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

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 419241-2:2019 sisaldab Euroopa standardi EN 419241-2:2019 ingliskeelset teksti.	This Estonian standard EVS-EN 419241-2:2019 consists of the English text of the European standard EN 419241-2:2019.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 27.02.2019.	Date of Availability of the European standard is 27.02.2019.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

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.

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of an identical text or by endorsement, at the latest by August 2019, and conflicting national standards shall be withdrawn at the latest by August 2019.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.