ICS 35.240.30 SLOVENSKÁ TECHNICKÁ NORMA November 2018

STN	Profily ochrany kryptografických modulov pre poskytovateľov dôveryhodných služieb Časť 5: Kryptografický modul pre dôveryhodné služby	STN EN 419221-5 97 6012

Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

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. 10/18

Obsahuje: EN 419221-5:2018

127425

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419221-5

May 2018

ICS 35.040.01; 35.240.30

English Version

Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

Profils de protection pour les modules cryptographiques de prestataires de services de confiance - Partie 5: Module cryptographique pour les services de confiance

Schutzprofile für kryptographische Module von Vertrauensdienstanbietern - Teil 5: Kryptographisches Modul für vertrauenswürdige Dienste

This European Standard was approved by CEN on 2 March 2018.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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, Serbia, 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: Rue de la Science 23, B-1040 Brussels

Ref. No. EN 419221-5:2018 E

Contents Page

Tables

Figures

European foreword

This document (EN 419221-5:2018) 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 European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by November 2018, and conflicting national standards shall be withdrawn at the latest by November 2018.

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 has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: 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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

Clause 4 provides the introductory material for the Protection Profile.

Clause 5 provides the conformance claim.

Clause 6 provides the Security Problem Definition. It presents the Assets, Threats, Organisational Security Policies and Assumptions related to the TOE.

Clause 7 defines the security objectives for both the TOE and the TOE environment.

Clause 8 presents the extended components that will be used in this PP.

Clause 9 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [CC2] and Part 3 [CC3] that are to be satisfied by the TOE.

Clause 10 provides rationales to demonstrate that:

- Security Objectives satisfy the policies and threats;
- SFR match the security Objectives;
- SFR dependencies are satisfied;
- The SARs are appropriate.

A Bibliography is provided to identify background material.

A Mapping to the EU ‘Requirements For Qualified Electronic Signature Creation Devices’ is provided in Annex A.

1 Scope

This part of EN 419221 specifies a Protection Profile for cryptographic modules which is intended to be suitable for use by trust service providers supporting electronic signature and electronic sealing operations, certificate issuance and revocation, time stamp operations, and authentication services, as identified by the (EU) No 910/2014 regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Regulation (EU) No 910/2014 eIDAS) in [10]. The Protection Profile also includes optional support for protected backup of keys.

The document follows the rules and conventions laid out in Common Criteria Part 1 [CC1], Annex B "Specification of Protection Profiles".

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model (Version 3.1 Revision 4, September 2012), CCMB-2012-09-001 [CC1]

Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, (Version 3.1 Revision 4, September 2012), CCMB-2012-09-002 [CC2]

Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, (Version 3.1 Revision 4, September 2012), CCMB-2012-09-003 [CC3]