

Application Interface for Secure Elements for Electronic
Identification, Authentication and Trusted Services -
Part 5: Trusted eService

This document is a preview generated by EVS

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 419212-5:2018 sisaldab Euroopa standardi EN 419212-5:2018 ingliskeelset teksti.	This Estonian standard EVS-EN 419212-5:2018 consists of the English text of the European standard EN 419212-5:2018.
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 04.04.2018.	Date of Availability of the European standard is 04.04.2018.
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.

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; telefon 605 5050; e-post 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; phone +372 605 5050; e-mail info@evs.ee

EUROPEAN STANDARD

EN 419212-5

NORME EUROPÉENNE

EUROPÄISCHE NORM

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 5: Trusted eService

Interface applicative des éléments sécurités pour les services électroniques d'identification, d'authentification et de confiance - Partie 5 : Services électroniques de confiance

Anwendungsschnittstelle für sichere Elemente zur elektronischen Identifikation, Authentisierung und für vertrauenswürdige Dienste - Teil 5: Vertrauenswürdige elektronische 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: Rue de la Science 23, B-1040 Brussels

Contents	Page
European foreword.....	4
Introduction	5
1 Scope.....	6
2 Normative references.....	6
3 Terms and definitions	6
4 Abbreviations and notation.....	6
5 Additional Service Selection.....	6
6 Client/Server Authentication	10
6.1 General.....	10
6.2 Client/Server protocols	10
6.3 Steps preceding the client/server authentication	11
6.4 Padding format	11
6.4.1 PKCS #1 v 1-5 Padding.....	11
6.4.2 PKCS #1 V 2.x (PSS) Padding	12
6.4.3 Building the DSI on ECDSA	13
6.5 Client/Server protocol	13
6.5.1 General.....	13
6.5.2 Step 1 — Read certificate	14
6.5.3 Step 2 — Set signing key for client/server internal authentication	15
6.5.4 Step 3 — Internal authentication	16
6.5.5 Client/Server authentication execution flow.....	18
6.5.6 Command data field for the client server authentication	19
7 Role Authentication.....	20
7.1 Role Authentication of the card	20
7.2 Role Authentication of the server	20
7.3 Symmetrical external authentication	20
7.3.1 Protocol	20
7.3.2 Description of the cryptographic mechanisms	24
7.3.3 Role description.....	25
7.4 Asymmetric external authentication	25
7.4.1 Protocol based on RSA.....	25
8 Symmetric key transmission between a remote server and the ICC.....	28
8.1 Steps preceding the key transport.....	28
8.2 Key encryption with RSA	28
8.2.1 General.....	28
8.2.2 PKCS#1 v1.5 padding	30
8.2.3 OAEP padding	30
8.2.4 Execution flow	31
8.3 Diffie-Hellman key exchange for key encipherment.....	33
8.3.1 General.....	33
8.3.2 Execution flow	35
9 Signature verification.....	37
9.1 General.....	37
9.2 Signature verification execution flow.....	37

9.2.1	General	37
9.2.2	Step 1: Receive Hash	37
9.2.3	Step 2: Select verification key	39
9.2.4	Step 3: Verify digital signature	39
10	Certificates for additional services	40
10.1	File structure.....	40
10.2	File structure.....	41
10.3	EF.C_X509.CH.DS.....	41
10.4	EF.C.CH.AUT	41
10.5	EF.C.CH.KE.....	42
10.6	Reading Certificates and the public key of CAs.....	42
11	APDU data structures.....	42
11.1	Algorithm Identifiers.....	42
11.2	General	42
11.3	CRTs.....	43
11.3.1	General	43
11.3.2	CRT DST for selection of ICC's private client/server auth. key	43
11.3.3	CRT AT for selection of ICC's private client/server auth. key.....	43
11.3.4	CRT CT for selection of ICC's private key.....	44
11.3.5	CRT DST for selection of IFD's public key (signature verification)	44
	Annex A (informative) Security Service Descriptor Templates.....	45
	Annex B (informative) Example of DF.CIA.....	51
	Bibliography	58

European foreword

This document (EN 419212-5:2018) 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 **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” [22].

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 ” [22] 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

Part 5 of this series contains Identification, Authentication and Digital Signature (IAS) services in addition to the QSCD mechanisms already described in Part 2 to enable interoperability and usage for IAS services on a national or European level.

It also specifies additional mechanisms like key decipherment, Client Server authentication, identity management and privacy related services.

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 for security operations*

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

PKCS #1 v2.1:2002, RSA Cryptography Standard, RSA Laboratories¹

3 Terms and definitions

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

4 Abbreviations and notation

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

5 Additional Service Selection

Additional services are typically used in the context of applications that use digital signatures.

A well-known additional service is the **client/server authentication**. In this case, the ICC is used as a crypto toolbox, e.g. in order to encrypt a challenge with a private key, being stored in the ICC. This is particularly helpful in applications, where a tamper resistant device is required for client/server authentication. A secure ICC has the necessary tamper resistant quality and may therefore be used efficiently to support the application in this context.

Document decryption is another known service which may be performed by the IFD. A terminal application receives a document, typically encrypted with a symmetric key. The symmetric key is also provided encrypted with a public key. The ICC contains the appropriate private key, deciphers the symmetric key and returns it to the terminal application.

While the typical usage of a signature card is the generation of a digital signature, an application might want to verify a signature with a public key, being stored in the ICC. In this case an additional service is invoked for **signature verification**.

¹ Available at www.rsasecurity.com/rsalabs/pkcs/pkcs-1/ <http://www.rsa.com/rsalabs/node.asp?id=2125>