SLOVENSKI STANDARD
SIST-TS CEN/TS 419261:2015

01-julij-2015

Varnostne zahteve za zaupanja vredne sisteme, ki upravljajo potrdila za elektronsko podpisovanje

Security requirements for trustworthy systems managing certificates for electronic signatures

Sicherheitsanforderungen für vertrauenswürdige Systeme zur Verwaltung von Zertifikaten für elektronische Signaturen

Exigences de sécurité pour systèmes de confiance gérant des certificats pour signature électronique

Ta slovenski standard je istoveten z: CEN/TS 419261:2015

ICS:

35.040	Nabori znakov in kodiranje informacij	Character sets and information coding
35.240.30	Uporabniške rešitve IT v informatiki, dokumentiranju in založništvu	IT applications in information, documentation and publishing

SIST-TS CEN/TS 419261:2015 en,fr,de

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 419261

March 2015

ICS 03.120.20; 35.040; 35.240.30

English Version

Security requirements for trustworthy systems managing certificates and time-stamps

Exigences de sécurité pour systèmes de confiance gérant des certificats et des horodatages

Sicherheitsanforderungen für vertrauenswürdige Systeme zur Verwaltung von Zertifikaten für elektronische Signaturen und Zeitstempel

This Technical Specification (CEN/TS) was approved by CEN on 18 November 2014 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.

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.

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

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

Ref. No. CEN/TS 419261:2015 E

Contents

Page

Foreword

This document (CEN/TS 419261:2015) 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 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 [Dir.1999/93/EC] and of REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Reg.910/2014/EU] 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.

NOTE According to Article 50 of Reg.910/2014/EU Directive 1999/93/EC is repealed with effect from 1 July 2016 and references to the repealed Directive shall be construed as references to the Regulation.

In 1999 the European Information and Communications Technologies 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 Normalization / 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 [Dir.1999/93/EC] and development of a European electronic signature infrastructure.

The CEN/ISSS Workshop on electronic signatures (WS/E-SIGN) resulted in a set of deliverables, CEN Workshop Agreements (CWA), which contributed towards those generally recognized standards.

In 2011 the European Commission (EC) with the support of the European Free Trade Association has signed a specific grant agreement with the European Committee for Standardization (CEN) regarding the update of the existing European e-Signature CEN Workshop Agreements (CWAs) in the framework of Phase 1 of the mandate M/460. The present document is such a CEN Workshop Agreement that was first created as a CWA and then updated into a Technical Specification (TS).

The purpose of this TS is to describe the security requirements for trustworthy systems managing certificates for electronic signatures and to define overall system security requirements, whereas EN 419221 specifies security requirements for cryptographic devices. The requirements were partly inspired by Common Criteria [CC] Part 2, but the TS is not compliant to [CC], as e.g. EN 419221. In consequence, this TS cannot be used to perform Common Criteria certifications of products.

The TS is intended for use by designers and developers of systems managing certificates and time-stamps, as well as customers of such systems.

Executive Summary

This Technical Specification specifies security requirements on products and technology components, used by Trust Service Providers (TSPs) for issuing and managing certificates as well as electronic time-stamps in the sense of the REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Reg.910/2014/EU].

The term TSP includes certification service providers (CSPs) issuing qualified certificates as defined in the Directive *"Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures"* [Dir.1999/93/EC]. These certificates are used in conjunction with electronic signatures and advanced electronic signatures in accordance with Directive 1999/93/EC [Dir.1999/93/EC]. Additionally, electronic time-stamps issued by a TSP provide evidence that the stamped data existed at a given time.

This Technical Specification contains the same requirements for TWS used by CSPs according to [Dir.1999/93/EC] and for TWS used by TSPs according to [Reg.910/2014/EU]. However, [Reg.910/2014/EU] allows TSPs to manage electronic time-stamps without managing certificates. This is not allowed for CSPs according to [Dir.1999/93/EC]. Therefore, this Technical Specification distinguishes between CSPs and TSPs with respect to the provided services where necessary.

TSPs need to use Trustworthy Systems (TWSs) for securely providing the following services, which are defined in this TS:

a) Registration Service - to verify the identity and, if applicable, any specific attributes of a subject;

b) Certificate Generation Service - to create certificates;

c) Dissemination Service - to provide certificates and policy information to subjects and relying parties;

d) Revocation Management Service - to allow the processing of revocation requests;

e) Revocation Status Service - to provide certificate revocation status information to relying parties;

f) Subject Device Provision Service – to prepare and provide a Signature Creation Device (SCDev) to subjects. This includes Qualifed electronic Signature and Seal Creation Device (QSCD) provision;

g) Time-stamping Service – provides a Time-stamping Service which may be needed for signature verification purposes.

