

This document is a preview generated by EVS

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

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

See Eesti standard EVS-EN 419212-1:2017 sisaldab Euroopa standardi EN 419212-1:2017 ingliskeelset teksti.	This Estonian standard EVS-EN 419212-1:2017 consists of the English text of the European standard EN 419212-1:2017.
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 419212-1**

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 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.

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>
<b>European foreword</b> .....	<b>5</b>
<b>Introduction</b> .....	<b>6</b>
<b>1 Scope</b> .....	<b>7</b>
<b>2 Normative references</b> .....	<b>7</b>
<b>3 Terms and definitions</b> .....	<b>7</b>
<b>4 Symbols and abbreviations</b> .....	<b>15</b>
<b>5 Management Summary</b> .....	<b>18</b>
<b>5.1 Motivation</b> .....	<b>18</b>
<b>5.2 What is in behind?</b> .....	<b>19</b>
<b>5.3 Use Cases</b> .....	<b>20</b>
<b>5.4 Privacy and Security</b> .....	<b>21</b>
<b>5.5 Overview - EU Directive and Regulation</b> .....	<b>21</b>
<b>5.6 Facts and Figures</b> .....	<b>22</b>
<b>Annex A (normative) Algorithm Identifiers — Coding and specification</b> .....	<b>23</b>
<b>Table A.1 — AlgIDs</b> .....	<b>24</b>
<b>Table A.2 — Coding of byte 3 and 4 (for hash calculation - byte 2 = '01' to '0F')</b> .....	<b>24</b>
<b>Table A.3 — Coding of byte 3 (for digital signature computation - byte 2 = '1x')</b> .....	<b>25</b>
<b>Table A.4 — Coding of byte 4 (for digital signature computation - byte 2 = '1x')</b> .....	<b>25</b>
<b>Table A.5 — Coding of byte 3 (for C/S authentication - byte 2 = '2x')</b> .....	<b>25</b>
<b>Table A.6 — Coding of byte 4 (for C/S authentication - byte 2 = '2x')</b> .....	<b>25</b>
<b>Table A.7 — Coding of byte 3 (for key decipherment - byte 2 = '3x')</b> .....	<b>26</b>
<b>Table A.8 — Coding of byte 4 (for key decipherment - byte 2 = '3x')</b> .....	<b>26</b>
<b>Table A.9 — Coding of byte 3 (for authentication protocol - byte 2 = '4x')</b> .....	<b>26</b>
<b>Table A.10 — Coding of byte 4 (for authentication protocol - byte 2 = '4x')</b> .....	<b>28</b>
<b>Table A.11 — Coding of byte 3 (for digital signature verification - byte 2 = '9x')</b> .....	<b>28</b>
<b>Table A.12 — Coding of byte 4 (for digital signature verification - byte 2 = '9x')</b> .....	<b>28</b>
<b>Table A.13 — Coding of byte 3 (for role authentication - byte 2 = 'Ax')</b> .....	<b>29</b>
<b>Table A.14 — Coding of byte 3 (for privacy features - byte 2 = 'Cx')</b> .....	<b>29</b>
<b>Table A.15 — Coding of byte 4 (for role authentication - byte 2 = 'Ax')</b> .....	<b>29</b>
<b>Table A.16 — Coding of byte 4 (for privacy feature - byte 2 = 'Cx')</b> .....	<b>29</b>
<b>Table A.17 — 1-byte Algorithm-ID coding</b> .....	<b>30</b>
<b>Annex B (informative) OID values</b> .....	<b>32</b>
<b>B.1 OIDs for certificate signatures</b> .....	<b>32</b>
<b>Table B.1 — Object identifier values related to a public key in a certificate</b> .....	<b>32</b>
<b>B.2 OIDs for key transport protocol</b> .....	<b>32</b>

