SLOVENSKI STANDARD
SIST EN 419251-2:2013

01-maj-2013

Varnostne zahteve naprav za overjanje - 2. del: Profil zaščite za razširitev zaupnega kanala za aplikacijo, ki generira certifikat

Security requirements for device for authentication - Part 2: Protection profile for extension for trusted channel to certificate generation application

Sicherheitsanforderungen für Geräte zur Authentifizierung - Teil 2: Schutzprofil für Erweiterung für vertrauenswürdigen Kanal zur zertifizierung von Generierungsanwendungen

Profils de protection pour dispositif d'authentification - Partie 2: Dispositf avec import de clé, génération de clé et administration: Communication sécurisée vers l'application de génération de certificats et l'application d'administration

Ta slovenski standard je istoveten z: **EN 419251-2:2013**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST EN 419251-2:2013 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419251-2

March 2013

ICS 35.240.15

English Version

Security requirements for device for authentication - Part 2: Protection profile for extension for trusted channel to certificate generation application

Profils de protection pour dispositif d'authentification - Partie 2: Dispositf avec import de clé, génération de clé et administration; Communication sécurisée vers l'application de génération de certificats et l'application d'administration

Sicherheitsanforderungen für Geräte zur Authentisierung - Teil 2: Schutzprofil für Erweiterung für vertrauenswürdigen Kanal zur Zertifikaterzeugungsanwendung

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 419251-2:2013: E

Contents

Page

Figures

Tables

Foreword

This document (EN 419251-2:2013) 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*;

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

— 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 16248-2.

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
Administrator
person who is allowed administration operations on the authentication device

Note 1 to entry: See 9.2 for more details.

4.2
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.

4.3
Certificate
electronic attestation, which links the APuK to a person and confirms the identity of that person (as defined in Directive [8], article 2, Clause 9)

4.4
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

4.5
Configuration
set of groups

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

4.6
Group
set of Assets, threats, objectives, and Requirements, addressing a specific function

Note 1 to entry: See [2].

4.7
Holder
legitimate holder of the authentication device

Note 1 to entry: See 9.2 for more details.

4.8
Issuer
user of the authentication device during personalisation

Note 1 to entry: See 9.2 for more details.

4.9
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]

4.10
PP collection
document defining groups and configurations

4.11
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.

4.12
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"]

4.13
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).

4.14
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).

4.15
User
current User of the TOE

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

4.16
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]

4.17
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 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 into 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 one configuration that comprises the following groups: Core, KeyImp, KeyGen, Admin, Trusted PersoAppli, Trusted AuthAppli, Trusted Verifier, Untrusted CA, and Unstrusted AdminAppli.

a) Core group

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

b) KeyImp group

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

c) KeyGen group

KeyGen group contains the security features directly linked to the On Board Key Generation (OBKG) of the Authentication Private Key.

d) Admin group

Admin group contains the security features directly linked to the following Administration functions, which take place during the Usage phase:

1) Import and export of the public key and certificate by administrator.

2) Storage and export of log data by administrator.

3) Reset of Holder authentication failures counter by administrator.

e) 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.

f) 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.

g) 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.

h) Untrusted CA group

Untrusted CA group contains the security features directly linked to the transfer of sensitive data between the CA and the TOE when these transfers do not take place in a protected environment. This means that the TOE has to establish a trusted channel with the CA.

i) Untrusted AdminAppli group

Untrusted AdminAppli group contains the security features directly linked to the transfer of sensitive data between the Administration application and the TOE when these transfers do not take place in a protected environment. This means that the TOE has to establish a trusted channel with the Administration application.

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. The holder can also generate the key pair. He then has to establish a trusted channel with the CA to transfer the public key that will be necessary to create the Certificate.

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], and [7] in order to define complementary security requirements for products offering both authentication and signature services.

