ILNAS

Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN 419241-1:2018

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

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

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

07/2018

National Foreword

This European Standard EN 419241-1:2018 was adopted as Luxembourgish Standard ILNAS-EN 419241-1:2018.

Every interested party, which is member of an organization based in Luxembourg, can participate for FREE in the development of Luxembourgish (ILNAS), European (CEN, CENELEC) and International (ISO, IEC) standards:

- Participate in the design of standards
- Foresee future developments
- Participate in technical committee meetings

https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html

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 ... 4
Introduction ... 6
1 Scope ... 7
1.1 General ... 7
1.2 Outside of the scope ... 7
1.3 Audience ... 7
2 Normative references ... 8
3 Terms and definitions ... 8
4 Symbols and abbreviations ... 10
5 Description of trustworthy systems supporting server signing ... 11
5.1 General ... 11
5.2 Signature creation and server signing objectives ... 11
5.3 Signature bound to a natural person or seal bound to a legal person ... 11
5.4 Sole control assurance levels ... 11
5.5 Batch server signing ... 12
5.6 Signing key and cryptographic module ... 12
5.7 Signer's authentication ... 12
5.7.1 Electronic identification means ... 12
5.7.2 Authentication Mechanism ... 12
5.7.3 Authentication target ... 13
5.7.4 Delegation of authentication to an external party ... 13
5.8 Signature activation data ... 14
5.9 Signature activation protocol ... 14
5.10 Signer's interaction component ... 14
5.11 Signature activation module ... 15
5.12 Environments ... 15
5.12.1 Tamper protected environment ... 15
5.12.2 TSP protected environment ... 15
5.12.3 Signer's environment ... 16
5.13 Functional model ... 16
5.13.1 General ... 16
5.13.2 Scope of requirements ... 16
5.13.3 Signature activation mechanisms ... 17
5.13.4 TW4S components ... 19
6 Security requirements ... 20
6.1 General ... 20
6.2 General security requirements (SRG) ... 20
6.2.1 Management (SRG_M) ... 20
6.2.2 Systems and operations (SRG_SO) ... 22
6.2.3 Identification and authentication (SRG_IA) ... 22
6.2.4 System access control (SRG_SA) ... 23
6.2.5 Key management (SRG_KM) ... 23
6.2.6 Auditing (SRG_AA) ... 26
6.2.7 Archiving (SRG_AR) ... 28

6.2.8 Backup and recovery (SRG_BK) 28
6.3 Core components security requirements (SRC) 29
6.3.1 Signing key setup (SRC_SKS) - Cryptographic key (SRC_ SKS.1) 29
6.3.2 Signer authentication (SRC_SA) 29
6.3.3 Digital signature creation (SRC_DSC) - Cryptographic operation (SRC_DSC.1) 30
6.4 Additional security requirements for SCAL2 (SRA) 30
6.4.1 General 30
6.4.2 Signature activation protocol and signature activation data (SRA_SAP) 30
6.4.3 Signing key management (SRA_SKM) 32
Annex A (normative) Requirements for electronic identification means, characteristics and design 34
A.1 Enrolment 34
A.1.1 Application and registration 34
A.1.2 Identity proofing and verification (natural person) 34
A.1.3 Identity proofing and verification (legal person) 37
A.1.4 Binding between the electronic identification means of natural and legal persons 39
A.2 Electronic identification means and authentication 40
A.2.1 Electronic identification means characteristics and design 40
A.2.2 Authentication mechanism 41
Bibliography 42

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**