PD CEN/TS 419221-2:2016

BSI Standards Publication

Protection Profiles for TSP cryptographic modules

Part 2: Cryptographic module for CSP signing operations with backup

Documents
Document Sharing Hub

Full document details: PD CEN/TS 419221-2:2016

National foreword

This Published Document is the UK implementation of CEN/TS 419221-2:2016.

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.

© The British Standards Institution 2016. Published by BSI Standards Limited 2016

ISBN 978 0 580 92180 3

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

Documents
Document Sharing Hub

Full document details: PD CEN/TS 419221-2:2016

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 419221-2

July 2016

ICS 35.240.30; 35.040

Supersedes CWA 14167-2:2004

English Version

Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup

Profils de protection pour modules cryptographiques utilisés par les prestataires de services de confiance - Partie 2 : Module cryptographique utilisé par le prestataire de services de certification pour les opérations de signature avec sauvegarde

Schutzprofile für kryptographische Module von vertrauenswürdigen Dienstanbietern - Teil 2: Schutzprofil für CSP Signieroperationen mit Sicherung

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

© 2016 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN/TS 419221-2:2016 E

Documents
Document Sharing Hub

Full document details: PD CEN/TS 419221-2:2016

Contents

Page

European foreword 4
Introduction 5
1 Scope 6
2 Normative references 6
3 Terms and definitions 6
4 PP Introduction 6
4.1 General 6
4.2 PP Reference 6
4.3 Protection Profile Overview 7
4.4 TOE Overview 8
4.4.1 TOE type 8
4.4.2 TOE Roles 9
4.4.3 Usage and major security features of the TOE 9
4.4.4 Available non-TOE hardware/software/firmware 11
5 Conformance Claim 11
5.1 CC Conformance Claim 11
5.2 PP Claim 11
5.3 Conformance Rationale 11
5.4 Conformance Statement 12
6 Security Problem Definition 12
6.1 Assets 12
6.1.1 General 12
6.1.2 TOE services 12
6.1.3 TOE Data 12
6.2 Threats 14
6.2.1 General 14
6.2.2 Threat agents 14
6.2.3 Threats description 15
6.2.4 Threats vs Threat agents 17
6.3 Organizational Security Policies 18
6.4 Assumptions 18
7 Security Objectives 19
7.1 General 19
7.2 Security Objectives for the TOE 19
7.3 Security Objectives for the Operational Environment 21
8 Extended Components Definitions 22
8.1 Extended Component Definitions 22
8.1.1 Family FCS_RND 22
8.1.2 Family FDP_BKP 23
9 Security Requirements 25
9.1 General 25
9.2 Subjects, objects, security attributes and operations 25
9.2.1 General 25

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

9.2.2 Subjects **25**
9.2.3 TOE Objects and security attributes **25**
9.2.4 TOE Operations **26**
9.3 Security Functional Requirements **27**
9.3.1 General **27**
9.3.2 Security audit (FAU) **27**
9.3.3 Cryptographic support (FCS) **29**
9.3.4 User data protection (FDP) **31**
9.3.5 Identification and authentication (FIA) **35**
9.3.6 Security management (FMT) **36**
9.3.7 Privacy (FPR) **37**
9.3.8 Protection of the TOE Security Functions (FPT) **39**
9.3.9 Trusted path (FTP) — Trusted path (FTP_TRP.1) **42**
9.4 Security Assurance Requirements **42**
9.5 Security Requirements Rationale **43**
9.5.1 Security Problem Definition coverage by Security Objectives **43**
9.5.2 Security Objectives coverage by SFRs **49**
9.5.3 SFR Dependencies **54**
9.5.4 Rationale for SARs **54**
9.5.5 AVA_VAN.5 Advanced methodical vulnerability analysis **54**

Bibliography **55**

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

European foreword

This document (CEN/TS 419221-2:2016) 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 14167-2:2004.

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 with 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.

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

Introduction

This 'Cryptographic Module for CSP Signing Operations with Backup - Protection Profile' (CMCSOB-PP) 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] as generally recognized standard for electronic-signature products in the Official Journal of the European Communities.

