SLOVENSKI STANDARD
SIST-TS CEN/TS 419221-3:2017

01-januar-2017

Zaščitni profili za TSP kriptografske module - 3. del: Kriptografski modul za CSP storitve generiranja ključa

Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services

Sicherheitsanforderungen für vertrauenswürdige Systeme zur Verwaltung von Zertifikaten für elektronische Signaturen - Teil 3: Kryptographisches Modul für CSP Schlüsselgenerierungsdienste - Schutzprofil (CMCKG-PP)

Exigences de sécurité concernant les systèmes fiables gérant des certificats de signatures électroniques - Partie 3 : Module cryptographique utilisé par le fournisseur de service de certification pour la création de clés - Profil de protection (CMCKG-PP)

Ta slovenski standard je istoveten z: **CEN/TS 419221-3:2016**

ICS:

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

SIST-TS CEN/TS 419221-3:2017 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 419221-3

July 2016

ICS 35.040; 35.240.30

Supersedes CWA 14167-3:2004

English Version

Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services

Profils de protection pour modules cryptographiques utilisés par les prestataires de services de confiance - Partie 3 : Module cryptographique utilisé par le prestataire de services de certification pour la génération de clés

Schutzprofile für kryptographische Module von vertrauenswürdigen Dienstanbietern - Teil 3: Kryptographisches Modul für CSP Schlüsselgenerierungsdienste

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 419221-3:2016 E

Contents

Page

European foreword

This document (CEN/TS 419221-3:2016) 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.

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 supersedes CWA 14167-3:2004.

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 of 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

0.1 General

This CEN Technical Standard specifying a Protection Profile for Cryptographic Module for CSP Key Generation Services 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 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 Protection Profile, as generally recognized standard for electronic-signature products in the Official Journal of the European Communities.

The Directive 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) issuing Qualified Certificates" (ETSI/TS 101 456), it is stated that the CA[1)] needs to ensure that:

any subject keys, that it generates, are generated securely and the secrecy of the subject's private key is ensured (see the Directive [1], Annex II (f) and (j)).

And, if the CA generates the subject keys:

a) CA-generated subject keys shall be generated using an algorithm recognized as being fit for the purposes of qualified electronic signatures during the validity of the certificate;

b) CA-generated subject keys shall be of a key length and for use with a public key algorithm which is recognized as being fit for the purposes of qualified electronic signatures during the validity time of the certificate;

c) CA-generated subject keys shall be generated and stored securely before delivery to the subject.

d) The subject's private key shall be delivered to the subject, if required via the subscriber, in a manner such that the secrecy and the integrity of the key is not compromised and, once delivered to the subject, the private key can be maintained under the subject's sole control.

e) Once delivered to the subject any copies of the subject's private key held by the CA shall be destroyed.

This Protection Profile (PP) defines the security requirements of a Cryptographic Module (CM) used by CSP as part of its trustworthy system to provide key generation services. The Cryptographic Module, which is the Target of Evaluation (TOE), is used for the creation of subscriber private keys, and loading them into secure signature creation devices (SSCD) as part of a subscriber device provision service. Such keys are referred to in this PP as subscriber signature creation data. A cryptographic module for CSP key generation services is needed particularly to import such key into the SSCD [8].

The subscriber signature creation data generated by the TOE may be used to produce qualified electronic signatures, as defined by the Directive, or electronic signatures not necessarily qualified (e.g. advanced electronic signatures, digital signatures for other purposes different than authentication, etc.).

The TOE may implement additional functions and security requirements, e.g. for CSP Signing Operations. However, these additional functions and security requirements are not subject of this PP.

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 [1] this PP aims to support.

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 PP is for use by the European Commission, with reference to Annex II (f) and Annex III, in accordance with this procedure.

The document has been prepared as a Protection Profile following the rules and formats of the Common Criteria version 3.1 R3 [2] [3] [4]. This PP has been evaluated, and the corresponding Common Criteria certificate can be found in Bibliographical Reference [5].

The set of algorithms and parameters for secure signature-creation devices shall be in accordance with national guidance, and subject to each Certification Body. Notwithstanding, recommendations for algorithms and parameters for secure electronic signatures are given in ETSI/TS 102 176 [6].

Correspondence and comments to this Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP) should be referred to:

Editor: Dr. Jorge López Hernández-Ardieta

Email: jlhardieta@indra.es

0.2 Document Structure

Clause 1 provides the scope of the Protection Profile.

