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