SLOVENSKI STANDARD
SIST-TS CEN/TS 419221-1:2017

01-januar-2017

Zaščitni profili za kriptografske module TSP - 1. del: Pregled

Protection Profiles for TSP cryptographic modules - Part 1: Overview

Schutzprofile für kryptographische Module von vertrauenswürdigen Dienstanbietern - Teil 1: Überblick

Profils de protection pour modules cryptographiques utilisés par les prestataires de services

Ta slovenski standard je istoveten z: CEN/TS 419221-1:2016

<u>**ICS:**</u>

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

SIST-TS CEN/TS 419221-1:2017 en,fr,de

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 419221-1

July 2016

ICS 35.040; 35.240.30

Supersedes CWA 14167-1:2003

English Version

Protection Profiles for TSP cryptographic modules - Part 1: Overview

Profils de protection pour modules cryptographiques utilisés par les prestataires de services de confiance - Partie 1 : Vue d'ensemble

Schutzprofile für kryptographische Module von vertrauenswürdigen Dienstanbietern - Teil 1: Überblick

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

Contents

Page

European foreword 3

Introduction 4

1 Scope 5

2 Normative references 5

3 Terms and definitions 5

4 Protection profiles specified in CEN/TS 419221 10

4.1 General 10

4.2 CEN/TS 419221-2: Cryptographic module for CSP signing operations with backup 10

4.3 CEN/TS 419221-3: Cryptographic module for CSP key generation services 10

4.4 CEN/TS 419221-4: Cryptographic module for CSP signing operations without backup 10

4.5 CEN/TS 419221-5: Cryptographic Module for Trust Services 10

Bibliography 12

European foreword

This document (CEN/TS 419221-1:2016) 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 14167-1:2003.

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

This multi-part standard specifies protection profiles for trust service provider cryptographic modules, as per common criteria (ISO/IEC 15408 series). Target applications include signing by certification service providers, as specified in Directive 1999/93, as well as supporting cryptographic services for use by trust service providers.

1 Scope

This Technical Specification provides an overview of the protection profiles specified in other parts of CEN/TS 419221.

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 419241, *Security Requirements for Trustworthy Systems Supporting Server Signing*

ISO/IEC 15408 (all parts)[1], *Information technology — Security techniques — Evaluation criteria for IT security*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
administrator
CSP user role that performs TOE initialization or other TOE administrative functions

Note 1 to entry: These tasks are mapped to the Crypto-officer role of the TOE.

3.2
advanced electronic signature
electronic signature which meets the following requirements (defined in Directive 1999/93/EC [1], Article 2.2):

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using means that the signatory can maintain under his sole control, and

d) it is linked to the data to which it relates in such a manner that any subsequent change of the data are detectable

3.3
authentication data
information used to verify the claimed identity of a user

[1] The following are equivalent to the aforementioned ISO/IEC 15408 standards:

— Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3. CCMB-2009-07-001, July 2009;

— Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 3. CCMB-2009-07-002, July 2009;

— Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 3. CCMB-2009-07-003, July 2009.

3.4
auditor
user exporting the TOE audit data and reviewing the audit data with tools in the TOE environment

3.5
backup
export of the CSP_SCD, the TSF data and the system data (backup data) sufficient to recreate the state of the TOE at the time the backup was created

Note 1 to entry: Backup is the only function which is allowed to export CSP_SCD and only if backup package is implemented.

3.6
certificate
electronic attestation which links the SVD to a person and confirms the identity of that person (defined in Directive 1999/93/EC [1], Article 2.9)

3.7
certificate generation application
CGA
collection of application elements which requests the SVD from the device generating the SCD/SVD pair for generation of the qualified certificate

Note 1 to entry: The CGA stipulates the generation of a correspondent SCD/SVD pair, if the requested SVD has not been generated by the SCD/SVD generation device yet. The CGA verifies the authenticity of the SVD by means of (a) the SSCD proof of correspondence between SCD and SVD and (b) checking the sender and integrity of the received SVD.

3.8
certification-service-provider
CSP
entity or a legal or natural person who issues certificates or provides other services related to electronic signatures (defined in Directive 1999/93/EC [1], Article 2.11)

Note 1 to entry: In common usage this is often referred to as Certification Authority (CA). A CSP is a type of TSP.

3.9
cryptographic module
set of hardware, software and firmware used to generate the Subscriber-SCD/Subscriber-SVD pair and which represents the TOE

3.10
CSP signature creation data
CSP_SCD
SCD which is used by the CSP, e.g. for the creation of advanced electronic signatures in qualified certificates or for signing certificate status information

3.11
CSP signature verification data
CSP_SVD
SVD which corresponds to the CSP_SCD and which is used to verify the advanced electronic signature in the qualified certificate or the certificate status information

3.12
data to be signed
DTBS
complete electronic data to be signed, such as QC content data or certificate status information

3.13
data to be signed representation
DTBS-representation
data sent to the TOE for signing which is:

a) a hash-value of the DTBS or

b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or

c) the DTBS itself

Note 1 to entry: The client indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in Case a) or the intermediate hash-value in Case b) is calculated by the client. The final hash-value in Case b) or the hash-value in Case c) is calculated by the TOE.

3.14
digital signature
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of that unit and protect against forgery e.g. by the recipient

3.15
Directive
Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1], which is also referred to as the “Directive” in the remainder of the PP

3.16
dual person control
special form of access control of a task which requires at least two users with different identities to be authenticated and authorized to the defined roles at the time this task is to be performed

3.17
hardware security module
HSM
cryptographic module used to generate the advanced signature in qualified certificates and which represents the TOE

3.18
list of approved algorithms and parameters
approved cryptographic algorithms and parameters for secure signature-creation devices that needs to be in accordance with national guidance, and subject to each Certification Body

Note 1 to entry: Notwithstanding, recommendations for algorithms and parameters for secure electronic signatures are given in ETSI/TS 119 312 [2].