Date: 2015-08

prTS 419221-1:2015

Protection Profiles for TSP cryptographic modules – Part 1: Overview

Document type: Technical Specification
Document language: E

Contents

Introduction

This multi-part standard specifies protection profiles for trust service provider cryptographic modules, as per common criteria (ISO/IEC 15408). 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 part of TS 419 221 provides an overview of the protection profiles specified in other parts of TS 419 221.

2 References

2.1 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.

[1] ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

[2] ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.

[3] ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.

NOTE 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.

2.2 Informative references

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

[i.2] ETSI TS 119 312 Electronic Signatures and Infrastructures – Cryptographic Suites

[i.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

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

[i.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

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 initialisation or other TOE administrative functions. These tasks are mapped to the Crypto-officer role of the TOE.

3.2
Advanced electronic signature
An electronic signature which meets the following requirements (defined in the Directive [i.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 is detectable.

3.3
Authentication data
Information used to verify the claimed identity of a user.

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 that 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 the Directive [i.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. 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 the Directive [i.1], article 2.11).

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

3.6
Cryptographic Module
Set of hardware, software and firmware used to generate the Subscriber-SCD/Subscriber-SVD pair and which represents the TOE.

3.7
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.

3.8
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.

3.9
Data to be signed (DTBS)
The complete electronic data to be signed, such as QC content data or certificate status information.

3.10
Data to be signed representation (DTBS-representation)
The 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.

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.

3.11
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.

3.12
Directive
Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [i.1] is also referred to as the ‘Directive’ in the remainder of the PP.

3.13
Dual person control
A special form of access control of a task which requires at least two users with different identities to be authenticated and authorised to the defined roles at the time this task is to be performed.

3.14
Hardware security module (HSM)
The cryptographic module used to generate the advanced signature in qualified certificates and which represents the TOE.

3.15
List of approved algorithms and parameters
Approved cryptographic 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 [i.2].

3.16
Qualified certificate (QC)
Certificate which meets the requirements laid down in Annex I of the Directive [i.1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [i.1] (defined in the Directive [i.1], article 2.10).

3.17
Reference authentication data (RAD)
Data persistently stored by the TOE for verification of the authentication attempt as authorised user.

3.18
Restore
Import of the backup data to recreate the state of the TOE at the time the backup was created.

3.19
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 [i.1]. (defined in the Directive [i.1], article 2.5 and 2.6).

3.20
Side-channel
Illicit information flow in result of the physical behaviour of the technical implementation of the TOE. 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.

3.21
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 [5], article 2.4).

3.22
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 [5], article 2.7).

3.23
Split knowledge procedure for key import
A 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.

3.24
SSCD provision service
Service that prepares and provides a SSCD to subscribers.

3.25
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 [i.3]). The subject may be a subscriber acting on its own behalf.

3.26
Subscriber
Entity subscribing with a trust service provider who is legally bound to any subscriber obligations (defined in ETSI EN 319 401 [i.4].

3.27
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.

3.28
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.

3.29
Subscriber Signature-Verification Data (Subscriber-SVD)
SVD which corresponds to the Subscriber-SCD and which is used to verify the qualified electronic signature.

3.30
System auditor of the CSP
A role in the IT environment of the TOE (certification service provider) authorised to view archives and audit logs of trustworthy systems.

3.31
Target of Evaluation (ToE)
set of software, firmware and/or hardware possibly accompanied by guidance (as defined in ISO/IEC 15408-1 [1]).

3.32
Trust Service
Electronic services which enhances trust and confidence in electronic transactions.

3.33
Trust Service Provider
Provider of electronic services which enhances trust and confidence in electronic transactions.

3.34
User
Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

3.35
User data
Data created by and for the user that does not affect the operation of the TOE Security Functionality (TSF).

3.36
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), 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.

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

4.2 Part 2: Cryptographic module for CSP signing operations with backup

Part 2 of TS 419 221 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 Part 3: Cryptographic module for CSP key generation services

Part 3 of TS 419 221 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 Part 4: Cryptographic module for CSP signing operations without backup

Part 4 of TS 419 221 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 Part 5: Cryptographic Module for Trust Services

This part of TS 419 221 specifies a protection profile for cryptographic modules used by trust service providers (as specified in Regulation (EU) No 910/2014 [i.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 end users, signing services as identified in TS 419 241, 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 TS 419 241.

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.