<b>Table B.2 — Object identifier values for the key transport protocol</b> .....	<b>33</b>
<b>B.3 OIDs for device authentication with privacy</b> .....	<b>33</b>
<b>Table B.3 — Object identifier values for device authentication with privacy</b> .....	<b>33</b>
<b>B.4 OIDs for password based mechanisms</b> .....	<b>34</b>
<b>Table B.4 — PACE OIDs</b> .....	<b>34</b>
<b>B.5 OIDs for mEAC protocol</b> .....	<b>34</b>
<b>B.5.1 OIDs for Chip Device Authentication</b> .....	<b>34</b>
<b>Table B.5 — Chip Device Authentication (DES/AES)</b> .....	<b>34</b>
<b>B.5.2 OIDs for Terminal Device Authentication</b> .....	<b>35</b>
<b>Table B.6 — Terminal Authentication (RSA/ECDSA)</b> .....	<b>35</b>
<b>B.6 OIDs for privacy protocols</b> .....	<b>36</b>
<b>B.6.1 OIDs for Restricted Identification</b> .....	<b>36</b>
<b>Table B.7 — OIDs for Restricted Identification</b> .....	<b>36</b>
<b>Table B.8 — OIDs for use in certificate extension</b> .....	<b>36</b>
<b>B.6.2 OIDs for Restricted Identification</b> .....	<b>36</b>
<b>Table B.9 — OIDs for use in auxiliary data verification</b> .....	<b>36</b>
<b>B.7 OIDs for mEAC based eServices - OIDs for Terminal Device Authentication in mEAC-based eServices</b> .....	<b>36</b>
<b>Table B.10 — OID values for the mEAC Terminal Authentication</b> .....	<b>36</b>
<b>B.8 OIDs for the PCA mechanism</b> .....	<b>37</b>
<b>Table B.11 — OID for the PCA mechanism</b> .....	<b>37</b>
<b>Annex C (informative) Build scheme for object identifiers defined by EN 419212</b> .....	<b>38</b>
<b>Figure C.1 — Build scheme for mEAC OIDs</b> .....	<b>39</b>
<b>Annex D (informative) Tutorial on Signature Technology</b> .....	<b>40</b>
<b>D.1 General</b> .....	<b>40</b>
<b>D.2 Signatures and keys</b> .....	<b>41</b>
<b>Table D.1 — Generating RSA keys</b> .....	<b>42</b>
<b>D.3 Signing documents</b> .....	<b>42</b>
<b>D.4 About certificates</b> .....	<b>43</b>
<b>D.5 The “chain of trust”</b> .....	<b>44</b>
<b>D.6 Multi step signature generation</b> .....	<b>44</b>
<b>D.6.1 General</b> .....	<b>44</b>
<b>D.6.2 Device authentication protocols</b> .....	<b>44</b>
<b>D.6.3 Secure Messaging</b> .....	<b>45</b>
<b>D.6.4 Password based device authentication</b> .....	<b>45</b>
<b>D.6.5 PIN entry</b> .....	<b>45</b>
<b>D.7 Signing the document</b> .....	<b>46</b>

<b>Annex E (informative) Guide to the EN 419212 .....</b>	<b>47</b>
<b>E.1 From EN 14890 to EN 419212.....</b>	<b>47</b>
<b>E.2 The EU Regulation 910/2014 and the Directive 1999/93/EU.....</b>	<b>48</b>
<b>E.3 Secure Elements (SE) .....</b>	<b>48</b>
<b>E.4 Specific protection required for contactless integrated circuits .....</b>	<b>49</b>
<b>E.4.1 General.....</b>	<b>49</b>
<b>E.4.2 Eavesdropping attacks .....</b>	<b>49</b>
<b>E.4.3 Skimming attack.....</b>	<b>49</b>
<b>E.4.4 Relay attack.....</b>	<b>49</b>
<b>E.4.5 Denial of Service (DoS) attack .....</b>	<b>49</b>
<b>E.4.6 Countermeasures .....</b>	<b>50</b>
<b>E.5 The Human-Machine Interface.....</b>	<b>50</b>
<b>E.6 Communications with the ICC and with the user .....</b>	<b>50</b>
<b>E.7 Information that should be initially communicated by the ICC to the IFD .....</b>	<b>51</b>
<b>E.8 User agreement using PINs.....</b>	<b>51</b>
<b>E.9 PIN unlocking.....</b>	<b>52</b>
<b>E.10 PIN change .....</b>	<b>52</b>
<b>E.11 User agreement using biometric information.....</b>	<b>52</b>
<b>E.12 User control using a local display and a local keyboard .....</b>	<b>52</b>
<b>E.13 Card applications .....</b>	<b>53</b>
<b>E.13.1 General.....</b>	<b>53</b>
<b>E.13.2 eSign card application .....</b>	<b>53</b>
<b>E.13.3 Device authentication mechanisms.....</b>	<b>53</b>
<b>E.13.4 Document Decryption mechanisms .....</b>	<b>53</b>
<b>E.14 Signature-/Seal functions.....</b>	<b>53</b>
<b>E.14.1 General.....</b>	<b>53</b>
<b>E.14.2 Digital signature/seal creation .....</b>	<b>54</b>
<b>E.14.3 Digital signature verification.....</b>	<b>54</b>
<b>E.14.4 Identification and authentication service.....</b>	<b>54</b>
<b>Bibliography.....</b>	<b>56</b>

## 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 **electronic IDentification, Authentication and Trust Services (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].

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].

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 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.

## 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 E-SIGN activities which did finally lead to this version of the signature standard.

## 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;