SLOVENSKI STANDARD
SIST EN 419221-5:2018

01-julij-2018

Zaščitni profili za ponudnike storitev zaupanja za kriptografske module - 5. del: Kriptografski modul za storitve zaupanja

Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services

Schutzprofile für kryptographische Module von Vertrauensdienstanbietern - Teil 5: Kryptographisches Modul für vertrauenswürdige Dienste

Profils de protection pour les modules cryptographiques de prestataires de services de confiance - Partie 5: Module cryptographique pour les services de confiance

Ta slovenski standard je istoveten z: **EN 419221-5:2018**

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general
35.240.30	Uporabniške rešitve IT v informatiki, dokumentiranju in založništvu	IT applications in information, documentation and publishing

SIST EN 419221-5:2018 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419221-5

May 2018

ICS 35.040.01; 35.240.30

English Version

Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

Profils de protection pour les modules cryptographiques de prestataires de services de confiance - Partie 5: Module cryptographique pour les services de confiance

Schutzprofile für kryptographische Module von Vertrauensdienstanbietern - Teil 5: Kryptographisches Modul für vertrauenswürdige Dienste

This European Standard was approved by CEN on 2 March 2018.

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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

Tables

Figures

European foreword

This document (EN 419221-5:2018) has been prepared by Technical Committee CEN/TC 224 “Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”, 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 November 2018, and conflicting national standards shall be withdrawn at the latest by November 2018.

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

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

Clause 4 provides the introductory material for the Protection Profile.

Clause 5 provides the conformance claim.

Clause 6 provides the Security Problem Definition. It presents the Assets, Threats, Organisational Security Policies and Assumptions related to the TOE.

Clause 7 defines the security objectives for both the TOE and the TOE environment.

Clause 8 presents the extended components that will be used in this PP.

Clause 9 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [CC2] and Part 3 [CC3] that are to be satisfied by the TOE.

Clause 10 provides rationales to demonstrate that:

— Security Objectives satisfy the policies and threats;

— SFR match the security Objectives;

— SFR dependencies are satisfied;

— The SARs are appropriate.

A Bibliography is provided to identify background material.

A Mapping to the EU 'Requirements For Qualified Electronic Signature Creation Devices' is provided in Annex A.

1 Scope

This part of EN 419221 specifies a Protection Profile for cryptographic modules which is intended to be suitable for use by trust service providers supporting electronic signature and electronic sealing operations, certificate issuance and revocation, time stamp operations, and authentication services, as identified by the (EU) No 910/2014 regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Regulation (EU) No 910/2014 eIDAS) in [10]. The Protection Profile also includes optional support for protected backup of keys.

The document follows the rules and conventions laid out in Common Criteria Part 1 [CC1], Annex B "Specification of Protection Profiles".

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model (Version 3.1 Revision 4, September 2012), CCMB-2012-09-001 [CC1]

Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, (Version 3.1 Revision 4, September 2012), CCMB-2012-09-002 [CC2]

Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, (Version 3.1 Revision 4, September 2012), CCMB-2012-09-003 [CC3]

3 Terms and definitions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 419221-1, Common Criteria Part 1 [CC1] and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
assigned key
key (usually a secret key) with the 'Assigned Flag' attribute set to 'assigned', meaning that:

— the 'Re-authorization conditions' and 'Key Usage' attributes cannot be changed;

— the Authorization Data attribute can only be changed by presentation of the current Authorization Data – it cannot be changed or reset by an Administrator;

— the key cannot be imported or exported.

Note 1 to entry: These properties of an Assigned Key support the sole control of a key that is required for secret keys used to create digital signatures.

3.1.2
Authorization Data
data, including data particular to the user, which is used to control access to (and thus use of) a key. Data particular to the user may include data derived from a secret known only by the user, data derived from a device held by the user and/or data derived from biometric features of the user. Other parts of the authorization data may include data held within the cryptographic module, data held by administrator(s) or data provided by the application

3.1.3
electronic seal
data in electronic form which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity

3.1.4
electronic timestamp
data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time

3.1.5
secret key
either a secret key used in symmetric cryptographic functions, or a private key used in asymmetric cryptographic functions

3.1.6
trust service
electronic service which enhances trust and confidence in electronic transactions

Note 1 to entry: Such trust services are typically but not necessarily using cryptographic techniques or involving confidential material.

3.2 Abbreviations

For the purposes of this document, the abbreviations given in EN 419221-1 and the following apply.

CC	Common Criteria
DTBS	Data To Be Signed
DTBS/R	Data To Be Signed or its unique Representation
EAL	Evaluation Assurance Level
IT	Information Technology
PCIe	Peripheral Component Interconnect Express
PP	Protection Profile
RNG	Random Number Generator
SAR	Security Assurance Requirements
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSP	Trust Service Provider

4 Protection Profile

4.1 General

This clause provides document management and overview information that is required to carry out Protection Profile registration. 4.2 “PP Reference” gives labelling and descriptive information necessary for registering the Protection Profile (PP). 4.3 “Protection Profile Overview” summarizes the PP in narrative form. 4.4 “TOE Overview” summarizes the TOE in a narrative form. As such, these subclauses give an overview to the potential user to decide whether the PP is of interest.

