SLOVENSKI STANDARD
SIST EN 419212-3:2018

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 - 3. del: Protokoli avtentikacije naprav

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 3: Device authentication protocols

Anwendungsschnittstelle für Smartcards als sichere Signaturerstellungseinheiten - Teil 3: Geräteauthentisierungsprotokolle

Interface applicative des éléments sécurisés utilisés comme dispositifs de création de signature électronique qualifiée (cachet) Partie 3: Protocoles d'authentification des dispositifs

Ta slovenski standard je istoveten z: EN 419212-3:2017

ICS:

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

SIST EN 419212-3:2018 en,fr,de

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419212-3

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 3: Device authentication protocols

Interface applicative des éléments sécurisés utilisés comme dispositifs de création de signature électronique qualifiée (cachet) Partie 3: Protocoles d'authentification des dispositifs

Anwendungsschnittstelle für Smartcards als sichere Signaturerstellungseinheiten - Teil 3: Geräteauthentisierungsprotokolle

This European Standard was approved by CEN on 17 March 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: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 419212-3:2017 E

Contents

European foreword ... 5
Introduction ... 6
1 Scope ... 7
2 Normative references ... 7
3 Device authentication ... 7
3.1 General ... 7
3.2 Asymmetric Authentication introduction ... 9
3.3 Certification authorities and certificates ... 9
3.3.1 Certificate chains ... 9
3.3.2 Usage of link certificates ... 10
3.4 Authentication environments ... 10
3.4.1 SCA in trusted environment ... 11
3.4.2 SCA in untrusted environment ... 11
3.4.3 Specification of the environment ... 11
3.4.4 Display message mechanism ... 11
3.4.5 Additional authentication environments ... 12
3.5 Key transport and key agreement mechanisms ... 12
3.6 Device authentication with privacy protection ... 12
3.6.1 General ... 12
3.6.2 Authentication steps ... 13
3.7 Privacy constrained Modular EAC (mEAC) protocol with non-traceability feature ... 31
3.7.1 General ... 31
3.7.2 Example for traceability case ... 31
3.7.3 Notation ... 32
3.7.4 Authentication steps ... 32
3.7.5 Unlinkablity Mechanism with individual private keys ... 45
3.8 Symmetric authentication scheme ... 54
3.8.1 General ... 54
3.8.2 Authentication steps ... 54
3.8.3 Session Key creation ... 58
3.9 Key transport protocol based on RSA ... 58
3.9.1 General ... 58
3.9.2 Authentication Steps ... 60
3.9.3 Session Key creation ... 68
3.10 Compute Session keys from key seed $K_{IFD/ICC}$ ... 68
3.10.1 General ... 68
3.10.2 Generation of key data ... 69
3.10.3 Partitioning of the key data ... 69
3.10.4 Algorithm and method specific definition for key derivation ... 69
3.10.5 Key derivation from passwords ... 72
3.11 Compute send sequence counter SSC ... 73
3.12 Post-authentication phase ... 73
3.13 Ending the secure session ... 74
3.13.1 General ... 74
3.13.2 Example for ending a secure session ... 74
3.13.3 Rules for ending a secure session ... 74

3.14 Reading the Display Message ... 75
3.15 Updating the Display Message ... 77

4 Data structures ... 78
4.1 General ... 78
4.2 CRTs ... 78
4.2.1 General ... 78
4.2.2 CRT AT for the selection of internal private authentication keys ... 78
4.2.3 CRT AT for selection of internal authentication keys ... 78
4.2.4 CRT for selection of IFD's PuK.CA_{IFD}.CS_AUT ... 79
4.2.5 CRT for selection of IFD's PuK.IFD.AUT ... 79
4.2.6 CRT AT for selection of the public DH / ECDH key parameters ... 80
4.2.7 GENERAL AUTHENTICATE DH key parameters used by the Privacy Protocol ... 80
4.2.8 CRT AT for selection of ICC's private authentication key ... 80
4.2.9 CRT for selection of IFD's PuK.IFD.AUT ... 81
4.2.10 CRT for selection of PrK.ICC.KA ... 81
4.3 Key transport device authentication protocol ... 82
4.3.1 EXTERNAL AUTHENTICATE ... 82
4.3.2 INTERNAL AUTHENTICATE ... 82
4.4 Privacy device authentication protocol ... 83
4.4.1 EXTERNAL AUTHENTICATE (DH case) ... 83
4.4.2 EXTERNAL AUTHENTICATE (ECDH case) ... 84
4.4.3 INTERNAL AUTHENTICATE (DH case) ... 85
4.4.4 INTERNAL AUTHENTICATE (ECDH case) ... 85

