SLOVENSKI STANDARD
SIST-TS CEN/TS 419221-4:2017

01-januar-2017

Zaščitni profili za TSP kriptografske module - 4. del: Kriptografski modul za postopke podpisovanja CSP brez varnostne kopije

Protection Profiles for TSP cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup

Sicherheitsanforderungen für vertrauenswürdige Systeme zur Verwaltung von Zertifikaten für elektronische Signaturen - Teil 4: Kryptographisches Modul für CSP Signieroperationen - Schutzprofil (CMCSO-PP)

Exigences de sécurité concernant les systèmes fiables gérant des certificats de signatures électroniques - Partie 4 : Module cryptographique pour les opérations de signature électronique des fournisseurs de services de certification - Profil de protection - CMCSO PP

Ta slovenski standard je istoveten z: CEN/TS 419221-4:2016

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general
35.100.05	Večslojne uporabniške rešitve	Multilayer applications

SIST-TS CEN/TS 419221-4:2017 en,fr,de

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 419221-4

July 2016

ICS 35.240.30; 35.040

Supersedes CWA 14167-4:2004

English Version

Protection Profiles for TSP cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup

Exigences de sécurité concernant les systèmes fiables gérant des certificats de signatures électroniques - Partie 4 : Module cryptographique pour les opérations de signature électronique des fournisseurs de services de certification - Profil de protection - CMCSO PP

Schutzprofile für kryptographische Module von vertrauenswürdigen Dienstanbietern - Teil 4: Schutzprofil für CSP Signieroperationen ohne Sicherung

This Technical Specification (CEN/TS) was approved by CEN on 8 May 2016 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TS 419221-4:2016 E

Contents

Page

European foreword

This document (CEN/TS 419221-4:2016) 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 document supersedes CWA 14167-4:2004.

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

CEN/TS 419221, *Protection Profiles for TSP cryptographic modules*, is currently composed with the following parts:

— *Part 1: Overview*;

— *Part 2: Cryptographic module for CSP signing operations with backup*;

— *Part 3: Cryptographic module for CSP key generation services*;

— *Part 4: Cryptographic module for CSP signing operations without backup*.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: 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.

Introduction

This 'Cryptographic Module for CSP Signing Operations - Protection Profile' (CMCSO-PP) is issued by the European Committee for Standardization.

The document is for use by the European Commission in accordance with the procedure laid down in Article 9 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [1] as generally recognized standard for electronic-signature products in the Official Journal of the European Communities.

The document has been prepared as a Protection Profile (PP) following the rules and formats of the Common Criteria version 3.1r3 [CC1] [CC2] [CC3].

The set of algorithms for secure signature-creation devices and parameters for algorithms for secure signature-creation devices is given in a separate document, ETSI/TS 102 176.

This document has been originally prepared as a single Protection Profile and approved as CWA 14167-2:2002. Afterwards, while reviewing this Protection Profile for the evaluation, in order to make it conformant to the Common Criteria 2.1, two Protection Profiles have been created for the same TOE, one including the mandatory function of key backup and the other excluding this function:

— Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP), version 0,28; CWA 14167-2:2004;

— Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP), version 0.28; CWA 14167-4:2004.

Correspondence and comments to this Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP) should be referred to:

Editor: Rémy DAUDIGNY

Email: remy.daudigny@thalesgroup.com

1 Scope

This Technical Specification specifies a protection profile for cryptographic modules used by certification service providers (as specified in Directive 1999/93) for signing operations, without key backup. Target applications include root certification authorities (certification authorities which issue certificates to other CAs and is at the top of a CA hierarchy) and other certification service providers where there is a high risk of direct physical attacks against the module.

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.

CEN/TS 419221-1:2016, Protection Profiles for TSP cryptographic modules — Part 1: Overview

ETSI/TS 101 456, *Electronic Signature and Infrastructure (ESI); Policy requirements for certification authorities issuing qualified certificates*

ETSI/TS 102 176, *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in CEN/TS 419221-1:2016 apply.

