SLOVENSKI STANDARD
SIST EN 419241-2:2019

01-maj-2019

Zaupanja vredni sistemi, ki podpirajo strežniško podpisovanje - 2. del: Zaščita profilov za QSCD za strežniško podpisovanje

Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

Vertrauenswürdige Systeme, die Serversignaturen unterstützen - Teil 2: Schutzprofil für qualifizierte Signaturerstellungseinheiten zur Serversignierung

Systèmes fiables de serveur de signature électronique - Partie 2 : Profil de protection de QSCD pour la signature par serveur

Ta slovenski standard je istoveten z: EN 419241-2:2019

ICS:

35.030	Informacijska varnost	IT Security
35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST EN 419241-2:2019 en,fr,de

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419241-2

February 2019

ICS 35.030

English Version

Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

Systèmes fiables de serveur de signature électronique - Partie 2 : Profil de protection de QSCD pour la signature par serveur

Vertrauenswürdige Systeme, die Serversignaturen unterstützen - Teil 2: Schutzprofil für qualifizierte Signaturerstellungseinheiten zur Serversignierung

This European Standard was approved by CEN on 26 November 2018.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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, Serbia, 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: Rue de la Science 23, B-1040 Brussels

Ref. No. EN 419241-2:2019 E

Contents

European foreword

This document (EN 419241-2:2019) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by August 2019, and conflicting national standards shall be withdrawn at the latest by August 2019.

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 has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: 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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

This Protection Profile for ‘QSCD for Server Signing’ (SAM-PP) is issued by the European Committee for Standardization (CEN) TC 224.

The document has been prepared as a Protection Profile (PP) following the rules and formats of Common Criteria version 3.1r4 [CC1], [CC2] and [ICC3].

This document is part of the EN 419241 series that consists of the following parts:

- EN 419241-1: Security Requirements for Trustworthy Systems Supporting Server Signing;
- EN 419241-2: This document

Further details of this series can be found in EN 419241-1.

Document Structure

Section 1 provides the introductory material for the Protection Profile.

Section 2 describes normative references

Section 3 describes terms and definitions

Section 4 contains the introduction

Section 5 provides the conformance claim

Section 6 provides the Security Problem Definition. It presents the Assets, Threats, Organisational Security Policies and Assumptions related to the TOE.

Section 7 defines the security objectives for both the TOE and the TOE environment.

Section 8 contains an extended component definition to include random number generation

Section 9 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [CC2] and Part 3 [CC3] that has to be satisfied by the TOE.

Section 10 provides rationales to demonstrate that:

- Security Objectives satisfy the policies and threats
- SFR match the security Objectives
- SFR dependencies are satisfied
- The SARs are appropriate.

A reference section is provided to identify background material.

An acronym list is provided to define frequently used acronyms.

1 Scope

This document specifies a protection profile for a Signature Activation Module (SAM), which is aimed to meet the requirements of a QSCD as specified in Regulation (EU) No 910/2014 [eIDAS].

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 419241-1, *Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements*

EN 419221-5, *Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services*

3 Terms, definitions, symbols and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 419241-1, EN 419221-5 and eIDAS article 3 an the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

NOTE Common Criteria terms and definitions are given in [CC1].

3.1.1
certificate
certificate for electronic signature as defined in [eIDAS] article 3

3.1.2
delegated party
subcontractor of the TSP or notified eID provider according to eIDAS regulation used for authentication

3.1.3
digital signature value
result of a cryptographic operation involving the signing key

Note 1 to entry: Within this document, Seal, Signature, Digital Signature or Digital Seal denote Digital Signature Value.

3.1.4
one-time signing key
signing key created, used and disposed based on one a single authorization, typically linked to a single session signing DTBS/R(s)

Note 1 to entry: Contrary to signing keys, which may be used in several signing sessions.

3.2 Symbols and abbreviations

CA	Certification Authority
CM	Cryptographic Module certified according to [EN 419 221–5]
CSR	Certification Signing Request
DTBS/R(s)	One or a set of DTBS/R.

