PD CEN/TS 419221-1:2016

BSI Standards Publication

Protection Profiles for TSP cryptographic modules

Part 1: Overview

bsi.

National foreword

This Published Document is the UK implementation of CEN/TS 419221-1:2016.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 92182 7

ICS 35.040; 35.240.30

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 July 2016.

Amendments issued since publication

Date	Text affected

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

Ref. No. CEN/TS 419221-1:2016 E

Contents

Page

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.