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 ... **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*

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.

3.4
auditor
user exporting the TOE audit data and reviewing the audit data with tools in the TOE environment

3.5
backup
export of the CSP_SCD, the TSF data and the system data (backup data) sufficient to recreate the state of the TOE at the time the backup was created

Note 1 to entry: Backup is the only function which is allowed to export CSP_SCD and only if backup package is implemented.

3.6
certificate
electronic attestation which links the SVD to a person and confirms the identity of that person (defined in Directive 1999/93/EC [1], Article 2.9)

3.7
certificate generation application
CGA
collection of application elements which requests the SVD from the device generating the SCD/SVD pair for generation of the qualified certificate

Note 1 to entry: The CGA stipulates the generation of a correspondent SCD/SVD pair, if the requested SVD has not been generated by the SCD/SVD generation device yet. The CGA verifies the authenticity of the SVD by means of (a) the SSCD proof of correspondence between SCD and SVD and (b) checking the sender and integrity of the received SVD.

3.8
certification-service-provider
CSP
entity or a legal or natural person who issues certificates or provides other services related to electronic signatures (defined in Directive 1999/93/EC [1], Article 2.11)

Note 1 to entry: In common usage this is often referred to as Certification Authority (CA). A CSP is a type of TSP.

3.9
cryptographic module
set of hardware, software and firmware used to generate the Subscriber-SCD/Subscriber-SVD pair and which represents the TOE

3.10
CSP signature creation data
CSP_SCD
SCD which is used by the CSP, e.g. for the creation of advanced electronic signatures in qualified certificates or for signing certificate status information

3.11
CSP signature verification data
CSP_SVD
SVD which corresponds to the CSP_SCD and which is used to verify the advanced electronic signature in the qualified certificate or the certificate status information

3.12
data to be signed
DTBS
complete electronic data to be signed, such as QC content data or certificate status information

3.13
data to be signed representation
DTBS-representation
data sent to the TOE for signing which is:

a) a hash-value of the DTBS or

b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or

c) the DTBS itself

Note 1 to entry: The client indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in Case a) or the intermediate hash-value in Case b) is calculated by the client. The final hash-value in Case b) or the hash-value in Case c) is calculated by the TOE.

3.14
digital signature
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of that unit and protect against forgery e.g. by the recipient

3.15
Directive
Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1], which is also referred to as the “Directive” in the remainder of the PP

3.16
dual person control
special form of access control of a task which requires at least two users with different identities to be authenticated and authorized to the defined roles at the time this task is to be performed

3.17
hardware security module
HSM
cryptographic module used to generate the advanced signature in qualified certificates and which represents the TOE

3.18
list of approved algorithms and parameters
approved cryptographic algorithms and parameters for secure signature-creation devices that needs to be in accordance with national guidance, and subject to each Certification Body

Note 1 to entry: Notwithstanding, recommendations for algorithms and parameters for secure electronic signatures are given in ETSI/TS 119 312 [2].

3.19
qualified certificate
QC
certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [1] (defined in the Directive [1], Article 2.10)

3.20
reference authentication data
RAD
data persistently stored by the TOE for verification of the authentication attempt as authorized user

3.21
restore
import of the backup data to recreate the state of the TOE at the time the backup was created

3.22
secure signature-creation device
SSCD
configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive [1]. (defined in the Directive [1], Articles 2.5 and 2.6)

3.23
side-channel
illicit information flow in result of the physical behaviour of the technical implementation of the TOE

Note 1 to entry: Side-channels are limited to interfaces not intended for data output like power consumption, timing of any signals and radiation. Side-channels might be enforced by influencing the TOE behaviour from outside.

3.24
signature-creation data
SCD
unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature (defined in the Directive [1], Article 2.4)

3.25
signature-verification data
SVD
data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature (defined in the Directive [1], Article 2.7)

3.26
split knowledge procedure for key import
process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key

3.27
SSCD provision service
service that prepares and provides a SSCD to subscribers

3.28
subject
entity identified in a certificate as the holder of the private key associated with the public key given in the certificate (defined in ETSI EN 319 411-2 [3])

Note 1 to entry: The subject may be a subscriber acting on its own behalf.

