SLOVENSKI STANDARD
SIST-TP CEN/TR 419030:2018

01-september-2018

Racionalizirana struktura za standardiziran elektronski podpis - Dobre prakse za MSP

Rationalized structure for electronic signature standardization - Best practices for SMEs

Cadre pour la normalisation de la signature électronique - Meilleures pratiques pour les PME

Ta slovenski standard je istoveten z: CEN/TR 419030:2018

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST-TP CEN/TR 419030:2018 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 419030

May 2018

ICS 35.030

English Version

Rationalized structure for electronic signature standardization - Best practices for SMEs

Cadre pour la normalisation de la signature électronique - Meilleures pratiques pour les PME

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 419030:2018 E

Contents

Page

European foreword ... 3
Introduction ... 4
1 Scope ... 5
2 Terms and definitions ... 5
3 Abbreviations ... 7
4 Electronic seals as per EU Regulation 910/2014 ... 9
5 SME's perspective ... 10
5.1 Reasons for signing or sealing ... 10
5.1.1 General ... 10
5.1.2 Electronic signing as a way to confirm a legal commitment or because of a legal requirement ... 11
5.1.3 Electronic signing as a matter of diligence / risk management ... 12
5.1.4 Electronic seals as a way to comply with an explicit legal requirement to apply a seal, stamp or comparable formal requirement ... 13
5.1.5 Electronic seals as a way to ensure the integrity and authenticity of a document ... 13
5.2 Who signs or seals? ... 13
6 Solutions ... 14
6.1 General ... 14
6.2 Signature creation ... 14
6.2.1 General ... 14
6.2.2 Remotely managed signature creation application and signature creation device ... 16
6.2.3 Remotely managed signature creation device ... 17
6.2.4 Remotely managed signature creation ... 17
6.2.5 Signature creation application and signature creation device in the hand of the signatory ... 18
6.2.6 Responsibilities of parties ... 19
6.2.7 Level of security and assurance on the issued signatures ... 20
6.3 Signature validation ... 21
6.4 Signature preservation ... 21
7 I'm a TSP? ... 22
8 Use-cases ... 23
8.1 Use-cases where the SME is signing ... 23
8.1.1 eInvoicing ... 23
8.1.2 eProcurement Directive ... 23
8.1.3 Accessing markets across the EU and the impact of the Services Directive ... 24
8.2 Use-cases where the SME and the SME's customers / partners are co-signing or co-sealing ... 25
9 Annex Digital signatures standardization ... 26
Bibliography ... 30

European foreword

This document (CEN/TR 419030:2018) 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 Regulation (EU) N° 910/2014) which addresses various services that can be used to support different types of electronic transactions and electronic signatures 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 electronic 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 document 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.

Further support is provided to the emerging cross-border use of eSignatures through other legal and policy instruments that affect electronic processes being used in the market today (e.g. eInvoicing Directive [3], Public Procurement Directive [4] and Services Directive [5]).

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.

The present document builds on CEN/TR 419040.

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.

1 Scope

This Technical Report aims to be the entry point in relation to electronic signatures for any SME that is considering to dematerialize paper-based workflow(s) and seeks a sound legal and technical basis in order to integrate electronic signatures or electronic seals in this process. It is not intended to be a guide for SMEs active in the development of electronic signatures products and services - they should rather rely on the series ETSI EN 319 for building their offer - but it is a guide for SMEs CONSUMING e-Signature products and services.

This document builds on CEN/TR 419040, "Guidelines for citizens", explaining the concept and use of electronic signatures, to further help SMEs to understand the relevance of using e-Signatures within their business processes. It guides SMEs in discovering the level of electronic Signatures which is appropriate for their needs, extends the work to specific use-case scenarios, paying special attention to technologies and solutions, and addresses other typical concrete questions that SMEs need to answer before any making any decisions (such as the question of recognition of their e-Signature by third parties, within their sector, country or even internationally).

Once the decision is taken to deploy electronic signatures or electronic seals in support of their business, SMEs will then typically collaborate with their chosen providers of e electronic signatures or electronic seals products or services, which can be done on the basis of ETSI TR 119 100 "Guidance on the use of standards for signature creation and validation", that helps enterprises fulfil their business requirements. The present document presents the concepts and use of the standards relevant for SMEs developed under the Rationalised Framework to SMEs.

2 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

2.1
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 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)]

2.2
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)]

2.3
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 [i.x]]

2.4
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)]

2.5
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)]

2.6
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)]

2.7
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)]

2.8
signature creation device
configured software or hardware used to create an electronic signature

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

2.9
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)]

2.10
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)]

2.11
signatory
natural person who creates an electronic signature

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

2.12
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]

2.13
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.]

2.14
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.]