5 CV_Certificates and Key Management ... 86
5.1 General ... 86
5.2 Level of trust in a certificate ... 86
5.3 Key Management ... 86
5.4 Certificate types ... 87
5.4.1 Card Verifiable Certificates ... 87
5.4.2 Signature-Certificates ... 88
5.4.3 Authentication Certificates ... 88
5.5 Use of the public key extracted from a CV-certificate ... 88
5.6 Validity of the key extracted from a CV-certificate ... 88
5.7 Structure of CVC ... 89
5.7.1 General ... 89
5.7.2 Non-self-descriptive certificates ... 89
5.7.3 Self-descriptive certificates ... 90
5.8 Certificate Content ... 90
5.8.1 General ... 90
CPI-Certificate Profile Identifier ... 91
5.8.2 CAR-Certification Authority Reference DO ... 92
5.8.3 CHR-Certificate Holder Reference DO ... 93
5.8.4 CHA-Certificate Holder Authorization Data Object (CHA-DO) ... 94
5.8.5 Role identifier specifications ... 95
5.8.6 User and service provider authentication ... 97
5.8.7 CHAT-Certificate Holder Authorization Template (CHAT) ... 98
5.8.8 OID — Object identifier ... 98
5.8.9 CEDT — Certificate Effective Date Template ... 98
5.8.10 CXDT — Certificate Expiration date Template ... 98
5.9 Certificate signature ... 99
5.9.1 General ... 99
5.9.2 Non self-descriptive certificates ... 99
5.9.3 Self-descriptive certificates ... 100

5.10 Coding of the certificate content 101
5.10.1 Non self-descriptive certificates 101
5.10.2 Self-descriptive certificates 101
5.10.3 Self-descriptive certificates for elliptic curve cryptography 102
5.11 Steps of CVC verification 105
5.11.1 General 105
5.11.2 First round: CVC verification from a Root PuK 106
5.11.3 Subsequent round(s) 107
5.12 Commands to handle the CVC 107
5.13 C_CV.IFD.AUT (non self-descriptive) 107
5.14 C_CV.CA.CS-AUT (non self-descriptive) 108
5.15 C.ICC.AUT 109
5.16 Self-descriptive CV Certificate (Example) 110
5.16.1 General 110
5.16.2 Public Key 110
5.16.3 Certificate Holder Authorization Template 111
5.16.4 Certificate Extension 111
5.16.5 ECDSA Signature 112

Annex A (informative) Device authentication Protocol Properties 113

Bibliography 115

European foreword

This document (EN 419212-3:2017) has been prepared by CEN/TC 224 "Personal identification, electronic signature and cards and their related systems and operations", 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.

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

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

This standard supports services in the context of electronic IDentification, Authentication and Trust Services (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 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" [1].

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 [1] 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. [24]

Part 2: "Signature and Seal Services" describes the specifications for signature generation according to the eIDAS regulation. [25]

Part 3: "Device Authentication" describes the device authentication protocols and the related key management services to establish a secure channel. [26]

Part 4: "Privacy specific Protocols" describes functions and services to provide privacy to identification services. [27]

Part 5: "Trusted eServices" describes services that may be used in conjunction with signature services described in Part 2. [28]

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

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 [25] 8.2.5 “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 either free of charge or 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 device authentication to be used for QSCDs in various contexts including:

- Device authentication protocols;
- Establishment of a secure channel;
- Data structures;
- CV-certificates;
- Key management.

