SLOVENSKI STANDARD
SIST-TP CEN/TR 419210:2019

01-maj-2019

Uporabnost standardov CEN za kvalificirano elektronsko napravo za ustvarjanje pečata v skladu z Uredbo EU št. 910/2014 (eIDAS)

Applicability of CEN Standards to Qualified Electronic Seal Creation Device under the EU Regulation N°910/2014 (eIDAS)

Anwendbarkeit von CEN Normen für qualifizierte elektronische Siegelerstellungseinheiten unter der eIDAS Verordnung.

Applicabilité des normes CEN aux dispositifs de création de cachet électronique qualifiés sous la régulation européenne n°910/2014 (eIDAS)

Ta slovenski standard je istoveten z: **CEN/TR 419210:2019**

ICS:

35.030	Informacijska varnost	IT Security
35.240.63	Uporabniške rešitve IT v trgovini	IT applications in trade

SIST-TP CEN/TR 419210:2019 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 419210

March 2019

ICS 35.030; 35.240.63

English Version

Applicability of CEN Standards to Qualified Electronic Seal Creation Device under the EU Regulation N°910/2014 (eIDAS)

Application des normes du CEN aux dispositifs de création de cachets électroniques qualifiés au titre du règlement européen n°910/2014 (eIDAS)

Anwendbarkeit von CEN Normen für qualifizierte elektronische Siegelerstellungseinheiten unter der Verordnung (EU) Nr. 910/2014 (eIDAS)

This Technical Report was approved by CEN on 18 February 2019. It has been drawn up by the Technical Committee CEN/TC 224.

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. CEN/TR 419210:2019 E

Contents

European foreword

This document (CEN/TR 419210:2019) 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.

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.

Introduction

EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (also known as eIDAS)[1] builds on the concept and requirements defined in the repealed EU Directive 1999/93 on Electronic Signatures [2]. eIDAS defines an electronic seal which authenticates the origin of data but created under control, as opposed to "sole control" for electronic signatures, of a legal person (e.g.. organization), as opposed to natural person (i.e. individual). Technically, electronic seals have similar requirements as electronic signatures and both can be based on digital signatures. eIDAS recognizes a special level of qualified electronic seal which is created using a qualified seal creation device (QSealCD) and supported by a qualified certificate, in the similar way as a qualified electronic signature is created using qualified signature creation device (QSigCD) supported by a qualified certificate. The requirements for a qualified seal creation device are described as "mutatis mutandis" as for a qualified signature creation device. The requirements for a qualified signature creation device are considered to be met by the equivalent defined in Directive 1999/93 referred to as a secure signature creation device (SSCD).

CEN has issued standards EN 419 211 parts 1 to 6, which were initially aimed at SSCD but have been accepted as applicable to QSigCD and QSealCD (COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016). Further standards have since been issued EN 419 221 part 5 and EN 419 241 parts 1 and 2 which can also be applied as QSigCD and QSealCD. However, for some use cases of electronic seals some standards may be considered more appropriate than others.

This document considers the legal requirements and practical use cases against the features of the standards to assist in selecting the most appropriate standard.

1 Scope

This document considers the legal requirements and practical use cases against the features of the CEN standards which may be used to support electronic seals in accordance to EU Regulation N° 910/2014 with the aim to provide guidance on the most appropriate standard to use in particular types of usage.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EU Regulation N° 910/2014 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 The term "seal" is used to denote "electronic seal", and "signature" is used to denote "electronic signature".

3.1.1
digital signature
data appended to, or a cryptographic transformation 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)

Note 1 to entry: Digital signature is a technical concept which may be related to the legal concept of electronic signature or electronic seal as defined in EU Regulation N° 910/2014.

3.1.2
signer
entity being the creator of a digital signature

Note 1 to entry: Signer is a technical concept which may be related to the legal concepts of signatory or creator of a seal.

3.2 Abbreviations

DTBS	Data To Be Signed
DTBS/R	Data to be signed or its unique representation
eIDAS	EU Regulation N° 910/2014 [1]
SSCD	secure signature creation device
TSP	trust service provider
QSealCD	qualified seal creation device
QSigCD	qualified signature creation device
QSCD	Either QSealCD or QSigCD
QTSP	qualified trust service provider

4 A consideration of relevant regulatory requirements

The following recitals and articles of eIDAS are considered to have impact on the requirements for electronic seals, which may or may not be supported by a QSealCD, in particular where they differ from electronic signatures. Those items considered most relevant are underlined.