The document has been prepared as a Protection Profile (PP) following the rules and formats of the Common Criteria version 3.1r3 [CC1] [CC2] [CC3].

The set of algorithms for secure signature-creation devices and parameters for algorithms for secure signature-creation devices is given in a separate document, ETSI/TS 102 176.

This document has been originally prepared as a single Protection Profile and approved as CWA 14167-2:2002. Afterwards, while reviewing this Protection Profile for the evaluation, in order to make it conformant to the Common Criteria 2.1, two Protection Profiles have been created for the same TOE, one including the mandatory function of key backup and the other excluding this function:

— Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP), version 0.28; CWA 14167-2:2004;

— Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP), version 0.28; CWA 14167-4:2004.

Correspondence and comments to this Cryptographic Module for CSP Signing Operations - Protection Profile with Backup (CMCSOB-PP) should be referred to:

Editor: Rémy DAUDIGNY

Email: remy.daudigny@thalesgroup.com

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

1 Scope

This Technical Specification 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.

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 Signature and Infrastructure (ESI); Policy requirements for certification authorities issuing qualified certificates*

ETSI/TS 102 176, *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures*

3 Terms and definitions

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

4 PP Introduction

4.1 General

This clause provides document management and overview information that is required to carry out protection profile registry. Therefore, Subclause 4.2 “PP Reference” gives labelling and descriptive information necessary for registering the Protection Profile (PP). Subclause 4.3 “Protection Profile Overview” summarizes the PP in narrative form. Subclause 4.4 “TOE Overview” summarizes the TOE in a narrative form. As such, these subclauses give an overview to the potential user to decide whether the PP is of interest. It is usable as standalone abstract in PP catalogues and registers.

4.2 PP Reference

Title	Cryptographic Module for CSP Signing Operations with backup – Protection Profile
CC revision	v3.1 release 3
PP version	v0.35
Authors	Rémy Daudigny
Publication Date	2015
Keywords	cryptographic module, CSP signing device, qualified certificate signing, certificate status information signing
Registration	419221–2

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

4.3 Protection Profile Overview

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 PP, 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)[1)] issuing Qualified Certificates" (ETSI/TS 101 456), it is stated that:

> *The CA shall ensure that CA keys are generated in accordance with industry standards, and*
>
> *The CA shall ensure that CA private keys remain confidential and maintain their integrity.*

This Protection Profile (PP) defines the security requirements of a Cryptographic Module (CM) used by CSP as part of its trustworthy system to provide signing services, such as Certificate Generation Service or Certificate Status Information Signing Services. The Cryptographic Module, which is the Target of Evaluation (TOE), is used for the creation of CSP key pairs, and their usage for the creation and verification of advanced electronic signatures in qualified certificates or certificate status information. The private keys are referred to in this PP as Certification Service Provider Signature-Creation Data (CSP-SCD). The public keys are referred as Certification Service Provider Signature-Verification Data (CSP-SVD).

The Protection Profile's primary scope is for signing qualified certificates. However components evaluated against this standard may be applied for other signature-creation tasks carried out by a certificate service provider (CSP) such as time-stamping, signing certificate revocation lists (CRLs) or issuing online certificate status protocol (OCSP) messages. It may also be used for other trusted service providers creating electronic signatures.

This PP is Common Criteria Part 2 extended and Common Criteria Part 3 conformant. The assurance level for this PP is EAL4, augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis).

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 Protection Profile is established by CEN/ISSS for use by the European Commission, with reference to Annex II (f), in accordance with this procedure.

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 EC 1999/93 [1] this PP aims to support.

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

4.4 TOE Overview

4.4.1 TOE type

The TOE is a Cryptographic Module (CM) used for the creation and usage of Certificate Service Provider Signature-Creation Data (CSP-SCD). The CM may optionally also perform hashing of the qualified certificate content.

The TOE is configured software and hardware that may be used to provide the following cryptographic functions:

a) generation of CSP-SCD;

b) usage of the CSP-SCD to create advanced electronic signatures for qualified certificates based on either:

   1) the hash value of the content of the qualified certificate, or

   2) an intermediate hash-value of a first part of the qualified certificate and a remaining part of the qualified certificate or

   3) the complete content of the qualified certificate, where the hashing is also performed in the CM (optional).

