SLOVENSKI STANDARD
SIST-TP CEN/TR 419200:2017

01-oktober-2017

Navodilo za elektronsko podpisovanje in druge podobne operacije

Guidance for signature creation and other related devices

Anleitung zur Signaturerstellung und andere ähnliche Geräte

Lignes directrices pour la création de signatires et autres dispositifs associés

Ta slovenski standard je istoveten z: **CEN/TR 419200:2017**

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST-TP CEN/TR 419200:2017 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 419200

May 2017

ICS 35.030; 35.240.30

English Version

Guidance for signature creation and other related devices

Lignes directrices pour la création de signatires 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

Ref. No. CEN/TR 419200:2017 E

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.

3 Symbols and abbreviations

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

C/S	Client/Server
CC	Common Criteria
CSP	Certification Service Provider
CV	Card Verifiable (certificate)
HIC	Health Insurance Card
HPC	Health Provider Card
IAS	Identification, Authentication and Signature
IBAN	International Bank Account Number
ICC	Integrated Circuit Card
MNO	Mobile Network Operator
PIN	Personal Identification Number
PIV	Personal Identity Verification (card)
PK	Public Key
PP	Protection Profile
QSCD	Qualified electronic Signature Creation Device
SC	Sole Control
SCA	Signature-Creation Application
SCC	Sole Control Component
SCDev	Signature Creation Device
SE	Secure Element
SIM	Subscriber Identity Module
SSA	Server Signing Application
SSCD	Secure Signature Creation Device
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STIC	Système de Traitement des Infractions Constatées (system for processing recorded infringements)
SVA	Signature-Validation Application
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TEE	Trusted Execution Environment
TLS	Transport Layer Security protocol
TSCM	Trustworthy Signature Creation Module
TSP	Trust Service Provider
TUI	Trusted User Interface (in the context of TEE)
TW4S	Trustworthy Systems Supporting Server Signing
UICC	Universal Integrated Circuit Card

4 Some concepts related to signature creation and other related devices

4.1 Different types of signatures and seals

Regulation (EU) 910/2014 [21] introduces several levels for signatures, starting from “basic” electronic signature up to advanced electronic signature. An advanced electronic signature created by a qualified electronic signature creation device and based on a qualified certificate is equivalent to a hand-written signature.

Regulation (EU) 910/2014 [21] introduces the notion of electronic seal, and gives several levels as for electronic signatures, starting from “basic” electronic seal up to advanced electronic seal. An advanced electronic seal created by a qualified electronic seal creation device and based on a qualified certificate can benefit from the presumption of integrity and correctness of origin of the data to which the seal is linked. The intention is e.g. to allow companies to issue business documents (e.g. invoices) matching EU legal requirements.

4.2 Signature versus seal

An electronic seal is the electronic equivalent of a seal or stamp which applied on a document guarantees its origin and integrity.

A seal can be viewed as an authority's proof of a document's content integrity, authenticity and level of authority, while a signature is a person's or legal entity’s commitment to the content of a document. A seal is created by a legal person (e.g. the tax revenue officer) and it expresses the will of the authority (the state) in whose name the seal-creator acts. A signature always expresses the will of the signer himself. Technically this means that a signature will always be confirmed by an explicit user verification entry (e.g. PIN verification); this will not be systematically the case for a seal (see EN 419212-2:2014 [26], Annex B, Table 1).

In the rest of this document there will be no particular notion of a seal since it technically compares to the signature and does not need additional specific standards.

4.3 What are a signature creation device or other related devices

4.3.1 General

The term “signature creation or other related devices” encompasses the signature creation device and other signature-related devices including identification device, authentication device, seal device or signature verification device (see Clause 5 for security services around electronic signature).

4.3.2 Qualified electronic signature creation device

An advanced electronic signature based on a qualified certificate and created by a qualified electronic signature creation device (QSCD) is equivalent to a hand-written signature and is legally recognized. Such QSCD is defined by Regulation (EU) 910/2014 as the following:

Qualified electronic signature creation device is an electronic signature creation device that meets the following requirements (Annex II):

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 assured;

   (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 first part of the definition (points 1. and 2.) are almost all the same as in Directive 1999/93/EC [20], and a common interpretation is to implement it as a Secure Element.

In the EN 419212 series [4] "Application Interfaces for secure elements used as Qualified electronic Signature (Seal-) Creation Devices", the device is clearly assimilated to a SE and the document describes all functional and security mechanisms, protocols and APDU commands to implement the European legal framework for electronic signatures. A SE compliant to the standard will be able to produce a "Qualified electronic signature" that fulfils the requirements of Regulation (EU) 910/2014 [21] and therefore can be considered equivalent to a hand-written signature.