4 Introduction

4.1 General

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

4.2 Protection Profile Reference

Title	Common Criteria Protection Profile – Protection Profile for QSCD for Server Signing
CC revision	v3.1 release 4
PP version	1.0
Authors	WG17
Keywords	Server Signing

4.3 Protection Profile Overview

4.3.1 European Legislation

The Regulation (EU) No 910/2014 [eIDAS] recital 52 considers the creation of remote electronic signatures, where the electronic signature creation data are managed remotely by a trust service provider on behalf of the signatory.

Such trust service providers should apply specific management and administrative security procedures in order to guarantee that the electronic signature creation environment is reliable and used under the sole control of the signatory.

This regulation requires, for qualified electronic signatures, the use of qualified electronic signature creation devices and for qualified electronic seals, the use of qualified electronic seal creation devices, as defined in the regulation. In the present document, both types of devices are referred to as QSCD.

4.4 TOE Overview

4.4.1 General

A trustworthy system supporting server signing (TW4S) is a system that offers remote digital signatures as a service. It ensures that signer's signing key or keys are only used under the sole control of the signer for the intended purpose.

In this document, the TW4S uses a Cryptographic Module to generate the signing key and create the digital signature value.

The system consists of a local and remote environment. The signer is in the local environment and interacts using a device (e.g. laptop, tablet or smart phone) with the Server Signing Application (SSA) in the remote environment.

The purpose of the interaction between the device and SSA is for the signer to utilize the SSAs signing service. The signature operation is performed using a Signature Activation Protocol (SAP), which requires that Signature Activation Data (SAD) be provided at the local environment. The SAD binds together three elements: signer authentication with the signing key and the data to be signed (DTBS/R(s)).

To ensure the signer has sole control of his signing keys, the signature operation needs to be authorized. This is carried out by a Signature Activation Module (SAM), which can handle one end point of SAP, verify SAD and activate the signing key within a Cryptographic Module. Both the Cryptographic Module and the SAM are to be located within a tamper protected environment. SAD verification means that the SAM checks the binding between the three SAD elements as well as checking that the signer is authenticated.

One of the three SAD elements is the signer authentication. The signer authentication is assumed to be conducted according to EN 419241-1 SCAL.2 for qualified signatures. This means signer authentication can be carried out in one of the following ways:

- Directly by the SAM. In this case the SAM verifies the signer’s authentication factor(s).
- Indirectly by the SAM. In this case, an external authentication service as part of the TW4S or a delegated party that verifies the signer’s authentication factor(s) and issues an assertion that the signer has been authenticated. The SAM shall verify the assertion.
- A combination of the two direct or indirect schemes, where a part of the signer authentication is done directly by the SAM and another part is done indirectly by the SAM.

In case the signer authentication is not performed directly by the SAM, the SAM has to assume (on the environment) that part of or complete authentication has taken place and rely on an assertion. In this PP signer authentication means that the signer has been authenticated in one of the three ways mentioned above.

The SAM module is the TOE of this PP. The TOE and Cryptographic Module certified against EN 419221-5 is required to obtain a QSCD.

The illustration below gives an overview of the environment on which the TOE is placed.

The signer is located in the local environment with a user interface on device (e.g. laptop, tablet, smartphone). The user interface can display documents for the signer. The device uses a signer interaction component (SIC) to communicate with the SSA. The SSA forwards the communication from the SIC or from the SSA to the QSCD. Inside the QSCD the SAM receives the messages and optionally communicates with the SSA to obtain relevant data. When the SAM module has verified SAD, it can authorize the activation of the signing key within the Cryptographic Module and produce a digital signature value. The value is returned to the SSA and may be further delivered to the SCA or SIC. From a TOE point of view the SSA and User Interface acts as supporting modules which displays document and forwards communication messages.

The TOE generates audit records for all security related events and relies on the SSA to store and provide access control for the records.

The TW4S relies on other services:

- Signers shall be identified and registered. It may involve establishment of authentication mechanism for a signer.
- Signing keys are certified by a Certification Authority.

- The Signature Creation Application is responsible for creating the signed document using the signature values provided by the TW4S.

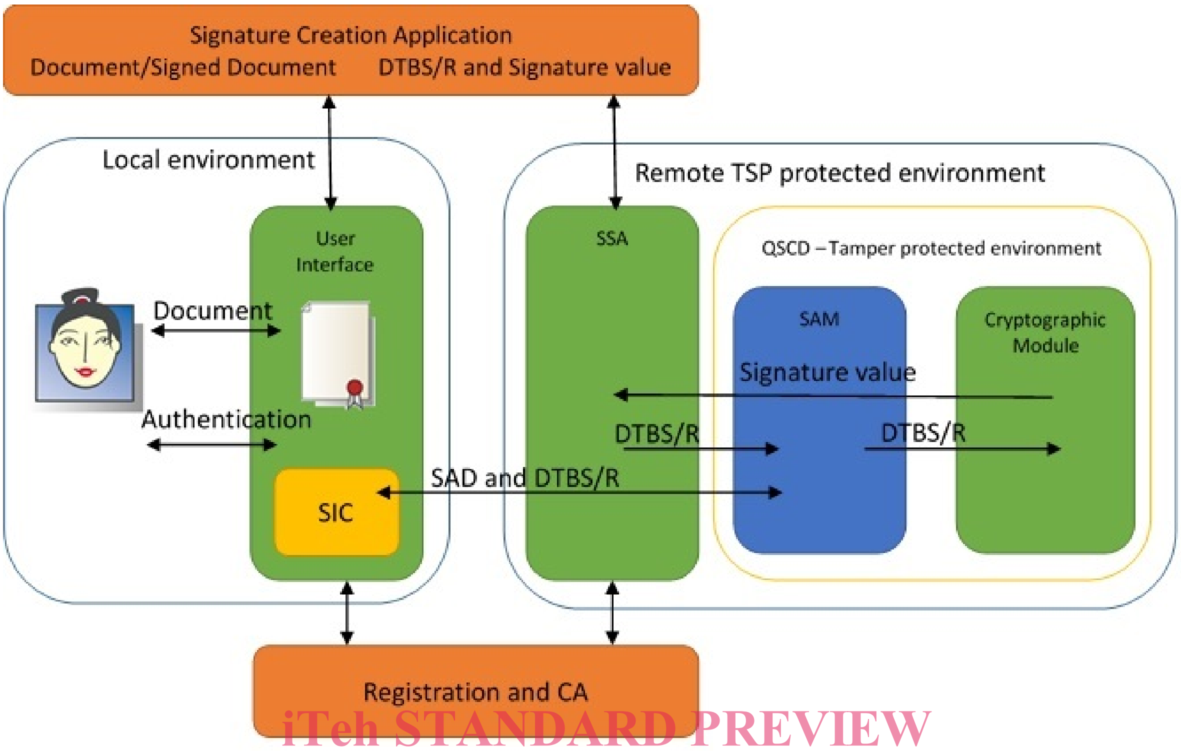

Figure 1

4.4.2 TOE type

The TOE is a software component, which implements the Signature Activation Protocol (SAP). It is either deployed within the tamper protected part of the Cryptographic Module or alternatively in a dedicated tamper protected environment, that is connected to the Cryptographic Module via a trusted channel.

It uses the Signature Activation Data (SAD) from the signer to activate the corresponding signing key for use in a Cryptographic Module.

Together the TOE and Cryptographic Module are a QSCD.

4.4.3 TOE life cycle

The TOE life cycle consists of successive phase for development, production, preparation and operational use.

Development: The TOE developer develops the TOE application and its guidance documentation using any appropriate guidance documentation for components working with the TOE, including the Cryptographic Module.

Delivery: The TOE is securely delivered from the TOE developer to the TSP.

Installation and configuration: The TSP installs and configures the TOE with the appropriate configuration and initialisation data. Installation may allow creating the Privileged Users.