The TOE may implement additional functions and security requirements, e.g. for the creation of Signature Creation Data (SCD) for loading into Secure Signature Creation Devices (SSCD) as part of a Subscriber Device Provision Service. However, these additional functions and security requirements are not subject of this Protection Profile.

The TOE shall provide the following additional functions to protect these cryptographic functions:

- user authentication;
- access control for the creation and destruction of keys;
- access control for usage of keys to create certificate signatures;
- auditing of security-relevant changes to the TOE;
- self-test of the TOE.

The TOE shall handle the following User Data:

c) CSP Signature Creation Data (CSP-SCD): private key of CSP, created and stored internally in the TOE;

d) data to be signed representation (DTBS-representation): the data to be signed by the TOE may e.g. be:

   1) Certificate hash value: imported to the TOE;

   2) Certificate contents (optional, when hashing is performed in the TOE), data to be hashed (fully or partially) and signed, imported to the TOE;

   3) other data to be signed by the TOE, such as CRL or the hash value of the CRL, or time-stamping content data;

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

e) certificate signature: created signature, exported from the TOE.

The TOE supports backup and restoration of CSP-SCD, other user data and TSF data to re-establish an operational state after failure. The TOE will protect the confidentiality of the backup data and detect loss of the integrity of the backup data while the IT-environment will ensure the availability of the backup data.

For the cryptographic functions, the TOE shall support the cryptographic algorithms specified in ETSI/TS 102 176, or a subset thereof.

4.4.2 TOE Roles

The TOE shall as a minimum support the following user categories (roles):

- **crypto-officer** (authorized to install, configure and maintain the TOE and to create, destruct, backup/restore data of keys);
- **crypto-user** (authorized to sign with existing CSP-SCDs);
- **auditor** (authorized to read audit data generated by the TOE and exported for audit review in the TOE environment).

The TOE may support other roles or sub-roles in addition to the roles specified above. The roles may also be allowed to perform additional functions provided by the TOE as long as the separation between different roles is given.

The interface to the TOE may either be shared between the different user categories, or separated for certain functions, for example configuration and key backup/restore.

Authentication of TOE users shall be identity-based.

Maintenance of the TOE as well as the management of the CSP-SCDs are highly critical operations that need to be related to the individual users that performed the operation. It is therefore required that for the roles System Auditor and Security officer of the CSP [CEN] the individual users shall be known by the TOE as Auditor and Crypto-officer and the TOE needs to perform identity based authentication for those roles. The Crypto-officer role is very powerful including user and key management. Therefore the Auditor role is implemented to watch on Crypto-officer's actions and to detect misuse of Crypto-officer's authorization.

The TOE manages two or more user identities for the role Crypto-officer to allow dual person control for security critical actions like generation of CSP-SCD and CSP-SVD generation, backup and restore. The end-users may access to the TOE signing service through a client application in the TOE environment. The client application acts as agent for these end-users with a TOE user identity in the Crypto-user role.

4.4.3 Usage and major security features of the TOE

In most cases the TOE will be a separate component with its own hardware and software, communicating via a well-defined physical and logical interface with the client application in the IT environment. Examples of physical interfaces that may be used to connect the TOE to the client application are the PCI bus, the SCSI bus, USB or Firewire.

Logically the TOE is responsible for protecting the CSP-SCD against disclosure, compromise and unauthorized modification and for ensuring that the TOE services are only used in an authorized way.

