SLOVENSKI STANDARD
SIST-TS CEN/TS 419241:2014

01-julij-2014

Varnostne zahteve za zaupanja vredne sisteme, ki podpirajo strežniško podpisovanje

Security Requirements for Trustworthy Systems Supporting Server Signing

Sicherheitsanforderungen für Vertrauenswürdige Systeme, die Serversignaturen unterstützen

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Exigences de sécurité pour des systèmes fiables de serveur de signature électronique

Ta slovenski standard je istoveten z: CEN/TS 419241:2014

SIST-TS CEN/TS 419241:2014
https://standards.iteh.ai/catalog/standards/sist/050147cc-4536-4923-8483-86ab792208b3/sist-ts-cen-ts-419241-2014

ICS:

35.240.99	Uporabniške rešitve IT na drugih področjih	IT applications in other fields

SIST-TS CEN/TS 419241:2014 **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST-TS CEN/TS 419241:2014

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST-TS CEN/TS 419241:2014
https://standards.iteh.ai/catalog/standards/sist/050147cc-453b-4923-8483-86ab792208b3/sist-ts-cen-ts-419241-2014

SIST-TS CEN/TS 419241:2014

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 419241

March 2014

ICS 35.240.99

English Version

Security Requirements for Trustworthy Systems Supporting Server Signing

Exigences de sécurité pour des systèmes fiables de serveur de signature électronique

Sicherheitsanforderungen für Vertrauenswürdige Systeme, die Serversignaturen unterstützen

This Technical Specification (CEN/TS) was approved by CEN on 14 October 2013 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

SIST-TS CEN/TS 419241:2014
https://standards.iteh.ai/catalog/standards/sist/050147cc-453b-4923-8483-86ab792208b3/sist-ts-cen-ts-419241-2014

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2014 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN/TS 419241:2014 E

SIST-TS CEN/TS 419241:2014

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS CEN/TS 419241:2014
https://standards.iteh.ai/catalog/standards/sist/050147cc-453b-4923-8483-86ab792208b3/sist-ts-cen-ts-419241-2014

SIST-TS CEN/TS 419241:2014

Foreword

This document (CEN/TS 419241:2014) 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] 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.

Successful implementation of European Directive 1999/93/EC on a community framework for electronic signatures requires standards for services, processes, systems and products related to electronic signatures as well as guidance for conformity assessment of such services, processes, systems and products.

In 1999 the European ICT Standards Board, with the support of the European Commission, undertook an initiative bringing together industry and public authorities, experts and other market players, to create the European Electronic Signature Standardization Initiative (EESSI).

Within this framework the Comité Européen de Normalisation / Information Society Standardization System (CEN/ISSS) and the European Telecommunications Standards Institute / Electronic Signatures and Infrastructures (ETSI/ESI) were entrusted with the execution of a work programme to develop generally recognized standards to support the implementation of Directive 1999/93/EC and the development of a European electronic signature infrastructure.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This document will describe security requirements for a server-side system using certificates in order to create advanced electronic signatures (AdES) in accordance with the requirements of the European Directive on Electronic Signature 1999/93. The signature is to be supported by a qualified certificate, or other public key certificate issued for the purposes of signing, issued by a Trust Services Provider (TSP) operating to recognized good practices (e.g. ETSI EN 319 411-3 (aka ETSI/TS 102 042) or ETSI EN 319 411-2 (aka ETSI/TS 101 456)). The document will include requirements for the use of the appropriate protection profiles for the Signature Creation Device (SCDev).

SIST-TS CEN/TS 419241:2014
https://standards.iteh.ai/catalog/standards/sist/050147ec-453b-4925-8483-86ab792208b3/sist-ts-cen-ts-419241-2014

The purpose of the trustworthy system is to produce an advanced electronic signature created under sole control of a natural person, or a legal person (such advanced electronic signatures produced by legal persons are called electronic seals).

The Signature Generation Service Provider (SGSP) operates the trustworthy system in an environment with a security policy which incorporates general physical, personnel, procedural and documentation security requirements as defined in ETSI EN 319 411-2 / ETSI EN 319 411-3.

This document is identified as CEN/TS 419241 within the Rationalised Framework for Electronic Signature Standardization ETSI SR 001 604.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this Technical Specification: 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, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

SIST-TS CEN/TS 419241:2014

Introduction

The European Directive 1999/93/EC establishes a framework of requirements for the use of electronic signatures. This Directive also introduces the notion of advanced electronic signature which is defined as legally equivalent to a hand-written one if generated by a physical person using a qualified certificate stored in a Secure Signature Creation Device (SSCD).