2.15
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]

3 Abbreviations

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

AdESig/AdESeal QC	An AdESig/AdESeal supported by a QC

AdESig/AdESeal	advanced electronic signature / seal as defined in the Regulation (EU) N° 910/2014 [1]
CA	Certification Authority
CAdES	CMS Advanced Electronic Signatures
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
CSP	Certification Service Provider
DA	Driving Application
DTBS	Data To Be Signed
EU	European Union
HSM	Hardware Security Module
ISO	International Organization for Standardization
LoA	Level of Assurance
LT	Long Term
LTA	Long Term Archive Validation Data
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PAdES	PDF Advanced Electronic Signatures
PDF	Portable Document Format
PIN	Personal Identification Number
PK	Public Key
PKI	Public Key Infrastructure
QC	Qualified Certificate
QES	qualified electronic signature or seal
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
SME	Small and medium size enterprise
SVA	Signature Validation Application
TSA	Time-Stamping Authority
TSP	Trust Service(s) Provider
VAT	Value Added Tax
XAdES	XML Advanced Electronic Signatures

4 Electronic seals as per Regulation (EU) N° 910/2014

The concepts relating to electronic signature and its legal validity are presented in CEN/TR 419040, "Guidelines for citizens". In addition, in the framework of SMEs it is important to introduce a companion concept, the electronic seal, which is defined by the Regulation as "*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*".

The electronic seal can be seen as the equivalent to a stamp on a paper document, i.e. attributed to a legal entity (such as a company or public administration) but not necessarily to an identified natural person (i.e. it is not necessarily possible to identify a specific person who applied the seal).

There are two major differences between an electronic seal and an electronic signature:

— the nature of the creator, which must be a legal person for an electronic seal and a natural person for an electronic signature; and

— the intended legal effect, which is the presumption of integrity of the data and of correctness of the origin of that data to which the seal is linked for the seal, and the equivalence to a handwritten signature for the electronic signature.

It shall also be noted that no pseudonym is allowed for an electronic seal certificate, while pseudonyms are allowed for electronic signature certificates.

However, the two concepts are similar conceptually and also technically:

— the definitions of advanced electronic seal and advanced electronic signature (AdESig/AdESealig and AdESig/AdESealeal) are quasi identical. A small difference is the requirement on the control of the electronic signature creation data that must be under the sole control of the signatory for the seal and under control of the creator of the seal for the seal. This is to reflect the fact that a seal belongs

to a legal person and contrarily to a natural person, the legal person can frequently be represented / controlled by more than one person.

— the definitions of validation and validation data are the same.

— the QSCD, qualified electronic seal creation device, is required to meet mutatis mutandis the Annex II requirements for qualified electronic signature creation device.

Technically speaking, the same technology will support equally (advanced) electronic seals and (advanced) electronic signatures. In particular, PKI such as presented in CEN/TR 419040, is well suited for AdESig/AdESeal.

For SMEs, electronic seals can be particularly important. Signatures are used by natural persons with the intent to sign, i.e. they are conceptually closely linked to the concept of hand written signatures. **It is nevertheless still possible to issue a signature that contains also the name of the organization the signatory is associated with or the signatory's quality or function in the organization.** This would be similar to the current practice of applying a hand written signature on a paper document and mentioning the signatory's name and title within a company: the signature in this case affirms the involvement of the specific natural person, but also emphasizes their role within the company.

NOTE The Regulation Recital 58 states "When a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable". It means that, according to national legislation and / or for backward compliance or any other reasons, it is still possible for a natural person who is entitled to represent a legal person (such as a CEO) to sign a data rather than sealing it, provided there is an entitled natural person to do so.

Electronic seals on the other hand are defined in the Regulation as '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'. In other words, they **do not contain an intent to sign**, but only an intent to ensure the origin and integrity. Seals emanate from legal entities, not natural persons. This makes them very useful for administrative processes where the responsible organization is relevant, but not necessarily the identity of the person (e.g. employee) involved (if there is any human intervention to begin with). **It is nevertheless still possible to issue a seal that contains the name of the person that has affixed it on behalf of the organization, for information.** This would be similar to the current practice of applying a stamp that identifies an organization and the person in charge of that organization (e.g. 'John Johnson - Secretary of company X'): the stamp in this case affirms the legal person from which the document emanates, but also stresses the involvement of the specific natural person who is in control of the issuance of such documents.

Finally, like for electronic signatures, the regulation distinguished between **basic**, **advanced** and **qualified** electronic seals. Here too, the distinction is intended to reflect the trustworthiness, level of assurance and legal reliability of the solution being used.

5 SME's perspective

5.1 Reasons for signing or sealing

5.1.1 General

The first most important step for a SME that intends to use electronic seals or signatures is to assess the business cases for signatures or seals, i.e. determining which documents will be sealed or signed (or even both), and why. There are different reasons that an SME might have for signing or sealing, which will impact their choice of technology. The paragraphs hereunder present a broad overview of potential reasons and the implications.