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

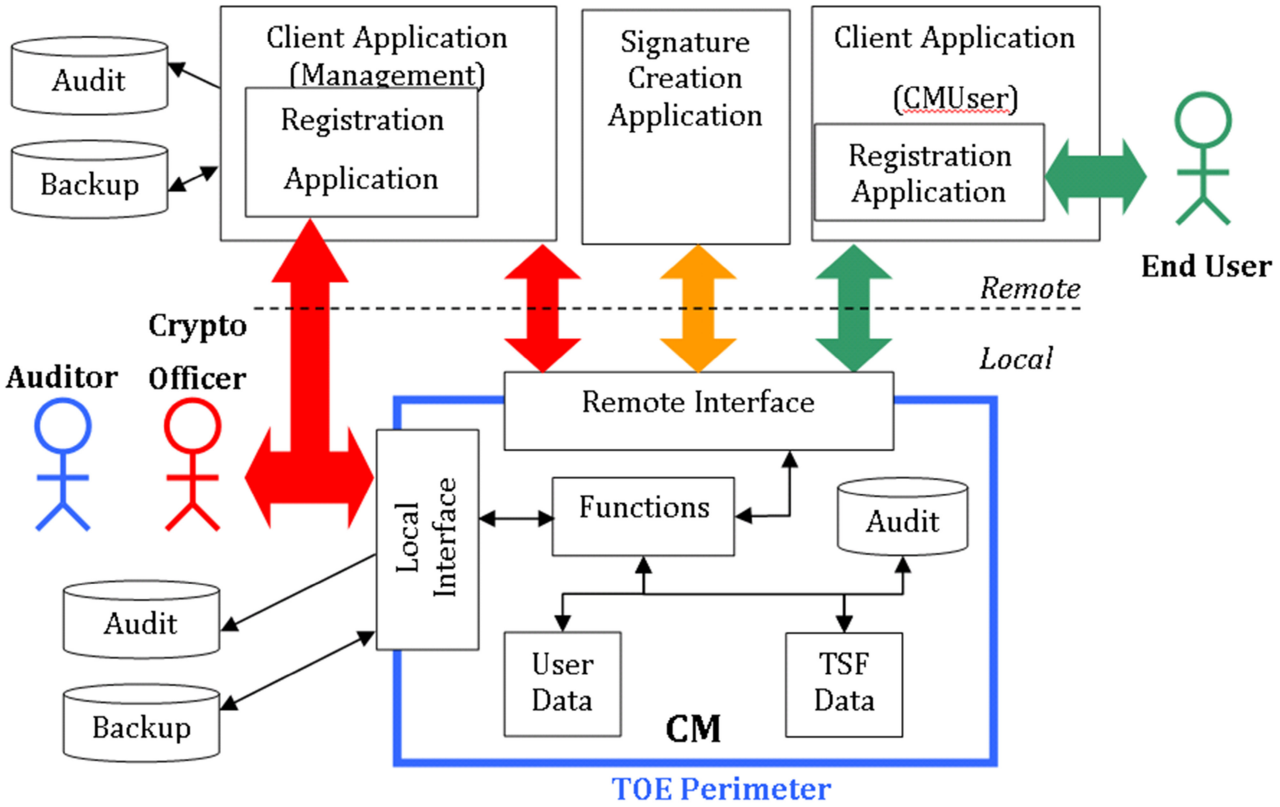

Figure 1 — TOE general overview

NOTE This diagram is illustrative. It needs not represent the exact implementation architecture.

As shown in Figure 1, no relation exists with Trusted Service Providers (TSP). The end-users will communicate with the client application, which in turn will call TOE services on behalf of the end-user. The client application provides the human interface for user identification and authentication. The client application is responsible for passing any user data in a correct way to the TOE. Different mechanisms may be used to protect the user data on its way from the originating user to the TOE, but all those mechanisms are not part of the TOE functionality and therefore not defined in this Protection Profile.

The TOE provides identification authentication, access control and audit for users of its services. The client application in the TOE environment may mediate the TOE signing function to its end-users. Therefore it is the responsibility of the client application to identify, authenticate and control access of its end-users gaining access to the TOE services provided for the Crypto-user role. The end-users authenticate themselves to the client application with his or her identity. The client application checks the authorization of the end-user for the TOE signing service. If the end-user is allowed to use the signing function the client application will authenticate them for the Crypto-user role to the TOE and will map the identity of the end-user to the Crypto-user role.

The client application performs identity-based auditing to support accountability for the cryptographic operations. While the TOE will only perform auditing for the client application the TOE environment audit might distinguish between the end-users of the client application.

