

STN	Profily ochrany kryptografických modulov pre poskytovateľov dôveryhodných služieb. Časť 2: Kryptografický modul pre poskytovateľov certifikačných služieb na podpisovanie so zálohou.	STN P CEN/TS 419221-2 97 6011
------------	--	---

Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 10/16

Táto predbežná STN je určená na overenie. Pripomienky zasielajte ÚNMS SR najneskôr do 31. 7. 2018.

Obsahuje: CEN/TS 419221-2:2016

123639

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, 2016
Podľa zákona č. 264/1999 Z. z. v znení neskorších predpisov sa môžu slovenské technické normy rozmnožovať a rozširovať iba so súhlasom Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

English Version

Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup

Profils de protection pour modules cryptographiques
utilisés par les prestataires de services de confiance -
Partie 2 : Module cryptographique utilisé par le
prestataire de services de certification pour les
opérations de signature avec sauvegarde

Schutzprofile für kryptographische Module von
vertrauenswürdigen Diensteanbietern - Teil 2:
Schutzprofil für CSP Signieroperationen mit 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

Contents	Page
European foreword.....	4
Introduction	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	6
4 PP Introduction.....	6
4.1 General.....	6
4.2 PP Reference.....	6
4.3 Protection Profile Overview.....	7
4.4 TOE Overview	8
4.4.1 TOE type	8
4.4.2 TOE Roles	9
4.4.3 Usage and major security features of the TOE.....	9
4.4.4 Available non-TOE hardware/software/firmware.....	11
5 Conformance Claim	11
5.1 CC Conformance Claim	11
5.2 PP Claim.....	11
5.3 Conformance Rationale.....	11
5.4 Conformance Statement	12
6 Security Problem Definition.....	12
6.1 Assets.....	12
6.1.1 General.....	12
6.1.2 TOE services.....	12
6.1.3 TOE Data.....	12
6.2 Threats.....	14
6.2.1 General.....	14
6.2.2 Threat agents.....	14
6.2.3 Threats description	15
6.2.4 Threats vs Threat agents	17
6.3 Organizational Security Policies.....	18
6.4 Assumptions.....	18
7 Security Objectives	19
7.1 General.....	19
7.2 Security Objectives for the TOE.....	19
7.3 Security Objectives for the Operational Environment	21
8 Extended Components Definitions	22
8.1 Extended Component Definitions	22
8.1.1 Family FCS_RND	22
8.1.2 Family FDP_BKP.....	23
9 Security Requirements.....	25
9.1 General.....	25
9.2 Subjects, objects, security attributes and operations	25
9.2.1 General.....	25

9.2.2	Subjects	25
9.2.3	TOE Objects and security attributes	25
9.2.4	TOE Operations	26
9.3	Security Functional Requirements.....	27
9.3.1	General	27
9.3.2	Security audit (FAU)	27
9.3.3	Cryptographic support (FCS).....	29
9.3.4	User data protection (FDP)	31
9.3.5	Identification and authentication (FIA)	35
9.3.6	Security management (FMT)	36
9.3.7	Privacy (FPR).....	37
9.3.8	Protection of the TOE Security Functions (FPT).....	39
9.3.9	Trusted path (FTP) — Trusted path (FTP_TRP.1)	42
9.4	Security Assurance Requirements	42
9.5	Security Requirements Rationale.....	43
9.5.1	Security Problem Definition coverage by Security Objectives.....	43
9.5.2	Security Objectives coverage by SFRs	49
9.5.3	SFR Dependencies	54
9.5.4	Rationale for SARs	54
9.5.5	AVA_VAN.5 Advanced methodical vulnerability analysis	54
	Bibliography	55

European foreword

This document (CEN/TS 419221-2:2016) 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 14167-2:2004.

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 with Backup - Protection Profile' (CMCSOB-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 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] 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 with Backup (CMCSOB-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, with key backup. Target applications include root certification authorities (certification authorities who issue certificates to other CAs and who are 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*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN