

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

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

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

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

Contents

EUROPEAN FOREWORD.....	4
INTRODUCTION.....	5
1 SCOPE.....	6
2 NORMATIVE REFERENCES.....	6
3 TERMS, DEFINITIONS, SYMBOLS AND ABBREVIATIONS	6
3.1 TERMS AND DEFINITIONS	6
3.2 SYMBOLS AND ABBREVIATIONS.....	7
4 INTRODUCTION.....	7
4.1 GENERAL.....	7
4.2 PROTECTION PROFILE REFERENCE	7
4.3 PROTECTION PROFILE OVERVIEW	7
4.4 TOE OVERVIEW	7
5 CONFORMANCE CLAIM	11
5.1 CC CONFORMANCE CLAIM.....	11
5.2 PP CLAIM	12
5.3 CONFORMANCE RATIONALE	12
5.4 CONFORMANCE STATEMENT	12
6 SECURITY PROBLEM DEFINITION.....	12
6.1 ASSETS	12
6.2 SUBJECTS	14
6.3 THREATS	15
6.4 RELATION BETWEEN THREATS AND ASSETS	18
6.5 ORGANISATIONAL SECURITY POLICIES	19
6.6 ASSUMPTIONS	20
7 SECURITY OBJECTIVES.....	21
7.1 GENERAL.....	21
7.2 SECURITY OBJECTIVES FOR THE TOE	21
7.3 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT	23
7.4 SECURITY PROBLEM DEFINITION AND SECURITY OBJECTIVES	25
7.5 RATIONALE FOR THE SECURITY OBJECTIVES	30
8 EXTENDED COMPONENTS DEFINITIONS.....	33
8.1 CLASS FCS: CRYPTOGRAPHIC SUPPORT.....	33
9 SECURITY REQUIREMENTS	34
9.1 TYPOGRAPHICAL CONVENTIONS	34
9.2 SUBJECTS, OBJECTS AND OPERATIONS	35
9.3 SFRS OVERVIEW	36
9.4 SECURITY FUNCTIONAL REQUIREMENTS	39
9.5 SECURITY ASSURANCE REQUIREMENTS	64

10	RATIONALE	65
10.1	SECURITY REQUIREMENTS RATIONALE	65
10.2	SFR DEPENDENCIES	72
10.3	RATIONALES FOR SARS	74
	BIBLIOGRAPHY	75

This document is a preview generated by EVS

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 and 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.