

ICS 35.030; 35.240.30

English Version

Guidance for signature creation and other related devices

Lignes directrices pour la création de signatures et
autres dispositifs associés

Anleitung zur Signaturerstellung und andere ähnliche
Geräte

This Technical Report was approved by CEN on 17 April 2017. 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: Avenue Marnix 17, B-1000 Brussels

Contents

Page

European foreword.....	4
Introduction	5
1 Scope.....	6
2 Terms and definitions	6
3 Symbols and abbreviations	7
4 Some concepts related to signature creation and other related devices.....	8
4.1 Different types of signatures and seals	8
4.2 Signature versus seal	8
4.3 What are a signature creation device or other related devices	8
4.3.1 General.....	8
4.3.2 Qualified electronic signature creation device	8
4.3.3 Qualified electronic seal creation device	10
4.4 Trusted versus un-trusted environment for electronic signature.....	10
4.5 Mobile environment.....	11
5 Types of services related to signature – Scoping factors	11
5.1 General.....	11
5.2 Services related to signature for a QSCD	12
5.2.1 General.....	12
5.2.2 Signature service.....	12
5.2.3 Privacy aspects.....	12
5.2.4 Identification service	14
5.2.5 Authentication service	14
5.2.6 Other potential services	14
5.3 Services related to signature for a TSP.....	16
5.3.1 General.....	16
5.3.2 Signature service.....	16
5.3.3 Certification Authority service.....	17
5.3.4 Other services.....	17
6 Selecting the Most Appropriate Standards and options	17
6.1 Sub-Areas of Standardization	17
6.1.1 General.....	17
6.1.2 Policy and security Requirements	18
6.1.3 Technical Specifications	20
6.1.4 Conformity Assessment	20
6.1.5 Interoperability Testing	20
6.2 Selection of standards	21
Annex A (informative) Business aspects/ Use cases from signature creation devices view	22
A.1 General.....	22
A.2 Telecommunications	22
A.3 Identity.....	22
A.4 Health	23
A.5 Corporate	23
A.6 Bank	24

Annex B (informative) Illustration of Application of Standards.....	25
B.1 General	25
B.2 Telecommunications.....	25
B.2.1 First example.....	25
B.2.2 Second example.....	25
B.3 Identity	25
B.3.1 General	25
B.3.2 First example.....	26
B.3.3 Second example.....	26
B.3.4 Third example.....	27
B.4 Health.....	27
B.4.1 First example.....	27
B.4.2 Second example.....	28
B.5 Corporate.....	28
B.5.1 First example.....	28
B.5.2 Second example.....	28
B.6 Bank.....	28
B.6.1 First example.....	28
B.6.2 Second example.....	29
Annex C (informative) Comparison of definitions between Directive 1999/93/EC and Regulation (EU) 910/2014.....	30
Bibliography	32

European foreword

This document (CEN/TR 419200:2017) 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 [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

Introduction

ETSI/TR 119 000 [16] provides a general structure for electronic signatures standardization outlining existing and potential standards for electronic signatures. This identifies six areas of standardization with a list of existing and potential future standards in each area.

This guide is part of a series of guidance documents assisting users and their suppliers in identifying the electronic signature standards and options relevant to their need. Each guide addresses a particular area as identified in ETSI/TR 119 000 [16].

This series is based on the process of selecting Business Scoping Parameters for each area of standardization based on an analysis of the business requirements. The selection of these scoping parameters is based on a process involving an analysis of the business requirements and associated risks leading to an identification of the policy and security requirements and the resulting Business Scoping Parameters from which the appropriate standards and options can be selected. Having identified the requirements in terms of Business Scoping Parameters for an area, each guidance document provides assistance in selecting the appropriate standards and options for that area. Where standards and options within one area make use of another area this is stated in terms of Scoping Parameters of that other area.

This guidance does not include any normative requirements but provides guidance on addressing the signature creation and other related devices area, on the selection of applicable standards and their options for a particular business implementation context and associated business requirements and on the implementation of a standard (or a series of standards).

This area covers signature devices but also electronic signature-related devices including (not exhaustively) authentication devices, identity devices offering value added services around electronic signatures. This list can be extended as further services that could be listed for devices are identified.

This general process of the selection of standards and options is described further in ETSI/TR 119 000:2015, 4.2.6 [16].

1 Scope

The Technical Report provides guidance on the selection of standards and options for the signature/seal creation and other related devices (area 2) as identified in the framework for standardization of signatures: overview ETSI/TR 119 000 [16].

The Technical Report describes the Business Scoping Parameters relevant to this area (see Clause 5) and how the relevant standards and options for this area can be identified given the Business Scoping Parameters (Clause 6).

The target audience of this document includes:

- business managers who potentially require support from electronic signatures/seals in their business and will find here an explanation of how electronic signatures/seals standards can be used to meet their business needs;
- application architects who will find here material that will guide them throughout the process of designing a system that fully and properly satisfies all the business and legal/regulatory requirements specific to electronic signatures/seals, and will gain a better understanding on how to select the appropriate standards to be implemented and/or used;
- developers of the systems who will find in this document an understanding of the reasons that lead the systems to be designed as they were, as well as a proper knowledge of the standards that exist in the field and that they need to know in detail for a proper development.

2 Terms and definitions

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

NOTE Legal definitions (from Directive 1999/93/EC [20] or Regulation (EU) 910/2014 [21]) relative to this document can be found in Annex C.

2.1 secure element

SE
tamper resistant component used to provide security, confidentiality, and multiple application environment required to support various business models

EXAMPLE UICC, embedded SE, smartSD, smart microSD, etc.

2.2 trusted execution environment

TEE
specific execution environment on the mobile phone (or any connected device) application processor that is made of both software and, depending of the support of the processor, hardware parts, to manage the access control to the memory management unit and define a boundary between secure and unsecure (mobile OS) execution environment

2.3 trusted user interface

TUI
means to securely address user interaction for sensitive applications through the display, keyboard, microphone, etc.