The client application that communicates with the TOE may itself consist of different parts implemented on different systems. For example, a client application that initiates the generation of qualified certificate may consist of two parts:

a) a registration application, which initializes the information for the certificate;

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

b) a signature-creation application, which may be:

1) a certification application, which verifies the integrity and authenticity of the request submitted by the registration application and then calls the TOE service to sign the certificate or

2) other applications requesting the TOE to sign DTBS-representations, e.g. certificate status information. The application verifies integrity and authenticity of the signature request.

When exporting the CSP-SCD or TSF data the TOE ensures the confidentiality and integrity of the CSP-SCD and the TSF data by the backup and restoration functions. The backup will export user data and TSF data (backup data) and the restore function will import the backup data for recreation of the state of the TOE at the time the backup was created. The IT-environment provides means of supporting the backup and restore functions of the TOE by ensuring the availability of the backup data.

Privileged users as Crypto-officer and Auditor can interact with the TOE through the local interface. They can also connect remotely to the TOE thanks to a Client Application that offers Management capabilities. This application performs identity-based auditing to support accountability for the privileged operations. The Client Application used for Management purposes and the Client Application used by the end-user are represented in Figure 1 as separate applications. Nevertheless, they are very similar (RBAC authentication, Registration of user for accountability…) and rely on the same security functions for protecting communications with the Cryptomodule.

Finally, the TOE supports a secure firmware update mechanism where updating data are protected in integrity, confidentiality and authenticity (signed).

4.4.4 Available non-TOE hardware/software/firmware

None. The TOE is an independent Cryptographic Module comprising its own hardware and software.

5 Conformance Claim

5.1 CC Conformance Claim

This protection profile is conformant to Common Criteria version 3.1 revision 3.

More precisely, this protection profile is:

— CC Part 1 [CC1],

— CC Part 2 extended [CC2],

— CC Part 3 conformant [CC3].

The assurance requirement of this Protection Profile is **EAL4 augmented**.

Augmentation results from the selection of:

— AVA_VAN.5 Advanced methodical vulnerability analysis

5.2 PP Claim

This PP does not claim conformance to any another Protection Profile.

5.3 Conformance Rationale

Since this PP is not claiming conformance to any other protection profile, no rationale is necessary here.

AVA Documents
Document Sharing Hub

Full document details: PD CEN/TS 419221-2:2016

5.4 Conformance Statement

This PP requires strict conformance of any ST or PP, which claims conformance to this PP.

6 Security Problem Definition

6.1 Assets

6.1.1 General

The primary assets that need to be protected by the TOE are presented below.

6.1.2 TOE services

R.SERVICES (I, A)

TOE services are:

1) generation and management (usage and destruction) of CSP key pair (SCD and SVD)

2) usage of CSP-SCD for signature

3) backup and restoration of TSF data

4) User Identity and Role management

5) Internal Audit

These services shall be protected in Integrity and Availability.

6.1.3 TOE Data

6.1.3.1 Keys

R.CSP-SCD (C, I, A)

As defined in the Directive ([1] Article 2 Paragraph 4) a Certification Service Provider Signature Creation Data (R.CSP-SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

CSP-SCD is a cryptographic private key that shall be protected in Confidentiality, Integrity and Availability.

R.CSP-SVD (I)

As defined in the Directive ([1] Article 2 Paragraph 4) a Certification Service Provider Signature Verification Data (R.CSP-SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;

The CSP-SVD shall be protected in Integrity.

R.BACKUP_KEY (C, I)

A cryptographic key used to provide a cryptographic checksum of backup data and encrypt backup data before exporting it to the TOE environment.

The cryptographic checksum for R.BACKUP_DATA shall be based on symmetric cryptographic algorithms (e.g. keyed hash) or asymmetric cryptographic algorithms (e.g. digital signatures).

R.BACKUP_KEY shall be protected in confidentiality and integrity.

R.BACKUP_KEY is kept by the TOE environment.

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

Application note: R.BACKUP_KEY may be a dual asset, depending on the developer implementation choices, divided in a cryptographic key to ensure integrity of R.BACKUP through the checksum and a cryptographic key to encrypt it.

6.1.3.2 Internal TOE Data

R.CM_FIRMWARE (I, Auth)

Embedded firmware of the cryptomodule.

The firmware implements the security mechanisms of the TOE, therefore it needs to be protected in integrity inside the cryptomodule.

