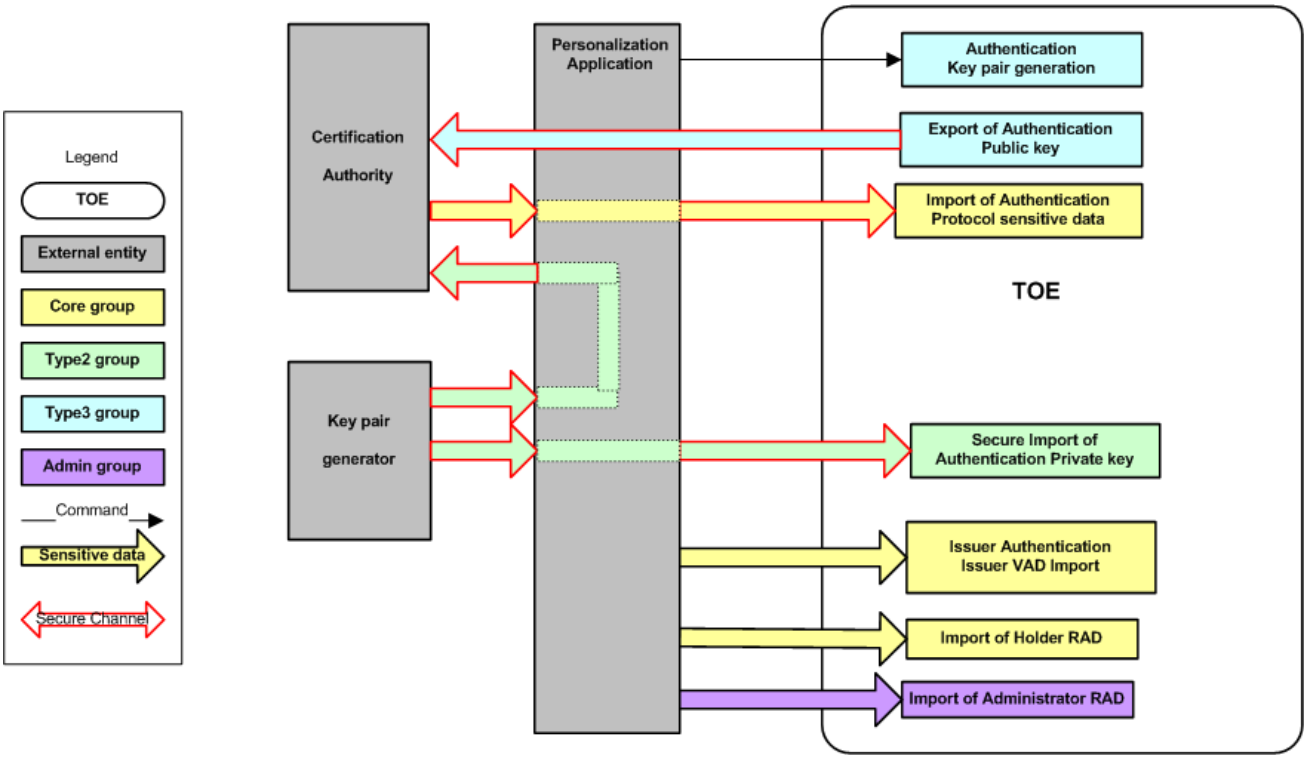

Figure 2 — Personalisation application environment

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.

Documents
Document Sharing Hub
Full document details: BS EN 419251-1:2013

7.3 Authentication application

7.3.1 General

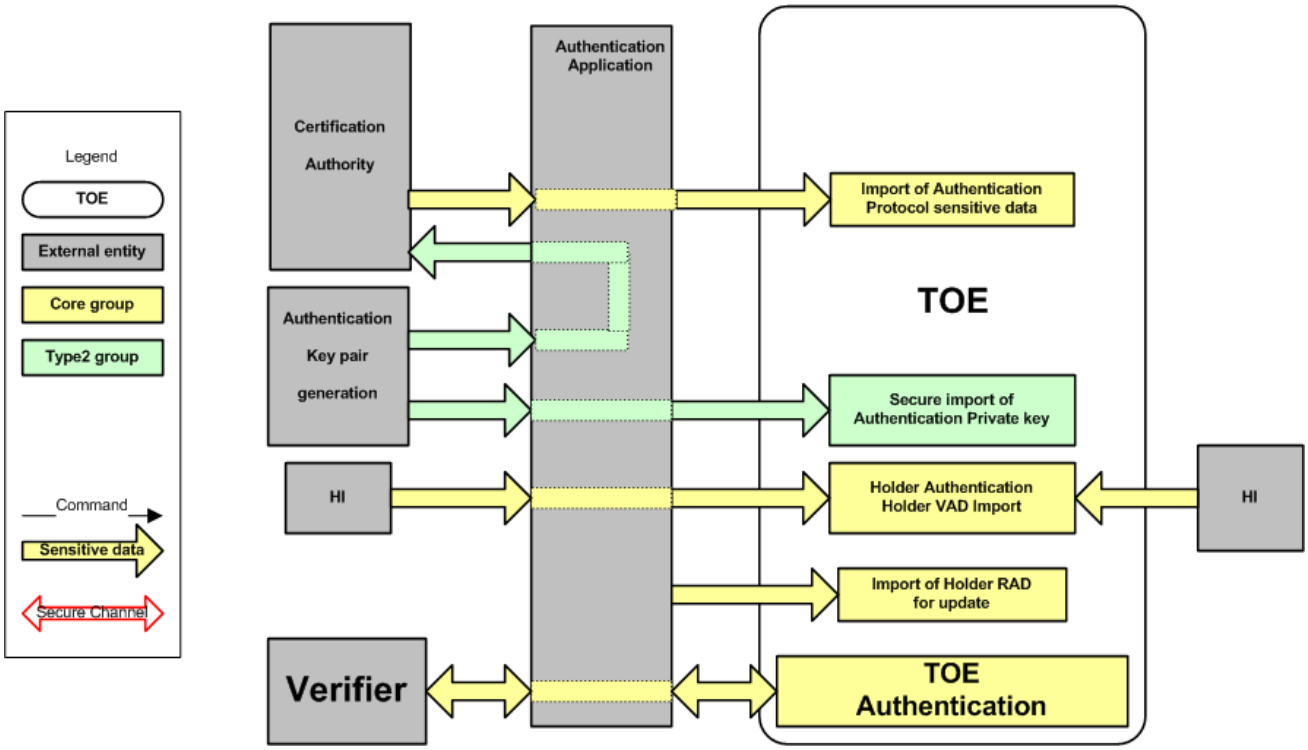

Figure 3 — Authentication application environment

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.

Documents
Document Sharing Hub
Full document details: BS EN 419251-1:2013

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.

Documents
Document Sharing Hub
Full document details: BS EN 419251-1:2013