SLOVENSKI STANDARD
SIST EN 419212-1:2018

01-februar-2018

Nadomešča:
SIST EN 419212-1:2015
SIST EN 419212-2:2015

Uporabniški vmesnik za varnostne elemente za elektronsko identifikacijo, avtentikacijo in zanesljivost storitev - 1. del: Uvod in splošne definicije

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 1: Introduction and common definitions

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Anwendungsschnittstelle für sichere Elemente, die als qualifizierte elektronischer Signatur-/Siegelerstellungseinheiten verwendet werden - Teil 1: Allgemeine Dienste

SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/401ccab1-c4f1-408d-beb3-87b0d10c8d1f/sist-en-419212-1-2018

Interface applicative des éléments sécurisés utilisés comme dispositifs de création de signature électronique qualifiée (cachet) - Partie 1 : Introduction et définitions communes

Ta slovenski standard je istoveten z: **EN 419212-1:2017**

ICS:

35.240.15	Identifikacijske kartice. Čipne kartice. Biometrija	Identification cards. Chip cards. Biometrics

SIST EN 419212-1:2018 **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST EN 419212-1:2018

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/401ccab1-c4f1-408d-bcb3-87b0d10c8d1f/sist-en-419212-1-2018

SIST EN 419212-1:2018

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419212-1

September 2017

ICS 35.240.15

Supersedes EN 419212-1:2014, EN 419212-2:2014

English Version

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 1: Introduction and common definitions

Interface applicative des éléments sécurisés utilisés comme dispositifs de création de signature électronique qualifiée (cachet) - Partie 1 : Introduction et définitions communes

Anwendungsschnittstelle für sichere Elemente, die als qualifizierte elektronischer Signatur-/Siegelerstellungseinheiten verwendet werden - Teil 1: Allgemeine Dienste

This European Standard was approved by CEN on 6 February 2017.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

SIST EN 419212-1:2018

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

© 2017 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN 419212-1:2017 E

SIST EN 419212-1:2018

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/4f...-a0b1-4f5-40ed-1ab3-
87b0d10c8d1f/sist-en-419212-1-2018

SIST EN 419212-1:2018

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/401ccab1-e4f1-408d-bcb3-87b0d10c8d1f/sist-en-419212-1-2018

SIST EN 419212-1:2018

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/401ccab1-c4f1-408d-bcb3-87b0d10c8d1f/sist-en-419212-1-2018

SIST EN 419212-1:2018

European foreword

This document (EN 419212-1:2017) has been prepared by Technical Committee CEN/TC 224 "Furniture", the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by March 2018, and conflicting national standards shall be withdrawn at the latest by March 2018.

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.

This document supersedes EN 419212-1:2014 and EN 419212-2:2014.

This standard supports services in the context of **e**lectronic **ID**entification, **A**uthentication and Trust **S**ervices (eIDAS) including signatures.

In EN 419212-2, the standard allows support of implementations of the European legal framework for electronic signatures, defining the functional and security features for a Secure Elements (SE) (e.g. smart cards) intended to be used as a Qualified electronic Signature Creation Device (QSCD) according to the Terms of the "European Regulation on Electronic Identification and Trust Services for electronic transactions in the internal market" [2].

iTeh STANDARD PREVIEW

A Secure Element (SE) compliant to the standard will be able to produce a "qualified electronic signature" that fulfils the requirements of Article of the Electronic Signature Regulation and therefore can be considered equivalent to a hand-written signature [2].

(standards.iteh.ai)

This standard consists of five parts:

SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/401ccab1-c4f1-408d-bcb3-87b0d1bed1f6/sist-en-419212-1-2018

Part 1: "Introduction and common definitions" describes the history, application context, market perspective and a tutorial about the basic understanding of electronic signatures. It also provides common terms and references valid for the entire 419212 series.

Part 2: "Signature and Seal Services" describes the specifications for signature generation according to the eIDAS regulation.

Part 3: "Device Authentication" describes the device authentication protocols and the related key management services to establish a secure channel.

Part 4: "Privacy specific Protocols" describes functions and services to provide privacy to identification services.

Part 5: "Trusted eServices" describes services that may be used in conjunction with signature services described in Part 2.

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

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: 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 the United Kingdom.

SIST EN 419212-1:2018

Introduction

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

The European Committee for Standardization (CEN) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning the mapping function given in EN 419212-2, clause 8.3.6 “Step 4.2 - Map nonce and compute generator point for integrated mapping”.