Moreover, as far as a firmware update process might be available during operational lifecycle steps of the TOE, updating data authenticity shall be checked by the cryptomodule prior to the installation.

This asset shall be protected in integrity and authenticity.

R.TSF_DATA (C, I, A)

TSF data includes:

— VAD and RAD;

— other system data not related to a user or role (system configuration data, audit data).

TSF data shall be protected in confidentiality, integrity and availability.

R.USERMGMT_DATA (I)

Non-confidential data related to a user or role (identifier, access control lists, role definitions, etc.).

This asset shall be protected in integrity.

6.1.3.3 External TOE Data

R.BACKUP_DATA (C, I)

Backup data are R.TSF_DATA and R.CSP-SCD, encrypted by R.BACKUP_KEY, with a cryptographic checksum, exported from the TOE, by the TOE, to the TOE environment and restored into the TOE.

This asset needs to be protected in confidentiality and integrity.

Availability of this data shall be ensured in the TOE environment.

R.DTBS_Representation (I)

Data To Be Signed Representation (DTBS_Representation) means the data sent to the TOE for signing and 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, i.e. the complete electronic data to be signed, such as QC content data or certificate status information.

The client indicates to the TOE the case of R.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.

R.DTBS_Representation shall be protected in integrity.

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

R.DSD (Auth)

Digitally Signed Data (DSD) is the result of the TOE signature function over the R.DTBS_Representation.

For example, R.DSD can be a time-stamp, a certificate, a certificate revocation list, a certificate status information, an online certificate status protocol (OCSP) messages or a CSP digital signature.

R.DSD shall be protected in authenticity.

6.2 Threats

6.2.1 General

The expected attackers are qualified so as to have HIGH attack potential, in accordance with the security assurance given by AVA_VAN.5 "*Advanced methodical vulnerability analysis*".

6.2.2 Threat agents

TA.EXTERNAL

This agent represents an entity that does not hold any authorized role to operate or interact with the TOE. This agent may operate through the remote or local interfaces, or even have direct physical access to the TOE.

Examples of this threat agent are:

— unauthorized CSP personnel,

— cybercriminals,

— hackers in general.

TA.INSIDER

This agent represents an entity that holds an authorized role to operate or interact with the TOE, and which has the intention to compromise the TOE assets. This agent may operate through the remote or local interfaces, or even have direct physical access to the TOE.

Examples of this threat agent are:

— auditors,

— crypto-officers.

TA.INADVERTENT

This agent represents an entity that holds an authorized role to operate or interact with the TOE, but which does not have the intention to compromise the TOE assets. This agent may operate through the remote or local interfaces, or even have direct physical access to the TOE.

Examples of this threat agent are:

— crypto-users via the cryptomodule-user role

— auditors,

— crypto-officers.

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

6.2.3 Threats description

6.2.3.1 Threats on Keys

T.BACKUP_KEY_Alteration *Alteration of backup key*

TA.EXTERNAL or TA.INSIDER might modify or alter R.BACKUP_KEY by interaction with the TOE logical internal functions, or within the TOE environment, in order to:

— invalidate the cryptographic checksum of R.BACKUP_DATA or

— invalidate decryption of R.BACKUP_DATA.

TA.INADVERTENT might also modify or alter R.BACKUP_KEY in the TOE environment within the session of a Crypto-officer whose responsibility is to load this data in the cryptomodule.

T.BACKUP_KEY_Derive Derivation of R.BACKUP_KEY

TA.EXTERNAL or TA.INSIDER might derive all or part of R.BACKUP_KEY using knowledge about the R.BACKUP_KEY operations (generation, usage, destruction), even during legitimate use of R.SERVICES.

T.BACKUP_KEY_Disclose *Disclosure of R.BACKUP_KEY*

TA.EXTERNAL or TA.INSIDER might disclose all or part of R.BACKUP_KEY over physical or logical TOE interface by bypassing the export control mechanisms.

T.CSP-SCD_Alteration *Alteration of the R.CSP-SCD*

TA.EXTERNAL or TA.INSIDER might modify or alter R.CSP-SCD by interaction with the TOE logical internal functions, in order to invalidate the electronic signature of R.DTBS_Representation.

