

Application Interface for Secure Elements for Electronic  
Identification, Authentication and Trusted Services -  
Part 2: Signature and Seal Services

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

See Eesti standard EVS-EN 419212-2:2017 sisaldab Euroopa standardi EN 419212-2:2017 ingliskeelset teksti.	This Estonian standard EVS-EN 419212-2:2017 consists of the English text of the European standard EN 419212-2:2017.
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 13.12.2017.	Date of Availability of the European standard is 13.12.2017.
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 419212-2

NORME EUROPÉENNE

EUROPÄISCHE NORM

December 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 2: Signature and Seal Services

Interface applicative des éléments sécurisés utilisés comme dispositifs de création de signature électronique qualifiée (cachet) - Partie 2 : Services de signatures et de cachets

Anwendungsschnittstelle für sichere Elemente, die als qualifizierte elektronische Signatur-/Siegelstellungseinheiten verwendet werden - Teil 2: Zusätzliche 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.

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

<b>Contents</b>	<b>Page</b>
European foreword .....	6
<b>1 Scope .....</b>	<b>8</b>
<b>2 Normative references .....</b>	<b>8</b>
<b>3 Terms and definitions .....</b>	<b>9</b>
<b>4 Symbols and abbreviations .....</b>	<b>9</b>
<b>5 Signature application .....</b>	<b>9</b>
5.1 Application Flow .....	9
5.2 Trusted environment versus untrusted environment.....	11
5.3 Selection of ESIGN application .....	12
5.3.1 General .....	12
5.3.2 Exceptions for Secure Messaging.....	13
5.4 Selection of cryptographic information application.....	13
5.5 Concurrent usage of signature applications .....	13
5.5.1 General .....	13
5.5.2 Methods of channel selection .....	14
5.5.3 Security issues on multiple channels .....	14
5.6 Security environment selection .....	14
5.7 Key selection .....	14
5.8 Security Services.....	15
<b>6 User verification.....</b>	<b>15</b>
6.1 General .....	15
6.2 Knowledge based user verification.....	16
6.2.1 General .....	16
6.2.2 Explicit user verification.....	16
6.2.3 Password-based mechanisms .....	18
6.2.4 Presentation formats .....	18
6.2.5 Retry and Usage counters.....	18
6.2.6 Password Change.....	19
6.2.7 Reset of RC and setting a new password .....	19
6.3 Biometric user verification .....	20
6.3.1 General .....	20
6.3.2 Retrieval of the Biometric Information Template.....	21
6.3.3 Performing the biometric user verification.....	22
6.3.4 Reset of RC.....	24
<b>7 Digital Signature Service.....</b>	<b>24</b>
7.1 General .....	24
7.2 Signature generation algorithms.....	25
7.3 Activation of digital signature service .....	25
7.4 General aspects .....	25
7.5 Signature Generation .....	27
7.5.1 General .....	27
7.5.2 No hashing in Card.....	27
7.5.3 Partial hashing.....	27
7.5.4 All hashing in ICC .....	29
7.6 Selection of different keys, algorithms and input formats .....	30
7.6.1 General .....	30
7.6.2 Restore an existing SE .....	31

7.6.3	Setting the Hash Template (HT) of a current Security Environment (SE) .....	31
7.6.4	Modify the Digital Signature Template (DST) of a current Security Environment (SE) .....	32
7.7	Read certificates and certificate related information .....	32
7.7.1	General.....	32
7.7.2	Read certificate related CIOs.....	33
7.7.3	Read signer's certificate from ICC .....	33
7.7.4	Retrieval of the signer's certificate from a directory service.....	34
8	Password-based authentication protocols .....	35
8.1	General.....	35
8.2	Notation .....	35
8.3	Authentication steps .....	36
8.3.1	General.....	36
8.3.2	Step 1 — Reading the protocol relevant public parameters .....	37
8.3.3	Step 2 — Set PBM parameters and generate blinding point.....	38
8.3.4	Step 3 — Get encrypted nonce.....	39
8.3.5	Step 4.1 — Map nonce and compute generator point for generic mapping.....	40
8.3.6	Step 4.2 — Map nonce and compute generator point for integrated mapping.....	41
8.3.7	Step 5 — Generate session keys.....	43
8.3.8	Step 6 — Explicit key authentication .....	43
9	Secure Messaging.....	44
9.1	General.....	44
9.2	CLA byte .....	45
9.3	TLV coding of command and response message.....	45
9.4	Treatment of SM-Errors.....	45
9.5	Padding for checksum calculation .....	46
9.6	Send sequence counter (SSC).....	46
9.7	Message structure of Secure Messaging APDUs .....	46
9.7.1	Cryptograms.....	46
9.7.2	Cryptographic Checksums .....	48
9.7.3	Final command APDU construction.....	51
9.8	Response APDU protection.....	52
9.9	Use of TDES and AES.....	56
9.9.1	TDES/AES encryption/decryption .....	56
9.9.2	CBC mode.....	57
9.9.3	Retail MAC with TDES .....	57
9.9.4	EMAC with AES .....	58
9.9.5	CMAC with AES .....	59
10	Key Generation.....	59
10.1	General.....	59
10.2	Signature key and certificate generation .....	60
11	Key identifiers and parameters .....	61
11.1	General.....	61
11.2	Key identifiers (KID).....	62
11.2.1	General.....	62
11.2.2	Secret and private keys.....	62
11.3	Public Key parameters.....	62
11.3.1	General.....	62
11.3.2	RSA public key parameters.....	62
11.4	Diffie-Hellman key exchange parameters.....	63
11.5	Authentication tokens in the protocols mEACv2 and PCA .....	63
11.5.1	General.....	63

