

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

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

See Eesti standard EVS-EN 419212-3:2017 sisaldab Euroopa standardi EN 419212-3:2017 ingliskeelset teksti.	This Estonian standard EVS-EN 419212-3:2017 consists of the English text of the European standard EN 419212-3:2017.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 20.09.2017.	Date of Availability of the European standard is 20.09.2017.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile [standardiosakond@evs.ee](mailto:standardiosakond@evs.ee).

ICS 35.240.15

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:  
Koduleht [www.evs.ee](http://www.evs.ee); telefon 605 5050; e-post [info@evs.ee](mailto:info@evs.ee)

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Homepage [www.evs.ee](http://www.evs.ee); phone +372 605 5050; e-mail [info@evs.ee](mailto:info@evs.ee)

EUROPEAN STANDARD

**EN 419212-3**

NORME EUROPÉENNE

EUROPÄISCHE NORM

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**

## 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 Unlinkability 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 <sub>IFD</sub> .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

<b>5.10</b>	<b>Coding of the certificate content.....</b>	<b>101</b>
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
<b>5.11</b>	<b>Steps of CVC verification .....</b>	<b>105</b>
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
<b>5.16</b>	<b>Self-descriptive CV Certificate (Example) .....</b>	<b>110</b>
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
<b>Annex A (informative) Device authentication Protocol Properties.....</b>		<b>113</b>
<b>Bibliography.....</b>		<b>115</b>

## 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.