7 TOE Environment

7.1 Overall view

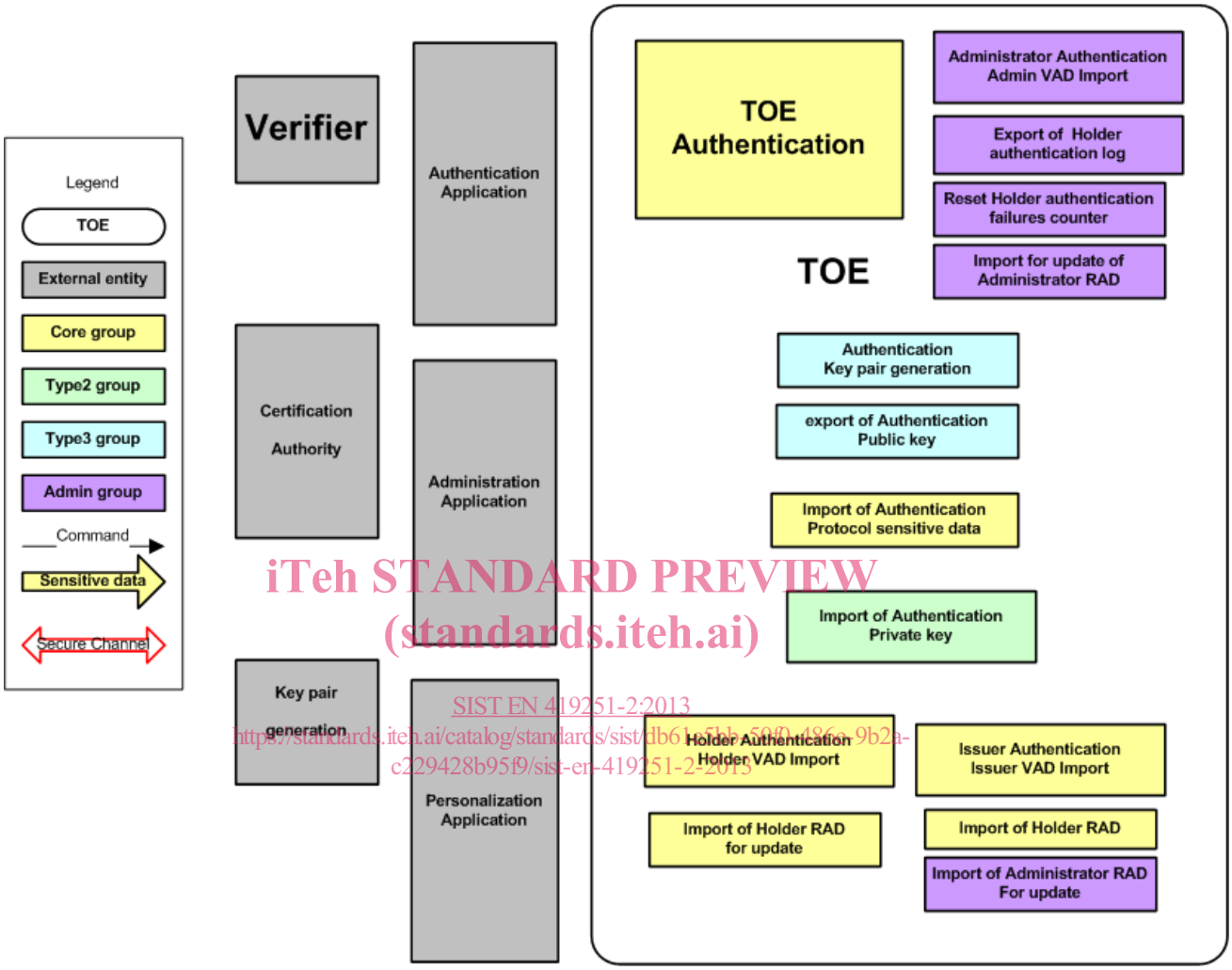

Figure 1 — TOE Security Features

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

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