Clause 2 provides normative references of applicability to this Protection Profile.

Clause 3 provides the terms and definitions used along the document.

Clause 4 contains the Introduction of the Protection Profile, including the PP reference and the TOE overview.

Clause 5 includes the conformance claims for this Protection Profile.

Clause 6 contains the security problem definition, including the set of TOE assets to protect, the expected threats to those assets, the organizational security policies in place and the assumptions made on the TOE.

Clause 7 contains the security objectives for the TOE and the TOE operational environment, and which address the threats, organizational security policies and assumptions considered. This section also includes a rational of correspondence between the security objectives and the threats, organizational security policies and assumptions.

Clause 8 contains the security functional requirements (SFR) and security assurance requirements (SAR) derived from the Common Criteria (CC) Part 2 [3] and Part 3 [4], respectively, and that need to be satisfied by the TOE and developer. This clause introduces first the formalism used to describe the operations (refinement, selection, assignment and iteration) applied along the SFR descriptions. After the SFR and SAR have been described, this section provides the rationale to explicitly demonstrate that the set of SFR are complete with respect to the objectives, and that each security objective is addressed by one or more SFR. Arguments are provided for the coverage of each objective. The rational part also provides a justification for the selection of EAL4+ AVA_VAN.5 as the assurance level.

Finally, a Bibliography is given.

1 Scope

This Technical Standard specifies a protection profile for cryptographic module for CSP key generation services.

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 Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, V1.4.3, May 2007*

3 Terms and definitions

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

4 General

4.1 PP reference

Title:	Cryptographic module for CSP key generation services protection profile CMCKG-PP
Author:	Jorge López Hernández-Ardieta
Version:	0.20
Publication date:	27th January 2015

4.2 TOE overview

4.2.1 TOE usage and major security features

The TOE is a Cryptographic Module (CM) used for the generation of subscribers Signature Creation Data (Subscriber-SCD) and Signature Verification Data (Subscriber-SVD) and their export to the subscribers Secure Signature Creation Devices (SSCD), in a manner that:

— the confidentiality and integrity of the Subscriber-SCD are maintained both when managed by the TOE and during transfer from the TOE to an external entity (i.e. the Subscriber-SSCD);

— the integrity of the Subscriber-SVD is maintained both when managed by the TOE and during transfer from the TOE to an external entity (i.e. the Subscriber-SSCD or the certificate generation application, CGA);

— the TOE services (generation of subscribers Subscriber-SCD/Subscriber-SVD and their export to the subscribers SSCD/CGA) are only used in an authorized way.

The TOE shall provide the following additional functions to protect the TOE services:

— user authentication;

— access control for use of the Subscriber-SCD/SVD generation and export functions;

— auditing of security-relevant changes to the TOE;

— self-test of the TOE.

The TOE shall handle the following User Data:

— Subscriber Signature Creation Data (Subscriber-SCD): private key of a subscriber created internally in the TOE and loaded into a SSCD;

— Subscriber Signature Verification Data (Subscriber-SVD): public key of a subscriber created internally in the TOE and loaded into a SSCD, transferred to a CGA, or both. This data may also be distributed to additional entities.

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

— crypto-officer, authorized to install, configure and maintain the TOE, and to generate and export Subscriber-SCD/SVD pairs;

— auditor, authorized to read audit data generated by the TOE and exported for audit review in the TOE environment.

The Crypto-officer is responsible for the day-by-day operation of the TOE, including user management. The TOE should manage two or more user accounts for the role Crypto-officer to allow dual person control for security critical actions like generation and export of Subscriber-SCD/SVD pairs.

The TOE supports a separate Auditor role authorized to manage and review audit data generated by the TOE in the TOE environment. The Crypto-officer will be able to read but not to delete audit data. The Auditor shall not be able to initiate the functions to generate and/or export Subscriber-SCD/Subscriber-SVD.

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. As stated above for the auditor role, none of those additional roles shall be able to generate and/or export Subscriber-SCD/SVD pairs.

The interface to the TOE may be either shared between the different user categories, or separated for certain functions. Authentication for all user categories shall be identity-based.

Next Figure shows an overview of the TOE and its relations with the operational environment and TOE users.