In SSCD[1)] PP EN 419211 [3] "Protection profiles for secure signature creation device ", smart card is indicated as a typical example for SSCD. Moreover, all products certified against the previous version of SSCD PP (CWA 14169) are smart cards, see for example French certification body ANSSI web site http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-conformes-sscd.html, German certification body BSI web site https://www.bsi.bund.de/certified_products/digital_signature, or more generic Common Criteria list of signature products web site http://www.commoncriteriaportal.org/products.

According to Article 51 (1) in the Regulation (EU) 910/2014 [21], an SSCD compliant with Directive 1999/93/EC [20] is compliant with the Regulation. This is highlighted by the study done by IAS experts team on behalf of the Commission to support the implementation of the eIDAS Regulation (EU) 910/2014 [21]: the documents SMART 2012/0001 [22] and [23] establish the SSCD PP EN 419211 [3] is compliant (except for terminology[1)]) to Regulation (EU) 910/2014 [21] and can be used as such as a reference for certification of QSCD. A Technical Report will detail the matching for terminology between Directive 1999/93/EC [20] and Regulation (EU) 910/2014 [21] (to be published by CEN/TC 224 WG17).

The second part of the definition (points 3. and 4.) clearly indicates that the generation and management of electronic signature can be done on behalf of the signatory, using a remote server. ETSI ESI is defining architecture and policy requirements in case of mobile environment

1) The SSCD PP EN 419211 has been finalized within Directive 1999/93/EC context. It is nevertheless compliant with the Regulation 910/2014/EU, except for the terminology (a TR will be provided by CEN for the mapping), and applicable as such.

(see ETSI SR 019 020 [11]). CEN/TC 224/WG 17 is working on the extension of the security requirements for trustworthy systems supporting server signing (CEN/TS 419241 [7]) to a protection profile to address this case (see 5.3.2).

4.3.3 Qualified electronic seal creation device

An advanced electronic seal based on a qualified certificate and created by a qualified electronic seal creation device is legally recognized. Such device is defined by Regulation (EU) 910/2014 [21] as the following:

Qualified electronic seal creation device is an electronic seal creation device that meets the same previous requirements, since Article 29 shall apply mutatis mutandis.

As already mentioned, a seal can be technically addressed by available signature standards, including the QSCDs' ones the EN 419211 series [3] and EN 419212 series [4].

4.4 Trusted versus un-trusted environment for electronic signature

Two environments can be distinguished with respect to signature creation applications.

If the SCA is in a trusted environment, the environment is considered to be trusted by the user. Device authentication is not required as the end-user knows the environment that s(he) will apply for signature. See Figure 1.

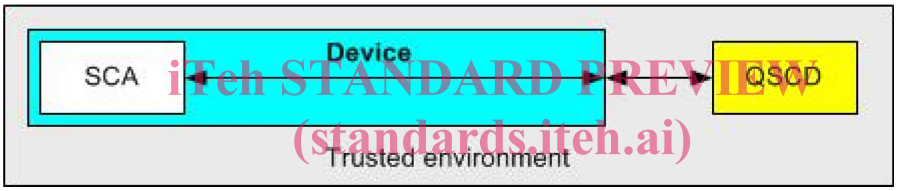

Figure 1 — Trust of the environment

If the SCA is in an un-trusted environment, a device authentication will be used if the operating environment of the QSCD cannot be entirely trusted by the user. This can be the case in public signature terminals or other devices that cannot provide an a-priori secure channel. See Figure 2.

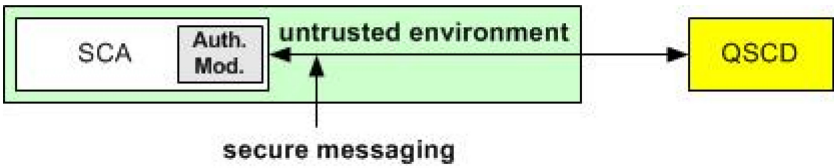

Figure 2 — Communication in untrusted environment

After successful device authentication, session keys are available on both sides to be used in subsequent protected transmissions (with secure messaging).

An example of a trusted environment is an environment not connected to the external world (inside an administration office).

The examples for an un-trusted environment are:

— SCA and QSCD are not at the same location;

— usage of biometrics if the sensor is off-card;

— usage of contactless cards.