SLOVENSKI STANDARD
SIST EN 419212-4:2018

01-september-2018

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

Uporabniški vmesnik za varnostne elemente za elektronsko identifikacijo, avtentikacijo in zanesljivost storitev - 4. del: Posebni protokoli zasebnosti

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 4: Privacy specific Protocols

Anwendungsschnittstelle für sichere Elemente, die als qualifizierte elektronische Signatur -/Siegelerstellungseinheiten verwendet werden - Teil 4: Datenschutzspezifische Protokolle

Interface applicative des éléments sécurisés pour les services électroniques d'identification, d'authentification et de confiance - Partie 4 : Protocoles spécifiques à la protection de la vie privée

Ta slovenski standard je istoveten z: **EN 419212-4:2018**

ICS:

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

SIST EN 419212-4:2018 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419212-4

April 2018

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 4: Privacy specific Protocols

Interface applicative des éléments sécurisés pour les services électroniques d'identification, d'authentification et de confiance - Partie 4 : Protocoles spécifiques à la protection de la vie privée

Anwendungsschnittstelle für sichere Elemente zur elektronischen Identifikation, Authentisierung und für vertrauenswürdige Dienste - Teil 4: Datenschutzspezifische Protokolle

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.

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.

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

Ref. No. EN 419212-4:2018 E

Contents

Page

European foreword

This document (EN 419212-4:2018) 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.

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 October 2018, and conflicting national standards shall be withdrawn at the latest by October 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 **Part 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 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”.

A Secure Element (SE) compliant to the standard will be able to produce a “qualified electronic signature” that fulfils the requirements of section 4, in particular Articles 26 (requirements for advanced electronic signatures) and 29 (requirements for qualified electronic signature creation devices) of the so-called eIDAS Regulation and therefore can be considered equivalent to a hand-written signature.

This standard consists of five parts:

- 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.

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.

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 419212-2:2017 8.2.

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.

1 Scope

This part specifies mechanisms for SEs to be used as privacy-enabled devices in the context of IAS, and fulfill the requirements of Article 5 of the so-called eIDAS Regulation about data processing and protection.

It covers:

- Age verification
- Document validation
- Restricted identification
- eServices with trusted third party based on ERA protocol

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 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-8:2016, *Integrated circuit(s) cards with contacts — Part 8: Commands and mechanisms for security operations*

Technical Guideline TR-03110 2.20, “Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE) and Restricted Identification (RI) Version 2.20 Beta”,, Privacy Context functions

3 Introduction

3.1 General

Privacy Context is an environment to be considered whereas a card holder may be exposed to an environment that might read privacy parameters from the card ahead of any device authentication. Such privacy parameters can be the unique Card ID or other personalized parameters that allow a tracking and profiling of the card holder.

For instance, if the nationality of a card holder can be identified by the nature of the card description parameters (e.g. algorithm ID), then a card holder of certain nationality could be exposed to observation. Privacy context describes the requirement to allow a card holder to be confident that privacy parameters will not be exposed to unauthorized environment.

ICC Cards used for eID functionality may need as well privacy features e.g. to conceal the identity or the specific profile of the ICC owner in open networks or for Machine to Machine (M2M) services.

One popular functionality represents the well known use of pseudonyms here implemented by the restricted identification or 4.3 “Enhanced Role Authentication (ERA) protocol” with the purpose that these pseudonyms are used for certain services (e.g. payment sector) and cannot be linked to a global profile of the owner.

Another application lies in the validation of the ICC for authorization to web services, (e.g. voting) where only as much information is to be revealed as necessary for the actual service. Another popular use is the age verification with information provided only to the extent that a person is older than a particular age but without revealing the actual age of the card holder.

Different privacy oriented protocols are described in the following sections.

3.2 Auxiliary Data Comparison

3.2.1 General

The COMPARE command specified in ISO/IEC 7816-4:2013, initiates a comparison of "comparison data" with non-volatile "reference data" in the ICC. The comparison data are provided by the IFD either in the COMPARE command or by an operation prior to the comparison e.g. as Auxiliary Data as described in EN 419212-3:2017, 3.6.4.5.

As with coding the comparison data in the compare command the command could be sent multiple times, the IFD could evaluate the actual auxiliary data (e.g. age) by additional verification attempts on selected auxiliary data content (e.g. variable age).

If the IFD is allowed to send the compare command only once, then such an attempt may be avoided. Sending the comparison data as auxiliary data within device authentication protocols as specified in this standard, avoid those attacks. The presentation of the auxiliary data are shown in 3.2.3 and shall be implemented according to TR 03110 2.20.

The presentation of auxiliary data are mandatorily to be provided by the General Authentication Procedure (GAP) according to TR 03110 2.20.

As there are several further options to prevent from exhaustive search and the actual exposure cannot be generalized due to the fact that the actual content of auxiliary data are not specified in this standard, the associated countermeasures to the above situation are out of the scope of this standard.

For the additional services several use cases e.g. perform age verification, document validity verification or other comparison are possible.

Each of these use cases requires an appropriate usage of the COMPARE command regarding P1, P2, and the data field. These parameters are described in the following.

The successful execution of the COMPARE command has no result on the internal status of the card.

3.2.2 Presentation of the auxiliary data

The auxiliary data are presented as part of the mEAC protocol (EN 419212-3:2017, clause 3.6), in two possible variants. These variants are described above and shown in Table 1.

Auxiliary data may have use cases as in the following examples:

- For Age Verification the terminal has to send the required date of birth threshold.