Although the use of a distorted CSP-SCD can be detected, the impacts for the organization issuing the signed data using the CSP-SCD (e.g. qualified certificates) can be high.

T.CSP-SCD_Derive *Deriving All or Parts of the R.CSP-SCD*

TA.EXTERNAL or TA.INSIDER might derive all or part of R.CSP-SCD using knowledge about the R.CSP-SCD operations (generation, usage and destruction), R.DTBS or R.CSP-SVD, even during legitimate use of R.SERVICES.

T.CSP-SCD_Disclose *Disclosing All or Part of the R.CSP-SCD*

TA.EXTERNAL or TA.INSIDER might disclose all or part of R.CSP-SCD over physical or logical TOE interface by bypassing the export control mechanisms.

T.CSP-SVD_Alteration *Alteration of the R.CSP-SVD*

TA.EXTERNAL or TA.INSIDER might alter R.CSP-SVD when R.CSP-SVD is exported from the TOE.

Although the use of a distorted CSP-SVD can be detected, the impacts for the organization issuing the signed data using the CSP-SCD (e.g. qualified certificates) can be high.

6.2.3.2 Threats on internal TOE Data

T.Bad_SW *Malicious Software during the Lifetime of the TOE*

TA.EXTERNAL or TA.INSIDER might try to modify or alter R.CM_FIRMWARE by loading malicious software into the TOE or interacting with the TOE logical interfaces, in order to modify or gain access to R.CSP-SCD, R.TSF_DATA, R.USERMGMT_DATA, R.BACKUP_KEY or R.SERVICES.

6.2.3.3 Threats on external TOE Data

T.Backup *Forging or corrupting backup data*

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016

TA.EXTERNAL, TA.INSIDER or TA.INADVERTENT might corrupt R.BACKUP_DATA within the TOE environment.

For instance, TA.INSIDER such as CSP personnel without expected clearance may forge backup data (R.BACKUP_DATA) for restoring forged VAD and RAD (R.TSF_DATA) into the TOE, in order to gain illicit access to R.SERVICES.

Finally, this threat might also lead for example to corruption of R.BACKUP_DATA within the TOE environment by TA.INADVERTENT, and R.TSF_DATA might be lost.

T.Data_Manipul *Manipulating data outside of the TOE*

TA.EXTERNAL or TA.INSIDER might manipulate R.DTBS_Representation within the TOE environment during its transfer from the client application to the TOE. This may result in the effect that the TOE signs data (corrupted R.DTBS_Representation) without the approval of the user under whose control the data are submitted to the TOE.

When performed within the client application such manipulations may not be detectable by the TOE itself and therefore this threat needs to be countered within the TOE environment.

Manipulation of data in the TOE environment might also occurs on R.USERMGMT_DATA within the session of a Crypto-officer whose responsibility is to load this data in the cryptomodule.

6.2.3.4 Threats on TOE Services

T.Insecure_Init *Insecure initialization of the TOE*

TA.INSIDER or TA.INADVERTENT may initialize the TOE with insecure R.TSF_DATA, R.USERMGMT_DATA.

For example, TA.INADVERTENT may initialize the TOE (R.SERVICES_4) with an outdated access control list (R.USERMANGT_DATA).

T.Malfunction *Malfunction of TOE*

There is no active agent for this threat.

An internal malfunction of TOE functions may result in:

- the modification of R.DTBS_Representation,
- misuse of R.SERVICES,
- disclosure or alteration of R.CSP-SCD
- disclosure or alteration of R.BACKUP_KEY
- denial of R.SERVICES for authorized users
- alteration of R.TSF_DATA or R.USERMGMT_DATA

This includes the destruction of the TOE as well as hardware failures, which prevent the TOE from performing its services.

This includes also the destruction of the TOE by environmental failure.

Finally, this includes any kind of physical tampering that induces erroneous behaviour from the underlying hardware or software of the ToE.

Technical failure may result in an insecure operational state violating the integrity and availability of the TOE services.

Documents
Document Sharing Hub
Full document details: PD CEN/TS 419221-2:2016