

TNI	Racionalizovaná štruktúra na štandardizáciu elektronického podpisu Usmernenia pre občanov	TNI CEN/TR 419040 36 9743
------------	--	---

Rationalized structure for electronic signature standardization - Guidelines for citizens

Táto technická normalizačná informácia obsahuje anglickú verziu CEN/TR 419040:2018.
This Technical standard information includes the English version of CEN/TR 419040:2018.

Táto technická normalizačná informácia bola oznámená vo Vestníku ÚNMS SR č. 10/18

127427

TECHNICAL REPORT**CEN/TR 419040****RAPPORT TECHNIQUE****TECHNISCHER BERICHT**

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

CEN/TR 419040:2018 (E)

Contents	Page
European foreword.....	4
Introduction	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	6
4 Abbreviations	8
5 What are (legally valid) electronic signatures?	9
5.1 Electronic signatures defined by the EU Regulation N° 910/2014	9
5.2 The underlying technology – Public key cryptography and digital signatures	10
5.2.1 Introduction	10
5.2.2 How it works	10
5.2.3 Ensuring trust.....	12
5.2.4 Functionalities offered by PKI based technologies: data integrity and authentication of origin.....	13
5.3 Where technical tools meet legal requirements.....	13
5.3.1 Introduction	13
5.3.2 Mapping the legal and the technical concepts	14
5.3.3 How digital signatures cover the legal requirements for AdESig.....	16
5.3.4 How digital signatures cover the legal requirements for QES.....	18
5.4 Other use-cases for digital signatures	19
6 Digital signatures– how does it work in real life applications?.....	19
6.1 The signature process	19
6.2 Creation	19
6.3 Validation.....	21
6.4 Augmentation	23
7 Digital signatures ancillary services and tools for use in practice.....	23
7.1 Introduction	23
7.2 Identifying the required level of signature.....	24
7.2.1 General.....	24
7.2.2 Use-cases for QES.....	24
7.2.3 Use-cases for non QES.....	24
7.3 Identifying required tools and services	25
7.3.1 Creation	25
7.3.2 Augmentation – when the signature needs to be preserved	26
7.3.3 Validation.....	26
7.3.4 Preservation.....	26
8 In case of dispute: evidence and proofs	27
8.1 General.....	27
8.2 Evidence present in the signed data.....	27
8.3 Evidence generally present in the certificate	28
8.4 Evidence present in the CA’s documentation.....	29
8.5 Evidence regarding Certificate Status	29
8.6 Evidence present in the Signature Policy	29
8.7 Evidence at the Registration Authority	30
8.8 Evidence not available through the signed message.....	31
9 What about the (international) recognition of electronic signatures?	31

9.1	Within Europe	31
9.2	Outside Europe	31
	Bibliography	33

CEN/TR 419040:2018 (E)**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.

CEN/TR 419040:2018 (E)**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.

koniec náhľadu – text ďalej pokračuje v platenej verzii STN