Recital (51) It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device.

Recital (52) The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply.

Recital (59) Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity.

Recital (65) In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers.

Article 3. (25) 'electronic seal' means 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;

Article 3.((31) 'electronic seal creation device' means configured software or hardware used to create an electronic seal;

Article 3.(32) 'qualified electronic seal creation device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II

Article 35.2 A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

Article 36 Requirements for advanced electronic seals *[compared with advanced electronic signatures].*

An advanced electronic seal shall meet the following requirements:

(a) it is uniquely linked to the creator of the seal; *[same as electronic signature.]*

(b) it is capable of identifying the creator of the seal*; [same as electronic signature.]*

(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and *[electronic signature requires "sole control"]*

(d) it is linked to the data to which it relates in such a way that any subsequent change in the data are detectable. *[electronic signature "linked to data signed therewith" which it is understood has the same technical implications.]*

Article 39 references Article 29, 30, 31 "mutatis mutandis";

Annex II Requirements For Qualified Electronic Signature Creation Devices:

1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:

    (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably ensured;

    (b) the electronic signature creation data used for electronic signature creation can practically occur only once;

    (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;

    (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.

2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.

3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.

4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:

    (a) the security of the duplicated data sets must be at the same level as for the original data sets;

    (b) the number of duplicated data sets shall not exceed the minimum needed to ensure continuity of the service.

The following qualified trust services identified in the Regulation require the use of advanced electronic seal or signature created by the qualified trust service provider:

- Article 33: Qualified validation service
- Article 42: time-stamp
- Article 44: registered delivery services
- Annex I: Certificate for electronic signature
- Annex III: Certificate for electronic seal
- Annex IV: Certificate for website authentication

In addition to these recitals, articles and Annex II requirements, the following relating directly to qualified electronic signatures and indirectly (mutatis mutandis) to qualified electronic seals can have impact on the technical requirements of QSealCD:

Article 26: An advanced electronic signature shall meet the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data 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 that any subsequent change in the data are detectable.

Article 30: Certification of qualified electronic signature creation devices

1. Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States. EN 28.8.2014 Official Journal of the European Union L 257/101

2. Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.

3. The certification referred to in paragraph 1 shall be based on one of the following:

(a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or

(b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.

The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article..

The following point is considered of particular significance in considering the differences in requirements between devices supporting signatures and seals in eIDAS:

Signatures require “sole control” whereas seals require “control” which implies differences in the form of control over the signing key, and in particular whether this has to be under the control of just one individual natural person or, in the case of a seal, may be under control of an organisational entity (see particularly 36 c highlighted above).

5 Features commonly required by use cases

5.1 Introduction

This clause identifies features commonly required by use cases employing seals such as identified in Annex A.

5.2 Features

5.2.1 Local / Remote

The QSealCD is either:

a) *Local*: Under direct control of the signer, or

b) *Remote*: Managed by a QTSP

5.2.2 Authentication Shared / Not Shared

The authentication data used to authorize use of a signing key protected by a QSealCD is under control of:

a) *Not shared*: An authorized individual person (or authorized application), or

b) *Shared*: A set of individuals (or authorized applications) applying organisational controls to restrict availability to authorized individuals.

5.2.3 Multiple Digital Signatures

A person or application(s) is authorized to use a signing key protected by a QSealCD to create:

a) *Single*: A single digital signature against a single data object or its representation (DTBS/R)

b) *Multiple Set*: Multiple digital signatures against a defined set of DTBS/R

c) *Multiple Limited*: A set of digital signatures against a set of DTBS/R limited by time or other usage parameter

d) *Multiple unlimited*: An unlimited set of digital signatures against a undefined set of DTBS/R

5.2.4 Key Shared / Not Shared

The key used to create a digital signature is under control of:

a) *Not Shared*: Single person representing a legal person (or authorized application), with other persons (or authorized applications) representing the same legal person having a different key.

b) *Shared*: Multiple persons (or authorized applications) who all represent the same legal person and share the same key .

5.2.5 Secure Environment

The security of the environment where the QSCD is managed:

a) *No Sec Requirement*: No specific requirements on environment security,

b) *Secured*: The QSealCD is used in a secure environment with physical access and use of the device is restricted to persons and applications trusted to act for the legal person.

c) *TSP*: The QSealCD is operated by an audited TSP (i.e. Qualified TSP).