11.5.2	TDES.....	63
11.5.3	AES.....	63
11.5.4	Ephemeral Public Key Data Object.....	63
11.6	The compression function Comp().....	63
11.7	DSA with ELC public key parameters .....	64
11.7.1	General .....	64
11.7.2	The plain format of a digital signature .....	65
11.7.3	The uncompressed encoding.....	65
11.8	ELC key exchange public parameters.....	65
12	AlgIDs, Hash- and DSI Formats .....	66
12.1	General .....	66
12.2	Algorithm Identifiers and OIDs .....	66
12.3	Hash Input-Formats.....	66
12.3.1	General .....	66
12.3.2	PSO:HASH without command chaining.....	67
12.3.3	PSO:HASH with command Chaining.....	67
12.4	Formats of the Digital Signature Input (DSI).....	68
12.4.1	General .....	68
12.4.2	DSI according to ISO/IEC 14888-2 (scheme 2).....	69
12.4.3	DSI according to PKCS #1 V 1.5.....	69
12.4.4	Digest Info for SHA-X Hash:Digest Info SHA:Digest Info .....	71
12.4.5	DSI according to PKCS #1 V 2.x MGF function.....	73
12.4.6	DSA with DH key parameters .....	74
12.4.7	Elliptic Curve Digital Signature Algorithm - ECDSA.....	74
13	Files.....	74
13.1	General .....	74
13.2	File structure.....	74
13.3	File IDs .....	75
13.4	EF.DIR.....	75
13.5	EF.SN.ICC .....	76
13.6	EF.DH .....	76
13.7	EF.ELC.....	77
13.8	EF.C.ICC.AUT.....	77
13.9	EF.C.CA <sub>ICC</sub> .CS-AUT .....	78
13.10	EF.C_X509.CH.DS.....	78
13.11	EF.C_X509.CA.CS (DF.ESIGN) .....	79
13.12	EF.DM .....	79
14	Cryptographic Information Application.....	79
14.1	General .....	79
14.2	ESIGN cryptographic information layout example.....	81
14.2.1	General .....	81
14.2.2	EF.CIAInfo .....	82
14.2.3	EF.AOD .....	84
14.2.4	EF.PrKD .....	88
14.2.5	EF.PuKD.....	92
14.2.6	EF.CD.....	93
14.2.7	EF.DCOD.....	95
Annex A (normative)	Security environments.....	100
Annex B (informative)	Seals and Signatures.....	108
Annex C (informative)	Remote Signatures .....	111

## European foreword

This document (EN 419212-2:2017) 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 June 2018, and conflicting national standards shall be withdrawn at the latest by June 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 **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" [2].

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 " [2] 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.

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.

## 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 Part 2, clause 8.3.6.

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 qualified signature creation devices covering

- Signature creation and mobile signature creation
- User verification
- Password based authentication

The specified mechanisms are suitable for other purposes like services in the context of [2].

The particular case of seal is also covered by the specification. The differences between seal and signature is exposed in Annex B. Annex B also explains how the mechanisms for SEs as qualified signature creation devices can be used for SEs as qualified seal creation devices.

Mobile signature is an alternative to the classical signature case which is performed by a secure element. Mobile signature is encouraged by the large widespread of mobile devices and the qualification authorized by the eIDAS Regulation [2]. The particular case of remote signature (or server signing) is covered by this specification in Annex C.

In the rest of this document, except Annex B, there will be no particular notion of a seal since it technically compares to the signature.

## 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 7816-8:2004, *Identification cards - Integrated circuit cards - Part 8: Commands for security operations*

ISO/IEC 7816-11:2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 7816-15, *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application*

ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO 11568-2:2012, *Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO/IEC 14888-2:2008, *Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms*

ISO/IEC 19794-2:2005, *Information technology — Biometric data interchange formats — Part 2: Finger minutiae data*

ISO/IEC 15946-5, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation, 2009-12-15*

BSI: "Technical report Signature creation and administration for eIDAS token", Part 1: Functional Specification Version 1.0 Date: 2015/07/21

BSI/TR-03110 "Part 2 – Protocols for electronic IDentification, Authentication and trust Services (eIDAS)", Version 2.20, January 22nd, 2015<sup>1</sup>

### **3 Terms and definitions**

For the purposes of this document, terms and definitions in EN 419212-1 apply.

### **4 Symbols and abbreviations**

For the purposes of this document, symbols and abbreviations in EN 419212-1 apply.

### **5 Signature application**

#### **5.1 Application Flow**

Figure 1 shows an execution flow for a signature creation as it is mandated in [1].

---

<sup>1</sup> Available at [https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03110/index\\_htm.html](https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html)