4.2 Protection Profile Reference

Title	Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services
CC revision	v3.1 release 4
PP version	1.0
Authors	CEN/TC 224
Keywords	cryptographic module

4.3 Protection Profile Overview

4.3.1 General

This Protection Profile (PP) defines the security requirements for cryptographic modules used by trust service providers supporting electronic signing and sealing operations and authentication services. It includes optional support for protected backup of keys.

The Protection Profile is aimed at supporting trust services providers as identified by the proposed regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS) in Regulation (EU) 910/2014 [7].

The Cryptographic Module, which is the Target of Evaluation (TOE), generates and/or protects secret keys and other sensitive data, and allows controlled use of these data for one or more cryptographic services in support of TSP trust services.

This PP is Common Criteria Part 2 [CC2] extended and Common Criteria Part 3 [CC3] conformant. The assurance level for this PP is EAL4, augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis).

4.3.2 EU Qualified Electronic Signature / Seal Creation Device

Cryptographic Modules certified to this PP are intended to meet the security assurance requirements of Qualified Electronic Signature, and Electronic Seal, Creation Devices for use by trust service providers as specified in Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [7], although its use is not necessarily limited to such services. For further information see Annex A.

This Protection Profile is established by CEN for use by trust services including qualified trust services as identified in [7].

4.4 TOE Overview

4.4.1 TOE type

4.4.1.1 General

The TOE is a cryptographic module suitable for use by trust service providers supporting electronic signature and electronic sealing operations, certificate issuance and revocation, time stamp operations, and authentication services (including support of authentication of client applications or authorized users of secret keys, and support of authentication for electronic identification), as identified by the (EU) No 910/2014 regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS) in [7]. The TOE may also support protected backup of keys.

The TOE provides cryptographic functions that support trust services but is not, in general, aware of the context in which a cryptographic function is used. Any such context is therefore the responsibility of client applications used by the trust service provider, and these client applications need to use the cryptographic functions in an appropriate way. In general this will be achieved by suitable configuration of the TOE and its stored data (for example: to ensure that secret keys intended for electronic signature creation are only available for use by the signatory to whom they are linked, the client application shall follow an appropriate process to generate the key pair, to maintain sole control of the secret key by the intended signatory, and to ensure that the key can only be used for signing). As well as providing cryptographic functions, the TOE manages and protects the cryptographic keys used by these functions[1].

The TOE is therefore a set of configured software and hardware. Due to the generic TOE definition in this PP, the particular hardware/software/firmware required by the TOE is not defined by this PP. A generic TOE architecture is shown in Figure 1.

[1] As described in footnote 6, this Protection Profile includes a refinement to ADV_ARC.1 to consider support keys used in the implementation of the TOE and its protection measures.