The device authentication protocols should apply to sole-control signature mandated by the EU-regulation eIDAS [1].

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 7816-6, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*

ISO/IEC 7816-8:2004, *Identification cards — Integrated circuit cards — Part 8: Commands for security operations*

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

ISO/IEC 14888-3:2016, *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

3 Device authentication

3.1 General

This clause assumes that device authentication has to be performed as required in 3.3.

Device authentication requires mandatory steps in order to provide a secure authentication. A device authentication is mutual and combines two mechanisms:

- an ICC verifies the external world (TDA) and itself verified by the external world (CDA);
- the two devices negotiate or exchange information to establish common symmetric session keys for subsequent operations.

After negotiation of the symmetric keys, a secure session is established. A secure session is a cryptographic protection of the messages from both sides. The cryptographic protection can be:

- a cryptographic checksum on a plain text for integrity protection and/or
- an encrypted message text for confidentiality protection (mandates cryptographic checksum).

Refer to "9 Secure Messaging" [25].

For performance reasons, the secure messaging keys are symmetric keys. Therefore this document describes the establishment of symmetric session keys only, and does not consider an option for asymmetric session keys.

Once the session keys are established, a trusted channel is available to protect or conceal the information transmitted over the interface. The application of Secure Messaging (SM) is **mandatory** for **every subsequent operation** to ensure the provision of an entirely trusted channel. For exceptions refer to "5.3 Selection of ESIGN application" [25]. The conditions to end a secure messaging session are given in 3.12.

This chapter describes the following device authentication mechanisms

- asymmetric session key transport mechanism based on RSA;
- asymmetric session key agreement mechanism with privacy protection;
- asymmetric session key agreement mechanism with non-traceability and privacy protection;
- symmetric authentication mechanism

in order to perform a mutual authentication protocol between IFD and ICC. The presentation of the asymmetric schemes is sequentially staged in order to trade off the security features with the required complexity of the authentication protocols.

NOTE Authentication in general requires a defined order of steps to be processed. Violation of this order may result in the ICC aborting the process. The mechanism to control the proper order of execution steps are out of the scope of this standard.

In order to distinguish which device authentication is the most appropriate for a given situation refer to Annex A.

For the use of certificates the following table indicates the correct certificate type for each device authentication protocol.

Table 1 — Certificate type for use with device authentication protocols

Certificate Device Auth.	CV Certificate self-descriptive	CV Certificate non self-descriptive	Attribute certificates self-descriptive
3.8 Key transport protocol	-	x	-
3.5 Privacy protocol RSA	-	x	-
3.5 Privacy protocol ELC	x	-	x
3.6 mEAC	x	-	x

3.2 Asymmetric Authentication introduction

The above steps result in a high level of security for device authentication. They contain some mandatory aspects of the device authentication protocols considered to comply with the claims of the ESIGN-G1 [23] document.

- The public key of the IFD shall not be used until successfully verified by a certificate.
- The device to be authenticated shall submit its identity relevant token to the authenticator in a secure way, typically this can be achieved implicitly if the identity is part of the certificate.
- For both sides of the authentication it is mandatory to have evidence (after authentication), that the authentication was made with the same entity that shares the session keys for the secure messaging.
- After device authentication a trusted channel has been established. Relevant subsequent commands shall use the secure messaging session.
- A display message may be used to indicate successful device authentication in order to inform the card holder of the presence of a secure channel. The application of the display message is described in 3.13.

3.3 Certification authorities and certificates

3.3.1 Certificate chains

Asymmetric authentication requires the presentation of public keys in certificates. A chain of certificates might have to be presented. To establish the 'starting point of trust' the first certificate sent to the ICC shall always be verifiable with a public key already existing in the ICC. The most general of such keys available in the ICC can be a Root CA public key. Each certificate introduces another public key, while the presented certificate is always signed with a key, trusted by the ICC.

As the key pair of the Root CA changes over time, link certificates provide a link between expired and valid key pairs (refer to 3.2.2).

The Root CA provides

- certificates for the subordinate CAs
- link certificates in order to convey the public key(s).