3.29
subscriber
entity subscribing with a trust service provider who is legally bound to any subscriber obligations (defined in ETSI EN 319 401 [4])

3.30
subscriber Signature-Creation Data
subscriber-SCD
SCD which is used by the Subscriber (the signatory) for the creation of qualified electronic signatures by means of a SSCD

3.31
subscriber Secure Signature-Creation Device
subscriber-SSCD
SSCD that contains the Subscriber-SCD (imported from the TOE) and which is used by the Subscriber (the signatory) for the creation of qualified electronic signatures

3.32
subscriber Signature-Verification Data
subscriber-SVD
SVD which corresponds to the Subscriber-SCD and which is used to verify the qualified electronic signature

3.33
system auditor of the CSP
role in the IT environment of the TOE (certification service provider) authorized to view archives and audit logs of trustworthy systems

3.34
Target of Evaluation
TOE
set of software, firmware and/or hardware possibly accompanied by guidance (as defined in ISO/IEC 15408-1)

3.35
trust service
electronic services which enhances trust and confidence in electronic transactions

3.36
trust service provider
provider of electronic services which enhances trust and confidence in electronic transactions

3.37
user
entity (human user or external IT entity) outside the TOE that interacts with the TOE

3.38
user data
data created by and for the user that does not affect the operation of the TOE Security Functionality (TSF)

3.39
verification authentication data
VAD
authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics

4 Protection profiles specified in CEN/TS 419221

4.1 General

This multi-part standard specifies protection profiles, as per common criteria (ISO/IEC 15408 series), for trust service provider cryptographic modules. 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.

The ISO/IEC 15408 series shall be used as the basis of these protection profiles.

4.2 CEN/TS 419221-2: Cryptographic module for CSP signing operations with backup

CEN/TS 419221-2 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.

4.3 CEN/TS 419221-3: Cryptographic module for CSP key generation services

CEN/TS 419221-3 specifies a protection profile for cryptographic modules used by certification service providers (as specified in Directive 1999/93) as part of its trustworthy system to provide key generation services. The cryptographic module, which is the Target of Evaluation, is used for the creation of subscriber private keys, and loading them into secure signature creation devices (as specified in Directive 1999/93) as part of a subscriber device provision service.

4.4 CEN/TS 419221-4: Cryptographic module for CSP signing operations without backup

CEN/TS 419221-4 specifies a protection profile for cryptographic modules used by certification service providers (as specified in Directive 1999/93) for signing operations, without key backup. Target applications include root certification authorities (certification authorities which issue certificates to other CAs and is 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.

4.5 CEN/TS 419221-5: Cryptographic Module for Trust Services

CEN/TS 419221-5[2] specifies a protection profile for cryptographic modules used by trust service providers (as specified in Regulation (EU) No 910/2014 [5]) for signing operations and authentication services. This protection profile includes support for protected backup of keys. The target of this part is:

a) provision of cryptographic support for trust service provider signing operations including applications such as certification authorities who issue qualified and non-qualified certificates to

[2] This NWI is registered in Projex (00224243) but has not been submitted to CEN Enquiry yet.

end users, signing services as identified in CEN/TS 419241, data “sealing” by or on behalf of a legal entity, time-stamping services and validation services; and

b) provision of both symmetric and asymmetric cryptographic support for trust service provider authentication services, for example for authenticating users of signing services as specified in CEN/TS 419241.

This profile assumes that the cryptographic module is in a physically secured environment and that there is a low risk of untrusted personnel having direct physical access to the device.

Bibliography

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[2] ETSI/TS 119 312, *Electronic Signatures and Infrastructures (ESI); Cryptographic Suites*

[3] ETSI EN 319 411-2, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates*

[4] ETSI EN 319 401, *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures*

[5] Regulation (EU) No 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.