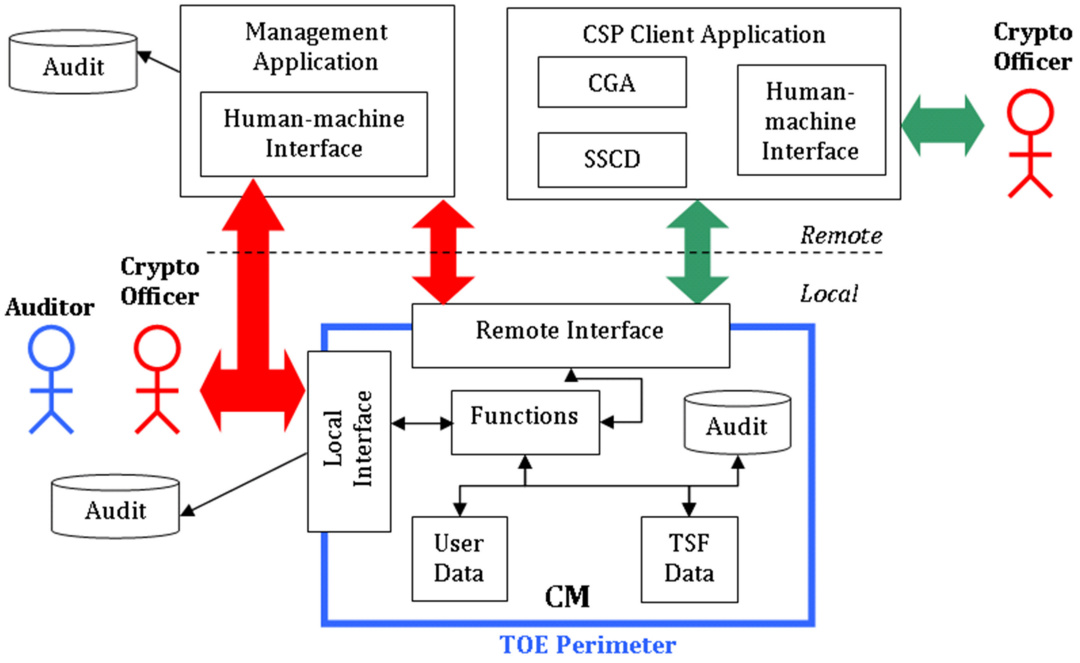

Figure 1 — TOE Overview

As can be seen in the Figure, no relation exists with Trusted Service Providers (TSP). Users can access the TOE services using local and remote interfaces. Users holding the role Crypto-officer or Auditor can access the TOE remotely, by means of the Management Application, or locally. In addition, Crypto-officers can also access the TOE in a remote manner using the CSP Client Application, which provides support to the CGA and SSCD operations.

4.2.2 TOE type

The TOE will be a separate component within the CSP boundaries with its own hardware and software, communicating via a well-defined physical and logical interface with the CSP Client Application and the Management Application. Examples of physical interfaces that may be used to connect the TOE to the CSP Client Application and Management Application are the PCI bus, the SCSI bus, USB or Firewire.

4.2.3 Available non-TOE hardware/firmware/software

None. The TOE is an independent cryptographic module comprising its own hardware, software and firmware.

5 Conformance Claims

5.1 CC conformance claim

This Protection Profile (PP) complies with Common Criteria, version 3.1, revision 3, July 2009, for both the content and presentation requirements.

All functional and assurance security requirements laid out in this PP comply with CC Part 2 and CC Part 3 respectively of the aforementioned Common Criteria version.

This PP is conforming to assurance package Evaluation Assurance Level 4 augmented (EAL4+) as defined in Part 3 of the aforementioned Common Criteria version. 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 other PP.

5.3 Conformance rationale

This PP does not provide a conformance rationale because it does not claim conformance to any other PP.

5.4 Conformance statement

The PP requires strict conformance of the ST or PP claiming conformance to this PP.

6 Security Problem Definition

6.1 TOE assets

The primary assets that need to be protected by the TOE are the following:

TOE services:

a) **R.SERVICES**: user identity and role management, generation of Subscriber-SCD/Subscriber-SVD and their export to the subscribers SSCD, and internal audit. TOE services shall be protected in integrity and availability.

TOE internal data:

b) **R.SUBSCRIBER-SCD**. Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature (defined in the Directive [1], Article 2.4). Subscriber-SCD shall be protected both in confidentiality and integrity.

c) **R.SUBSCRIBER-SVD**. Data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature (defined in the Directive [1], Article 2.4). Subscriber-SVD shall be protected in integrity.

d) **R.AUDIT_DATA**. Internal audit records and that shall be protected in integrity and availability.

e) **R. TSF_DATA**: TSF data, including:

   1) VAD and RAD, which shall be protected in confidentiality, integrity and availability.

