PD CEN/TS 419221-3:2016

BSI Standards Publication

Protection Profiles for TSP Cryptographic modules

Part 3: Cryptographic module for CSP key generation services

bsi.

National foreword

This Published Document is the UK implementation of CEN/TS 419221-3:2016.

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 92179 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 419221-3

July 2016

ICS 35.040; 35.240.30

Supersedes CWA 14167-3:2004

English Version

Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services

Profils de protection pour modules cryptographiques utilisés par les prestataires de services de confiance - Partie 3 : Module cryptographique utilisé par le prestataire de services de certification pour la génération de clés

Schutzprofile für kryptographische Module von vertrauenswürdigen Dienstanbietern - Teil 3: Kryptographisches Modul für CSP Schlüsselgenerierungsdienste

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 419221-3:2016 E

Contents

Page

European foreword

This document (CEN/TS 419221-3:2016) 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.

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 supersedes CWA 14167-3:2004.

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 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

0.1 General

This CEN Technical Standard specifying a Protection Profile for Cryptographic Module for CSP Key Generation Services 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], referred to as the 'Directive' in the remainder of the Protection Profile, as generally recognized standard for electronic-signature products in the Official Journal of the European Communities.

The Directive states in Annex II that certification-service-providers must:

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data.

In the supporting ETSI Technical Specification "Policy Requirements for Certification Authorities (CA) issuing Qualified Certificates" (ETSI/TS 101 456), it is stated that the CA[1)] needs to ensure that:

any subject keys, that it generates, are generated securely and the secrecy of the subject's private key is ensured (see the Directive [1], Annex II (f) and (j)).

And, if the CA generates the subject keys:

a) CA-generated subject keys shall be generated using an algorithm recognized as being fit for the purposes of qualified electronic signatures during the validity of the certificate;

b) CA-generated subject keys shall be of a key length and for use with a public key algorithm which is recognized as being fit for the purposes of qualified electronic signatures during the validity time of the certificate;

c) CA-generated subject keys shall be generated and stored securely before delivery to the subject.

d) The subject's private key shall be delivered to the subject, if required via the subscriber, in a manner such that the secrecy and the integrity of the key is not compromised and, once delivered to the subject, the private key can be maintained under the subject's sole control.

e) Once delivered to the subject any copies of the subject's private key held by the CA shall be destroyed.

This Protection Profile (PP) defines the security requirements of a Cryptographic Module (CM) used by CSP as part of its trustworthy system to provide key generation services. The Cryptographic Module, which is the Target of Evaluation (TOE), is used for the creation of subscriber private keys, and loading them into secure signature creation devices (SSCD) as part of a subscriber device provision service. Such keys are referred to in this PP as subscriber signature creation data. A cryptographic module for CSP key generation services is needed particularly to import such key into the SSCD [8].

The subscriber signature creation data generated by the TOE may be used to produce qualified electronic signatures, as defined by the Directive, or electronic signatures not necessarily qualified (e.g. advanced electronic signatures, digital signatures for other purposes different than authentication, etc.).

The TOE may implement additional functions and security requirements, e.g. for CSP Signing Operations. However, these additional functions and security requirements are not subject of this PP.

1) In the remainder of this PP the term "Certificate Service Provider (CSP)" is used instead of the commonly used term "Certification Authority (CA)", as the former is employed by the Directive [1] this PP aims to support.

In Article 3.5, the Directive further states that:

The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognized standards for electronic-signature products in the Official Journal of the European Communities. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.

This PP is for use by the European Commission, with reference to Annex II (f) and Annex III, in accordance with this procedure.

The document has been prepared as a Protection Profile following the rules and formats of the Common Criteria version 3.1 R3 [2] [3] [4]. This PP has been evaluated, and the corresponding Common Criteria certificate can be found in Bibliographical Reference [5].

The set of algorithms and parameters for secure signature-creation devices shall be in accordance with national guidance, and subject to each Certification Body. Notwithstanding, recommendations for algorithms and parameters for secure electronic signatures are given in ETSI/TS 102 176 [6].

Correspondence and comments to this Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP) should be referred to:

Editor: Dr. Jorge López Hernández-Ardieta

Email: jlhardieta@indra.es

0.2 Document Structure

Clause 1 provides the scope of the Protection Profile.

Clause 2 provides normative references of applicability to this Protection Profile.

Clause 3 provides the terms and definitions used along the document.

Clause 4 contains the Introduction of the Protection Profile, including the PP reference and the TOE overview.

Clause 5 includes the conformance claims for this Protection Profile.

Clause 6 contains the security problem definition, including the set of TOE assets to protect, the expected threats to those assets, the organizational security policies in place and the assumptions made on the TOE.

Clause 7 contains the security objectives for the TOE and the TOE operational environment, and which address the threats, organizational security policies and assumptions considered. This section also includes a rational of correspondence between the security objectives and the threats, organizational security policies and assumptions.

Clause 8 contains the security functional requirements (SFR) and security assurance requirements (SAR) derived from the Common Criteria (CC) Part 2 [3] and Part 3 [4], respectively, and that need to be satisfied by the TOE and developer. This clause introduces first the formalism used to describe the operations (refinement, selection, assignment and iteration) applied along the SFR descriptions. After the SFR and SAR have been described, this section provides the rationale to explicitly demonstrate that the set of SFR are complete with respect to the objectives, and that each security objective is addressed by one or more SFR. Arguments are provided for the coverage of each objective. The rational part also provides a justification for the selection of EAL4+ AVA_VAN.5 as the assurance level.

Finally, a Bibliography is given.

1 Scope

This Technical Standard specifies a protection profile for cryptographic module for CSP key generation services.

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 Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, V1.4.3, May 2007*

3 Terms and definitions

For the purposes of this document, the terms and definitions contained in CEN/TS 419221-1:2016 apply.

4 General

4.1 PP reference

Title:	Cryptographic module for CSP key generation services protection profile CMCKG-PP
Author:	Jorge López Hernández-Ardieta
Version:	0.20
Publication date:	27th January 2015

4.2 TOE overview

4.2.1 TOE usage and major security features

The TOE is a Cryptographic Module (CM) used for the generation of subscribers Signature Creation Data (Subscriber-SCD) and Signature Verification Data (Subscriber-SVD) and their export to the subscribers Secure Signature Creation Devices (SSCD), in a manner that:

— the confidentiality and integrity of the Subscriber-SCD are maintained both when managed by the TOE and during transfer from the TOE to an external entity (i.e. the Subscriber-SSCD);

— the integrity of the Subscriber-SVD is maintained both when managed by the TOE and during transfer from the TOE to an external entity (i.e. the Subscriber-SSCD or the certificate generation application, CGA);

— the TOE services (generation of subscribers Subscriber-SCD/Subscriber-SVD and their export to the subscribers SSCD/CGA) are only used in an authorized way.

The TOE shall provide the following additional functions to protect the TOE services:

— user authentication;

— access control for use of the Subscriber-SCD/SVD generation and export functions;