Since the publication of the Directive, other forms of electronic signatures have appeared in order to meet market needs (e.g. e-Invoicing, e-Procurement). These other forms do not necessarily require the use by a natural or legal person of a secure signature creation device and/or qualified certificate.

One of these forms is an electronic signature created using a networked server. The Signature Creation Data (SCD) is under control of an individual user but held centrally within a shared server, instead on a secure signature creation device held by the signatory.

It is not the intent of this standard to limit the type of public key certificate, qualified or otherwise, used by the networked signing server.

The main objective of this standard is to define requirements and recommendations for a networked signing server which may process electronic certificates used by natural or legal persons for electronically signing documents.

This document specifies basic requirements for server signing. Additional specifications may be issued which provide more detailed requirements. For further details see ETSI SR 001 604.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS CEN/TS 419241:2014
https://standards.iteh.ai/catalog/standards/sist/050147cc-453b-4923-8483-86ab792208b3/sist-ts-cen-ts-419241-2014

SIST-TS CEN/TS 419241:2014

1 Scope

1.1 General

This document specifies security requirements and recommendations for Trustworthy System Supporting Server Signing (TW4S) that generate advanced electronic signatures as defined in Directive 1999/93/EC. This document may also be applied to electronic signatures complying to Article 5(1) of Directive 1999/93/EC employing a Secure Signature Creation Device (SSCD) compliant with Annex III and supported by a qualified electronic signature.

The Server Signing Application (SSA) runs on a networked server supporting one or more signatories to remotely sign electronic documents using centralized signature keys held on the signing server under sole control of the signatory.

An SSA is intended to deliver to the user or to some other application process in a form specified by the user, an Advanced- or where applicable a Qualified - Electronic Signature associated with a Signer's Document as a Signed Data Object.

This document:

— 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 SSA.

— specifies security requirements for sensitive system components which may be used by the SSA (e.g. Signature Creation Device (SCDev)).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS CEN/TS 419241:2014
https://standards.iteh.ai/catalog/standards/sist/050147cc-4530-4923-8483-86ab792208b3/sist-ts-cen-ts-419241-2014

This document does not specify technologies and protocols, but rather identifies requirements on the security on technologies to be employed.

1.2 Out of scope

The following aspects are considered to be out of scope:

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

— any application or system outside of the SSA,

— the legal interpretation of any form of signature (e.g. the implications of countersignatures, of multiple signatures and of signatures covering complex information structures containing other signatures).

1.3 Audience

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

— providers of SSA systems.

— Trust Service Providers (TSP) offering signature generation service.

SIST-TS CEN/TS 419241:2014

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 419211 (all parts), *Protection profiles for secure signature creation device*

CWA 14167-2, *Cryptographic module for CSP signing operations with backup — Protection profile — CMCSOB PP*

CWA 14167-3, *Cryptographic module for CSP key generation services protection profile — CMCKG-PP*

CWA 14167-4, *Cryptographic module for CSP signing operations — Protection profile — CMCSO PP*

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

ISO/IEC 19790:2006, *Information technology — Security techniques — Security requirements for cryptographic modules*

3 Terms and definitions

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1
Advanced Electronic Signature
electronic signature which meets the following requirements:

SIST-TS CEN/TS 419241:2014
https://standards.iteh.ai/catalog/standards/sist/050147cc-453b-4923-8483-86ab792208b3/sist-ts-cen-ts-419241-2014

— it is uniquely linked to the signer;

— it is capable of identifying the signer;

— it is created using means that the signer can maintain under his sole control; and

— it is linked to the data to which it relates in such a manner that any subsequent alteration of the data is detectable

[SOURCE: Directive 1999/93/EC]

3.2
Certificate
electronic attestation that links a signature verification data to a person, and confirms the identity of that person

[SOURCE: Directive 1999/93/EC]

3.3
Certificate Identifier
unambiguous identifier of a Certificate

3.4
Certification Service Provider
entity or a legal or natural person who issues certificates or provides other services related to electronic signatures

[SOURCE: Directive 1999/93/EC]

SIST-TS CEN/TS 419241:2014

3.5
Data Content Type
signature attribute that expresses the encoding format of the Signers' Document (SD)

3.6
Data To Be Signed
data (e.g. a document or parts of a document) to be signed as well as any signature attributes that are bound together with the data by the signature

NOTE Data To Be Signed is the input to the cryptographic signing algorithm. The specific way that Data To Be Signed and any signature attributes are fed as input is defined in the specifications of the signature type in use.