TSP shall follow:

h) "General Security Requirements" specified in 5.2 that are applicable to all previously mentioned services;

i) Security requirements specified in 5.3, 5.4 and 5.5 that are specific to some of the previously mentioned services.

In accordance with Directive1999/93/EC, CSPs need to establish and maintain the first five core services relevant for the issuance and management of qualified certificates (Registration Service, Certificate Generation Service, Dissemination Service, Revocation Management Service, and Revocation Status Service). The other two services (Subject Device Provision Service and Time-stamping Service) are optional ones and are not required to be established and maintained by CSPs, because of having not being specifically addressed in Directive1999/93/EC.

TSPs managing certificates and operating in accordance with Regulation (EU) No 910/2014 [Reg.910/2014/EU] will need to establish and maintain the first five core services relevant for the issuance and management of qualified certificates (Registration Service, Certificate Generation Service, Dissemination Service, Revocation Management Service, and Revocation Status Service). The Subject Device Provision Service is an optional service for such a TSP. TSP managing electronic time-stamps need to establish and maintain the Time-stamping Service relevant for the issuance and management of electronic time-stamps.

TSPs issuing:

j) Certificates according to ETSI/TS 119 411-1 or TS 119 411-2 (or equivalent ENs to be subsequently published) and/or

k) Time-stamps according to ETSI/TS 119 421 (or equivalent EN to be subsequently published)

may use TWSs that have been independently assessed against the relevant security requirements defined in this Technical Specification and declared as being compliant to these requirements. In this case, TSP may reduce their burden to establish conformance of their policy to the relevant standards and in meeting the requirements of Dir.1999/93/EC and/or [Reg.910/2014/EU].

Guidance for conformity assessment to the security requirements defined in this TS can be found in CWA 14172-3.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement 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.

Introduction

The European Directive 1999/93/EC and the Regulation (EU) No 910/2014 [Reg.910/2014/EU] establish a framework of requirements for the use of electronic signatures which are legally equivalent to hand-written signatures. This is the case for “advanced electronic signatures” which are based on a “qualified certificate” and which are created by a “secure-signature-creation device” according to Article 5.1 of 1999/93/EC and qualified signatures according to Article 25.2 of [Reg.910/2014/EU].

In particular, Annex II of Dir. 1999/93/EC and Article 24.2 (e) of [Reg.910/2014/EU] provide the requirements to be followed by TSP when issuing qualified certificates (QCs) and qualified TSP providing qualified trust services. More specifically, they shall

- use trustworthy systems and products which are protected against modification and ensure the technical security of the processes supported by them.

This Technical Specification defines security requirements for TWSs within the scope of the services a TSP needs to provide. It is assumed that TWSs being compliant to relevant security requirements of this TS may be adopted by TSPs to reduce their effort in deploying systems meeting Dir.1999/93/EC and/or [Reg.910/2014/EU]. This approach should support industry in developing systems which meet the requirements laid down in Annex II (f) of Dir.1999/93/EC and in Article 24.2 (e) of [Reg.910/2014/EU].

ETSI TS 119 411-1, 119 411-2, and 119 421 have been taken into account as reference. As a consequence, TWSs already compliant to relevant security requirements of this TS will require minimal configuration by TSPs using them, to meet the security requirements for TWS defined in ETSI TS 119 411-1, 119 411-2, and 119 421 (or equivalent ENs to be subsequently published). In addition, compliant TWS may be used by different TSPs without the need to repeat the conformity assessment.

TWSs for TSPs managing certificates shall comply with the security requirements defined in 5.2 and 5.3 to support TSPs in providing the following core services:

a) Registration of subject information (Registration Service);

b) Certificate generation (Certificate Generation Service);

c) Certificate dissemination (Dissemination Service);

d) Certificate revocation management (Revocation Management Service);

e) Certificate revocation status provision (Revocation Status Service).

TWS for TSPs managing certificates may comply with the other security requirements defined in 5.4 and 5.5 to support TSPs in providing the following supplementary services:

f) SCDev / QSCD production (Subject Device Provision Service);

g) Time-stamping functions (Time-Stamping Service).

TWS for TSPs managing electronic time-stamps shall comply with requirements defined in 5.5 to provide the Time-Stamping Service and may provide the other services, either a) – e) or a) – f) and comply with the corresponding requirements, defined in 5.2 and 5.3 or 5.2, 5.3, and 5.4, respectively.