The patent relates to “Sagem, MorphoMapping Patents FR09-54043 and FR09-54053, 2009”.

CEN takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has ensured CEN that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with CEN. Information may be obtained from:

Morpho

11, boulevard Galliéni

92445 Issy-les-Moulineaux Cedex

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. CEN shall not be held responsible for identifying any or all such patent rights.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/401ccab1-c4f1-408d-bcb3-87b0d10c8d1f/sist-en-419212-1-2018

SIST EN 419212-1:2018

1 Scope

This part is an informative introduction into the following parts. It gives guidance to the following parts in order to allow an efficient usage of the provided information. Therefore Part 1 provides history, application context, market perspective and a tutorial about the basic understanding of electronic signatures.

- Clause 3 provides "Terms and definitions" covering all parts of this standards. The specific parts will contain a similar section which refers to the clause of this Part 1.
- Clause 4 provides "Symbols and abbreviations" covering all parts of this standards. The specific parts will contain a similar section which refers to the clause of this Part 1.
- Clause 5 provides a Management Summary that describes the market context in which electronic signatures are typically
- Annex A provides the algorithm identifies for all parts of the standard.
- Annex B provides the algorithm identifies for all parts of the standard.
- Annex C provides the build scheme for object identifiers for all parts of the standard.
- Annex D "Tutorial on Signature Technology" provides a tutorial which helps the first reader to get familiar with signature technology and its relation to the society that it serves.
- Annex E "Guide to the EN 419212" explains the historical and technical evolution of the ESIGN activities which did finally lead to this version of the signature standard.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/401ccab1-c4f1-408d-bcb3-87b0d10c8d1f/sist-en-419212-1-2018

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7816-3:2006, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

ISO/IEC 9796-2:2010, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO 7498-2, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

3 Terms and definitions

For the purposes of Part 1 to 5 of this series of standards, the following terms and definitions apply.

NOTE These definitions are in compliance with those given in the revision of ISO/IEC 7816-4.

3.1
advanced electronic seal
electronic seal which meets the following requirements:

a) it is uniquely linked to the creator of the seal;

b) it is capable of identifying the creator of the seal;

SIST EN 419212-1:2018

c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and

d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable;

3.2
advanced electronic signature
data in electronic form which are attached to or logically associated with other electronic data to ensure the origin and the integrity of the associated data electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory

c) it is created using means that the signatory can maintain under his sole control;

d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

3.3
anonymity
assurance that a user may use a resource or service without disclosing their user identity

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.4
anonymization
process that removes the association between an identifying data set and a data subject

SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/401ccab1-c4f1-408d-bcb3-87b0d10c8d1f/sist-en-419212-1-2018

3.5
anonymized data
data that was once linked to an individual but can now no longer be related to them

3.6
anonymous data
data that cannot be linked to a specific individual

3.7
answer-to-Reset file
elementary file which indicates operating characteristics of the card

3.8
a priori trusted
operating environment which by definition can be trusted without further device authentication

Example**:** An example of this is the use within a company, where any available access point is connected to a trusted network.

3.9
authentication
electronic process that allows the confirmation of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic data

SIST EN 419212-1:2018

3.10
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

3.11
command-response pair
set of two messages: a command followed by a response

3.12
confidentiality protection
prevention of information disclosure to unauthorized individuals, entities or systems [ISO 7498-2]

3.13
creator of seal
legal person who creates an electronic seal

3.14
data unit
smallest set of bits which can be unambiguously referenced

3.15
data element
item of information seen at the interface for which are defined a name, a description of logical content, a format and a coding

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.16
data object
information seen at the interface which consists of a tag, a length and a value (i.e., a data element)

SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/401cab1e-4f7e-408d-be53-87b0d10c8d1f/sist-en-419212-1-2018

Note 1 to entry: In this specification, data objects are referred to as BER-TLV data objects. Refer to ISO/IEC 7816-4.