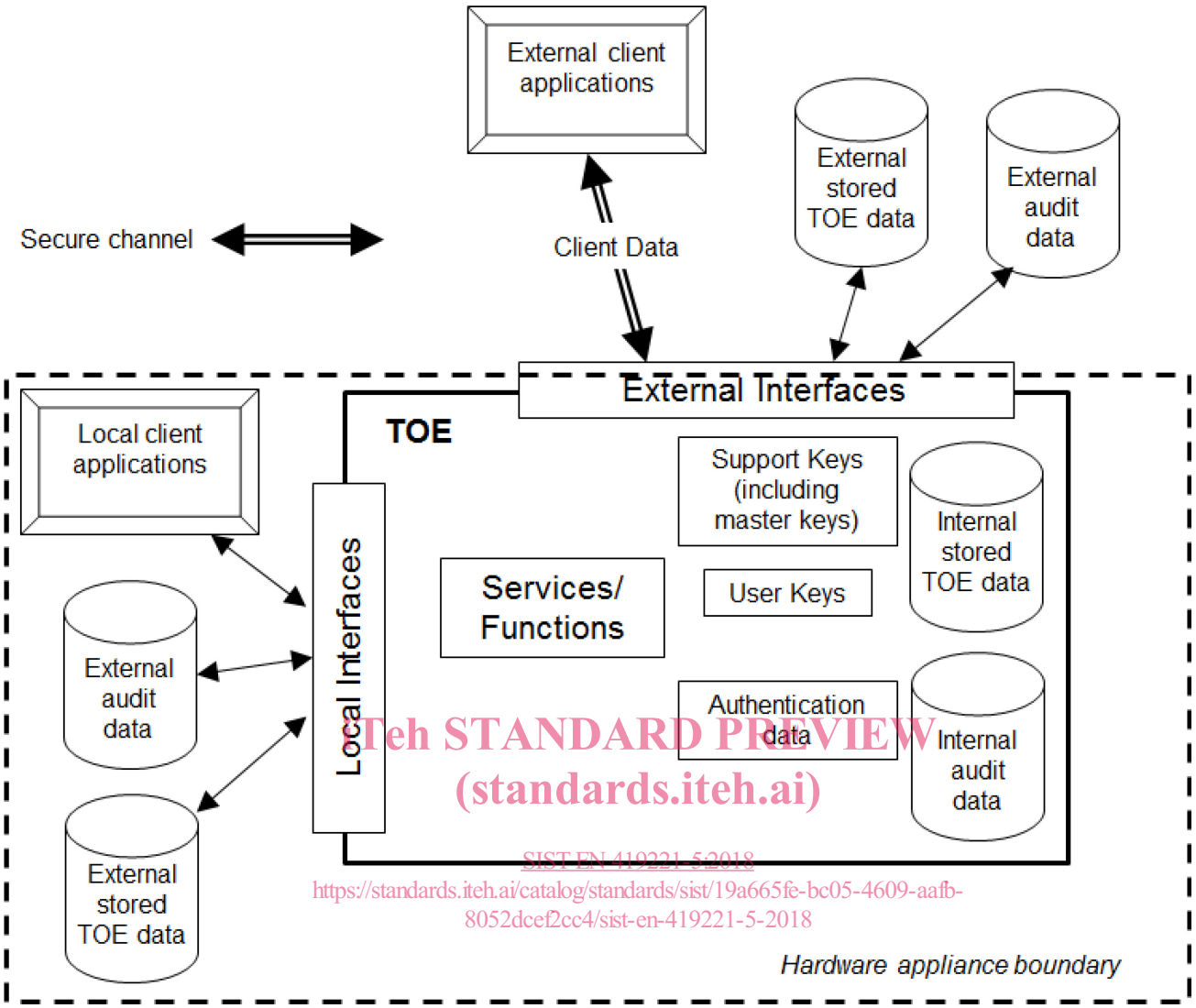

Figure 1 — Generic TOE Architecture

The hardware appliance boundary in Figure 1 represents the enclosure of the computing appliance which hosts the TOE. This can be a server, a PC or equivalent.

Local client applications reside in the same hardware appliance as the TOE, e.g. in the case of the TOE being a PCIe card inside a server, local client applications are the applications running within the same server boundary and using the TOE's services through the PCIe bus. Another example of local client application is an embedded application running inside the physical boundary of the TOE.

External client applications communicate remotely with the TOE through a network connection.

In all cases, the Client Application is outside the scope of the TOE.

A specific TOE will not necessarily include all of the elements shown in Figure 1. A TOE that comprises a PCIe card located in a server may have only local interfaces, e.g. for local client applications and storage of audit and TOE data within the server hardware boundary (which in this case is the hardware appliance boundary in Figure 1), but a dedicated cryptographic module might not include any such local storage and may use only external interfaces. The Security Target for each specific TOE is required to make clear what resources and channels are provided by that TOE.

The TOE is intended to support the provision of cryptographic functions for use by trust service providers.

The TOE implements separate authentication or authorization[2] of the following distinct types of entity:

— administrators of the TOE;

— application users of TOE cryptographic functions (local or external client applications, authenticated by their use of secure channels);

— users of secret keys (which in at least some cases need to have their use limited to a certain natural person or legal person[3]).

Acceptable authentication mechanisms include but are not limited to:

— Shared secret (e.g. password or key);

— Authentication based on asymmetric cryptography;

— Physical tokens;

— Biometrics;

— One time password.

More specific requirements on authentication may be applicable in the case of a TOE performing remote signing, as noted in 4.4.2.3, but these requirements are based on conformance with further Protection Profiles or other system security requirements directed specifically at remote signing.

If the TOE supports external client applications, then they are required to use a channel that provides authentication of its end-points and protection of confidentiality and integrity of data sent on the channel[4]. Where local client applications are connected to the TOE by a channel such as a PCIe bus within the same hardware appliance protected by measures in the physical environment, then the secure environment may be considered sufficient to provide the authentication, confidentiality and integrity protection needed for communication between the TOE and local applications. Secure channels may also exist between external and local client applications, but these are not within the scope of this Protection Profile.

Authorization as a user of a secret key is always separately required before a key can be used in a cryptographic function (or exported), regardless of any other authorization that may have been established for administrators or client applications. This requirement reflects the distinct activities that are being authorized in each case. Authorization to act as an administrator is an authorization to carry out management activities on the TOE, but not to *use* keys (in fact the requirement to be able to support sole control of a signature key means that in such cases an administrator shall not have access to use keys or to be able to access their values, unless the administrator happens also to demonstrate authorization as the owner of that key). Client applications are authorized to connect to the TOE in order to be able to invoke cryptographic functions, but the ownership of keys used in such functions

---

[2] In this document 'authentication' implies that the user is specifically identified, whereas 'authorization' implies that the authority of the user to use the key is established but the identity of the individual may not be known (e.g. where a single key is available to a number of individuals using a shared passphrase). As noted elsewhere, it is the responsibility of client applications to ensure that they use the correct mechanism for the context of the relevant keys and cryptographic functions.

[3] More details of these requirements and the definitions of natural and legal persons can be found in [10].

[4] A TOE may provide some additional channels that provide only authentication and integrity protection, but it shall provide at least one channel that is also capable of protecting confidentiality.