Operational phase: In operation, the TOE can be used by Privileged Users to create Privileged Users and Signers. Privileged Users can maintain TOE configuration. Privileged Users and Signers may generate signature keys for a Signer. Privileged Users and Signers can supply the data to be signed to the TOE, but only Signer can authorize a signature creation.

The TOE end of life is out of the scope of this document.

4.4.4 Usage and major security features of the TOE

The major security features of the TOE are:

- Operator management:
  - Privileged Users can create other Privileged Users.
- System management
  - Privileged Users can handle system configuration.
- Signer management covers:
  - Privileged Users can create Signers
  - Privileged Users can assign one of the three authentication schemes (direct, indirect or mixed) to a Signer.
  - Privileged Users or Signers can generate signing keys and signature Verification Data (SVD) using a Cryptographic Module and assign the signing key identifier and SVD to a Signer.
  - Privileged Users or Signers can disable a signing key identifier to be used by a Signer.
- Signature operation
  - Privileged Users or Signers can supply a DTBS/R(s) to be signed.
  - The link between signer authentication, DTBS/R(s) and signing key identifier is handled by the Signature Activation Data (SAD). This SAD is securely exchanged with the TOE using the Signature Activation Protocol (SAP). Within the TOE the following actions are performed:
    - The SAD is verified in integrity.
    - The SAD is verified that it binds together the Signer authentication, a DTBS/R(s) and signing key identifier.
    - The Signer identified in the SAD is authenticated using one of the three authentication schemes.
    - The DTBS/R(s) used for signature operations is bound to the SAD.
    - The signing key identifier is assigned to the Signer.
    - The TOE uses Authorization Data to activate the signing key within the Cryptographic Module.
    - The TOE uses the Cryptographic Module to create signatures.
- The TOE generates audit records for all security related events and relies on the SSA to store and provide access control for the records.

The TOE handles data assets as specified in 6.1.

4.4.5 TOE Environment general overview

This PP is aimed to support TSPs requiring to use a QSCD for server signing.

The TOE is expected to:

1. operate as parts of server signing system as specified in EN 419241-1
2. be used by a TSP applying security policies as required by TSPs providing signature creation services
3. be used in conjunction with TSPs issuing certificates

4.4.6 Available non-TOE hardware/software/firmware

The TOE needs, at least, the following hardware/software/firmware to operate:

- A Signature Creation Application (SCA) that manages the document to be signed and transfers that to the SSA, either directly or through the SIC.
- A SSA component that handles communications between SAM in the QSCD and SIC in the signer device.
- A SIC used locally by the signer to communicate with the remote systems.
- A Cryptographic Module certified against EN 419221-5, which supports the operation of the TOE.

4.4.7 Options

The Protection Profile includes options, which the ST writer shall specify. To assist the ST writer identifying these options, they are summarized in Table 1.

Table 1

Option	Description
Deployment	The TOE may be deployed in a Cryptographic Module or in a dedicated hardware module. The ST writer shall pay special attention to the SFRs FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FCS_RNG.1, FPT_PHP.1, FPT_PHP.3 and FTP_ITC.1/CM as these SFRs may be met differently depending on the deployment.

5 Conformance Claim

5.1 CC Conformance Claim

This protection profile (PP) claims to be Common Criteria Part 2 extended and Common Criteria Part 3 conformant and written according to the Common Criteria version 3.1 R4 [CC1], [CC2] and [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 other Protection Profile.

5.3 Conformance Rationale

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

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

The TOE has the following assets, which are to be protected in integrity and confidentiality as described below. The TOE shall ensure that whenever an asset is persisted outside the TOE, the TOE has performed the necessary cryptographic operations to enforce confidentiality and detect if an asset has been modified. Access control to TOE assets outside the TOE are to be enforced by the environment.

R.Signing_Key_Id: The signing key is the private key of an asymmetric key pair used to create a digital signature under the signer's sole control. The signing key can only be used by the Cryptographic Module. The TOE uses the asset R.Signing_Key_Id, which identifies a signing key in the Cryptographic Module. The binding of the R.Signing_Key_Id with R.Signer shall be protected in integrity.