3.17
dedicated file
file containing file control information and, optionally, memory available for allocation. It may be the parent of EFs and/or DFs

3.18
device authentication
process of validating the credentials of a device

3.19
DF name
string of bytes which uniquely identifies a dedicated file in the card

3.20
digital signature
data appended to – or a cryptographic transformation 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

SIST EN 419212-1:2018

3.21
electronic seal
data in electronic form which are attached to or logically associated with other electronic data to ensure the origin and the integrity of the associated data

3.22
electronic seal creation device
configured software or hardware used to create an electronic seal

3.23
electronic signature
data in electronic form which are attached to or logically associated with other electronic data and which are used by the signatory to sign

3.24
electronic signature creation device
configured software or hardware used to create an electronic signature

3.25
qualified electronic seal
advanced electronic seal which is created by a qualified electronic seal creation device, and which is based on a qualified certificate for an electronic seal. A qualified certificate is specified in [eIdasReg#1]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.26
qualified electronic seal creation device
electronic seal creation device that creates a qualified electronic seal

SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/401ccab1-c4f1-408d-bcb3-87b0d10e8d1f/sist-en-419212-1-2018

3.27
qualified electronic signature creation device
electronic signature creation device which meets the requirements as follows:

1. It 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 ensured;

   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

SIST EN 419212-1:2018

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

3.28
elementary file
set of data units or records which share the same file identifier. It cannot be the parent of another file

3.29
file control parameters
logical, structural and security attributes of a file

3.30
file identifier
2-bytes binary value used to address a file

3.31
forward secrecy
security property of a protocol, that guarantees that the disclosure of long-term private key does not enable an opponent to compromise the secrecy property of the executions of the protocol made in the past, for example, by re-computing previously derived keys

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.32
identification
unique association of a set of descriptive parameters to an individual within a given context

SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/401ccab1-c4f1-408d-bcb3-87b04f10c8d1/sist-en-419212-1-2018

3.33
integrity protection
integrity protection is a mechanism ensuring that data cannot be modified undetectably

3.34
master file
mandatory unique dedicated file representing the root of the file structure

3.35
message
string of bytes transmitted by the interface device to the card or vice-versa, excluding transmission-oriented characters as defined in ISO/IEC 7816-3

3.36
mutual authentication
authentication where both parties (ICC and IFD) are authenticated to each other

3.37
non-traceability
refer to traceless authentication

SIST EN 419212-1:2018

3.38
parent file
dedicated file immediately preceding a given file within the hierarchy

3.39
password
data which may be required by the application to be presented to the card by its user. A password in the context of this specification is a string of numbers and/or ASCII characters

3.40
path
concatenation of file identifiers without delimitation. If the path starts with the identifier of the master file, it is an absolute path

3.41
privacy
privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others [ISO 7498-2]

3.42
private key
that key of an entity's asymmetric key pair that should only be used by that entity

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.43
pseudonym
identifier that contains sufficient information to allow a verifier to establish a unique link to an entity

SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/401ccab1-c4f1-408d-bcb3-87b0d10c8d1f/sist-en-419212-1-2018

Note 1 to entry: A pseudonym can be used to reduce privacy risks that are associated with the use of identifiers with fixed or known values.

Note 2 to entry: A pseudonym can be an identifier with a value chosen by the person, or assigned randomly.

3.44
pseudonymisation
particular type of anonymization that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms

3.45
pseudonymised data
data that can only be linked to such a person if one has possession of a decoding “key”

3.46
pseudonymity
pseudonymity is the ensurance that a user may use a resource or service without disclosing its user identity but can still be accountable for its use

3.47
public key
public part of an asymmetric key pair

SIST EN 419212-1:2018

3.48
qualified electronic signature
advanced electronic signature which is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures

3.49
record
string of bytes which can be handled as a whole by the card and referenced by a record number

3.50
record number
sequential number assigned to each record which uniquely identifies the record within its elementary file

3.51
retry counter
counter being used to count the number of erroneous usages of a related (security) object. If the object (e.g. password entry) was used correctly (correct password entered) then the retry counter is reset to its initial value. A typical value of a retry counter is 3

3.52
secret key
key used in symmetric algorithms

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.53
security environment
condition of use of objects in the card including stored data and data processing functions, expressed as a data element containing one or more access rules

SIST EN 419212-1:2018
https://standards.iteh.ai/catalog/standards/sist/401ccab1-c4f1-408d-bcb3-87b0d10c8d1f/sist-en-419212-1-2018

3.54
signatory
natural person who creates an electronic signature

3.55
signature creation device
secure device which is able to create a signature from its stored data and functionality

3.56
traceless authentication
traceless authentication is an authentication which does not give any persistent cryptographic proof that the authentication has occurred

3.57
trustable environment
operating environment that avoids tampering with data seen at the communication interface by the definition of its physical location, physical security protection or physical access conditions or other measures

3.58
trusted environment
environment the user has decided to trust

Note 1 to entry: In very few cases it is possible for a user to decide whether an evironment ist trustable or not. Therefore it is highly recommended that if a user ist not sure that an environment is a-priori trusted, not to enter