4 PP Introduction

4.1 General

This clause provides document management and overview information that is required to carry out protection profile registry. Therefore, Subclause 4.2 “PP Reference” gives labelling and descriptive information necessary for registering the Protection Profile (PP). Subclause 4.3 “Protection Profile Overview” summarizes the PP in narrative form. Subclause 4.4 “TOE Overview” summarizes the TOE in a narrative form. As such, these clauses give an overview to the potential user to decide whether the PP is of interest. It is usable as standalone abstract in PP catalogues and registers.

4.2 PP Reference

Title	Cryptographic Module for CSP Signing Operations – Protection Profile
CC revision	v3.1 release 3
PP version	v0.33
Authors	Rémy Daudigny
Publication Date	2015
Keywords	cryptographic module, CSP signing device, qualified certificate signing, certificate status information signing
Registration	419221–4

4.3 Protection Profile Overview

The Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 *on a Community framework for electronic signatures* [1], referred to as the 'Directive' in the remainder of the PP, states in Annex II that:

> *Certification-service-providers must:*
>
> *(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;*
>
> *(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;*

In the supporting ETSI Technical Specification "Policy Requirements for Certification Authorities (CA)[1)] issuing Qualified Certificates" (ETSI/TS 101 456), it is stated that:

> *The CA shall ensure that CA keys are generated in accordance with industry standards, and*
>
> *The CA shall ensure that CA private keys remain confidential and maintain their integrity.*

This Protection Profile (PP) defines the security requirements of a Cryptographic Module (CM) used by CSP as part of its trustworthy system to provide signing services, such as Certificate Generation Service or Certificate Status Information Signing Services. The Cryptographic Module, which is the Target of Evaluation (TOE), is used for the creation of CSP key pairs, and their usage for the creation and verification of advanced electronic signatures in qualified certificates or certificate status information. The private keys are referred to in this PP as Certification Service Provider Signature-Creation Data (CSP-SCD). The public keys are referred as Certification Service Provider Signature-Verification Data (CSP-SVD).

The Protection Profile's primary scope is for signing qualified certificates. However components evaluated against this standard may be applied for other signature-creation tasks carried out by a certificate service provider (CSP) such as time-stamping, signing certificate revocation lists (CRLs) or issuing online certificate status protocol (OCSP) messages. It may also be used for other trusted service providers creating electronic signatures.

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

In Article 3.5, the Directive further states that:

> *The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognized standards for electronic-signature products in the Official Journal of the European Communities. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards."*

This Protection Profile is established by CEN/ISSS for use by the European Commission, with reference to Annex II (f), in accordance with this procedure.

1) In the remainder of this PP the term 'Certificate Service Provider (CSP)' is used instead of the commonly used term 'Certification Authority (CA)', as the former is employed by the Directive EC 1999/93 [1] this PP aims to support.

4.4 TOE Overview

4.4.1 TOE type

The TOE is a Cryptographic Module (CM) used for the creation and usage of Certificate Service Provider Signature-Creation Data (CSP-SCD). The CM may optionally also perform hashing of the qualified certificate content.

The TOE is configured software and hardware that may be used to provide the following cryptographic functions:

a) Generation of CSP-SCD

b) Usage of the CSP-SCD to create advanced electronic signatures for qualified certificates based on either

   1) the hash value of the content of the qualified certificate, or

   2) an intermediate hash-value of a first part of the qualified certificate and a remaining part of the qualified certificate or

   3) the complete content of the qualified certificate, where the hashing is also performed in the CM (optional).

The TOE may implement additional functions and security requirements, e.g. for the creation of Signature Creation Data (SCD) for loading into Secure Signature Creation Devices (SSCD) as part of a Subscriber Device Provision Service. However, these additional functions and security requirements are not subject of this Protection Profile.

The TOE shall provide the following additional functions to protect these cryptographic functions:

- User authentication
- Access control for the creation and destruction of keys
- Access control for usage of keys to create certificate signatures
- Auditing of security-relevant changes to the TOE
- Self-test of the TOE

The TOE shall handle the following User Data:

c) CSP Signature Creation Data (CSP-SCD): private key of CSP, created and stored internally in the TOE

d) Data to be signed representation (DTBS-representation): The data to be signed by the TOE may e.g. be:

   1) Certificate hash value: imported to the TOE

   2) Certificate contents (optional, when hashing is performed in the TOE), data to be hashed (fully or partially) and signed, imported to the TOE

   3) other data to be signed by the TOE, such as CRL or the hash value of the CRL, or time-stamping content data

e) Certificate signature: created signature, exported from the TOE.