All security requirements defined in this TS are either:

h) mandatory (indicated by SHALL (NOT) or SHALL (NOT));

i) recommended (indicated by SHOULD (NOT) or (NOT) RECOMMENDED); or

j) optional (MAY or MAY (NOT)).

1 Scope

1.1 General

This Technical Specification establishes security requirements for TWSs that can be used by a TSP in order to issue QCs and Non-Qualified Certificates (NQCs) as well as electronic time-stamps in accordance with Dir.1999/93/EC and with [Reg.910/2014/EU].

Security requirements for the Subject Device Provision Service, which includes SCDev/QSCD provision to subjects, are defined in this TS. However, requirements specific to SCDev/QSCD devices, as used by subjects of the TSP, are outside the scope of this TS. These requirements are defined as Common Criteria [CC] Protection Profiles (PP) in the EN 419211 series.

Recommendations for the cryptographic algorithms to be supported by TWSs are provided in ETSI/TS 119 312.

Although this TS is based on the use of public key cryptography, it does not require or define any particular communication protocol or format for electronic signatures, certificates, certificate revocation lists, certificate status information and time-stamp tokens. It only assumes certain types of information to be present in the certificates in accordance with Annex I of Dir.1999/93/EC and of [Reg.910/2014/EU]. Interoperability between TSP systems and subject systems is outside the scope of this document.

The use of TWSs that are already compliant to relevant security requirements of this TS should support TSPs in reducing their burden to establish conformance of their policy to ETSI TS 119 411-1, 119 411-2, and 119 421 (or equivalent ENs to be subsequently published) and in meeting the Annex I and Annex II requirements of Dir.1999/93/EC as well as the requirements from Annex I and Article 24.2 (e) of [Reg.910/2014/EU].

1.2 European Regulation-specific

The main focus of this document is on the requirements in Article 24.2 (e) of [Reg.910/2014/EU] whilst still facilitating the meeting of requirements in Dir.1999/93/EC, Annex II (f). In considering [Reg.910/2014/EU] it is important to take into account the following requirements of particular relevance to TSP trustworthy systems:

a) Article 24.2 (f) – “use trustworthy systems to store data provided to it, in a verifiable form so that:

   (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,

   (ii) only authorised persons can make entries and changes to the stored data,

   (iii) the data can be checked for authenticity”;

b) Article 24.2 (g) – “take appropriate measures against forgery and theft of data”;

c) Article 24.2 (h) – “record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically”;

d) Article 24.2 (j) – “ensure lawful processing of personal data in accordance with Directive 95/46/EC”;

e) Article 24.2 (k) – “in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database”;

f) Article 24.3 – "If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication";

g) Article 24.4 – "With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient";

h) Article 42.1 – "A qualified electronic time stamp shall meet the following requirements:

   (i) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

   (b) it is based on an accurate time source linked to Coordinated Universal Time; and

   (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method";

i) Annexes I, III, IV – requirements on data in qualified certificates

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*

ETSI TS 119 411-1, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements*

ETSI TS 119 411-2, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy Requirements for trust service providers issuing EU qualified certificates*

ETSI TS 119 421, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing Electronic Time-Stamps*

NOTE Equivalent ENs will be published in 2015.

3 Terms, definitions, symbols and abbreviations

3.1 Terms and definitions

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

3.1.1
activation data
data values, other than keys, that are required to operate cryptographic devices and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share)

[SOURCE: RFC 3647:2014, Clause 2]

3.1.2
advanced electronic signature
electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using means that the signatory can, with a high level of confidence, use under his sole control; and

d) it is linked to the data signed therewith in such a way subsequent change in the data is detectable

[SOURCE: Reg.910/2014/EU]

3.1.3
authentication data
data used to verify the claimed identity of a user requesting services from TWS

3.1.4
certificate
electronic attestation which links signature-validation-data to a person and confirms the name or the pseudonym of that person

[SOURCE: Reg.910/2014/EU]

3.1.5
certificate generation service
service that creates and signs certificates based on the identity and other attributes verified by the registration service

3.1.6
certificate policy
named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

[SOURCE: ISO/IEC 9594-8:2014, 3.5.10 ITU-T X.509; modified — An example in the original definition has not been included here.]

3.1.7
certification authority
CA
authority trusted by one or more users to create and assign certificates and which optionally may create the users’ keys

[SOURCE: ISO/IEC 9594-8:2014, 3.5.16; ITU-T X.509, modified — The definition has been altered.]

