Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 419241-1:2018 sisaldab Euroopa standardi EN 419241-1:2018 ingliskeelset teksti.	This Estonian standard EVS-EN 419241-1:2018 consists of the English text of the European standard EN 419241-1:2018.
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 04.07.2018.	Date of Availability of the European standard is 04.07.2018.
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 419241-1

July 2018

ICS 35.030

Supersedes CEN/TS 419241:2014

English Version

Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

Systèmes fiables de serveur de signature électronique - Partie 1: Exigences de sécurité générales du système

Vertrauenswürdige Systeme, die Serversignaturen unterstützen - Teil 1: Allgemeine Systemsicherheitsanforderungen

This European Standard was approved by CEN on 30 April 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 419241-1:2018 E

Contents

Page

European foreword

This document (EN 419241-1:2018) 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 January 2019, and conflicting national standards shall be withdrawn at the latest by January 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 supersedes CEN/TS 419241:2014.

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

Successful implementation of European Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (referred in this document as the eIDAS [4] Regulation), requires standards for services, processes, systems and products related to trust services as well as guidance for conformity assessment of such services, processes, systems and products.

In line with Standardization Mandate 460, consequently issued by the Commission to CEN, CENELEC and ETSI for updating the existing eSignature standardization deliverables, CEN and ETSI have set up the eSignature Coordination Group in order to coordinate the activities achieved for Mandate 460. One of the first tasks was to establish a rationalized framework, the second phase to deliver a set of standards in order to cover the Trust Services defined in the eIDAS [4] Regulation.

This document, being part of the set of European Standards, is aimed to meet the requirements of the eIDAS [4] Regulation for remote use of a signature creation device by a set of security requirements for a server-side system using private signing keys managed by a trust service provider in order to create digital signatures.

The purpose of the trustworthy system is to create a digital signature under sole control of a natural person, or under control of a legal person which may be incorporated into an electronic signature or an electronic seal as defined in the eIDAS [4] Regulation.

This standard is identified as EN 419241-1. A complete framework for standardization of signatures can be found in ETSI TR 119 000.

This series of European Standards consists of the following parts under the general title *Trustworthy Systems Supporting Server Signing*:

— *Part 1: General System Security Requirements*

— *Part 2: Protection Profile for QSCD for Server Signing*

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

The European Regulation eIDAS establishes a legal framework of requirements for electronic signatures. This regulation also introduces the notion of electronic signatures which are created using a remote signature creation device to increase usage in the light of its multiple economic benefits and ease of use. The eIDAS [4] Regulation also introduces the concept of electronic seal which has similar technical properties to electronic signatures, but with a lower level of sole control. Both electronic signatures and electronic seals use technology based around asymmetric cryptography commonly referred to as digital signatures.

However, in order to ensure that such remotely created digital signatures receive the same legal recognition as digital signatures created in an entirely user-managed environment (e.g. using smart cards), remote signature services providers should apply specific management and administrative security procedures, and use reliable systems and products, including secure electronic communication channels, in order to guarantee that the server signing environment is reliable and that signing keys are used with a high level of confidence, under the sole control of the signer.

The main objective of this standard is to define requirements and recommendations for a networked signing server which may manage signing keys used by natural or legal persons for the creation of digital signatures.

This part of the series of European Standards specifies the general requirements of systems for server signing. Additional specifications (e.g. protection profiles) may be issued which provide more detailed requirements for particular components of the system.

It is assumed that the Trust Service Provider (TSP) which provides signature creation services, operates the trustworthy system in an environment with a security policy which incorporates general physical, personnel, procedural and documentation security requirements for TSPs providing signature creation services.

It is recommended to follow, e.g. ETSI EN 319 401 to ensure that the above requirements are met.

The present standard does not aim at limiting the legal form of signatures created; it could be electronic signature or electronic seals, qualified or not.

Correspondence and comments to this Security Requirements for Trustworthy Systems Supporting Server Signing should be referred to:

Editor: Franck Leroy

Email: **franck.leroy@docapost.fr**

1 Scope

1.1 General

This document specifies security requirements and recommendations for Trustworthy Systems Supporting Server Signing (TW4S) that generate digital signatures.

The TW4S is composed at least of one Server Signing Application (SSA) and one Signature Creation Device (SCDev) or one remote Signature Creation Device.

A remote SCDev is a SCDev extended with remote control provided by a Signature Activation Module (SAM) executed in a tamper protected environment. This module uses the Signature Activation Data (SAD), collected through a Signature Activation Protocol (SAP), in order to guarantee with a high level of confidence that the signing keys are used under sole control of the signer.

The SSA uses a SCDev or a remote SCDev in order to generate, maintain and use the signing keys under the sole control of their authorized signer. Signing key import from CAs is out of scope.

So when the SSA uses a remote SCDev, the authorized signer remotely controls the signing key with a high level of confidence.

A TW4S is intended to deliver to the signer or to some other application, a digital signature created based on the data to be signed.

This standard:

— provides commonly recognized functional models of TW4S;

— specifies overall requirements that apply across all of the services identified in the functional model;

— specifies security requirements for each of the services identified in the TW4S;

— specifies security requirements for sensitive system components which may be used by the TW4S.

This standard is technology and protocol neutral and focuses on security requirements.

1.2 Outside of the scope

The following aspects are considered outside of the scope of this document:

— other trusted services that may be used alongside this service such as certificate issuance, signature validation service, time-stamping service and information preservation service;

— any application or system outside of the TW4S (in particular the signature creation application including the creation of advanced signature formats);

— signing key and signing certificate import from CAs;

— the legal interpretation of the form of signature (e.g. electronic signature, electronic seal, qualified or otherwise).

1.3 Audience

This standard specifies security requirements that are intended to be followed by:

— providers of TW4S systems;

— Trust Service Providers (TSP) offering a signature creation service.

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.

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

FIPS PUB 140-2, *Security requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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

3.1
authentication
provision of assurance in the identity of an entity

[SOURCE: ISO/IEC 18014-2:2009]

3.2
authentication Factor
piece of information and/or process used to authenticate or verify the identity of an entity

[SOURCE: ISO/IEC 19790:2012]

3.3
data to be signed representation
data formatted which is used to compute the digital signature value (e.g. hash value)

[SOURCE: ETSI/TR 119 001:2016]

3.4
digital signature
data unit appended to, or a cryptographic transformation of a data that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[SOURCE: ETSI/TR 119 001:2016]

3.5
eIDAS Regulation
Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC