SLOVENSKI STANDARD
SIST-TP CEN/TR 419010:2017

01-oktober-2017

Krovna določila za standardizacijo podpisov - Razširjena struktura, vključno z elektronsko identifikacijo in avtentifikacijo

Framework for standardization of signatures - Extended structure including electronic identification and authentication

Rahmen für die Normung von Signaturen - Erweiterte Struktur einschließlich elektronischer Identifizierung und Authentifizierung

Cadre pour la normalisation des signatures - Structure étendue incluant l'identification et l'authentification électronique

Ta slovenski standard je istoveten z: **CEN/TR 419010:2017**

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST-TP CEN/TR 419010:2017 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 419010

May 2017

ICS 35.030; 35.240.30

English Version

Framework for standardization of signatures - Extended structure including electronic identification and authentication

Cadre pour la normalisation des signatures - Structure étendue incluant l'identification et l'authentification électronique

Rahmen für die Normung von Signaturen - Erweiterte Struktur einschließlich elektronischer Identifizierung und Authentifizierung

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 419010:2017 E

Contents

Page

European foreword

This document (CEN/TR 419010:2017) 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

The Digital Agenda for Europe mentions in Pillar I (Digital Single Market) the Action 8 (Revision of the eSignature Directive), and this includes mutual recognition of electronic identification.

The first phase of Standardization Mandate M/460 [27], issued by the Commission to CEN, CENELEC and ETSI for updating the existing eSignature standardization deliverables, produced a rationalized framework to be the entry point for electronic signature standardization and overcome the complexity of standardization landscape within the context of the Signature Directive 1999/93/EC [26], taking into account possible revisions to this Directive, and proposes a future work programme to address any elements identified as missing in this rationalized framework.

To take into account the needs for electronic identification and authentication, identified as a gap from the ETSI/CEN framework for standardization of signatures ETSI/TR 119 000 [23], it was decided to study the standardization landscape around electronic identification and authentication as distinct from electronic signatures, identifying gaps and needs for standardization.

The Commission adopted the Regulation (EU) 910/2014 [27] on electronic identification and trust services for electronic transactions in the internal market on 23rd July 2014, to provide a legal framework which includes consistent and coherent provisions on electronic identification and trust services in order to overcome the deficiencies of the eSignatures Directive 1999/93/EC [26] and to provide legal measures on cross-border mutual recognition and acceptance of national eIDs.

The Commission published CIR 2015/1502 [30] on assurance levels for electronic identification means and CIR 2015/1501 [29] on interoperability framework to help the development of interoperable identity schemes across MS.

The eIDAS Expert Group has published a set of technical specifications [31] for the eIDAS interoperability framework, including a document of architecture and a document of cryptographic requirements, to complement the CIR 2015/1501 [29]. This is considered to address the interoperability requirements for use of eIDs across Europe.

This document analyses the impact of these two CIRs firstly on the already published standards identified in the ETSI/CEN framework for standardization of signatures ETSI/TR 119 000 [23] and secondly on potential requirements for further standards for harmonizing national approaches to identification and authentication as a new area in the ETSI/CEN framework for standardization of signatures ETSI/TR 119 000 [23].

1 Scope

The regulation on electronic identification and trusted eServices (eIDAS regulation) clearly extends the current Electronic Signature Directive from electronic signature towards electronic identification and electronic authentication. These two topics are closely linked to electronic signature and are considered in this context in this document. There are many documents, standards, industrial initiatives and European projects on identification and authentication, but the scope here is limited to electronic signature context, and wider to electronic transactions in the internal market.

The present Technical Report is twofold.

It firstly does a brief analysis of the implementing acts on electronic identities CIR 2015/1501 [29] and CIR 2015/1502 [30] and how this is addressed by the eID interoperability framework [31]. It secondly establishes what areas of existing standards are impacted by the eID framework and what further areas of standardization could assist nations in providing eID services.

2 Terms and definitions

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

NOTE Reg stands for the eIDAS Regulation [28], ISO for ISO/IEC 29115 [40] and CIR for CIR 2015/1501 [29] or CIR 2015/1502 [30]). Refer also to ETSI/TR 119 001 [24].

2.1
Authentication (ISO)
verification that an entity is the claimed one

2.2
Authentication (Reg)
electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed

2.3
Authentication factor (ISO)
piece of information and/or process used to authenticate or verify the identity of an entity

Note 1 to entry: Authentication factors are divided into four categories:

— something an entity has (e.g. device signature, passport, hardware device containing a credential, private key);

— something an entity knows (e.g. password, PIN);

— something an entity is (e.g. biometric characteristic); or

— something an entity typically does (e.g. behaviour pattern).

2.4
Authentication factor (CIR)
factor confirmed as being bound to a person, which falls into any of the following categories:

— ‘possession-based authentication factor’ means an authentication factor where the subject is required to demonstrate possession of it;

— ‘knowledge-based authentication factor’ means an authentication factor where the subject is required to demonstrate knowledge of it;

— ‘inherent authentication factor’ means an authentication factor that is based on a physical attribute of a natural person, and of which the subject is required to demonstrate that they have that physical attribute

2.5
Identity (ISO)
set of attributes related to an entity

Note 1 to entry: Within a particular context, an identity can have one or more identifiers to allow an entity to be uniquely recognized within that context.

2.6
Electronic identification (Reg)
process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person

2.7
Node (CIR)
connection point which is part of the electronic identification interoperability architecture and is involved in cross-border authentication of persons and which has the capability to recognize and process or forward transmissions to other nodes by enabling the national electronic identification infrastructure of one MS to interface with national electronic identification infrastructures of other MSs

2.8
Node Operator (CIR)
entity responsible for ensuring that the node performs correctly and reliably its functions as a connection point

2.9
Level of eID assurance (Reg)
degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned

Note 1 to entry: The regulation defines three levels: low, substantial and high; these are detailed in CIR 2015/1502 [30].

2.10
Signatory (Reg)
natural person who creates an electronic signature

3 Symbols and abbreviations

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

CC	Common Criteria
CIR	Commission Implementing Regulation
eSENS	Electronic Simple European Networked Services
IAS	Identification, Authentication, Signature

ICC	Integrated Circuit Card
IdP	Identity Provider
MAC	Message Authentication Code
MNO	Mobile Network Operator
MRED	Machine-Readable Electronic Documents
MS	Member State
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PP	Protection Profile
QAA	Quality of Authentication Assurance (STORK)
QSCD	Qualified Signature/Seal Creation Device
RA	Registration Authority
RF	Rationalized Framework
RP	Relying Party
SAD	Signature Activation Data
SAML	Security Assertion Markup Language
SAP	Signature Activation Protocol
SCA	Signature-Creation Application
SE	Secure Element
SIM	Subscriber Identity Module
SP	Service Provider
SSCD	Secure Signature Creation Device
STORK	Secure identiTy acrOss boRders linKed
TLS	Transport Layer Security
TR	Technical Report
TS	Technical Specification
TSP	Trust Service Provider
TSCM	Trustworthy Signature Creation Module
TTP	Trusted Third Party

4 Overview of the eID landscape in official documents

4.1 Overview of CIR 2015/1502

CIR 2015/1502 [30] describes technical specifications and procedures for the three assurance levels of the Regulation (low, substantial and high) for electronic identification means issued by a MS having notified its electronic identification scheme.

The document details requirements for:

— enrolment (application, registration, identity proofing and verification),