Application Note 1

The integrity and confidentiality of the signing key and the link between the R.Signing_Key_Id and the signing key is the responsibility of the Cryptographic Module. The TOE shall ensure that only the signer can use the signing key under his sole control.

R.Authorisation_Data: is data used by the TOE to activate a signing key in the Cryptographic Module. The signing key is identified by R.Signing_Key_Id. It shall be protected in integrity and confidentiality.

Application Note 2

The R.Authorisation_Data are used by the Cryptographic Module to activate a signing key. The data may be an asset of the TOE or derived by the TOE from the SAD. In both cases, the TOE shall verify the SAD before the R.Authorisation_Data are used to activate the signing key in the Cryptographic Module.

If the TOE derives the R.Authorisation_Data from SAD then this data may not be held by the TOE.

R.SVD: signature verification data are the public part, associated with the signing key, to perform digital signature verification. The R.SVD shall be protected in integrity.

The TOE uses a Cryptographic Module for signing key pair generation. As part of the signing key pair generation, Cryptographic Module provides the TOE with R.Signing_Key_Id and R.SVD. The TOE provides the R.SVD to the SSA for further handling for the key pair to be certified.

R.DTBS/R: set of data which is transmitted to the TOE for digital signature creation on behalf of the signer. The DTBS/R(s) is transmitted to the TOE. The R.DTBS/R shall be protected in integrity. The transmission of the DTBS/R(s) to the TOE shall require the sending party - Signer or Privileged User - to be authenticated.

Application Note 3

The confidentiality of the R.DTBS/R is not required by Regulation (EU) No 910/2014 [eIDAS].

R.SAD: signature activation data are a set of data involved in the signature activation protocol, which activates the signature creation data to create a digital signature under the signer's sole control. The R.SAD shall combine:

- The signer's strong authentication as specified in EN 419241-1
- If a particular key is not implied (e.g a default or one-time key) a unique reference to R.Signing_Key_Id.
- A given R.DTBS/R.

The R.SAD shall be protected in integrity and confidentiality.

Application Note 4

If the SAD does not require encrypted data then the confidentiality requirement is considered fulfilled. The ST writer shall describe which part of the SAD shall be protected in confidentiality.

Application Note 5

The R.SAD may include some or all authentication factors or evidence from other systems that some or all authentication factors have been verified.

Application Note 6

The unique reference to R.Signing_Key_Id in the R.SAD could be a certificate, a key identifier or derived information obtained from the signer's authentication.

Some solutions may use one-time signing keys, which are generated, certified and used within a limited signing session. The derived information from the signer's authentication may be used to provide session separation if a signer has multiple simultaneous signing sessions with the TOE, or to derive a R.Signing_Key_Id if the key is a one-time key. At the end of the session, the signing key is reliably deactivated.

For solutions that only handle one signing key for each signer, the reference to the R.Signing_Key_Id may also be implied and omitted from the SAD.

The ST writer shall describe what R.Signing_Key_Id is for a specific TOE.

R.Signature: is the result of the signature operation and is a digital signature value. R.Signature is created on the R.DTBS/R using R.Signing_Key_Id by the Cryptographic Module under the signer's control as part of the SAP. The R.Signature shall be protected in integrity. The R.Signature can be verified outside TOE using R.SVD.

R.Audit: is audit records containing logs of events requiring to be audited. The logs are produced by the TOE and stored externally. The R.Audit shall be protected in integrity.

R.Signer: is a TOE subject containing the set of data that uniquely identifies the signer within the TOE. The R.Signer shall be protected in integrity and confidentiality.

Application Note 7

It is only within the TOE the R.Signer needs to be unique. It is not the responsibility of the TOE to establish a connection between the R.Signer and the signer's identity. The signer is said to own the R.Signer object which uniquely identifies him within the TOE.

Application Note 8

The R.Signer can include references to zero, one or several R.Signing_Key_Ids and R.SVDs.

Application Note 9