- For Document Validity Verification the terminal has to send the current date

The following is an example that shows Table 34 in Part 3 but highlights the added steps relevant to the verification of the auxiliary data. The table relates to the mEAC protocol as described in EN 419212-3:2017, 3.6.

Table 1 — Reference device authentication scheme mEAC

Stage	Step	IFD	Transmission	ICC
A	1	READ BINARY of file containing protocol related parameters (e.g. public parameters etc.) GET DATA to read public parameters from EF.DH.	→ ←	Read parameters Data are in response APDU
Protocol relevant data are available to the terminal.				
B	2 condi-tional	In case of a remote interface: Proof of user presence: User is requested to prove presence by presentation of e.g. PIN	→ ←	Verify user presence Response: OK
In case of a remote interface or a contactless local interface, proof of user presence shall be given by mechanisms defined in 6 "User verification" in order to avoid skimming attacks.				
	10	For mEACv1 perform the steps 10–13 here. For backward compatibility to EACv1.1 protocol variant, step 11 and step 12 may alternatively be replaced by step 11’ applying MSE SET KAT command (see EN 419212-3:2017, 3.6.3.11)		
	11			
	12			
	13			
	3	Select and/or verify PuK.RCA.AUT.	→ ←	Select and/or verify key. Response: OK
	4	PSO:Verify Certificate C_CV.CAIFD.CS_AUT	→ ←	Verify certificate.
The verification of certificates along a certificate chain may continue until the CA's key is available in the ICC that signed the IFD's certificate and delivers **PuK.IFD.AUT**.				
	5	Select and/or verify PuK.CA$_{\text{IFD}}$.CS_AUT.	→ ←	Select and/or verify key. Response: OK
	6	PSO:Verify Certificate C_CV.IFD.AUT	→ ←	Verify certificate. Response: OK
The Public Key of the IFD is now known to the ICC, and can be trusted.				
D	7	MSE:SET AT (PuK.IFD.AUT) Select IFDs public key and select the key parameters for the consecutive operation, send compressed ephemeral public key Comp(PuK.IFD.KA) **and optionally auxiliary data** For the use of AUX.Data refer to 3.2.	→ ←	Select PuK of IFD, Store Comp(PuK.IFD.KA) **Store auxiliary data (optional)** Response: OK
	8	GET CHALLENGE	→ ←	RND.ICC

Stage	Step	IFD	Transmission	ICC
	9	EXTERNAL AUTHENTICATE By computing the digital signature DS[PrK.IFD.AUT](**S**) with **S** = [SN.ICC II RND.ICC || Comp(PuK.IFD.KA) || **AUX.Data]**	→ ←	ICC verifies signature. The IFD's identity is implicitly verified as known by the certificate C_CV.IFD.AUT. Response: OK
ICC has now authenticated the IFD				
E	10	**Conditional** – only if C.ICC.AUT is available: READ BINARY to obtain C.ICC.AUT or PuK.ICC.KA	→ ←	Read C.ICC.AUT or PuK.**ICC**.KA Data are in response APDU
	11	MSE SET AT Set PrK.ICC.KA for authentication	→ ←	Set PrK.ICC.KA Response: OK
	12	GENERAL AUTHENTICATE (compliant to ISO/IEC 7816-4:2013, 11.5.5) send PuK.IFD.KA Compute MAC[K_{MAC}](PuK.IFD.KA) and compare with received value Generate new session keys K_{ENC} and K_{MAC}	→ ←	Compute *Comp*(PuK.IFD.KA) and compare with hash value obtained in step 7. Generate new session keys K_{ENC} and K_{MAC} **Response:** OK and MAC[K_{MAC}](PuK.IFD.KA) and RND2.ICC
	13	**Establish secure session** The secure messaging session is restarted with session keys generated in step 11' or 12.		
Secure channel (ICC- server) is now established and two-way authentication is complete; If Step 10 is not performed, then Step 10 shall be performed in secure messaging mode as Step 14 (not shown in this example).				
	14	**COMPARE BINARY** send reference (i.e. OID) of AUX.Data given in step 7 and send mode of comparison		
	15	Repeat step 14 until all auxiliary data verifications are processed		
IFD has now verified auxiliary data				

The AUX.Data itself is a construction of data objects that comprise an OID and associated comparison data.

AUX.Data = DO.AUX1 || DO.AUX2 || .. || DO.AUXn

with

DO.AUX = ‘73’ L_{73} '06' L_{06} OID || '53' L_{53} < comparison data >

The OID describes the use and associated service for the DO '53' < comparison data > .

3.2.3 Age Verification

Age verification is one possible application of AUX.Data on the ICC. The IFD may send an age threshold value as part of the AUX data in the device authentication protocol or in the appropriate C.IFD.AUT certificate. The ICC can return acceptance or refusal without having to reveal the actual age of the card holder.

NOTE Cryptologically the age can be evaluated by the IFD using an exhaustive binary search, seven attemps would cover the range from 1 ... 128 years. Storing the threshold value as part of the IFD's certificate makes the process less flexible, however, this would avoid leakage of the age through a binary search.

Table 2 — COMPARE operation — command APDU

Command Parameter	Meaning
CLA	according to ISO/IEC 7816-4
INS	‘33’ COMPARE
P1	‘00’ = COMPARE BINARY
P2	‘00’
Lc field	Lc = < length of command data field >
Data field	‘06’ L_{06} < OID associating the comparison data >

The result is indicated by the status word in the command response. The COMPARE function is described in 11.6.1 of ISO/IEC 7816-4:2013.

The response data field is empty.

Table 3 — COMPARE operation — response

Response Parameter	Meaning
Data field	empty
SW1-SW2	Refer to ISO/IEC 7816-4