In order to use an ESIGN application a mutual authentication between ICC and customer terminal is required by the security policy. As PK algorithms are to be employed ICC and IFD authentication certificates are required.

The ICC is the carrier of the ICC authentication certificate; carrier of the IFD authentication certificate could be a plug-in ICC as an example for the realization of an authentication module inside the Signature Creation Application (SCA).

The handling of the DOs 5.7.9 and 5.7.10 are out of the scope of this standard.

3.3.2 Usage of link certificates

A typical use of link certificates is to provide a link between expired and valid Root-CA key pairs.

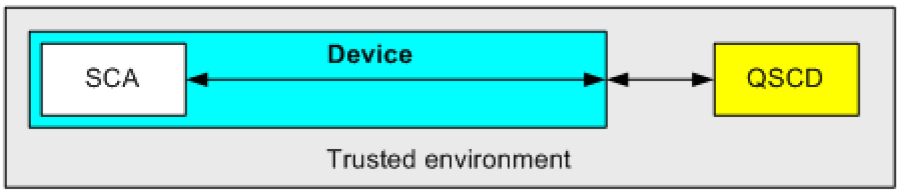

Figure 1 — Usage of link certificates for different key versions

The example above shows PuK.CA.AUT(2002) available at the ICC. This key was brought to the ICC in 2002, however in 2003 the root key was changed and another key chain

C.RCA.AUT(2003) → C.CA.AUT(2003) → C.IFD.AUT(2003)

was used when generating the IFD's certificate C.IFD.AUT(2003).

In order to allow authentication of the IFD, in the above example the ICC might have to receive a link certificate LC.RCA.AUT(2003) first. This certificate is signed with the PrK.RCA.AUT(2002) and it transports the PuK.RCA.AUT(2003).

After having verified the link certificate LC.RCA.AUT(2003) the ICC may now receive the certificates of the 2003-chain up to the C.IFD.AUT which carries the final public key required for authentication.

If it can verify the incoming certificate with an existing public key, the ICC accepts the transported public key and may use it for the next instance of the chain. The 'start of trust' is always established with the first certificate, being verified with a public key that is available in the ICC.

The example in Figure 1 considers a static Root CA key stored in the ICC. Hence, an IFD shall present a proper link certificate in every device authentication session.

Alternatively, an ICC may provide the possibility to permanently store the new Root CA key, which would require the import of a link certificate only once. If the trust anchor has been permanently updated within the ICC, the 'start of trust' for subsequent device authentications is the new Root CA key. The certificate chain to be presented by the IFD is shortened.

When verifying a certificate, the verifier shall verify the correct role of the signer. Only those roles being allowed to sign certificates may be accepted for the presentation of a certificate chain. The role of a certificate holder is specified in 5.7.4.

3.4 Authentication environments

NOTE In [22] two environments are distinguished with respect to signature creation applications.

3.4.1 SCA in trusted environment

The environment is considered to be trusted by the user. Device authentication is not required as the card holder knows the trusted environment that s(he) will apply the card to.

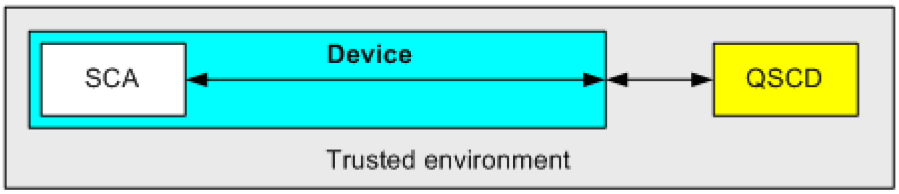

Figure 2 — Trust of the environment

3.4.2 SCA in untrusted environment

A device authentication shall be used if the operating environment of the ICC cannot be entirely trusted. This can be the case in public signature terminals or other devices, that cannot provide an a-priori secure channel.

Figure 3 — Communication in untrusted environment

Device authentication is mutual. The ICC shall authenticate the IFD and vice versa. The order of authentication, however, may differ, depending on the implemented scheme.