   2) Non-confidential user/role related data (identifier, access control lists, role definitions, etc.). These data shall be protected in integrity.

Next table correlates the TOE internal data types explained above with those data types considered in the formalization of the security functional requirements (SFR):

TOE internal data type	SFR-related data type
R.SUBSCRIBER-SCD	User data[a]
R.SUBSCRIBER-SVD	
R.AUDIT_DATA	
R. TSF_DATA	TSF data[b]

[a] Data for the user that does not affect the operation of the TSF (TOE Security Functionality). For example, in the case of R.AUDIT_DATA, the audit records generated internally in the TOE are intended to be revised by the Auditor.

[b] Data for the operation of the TOE upon which the enforcement of the SFR relies.

6.2 Threats

The expected attackers are qualified so as to have high attack potential, in accordance with the security assurance given by AVA_VAN.5 Advanced methodical vulnerability analysis.

The expected threat agents are:

— **TA.EXTERNAL**

This agent represents an entity that does not hold any authorized role to operate or interact with the TOE. This agent may operate through the remote or local interfaces, or even have direct physical access to the TOE. Examples of this threat agent are: unauthorized CSP personnel, cybercriminals, and hackers in general.

— **TA.INSIDER**

This agent represents an entity that holds an authorized role to operate or interact with the TOE, and which has the intention to compromise the TOE assets. This agent may operate through the remote or local interfaces, or even have direct physical access to the TOE. Examples of this threat agent are: auditors and crypto-officers.

— **TA.INADVERTENT**

This agent represents an entity that holds an authorized role to operate or interact with the TOE, but which does not have the intention to compromise the TOE assets. This agent may operate through the remote or local interfaces, or even have direct physical access to the TOE. Examples of this threat agent are: auditors and crypto-officers.

The expected threats to the TOE may be:

— **T.Bad_SW** Malicious Software during the Lifetime of the TOE

A TA.EXTERNAL or a TA.INSIDER might try to load malicious software into the TOE in order to modify or gain illicit access to R.SUBSCRIBER-SCD, R.AUDIT_DATA, R.TSF_DATA or R.SERVICES.

For example, a TA.EXTERNAL, using the TOE remote interface, may inject a malicious code (malware) into the TOE. Later on, this malware may compromise the confidentiality of the R.SUBSCRIBER-SCD by exfiltrating its value from the TOE boundaries.

— **T.Insecure_Init** Insecure Initialization of the TOE

A TA.EXTERNAL, a TA.INSIDER or a TA.INADVERTENT may initialize the TOE with insecure R.TSF_DATA.

— **T.Malfunction** Malfunction of TOE

There is no active agent for this threat.

An internal malfunction of TOE functions may result in:

- misuse of R.SERVICES,
- disclosure or alteration of R.SUBSCRIBER-SCD,
- alteration of R.SUBSCRIBER-SVD,
- denial of R.SERVICES for authorized users,
- alteration of R.AUDIT_DATA or R.TSF_DATA.

This includes the destruction of the TOE as well as hardware failures, which prevent the TOE from performing its services.

This includes also the destruction of the TOE by environmental failure.

Finally, this includes some kind of physical tampering that induces erroneous behaviour from the underlying hardware or software of the ToE.

Technical failure may result in an insecure operational state violating the integrity and availability of the TOE services.

The correct operation of the TOE also depends on the correct operation of critical hardware components. Critical components might be:

- the central processing unit
- a coprocessor for accelerating cryptographic operations
- a physical random number generator
- storage devices used to temporarily store cryptographic keys
- physical I/O device drivers

— **T.Misuse** Misuse of TOE

A TA.INSIDER or a TA.INADVERTENT, who has access to the TOE R.SERVICES, uses these services in a manner for which they are not intended to, or without proper authorization, having an impact on the R.SUBSCRIBER-SCD, R.SUBSCRIBER-SVD, R.AUDIT_DATA or R.TSF_DATA.

For instance, a TA.INSIDER such as CSP personnel without authorization to generate R.SUBSCRIBER-SCD and R.SUBSCRIBER-SVD pairs may misuse the TOE R.SERVICES to do so.

— **T.Phys_Manipul** Physical Manipulation of the TOE

A TA.EXTERNAL or a TA.INSIDER may try to physically manipulate the TOE with the intent to derive all or part of the R.SUBSCRIBER-SCD (by side channel for example), to misuse TOE