The TOE does not support backup and restoration of data. For the cryptographic functions, the TOE shall support the cryptographic algorithms specified in ETSI/TS 102 176, or a subset thereof.

4.4.2 TOE Roles

The TOE shall as a minimum support the following user categories (roles):

- **Crypto-officer** (authorized to install, configure and maintain the TOE and to create and destruct the CSP-SCD)
- **Crypto-user** (authorized to sign with existing CSP-SCDs)
- **Auditor** (authorized to read audit data generated by the TOE and exported for audit review in the TOE environment)

The TOE may support other roles or sub-roles in addition to the roles specified above. The roles may also be allowed to perform additional functions provided by the TOE as long as the separation between different roles is given.

The interface to the TOE may either be shared between the different user categories, or separated for certain functions, for example configuration.

Authentication of TOE users shall be identity-based.

Maintenance of the TOE as well as the management of the CSP-SCDs are highly critical operations that need to be related to the individual users that performed the operation. It is therefore required that for the roles System Auditor and Security officer of the CSP [CEN] the individual users shall be known by the TOE as Auditor and Crypto-officer and the TOE needs to perform identity based authentication for those roles. The Crypto-officer role is very powerful including user and key management. Therefore the Auditor role is implemented to watch on Crypto-officer's actions and to detect misuse of Crypto-officer's authorization.

The TOE manages two or more user identities for the role Crypto-officer to allow dual person control for security critical actions like generation of CSP-SCD and CSP-SVD generation. The end-users may access to the TOE signing service through a client application in the TOE environment. The client application acts as agent for these end-users with a TOE user identity in the Crypto-user role.

4.4.3 Usage and major security features of the TOE

In most cases the TOE will be a separate component with its own hardware and software, communicating via a well-defined physical and logical interface with the client application in the IT environment. Examples of physical interfaces that may be used to connect the TOE to the client application are the PCI bus, the SCSI bus, USB or Firewire.

Logically the TOE is responsible for protecting the CSP-SCD against disclosure, compromise and unauthorized modification and for ensuring that the TOE services are only used in an authorized way.

