

STN	Profily ochrany kryptografických modulov pre poskytovateľov dôveryhodných služieb. Časť 1: Prehľad.	STN P CEN/TS 419221-1 97 6011
------------	--	---

Protection Profiles for TSP cryptographic modules - Part 1: Overview

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 419221-1:2016

123638

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 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 Diensteanbietern - 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*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN

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.