SLOVENSKI STANDARD
SIST-TP CEN/TR 419040:2018

01-september-2018

Racionalizirana struktura za standardiziran elektronski podpis - Smernice za državljane

Rationalized structure for electronic signature standardization - Guidelines for citizens

Cadre pour la normalisation de la signature électronique - Lignes directrices pour les citoyens

Ta slovenski standard je istoveten z: CEN/TR 419040:2018

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST-TP CEN/TR 419040:2018 en,fr,de

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 419040

May 2018

ICS 35.030

English Version

Rationalized structure for electronic signature standardization - Guidelines for citizens

Cadre pour la normalisation de la signature électronique - Lignes directrices pour les citoyens

This Technical Report was approved by CEN on 9 March 2018. 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 419040:2018 E

Contents Page

European foreword

This document (CEN/TR 419040:2018) has been prepared by Technical Committee CEN/TC 224 “Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”, 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

Today, it is possible to electronically sign data to achieve the same effects as when using a hand-written signature. Such electronic signatures benefit from full legal recognition due to the EU Regulation N° 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [1] (hereafter referred to as EU Regulation N° 910/2014) which addresses various services that can be used to support different types of electronic transactions and electronic signature in particular.

The use of secure electronic signatures should help the development of online businesses and services in Europe. The European Commission standards initiative aims at answering immediate market needs by:

— securing online transactions and services in Europe in many sectors: e-business, e-administration, e-banking, online games, e-services, online contract, etc.;

— contributing to a single digital market;

— creating the conditions for achieving the interoperability of e-signatures at a European level.

Besides the legal framework, the technical framework at the present time is very mature. Citizens routinely sign data electronically by using cryptographic mechanisms such as, e.g. when they use a credit card or debit card to make a payment. Electronic signatures implemented by such cryptographic mechanisms are called “digital signatures”. Appropriate technical methods for digital signature creation, validation and preservation, as well as ancillary tools and services provided by trust service providers (TSPs), are specified in a series of documents developed along with the present document.

The present document is part of a rationalized framework of standards (see ETSI TR 119 000 [6]) realized under the Standardization Mandate 460 issued by the European Commission to CEN, CENELEC and ETSI for updating the existing standardization deliverables.

In this framework, CEN is in charge of issuing Guidelines for electronic signatures implementation. These guidelines are provided through two documents:

— CEN/TR 419030, “Rationalized structure for electronic signature standardization - Best practices for SMEs”, aligned with standards developed under the Rationalised Framework as described by ETSI SR 001 604, and

— CEN/TR 419040, “Rationalized structure for electronic signature standardization - Guidelines for citizens”, explaining the concept and use of electronic signatures.

These two documents differ slightly from the other documents in the Technical Framework since they go beyond the technical concept of “digital signature” and deal also with the legal concepts of electronic signatures and electronic seals. The concept of electronic seal specified in the Regulation, which is technically close to the electronic signature, is developed in CEN/TR 419030 and not in the present document as it relates to legal person and not to natural persons as are the citizens The present document concerning the citizens is focusing on electronic signature that are created by natural persons.

1 Scope

This Technical Report aims to help citizens to understand the relevance of using electronic signature within their day-to-day lives. It also explains the legal and the technical backgrounds of electronic signatures.

This document gives guidance on the use of electronic signatures and addresses typical practical questions the citizen may have on how to proceed to electronically sign, where to find the suitable applications and material.

2 Normative references

There are no normative references in this document.

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
advanced electronic signature
electronic signature which meets the requirements set out in Article 26 of Regulation (EU) N° 910/2014 [1]

Note 1 to entry: 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/her 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.

[SOURCE: Regulation (EU) N° 910/2014 [1], Article 3 (11)]

3.2
electronic signature (from the regulation)
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: Regulation (EU) N° 910/2014 [1], Article 3 (10)]

3.3
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/IEC 7498 / ITU-T/Recommendation X.800]

3.4
trust service provider
natural or legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider

[SOURCE: Regulation (EU) N° 910/2014 [1], Article 3 (19)]

3.5
trust service
electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication, or

(c) the preservation of electronic signatures, seals or certificates related to those services

[SOURCE: Regulation (EU) N° 910/2014 [1], Article 3 (16)]

Note 1 to entry: The concept of electronic seal specified in the Regulation is not developed in the present document as it relates to legal person and not to natural person as are the citizens. More details can be found in the companion document CEN/TR 419030.

3.6
qualified trust service
trust service that meets the applicable requirements laid down in this Regulation

[SOURCE: Regulation (EU) N° 910/2014 [1], Article 3 (17)]

3.7
qualified trust service provider
trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body

[SOURCE: Regulation (EU) N° 910/2014 [1], Article 3 (20)]

3.8
signature creation device
configured software or hardware used to create an electronic signature

[SOURCE: Regulation (EU) N° 910/2014 [1], Article 3 (22)]

3.9
qualified electronic signature
advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures

[SOURCE: Regulation (EU) N° 910/2014 [1], Article 3 (12)]

3.10
certificate for electronic signature
electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person

[SOURCE: Regulation (EU) N° 910/2014 [1], Article 3 (14)]

3.11
signatory
natural person who creates an electronic signature

[SOURCE: Regulation (EU) N° 910/2014 [1] Article 3 (9)]

3.12
certificate
public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it

Note 1 to entry: The term certificate is used for public key certificate within the present document.