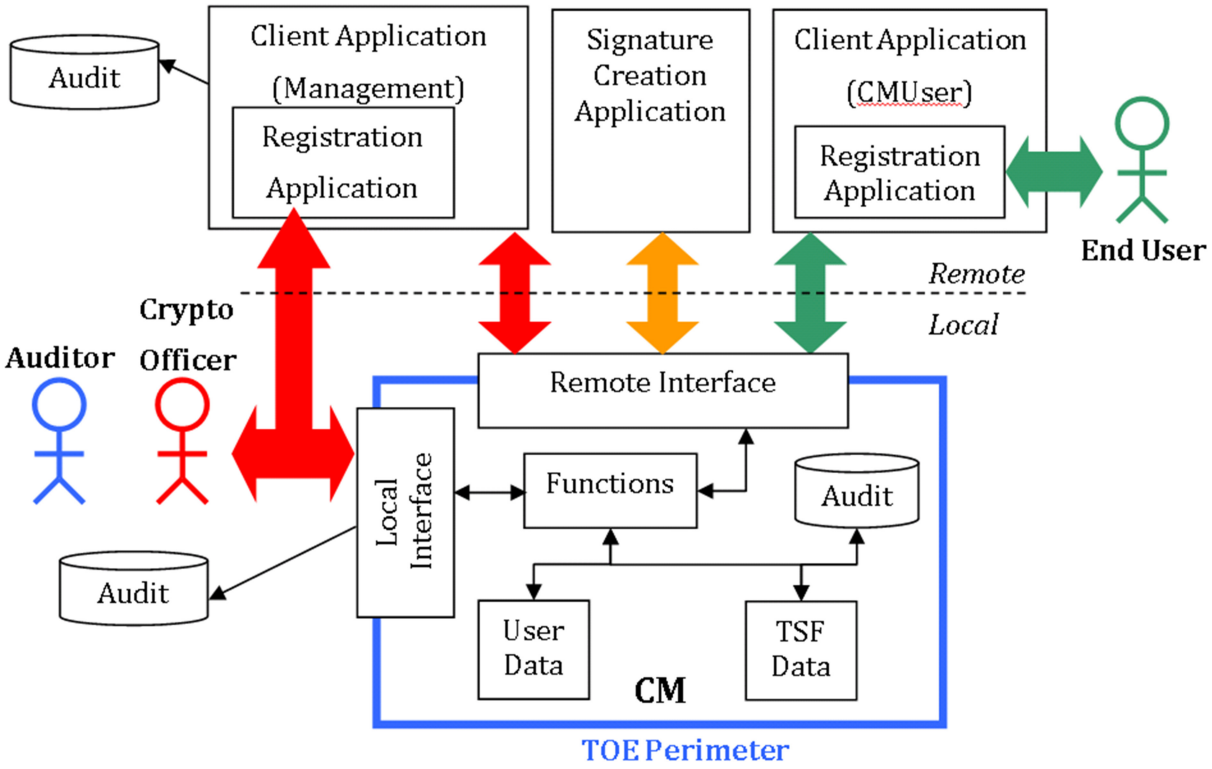

Figure 1 — TOE general overview

NOTE This diagram is illustrative. It need not represent the exact implementation architecture

As shown in Figure 1, no relation exists with Trusted Service Providers (TSP). The end-users will communicate with the client application, which in turn will call TOE services on behalf of the end-user.. The client application provides the human interface for user identification and authentication. The client application is responsible for passing any user data in a correct way to the TOE. Different mechanisms may be used to protect the user data on its way from the originating user to the TOE, but all those mechanisms are not part of the TOE functionality and therefore not defined in this Protection Profile.

The TOE provides identification authentication, access control and audit for users of its services. The client application in the TOE environment may mediate the TOE signing function to its end-users. Therefore it is the responsibility of the client application to identify, authenticate and control access of its end-users gaining access to the TOE services provided for the Crypto-user role. The end-users authenticate themselves to the client application with his or her identity. The client application checks the authorization of the end-user for the TOE signing service. If the end-user is allowed to use the signing function the client application will authenticate them for the Crypto-user role to the TOE and will map the identity of the end-user to the Crypto-user role. The client application performs identity-based auditing to support accountability for the cryptographic operations. While the TOE will only perform auditing for the client application the TOE environment audit might distinguish between the end-users of the client application.

The client application that communicates with the TOE may itself consist of different parts implemented on different systems. For example, a client application that initiates the generation of qualified certificate may consist of two parts:

a) a registration application, which initializes the information for the certificate.

b) a signature-creation application, which may be

1) a certification application, which verifies the integrity and authenticity of the request submitted by the registration application and then calls the TOE service to sign the certificate or

2) other applications requesting the TOE to sign DTBS-representations, e.g. certificate status information. The application verifies integrity and authenticity of the signature request.

Privileged users as Crypto-officer and Auditor can interact with the TOE through the local interface. They can also connect remotely to the TOE thanks to a Client Application that offers Management capabilities. This application performs identity-based auditing to support accountability for the privileged operations. The Client Application used for Management purposes and the Client Application used by the end-user are represented in Figure 1 as separate applications. Nevertheless, they are very similar (RBAC authentication, Registration of user for accountability …) and rely on the same security functions for protecting communications with the Cryptomodule.

Finally, the TOE supports a secure firmware update mechanism where updating data are protected in integrity, confidentiality and authenticity (signed).

4.4.4 Available non-TOE hardware/software/firmware

None. The TOE is an independent Cryptographic Module comprising its own hardware and software.

5 Conformance Claim

5.1 CC Conformance Claim

This protection profile is conformant to Common Criteria version 3.1 revision 3.

More precisely, this protection profile is:

- CC Part 1 [CC1],
- CC Part 2 extended [CC2],
- CC Part 3 conformant [CC3].

The assurance requirement of this Protection Profile is **EAL4 augmented**.

Augmentation results from the selection of:

- AVA_VAN.5 Advanced methodical vulnerability analysis

5.2 PP Claim

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

5.3 Conformance Rationale

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

5.4 Conformance Statement

This PP requires strict conformance of any ST or PP, which claims conformance to this PP.