3.7
Electronic Signature
data in electronic form attached to - or logically associated with - other electronic data and which serves as a method of authentication of that data

[SOURCE: Directive 1999/93/EC]

3.8
Qualified Certificate
certificate which meets the requirements laid down in Annex I of the Directive [i.e. Dir. 1999/93/EC] and is provided by a certification service provider who fulfils the requirements laid down in Annex II of that Directive

[SOURCE: Directive 1999/93/EC]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.9
Qualified Electronic Signature
advanced electronic signature which is based on a qualified certificate and which is created by a secure signature creation device

SIST-TS CEN/TS 419241:2014
https://standards.iteh.ai/catalog/standards/sist/050147cc-453b-4923-8483-86ab79220885/sist-ts-cen-ts-419241-2014

Note 1 to entry: This definition based on Article 5.1 of Directive 1999/93/EC.

3.10
Secure Signature Creation Device
signature creation device that meets the requirements laid down in Annex III of the EU Directive

[SOURCE: Directive 1999/93/EC]

3.11
Signatory
Signer
person who holds a signature creation device and acts either on his own behalf or on behalf of the natural or legal person he represents

[SOURCE: Directive 1999/93/EC]

Note 1 to entry: The term 'signer' is used throughout this document as a synonym.

3.12
Server Signing Application
application that provides a remote access to the Signature Creation Application (SCA)

3.13
Signature Creation Application
application that creates an electronic signature, using the digital signature produced by an SCDev connected to the SCA

SIST-TS CEN/TS 419241:2014

3.14
Signature Creation Data
unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature

[SOURCE: Directive 1999/93/EC]

3.15
Signature Creation Data Identifier
unambiguous identifier of a SCD

3.16
Signature Creation Device
configured software or hardware used to implement the SCD

[SOURCE: Directive 1999/93/EC]

Note 1 to entry: Secure Signature Creation Device (SSCD) or Hardware Security Module (HSM) are examples of Signature Creation Devices (SCDev).

3.17
Signature Creation Environment
physical, geographical and computational environment of the signature creation system

3.18
Signature Generation Service Provider
Trust Service provider which provides trust services that allow secure remote management of signatory's signature creation device and generation of electronic signatures by means of such a remotely managed device

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS CEN/TS 419241:2014
https://standards.iteh.ai/catalog/standards/sist/050147cc-453b-4923-8483-86ab792208b3/sist-ts-cen-ts-419241-2014

3.19
Signature Invocation
non-trivial interaction between the signer and the SSA or SCDev that is necessary to invoke the start of the signing process in the SSA/SCDev to generate the Signed Data Object (SDO), and that is the 'Wilful Act' of the signer

3.20
Signature Policy
set of rules for the creation and validation of an electronic signature, that defines the technical and procedural requirements for electronic signature creation and validation, in order to meet a particular business need, and under which the signature can be determined to be valid

[SOURCE: ETSI/TS 101 733]

3.21
Signature Suite
combination of a signature algorithm with its parameters, a key generation algorithm, a padding method, and a cryptographic hash function

[SOURCE: ETSI/TS 102 176]

3.22
Signed Data Object (s)
document(s) or parts of the document(s) for which an electronic signature has been generated, along with the electronic signature

SIST-TS CEN/TS 419241:2014

3.23
Signer's Activation Data
data (e.g. PIN, password or biometric data, one time password or cryptographically generated authentication token) which is used to authenticate the signer to the SCDev and which is required to allow the use of the SCD held on the SCDev and which may be referred to as 'Activation Data' in other documents

3.24
Signer's/Signers' Document
document for which one or more signers intend to create an Electronic Signature or for which an Electronic Signature was created

3.25
Trusted Path
path between two entities or components within an SSA that provides integrity and authenticity

3.26
Trust Service Provider
entity which provides electronic services which enhances trust and confidence in electronic transactions

3.27
Trustworthy System Supporting Server Signing
Server-side system using SCD in order to create Advanced Electronic Signatures (AdES) in accordance with the requirements of the European Directive on Electronic Signatures [i.e. Directive 1999/93/EC]

Note 1 to entry: The system includes at least an SSA and an SCDev.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4 Symbols and abbreviations

SIST-TS CEN/TS 419241:2014
https://standards.iteh.ai/catalog/standards/sist/0501f7ce-4356-4925-84a3-86ab792208b3/sist-ts-cen-ts-419241-2014

AdES	Advanced Electronic Signature
CC	Common Criteria, ISO/IEC 15408, *Evaluation criteria for IT security*
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CEN/ISSS	CEN Information Society Standardization System
CSP	Certification Service Provider
DTBS	Data to be Signed
EAL	Evaluation Assurance Level
EC	European Commission
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ISSS	Information Society Standardization System
PIN	Personal Identification Number
PKC	Public Key Certificate
QC	Qualified Certificate
QES	Qualified Electronic Signature
SAD	Signer's Activation Data
SCA	Signature Creation Application
SCD	Signature Creation Data