After successful device authentication, session keys are available on both sides to be used in subsequent transmissions. The appropriate secure messaging is in compliance with ISO/IEC 7816-4 and described in “9 Secure Messaging” [25].

Examples for an untrusted environment are:

- SCA and QSCD are not at the same location, i.e. the card is remote;
- usage of biometrics if the sensor is off-card;
- usage of contactless cards.

3.4.3 Specification of the environment

In general the IFD cannot evaluate a priori whether an environment is trustable or not. Therefore it shall be left to the card holder to decide, whether he may trust the application environment or not. The initiation of a device authentication in the application environment is out of the scope of this specification.

3.4.4 Display message mechanism

Given, the card holder has initiated a device authentication this specification proposes a 'display message' mechanism in order to verify that the device authentication has been performed successfully. If used, after successful device authentication, a display message shall indicate the successful device authentication in order to inform the user about the existence of a trusted channel. The application of the display message is described in 3.13.

3.4.5 Additional authentication environments

Device authentication may also be applied or necessary for multiple entity personalization (not in the scope of this standard).

3.5 Key transport and key agreement mechanisms

Key transport is the process of transferring a secret key, chosen by one entity (or a trusted centre), to another entity. Key transport requires encryption of the key part, and this is typically done using asymetric techniques and the public key of the counterpart. If used, for the establishment of secure messaging, key transport is used in both directions in order to derive a common key in the IFD and ICC.

Key agreement is the process of establishing a shared secret key between two entities A and B in such a way that neither of them can predetermine the value of the shared secret key. Key agreement mechanisms may be integrated in the device authentication.

In the context of session key establishment, 'implicit key authentication' means that after the execution of the mechanism only the participating entities can be in possession of the correct shared secret key.

This specification describes the following protocols:

- 3.5 Device authentication with privacy protection
- 3.6 Privacy constrained Modular EAC (mEAC) protocol with non-traceability feature
- 3.7 Symmetric authentication scheme

  and the legacy protocol
- 3.8 Key transport protocol based on RSA

Information on the recommended use of the protocols can be found in Annex A.

3.6 Device authentication with privacy protection

3.6.1 General

In device authentication with privacy protection, to avoid the ICC disclosing private information, such as identity, a secure channel session is established before any other operation. To do so, the protocol starts with an DH:EC Diffie-Hellman key exchange and then authenticates the IFD first before the ICC. The notion “**DH**” indicates “unauthenticated Diffie-Hellman” whereas “**EC**” assigns “elliptic curve Diffie-Hellmann” – both are valid alternatives and the following steps reflect both of them equally.

The protocol is recommended wherever the identity of the ICC shall not be revealed to either the IFD, or to an attacker tapping the communication before the IFD has been authenticated.

Five main phases may be distinguished:

i) Set the privacy protection.

ii) Transport of the IFD public key to the ICC.

iii) External authentication of the IFD.

iv) Transport of the ICC public key to the IFD.

v) Internal authentication of the ICC.

Usage of the privacy protocol mandates that the IFD is authenticated first.

3.6.2 Authentication steps

3.6.2.1 General

The following table shows device authentication with privacy protection and key agreement. The information in the fields is simplified. A detailed description of the coding is specified below.

DF.CIA shall only be readable to the extend that no personal information is read from the ICC until Step 11 is successfully accomplished. Until then, no information specific to the card holder (in contrast to the ICC's capabilities) shall be readable from DF.CIA.

Table 2 — Reference device authentication scheme 1 with Diffie-Hellman Key Exchange

Phase	Step	IFD	Transmission	ICC
1	1	READ BINARY of file DH **DH:** public parameters DH.P **EC:** public parameters ECDH.P.	→ ←	**DH:** Read DH key parameters *p, q* and *g* from specified file. **EC:** Read public parameters from specified file. Data are in response APDU
	1'(alt)	GET DATA for protocol related parameters **DH:** DH.P **EC:** ECDH.P		
	2	MSE:SET:**AT**[1] Set [DH | EC] DH algorithm	→ ←	OK