3.1.8
certification-service-provider
entity or a legal or natural person who issues certificates or provides other services related to electronic signatures

[SOURCE: Dir.1999/93/EC]

3.1.9
cryptographic device
hardware-based cryptographic device that generates stores and protects cryptographic keys and provides a secure environment for the execution of cryptographic functions

3.1.10
digital signature
data appended to, or a cryptographic transformation (see cryptography) of, a data unit 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: ISO 7498-2:1989, 3.3.26]

3.1.11
dissemination service
service that disseminates certificates to subjects, and if the subject consents, to relying parties and that also disseminates the CA's policy & practice information to subjects and relying parties

3.1.12
electronic seal
data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity

[SOURCE: Reg.910/2014/EU]

3.1.13
electronic signature
data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign

[SOURCE: Reg.910/2014/EU]

3.1.14
electronic signature / seal creation device
configured software or hardware used to create an electronic signature / seal

[SOURCE: Reg.910/2014/EU]

3.1.15
end-entity
certificate subject which uses its private key for purposes other than signing certificates

[SOURCE: ISO/IEC 9594-8:2014, 3.5.26; ITU-T X.509, modified — One out two possible definitions in the original text has been retained here.]

3.1.16
hash function
function which maps string of bits to fixed-length strings of bits, satisfying the following two properties:

a) it is computationally infeasible to find for a given output an input which maps to this output;

b) it is computationally infeasible to find for a given input a second input which maps to the same output.

[SOURCE: ISO/IEC 10118-1:2000, 3.5; modified — A note that was part of the original definition is not kept here.]

3.1.1715
nonce
randomly-generated value used in a communication protocol to ensure old messages cannot be reused in replay attacks

3.1.18
private key
key of an entity's asymmetric key pair which should only be used by that entity

[SOURCE: ISO/IEC 9798-1:2010, 3.22; modified — A small part of the original definition has been cut.]

3.1.19
public key
key of an entity's asymmetric key pair which can be made public

[SOURCE: ISO/IEC 9798-1:2010, 3.25]

3.1.20
qualified certificate
certificate that is issued by a qualified trust service provider and which meets the requirements laid down in Annex I of Reg.910/2014/EU

[SOURCE: Reg.910/2014/EU]

3.1.21
qualified electronic signature
advanced electronic signature that is created by a qualified signature / seal creation device and which is based on a qualified certificate

[SOURCE: Reg.910/2014/EU]

3.1.22
qualified electronic signature / seal creation device
electronic signature creation device that meets the requirements laid down in Annex II of Reg.910/2014/EU

[SOURCE: Reg.910/2014/EU]

3.1.23
registration service
service that verifies the identity and, if applicable, any specific attributes of a subject, and the results of which are passed to the Certificate Generation Service

3.1.24
relying party
user or agent that relies on the data in a certificate in making decisions

[SOURCE: RFC 5280:2008]

3.1.25
revocation management service
service that processes requests and reports relating to revocation to determine the necessary action to be taken, and the results of which are distributed through the Revocation Status Service

3.1.26
revocation status service
service that provides certificate revocation status information to relying parties and that may be a real-time service or may be based on revocation status information which is updated at regular intervals

3.1.27
secure-signature-creation device
signature-creation device which meets the requirements laid down in Annex III of Dir.1999/93/EC

[SOURCE: Dir.1999/93/EC]

3.1.28
security perimeter
one or more areas that are not necessarily co-located, where TWS are sited with relevant ancillary equipment (power supply, air conditioning, access control system, intrusion alarm system, fire protection and prevention system)

3.1.29
security policy
set of rules laid down by the security authority governing the use and provision of security services and facilities

[SOURCE: ISO/IEC 9594-8:2014, 3.5.60; ITU-T X.509]

3.1.30
self-signed certificate
certificate for one CA signed by that CA

[SOURCE: RFC 5280:2008]

3.1.31
signatory
person who creates an electronic signature

Note 1 to entry: The term signer is sometimes used as a synonym.

[SOURCE: Reg.910/2014/EU]

3.1.32
signature-creation data
unique data which is used by the signatory to create an electronic signature

[SOURCE: Dir.1999/93/EC and Reg.910/2014/EU]

3.1.33
signature-creation device
configured software or hardware used to create an electronic signature

[SOURCE: Reg.910/2014/EU]

3.1.34
subject
entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

3.1.35
subject device provision service
service that prepares and provides a Signature Creation Device to subjects

3.1.36
trustworthy system
information system or product implemented as either hardware and/or software that produces reliable and authentic records which are protected against modification and additionally ensures the technical and cryptographic security of the processes supported by it

3.1.37
time-stamp token
data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time