[SOURCE: ISO/IEC 9594-8 / ITU-T Recommendation X.509]

3.13
entity authentication
means the corroboration of the claimed identity of an entity and a set of its observed attributes

[SOURCE: Modinis Study on Identity Management in eGovernment – Common terminological framework for interoperable electronic identity management, v2.01, November 23, 2005.]

3.14
data authentication
means the corroboration that the origin and the integrity of data are as claimed

[SOURCE: Modinis Study on Identity Management in eGovernment – Common terminological framework for interoperable electronic identity management, v2.01, November 23, 2005.]

3.15
data authentication data
means data in electronic form which are attached to or logically associated with other electronic data and which corroborates the identity of the entity at the origin of the associated data and the integrity of the associated data.

[SOURCE: Feasibility study on an electronic identification, authentication and signature policy (IAS) carried out for the European Commission by DLA Piper, SEALED, time.lex, Price Waterhouse Coopers and Studio Genghini & Associati, 2013]

4 Abbreviations

For the purposes of this document, the following abbreviations apply.

AdESig_QC	An advanced electronic signature / seal as defined in the Regulation supported by a QC
AdESig	advanced electronic signature as defined in the Regulation [1]
CA	Certification Authority
CRL	Certificate Revocation List
CSP	Certification Service Provider
DA	Driving Application
EC	European Commission

EU	European Union
ISO	International Organization for Standardization
LoA	Level of Assurance
OCSP	Online Certificate Status Protocol
PDF	Portable Document Format
PIN	Personal Identification Number
PK	Public Key
PKI	Public Key Infrastructure
QC	Qualified Certificate
QES	qualified electronic signature
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service(s) Provider
RA	Registration Authority
SCA	Signature Creation Application
SCD	Signature Creation data
SCDev	Signature Creation Device
SVA	Signature Validation Application
TSA	Time-Stamping Authority
TSP	Trust Service(s) Provider

5 What are (legally valid) electronic signatures?

5.1 Electronic signatures defined by the EU Regulation N° 910/2014

The Regulation (EU) N° 910/2014 defines electronic signature as "*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*". Electronic signatures are created by an electronic '**signature creation device**', which is "*a configured software or hardware used to create an electronic signature and by means of an* '**electronic signature creation data**' (i.e. *"a unique data which is used by the signatory to create an electronic signature")*".

Electronic signatures shall not be denied legal effect and admissibility as evidence in legal proceedings.

Within the electronic signature family, the Regulation (EU) N° 910/2014 defines subsets of electronic signature that provide a greater legal predictability up to a level that benefit from the legal equivalence to handwritten signatures:

- the **advanced electronic signature (AdESig)** – which requires some security features such as defined in Clause 3;

- the **qualified electronic signature (QES)** – which is an advanced electronic signature which provides additional level of assurance on the identity of the signatory and an enhanced protection and level of assurance on the signature creation. A special device is required for the creation of QES (a Qualified Signature Creation Device, QSCD). **A QES shall have the equivalent legal effect of a handwritten signature and shall be recognized as a qualified electronic signature in all European Member States.** Besides the fact that a QES is equivalent to a handwritten signature, it also benefits from legal protection with regard to acceptation; anyone who receives such a signature has to accept it. Also, in the case of litigation with the service providers supporting the QES ancillary services, it is not up to the person claiming the damage to support the burden of proof, but well up to the Qualified Service Provider to prove that it has not acted negligently.

NOTE The Regulation also defines an intermediary level, the AdESig_QC, that has the same legal value as the AdESig but brings more assurance on the identity of the signatory. This will be discussed later on in the present document.

5.2 The underlying technology – Public key cryptography and digital signatures

5.2.1 Introduction

Asymmetric cryptography is a technology that enables the creation of **digital signatures** (the technical concept defined by ISO, see Clause 3).

As demonstrated in the next subclause, digital signature is a technique that allows the legal requirements for the 3 levels of electronic signature defined in the Regulation (EU) N° 910/2014 (i.e. simple, advanced and qualified signatures) to be met. In the current state of the art, QES are only possible with such technologies.

NOTE 1 In the present document, the terms “electronic signature” refer to the legal concept while the terms “digital signature” refer to the PKI based underlying technology.

NOTE 2 The terms signer or signatory can be used to refer to the person that creates a digital signature. The European Regulation uses the term signatory. It is limited to natural person creating electronic signatures (see below). The present document uses the term signatory to refer to electronic signatures such as addressed by the European regulation, and the more generic term signer for any context.

5.2.2 How it works

Each signer owns a key pair made of a private and a public key (the asymmetric cryptography technology is also often referred to as “Public Key cryptography”):

— The private key is a secret code used by a mathematical function in order to render data unintelligible (i.e. encrypt data).

— The public key is a public code used by the reverse mathematical function in order to retrieve the initial data from the encrypted data.

If we schematize the private key by ‘*1100101*’ and the encryption function by 🔒, and the public key by ‘*0100001*’ and the decryption function by 🔑 we can illustrate the digital signature process as follows (the actual protocol is slightly more complicated, the schematization