

Application Interface for smart cards used as Secure
Signature Creation Devices - Part 2: Additional Services

This document is a preview generated by EVS

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 419212-2:2014 sisaldab Euroopa standardi EN 419212-2:2014 ingliskeelset teksti.	This Estonian standard EVS-EN 419212-2:2014 consists of the English text of the European standard EN 419212-2:2014.
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 10.12.2014.	Date of Availability of the European standard is 10.12.2014.
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:

Aru 10, 10317 Tallinn, Eesti; 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:

Aru 10, 10317 Tallinn, Estonia; homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

English Version

Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional services

Interface applicative des cartes à puces utilisées comme
dispositifs de création de signature numérique sécurisés -
Partie 2 : Services complémentaires

Anwendungsschnittstelle für Chip-Karten, die zur
Erzeugung qualifizierter elektronischer Signaturen
verwendet werden - Teil 2: Zusätzliche Dienste

This European Standard was approved by CEN on 27 September 2014.

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, 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

Foreword.....	5
1 Scope	7
2 Normative references	7
3 Terms and definitions	7
4 Abbreviations and notation	9
5 Additional Service Selection	11
6 Client/Server Authentication	14
6.1 Client/Server protocols	14
6.2 Steps preceding the client/server authentication	15
6.3 Padding format.....	15
6.3.1 PKCS #1 v 1-5 Padding	15
6.3.2 PKCS #1 V 2.x (PSS) Padding.....	16
6.3.3 Building the DSI on ECDSA	17
6.4 Client/Server protocol	18
6.4.1 Step 1 — Read certificate.....	18
6.4.2 Step 2 — Set signing key for client/server internal authentication	19
6.4.3 Step 3 — Internal authentication.....	20
6.4.4 Client/Server authentication execution flow	22
6.4.5 Command data field for the client server authentication	24
7 Role Authentication	25
7.1 Role Authentication of the card	25
7.2 Role Authentication of the server	25
7.3 Symmetrical external authentication	25
7.3.1 Protocol	25
7.3.2 Description of the cryptographic mechanisms	30
7.3.3 Role description.....	30
7.4 Asymmetric external authentication.....	31
7.4.1 Protocol based on RSA.....	31
7.4.2 Protocol based on modular Enhanced Role Authentication (mERA)	34
8 Symmetric key transmission between a remote server and the ICC	49
8.1 Steps preceding the key transport.....	49
8.2 Key encryption with RSA	49
8.2.1 PKCS#1 v1.5 padding.....	50
8.2.2 OAEP padding.....	50
8.2.3 Execution flow.....	51
8.3 Diffie-Hellman key exchange for key encipherment	54
8.3.1 Execution flow.....	56
9 Signature verification	58
9.1 Signature verification execution flow	58
9.1.1 Step 1: Receive Hash	59
9.1.2 Step 2: Select verification key	60
9.1.3 Step 3: Verify digital signature	61
10 Certificates for additional services	62
10.1 File structure	63
10.2 EF.C_X509.CH.DS	63
10.3 EF.C.CH.AUT	63
10.4 EF.C.CH.KE.....	63
10.5 Reading Certificates and the public key of CAs.....	64
11 Privacy Context functions	65

11.1	Introduction.....	65
11.2	Auxiliary Data Comparison.....	65
11.2.1	Presentation of the auxiliary data.....	66
11.2.2	Age Verification.....	68
11.2.3	Document Validation.....	69
11.3	Restricted Identification.....	70
11.3.1	Command APDU for Step RI:1.....	73
11.3.2	Command APDU for Step RI:2.....	74
11.4	eServices with trusted third party protocol.....	77
11.4.1	mERA-based eServices with trusted third party protocol.....	78
11.4.2	mEAC-based eServices with trusted third party.....	83
11.5	eServices with two party protocols.....	86
11.5.1	mEAC-based eServices with on-line two party protocol.....	86
11.5.2	mEAC-based eServices with off-line two party protocol.....	87
12	APDU data structures.....	89
12.1	Algorithm Identifiers.....	89
12.2	CRTs.....	89
12.2.1	CRT DST for selection of ICC's private client/server auth. key.....	89
12.2.2	CRT AT for selection of ICC's private client/server auth. key.....	89
12.2.3	CRT CT for selection of ICC's private key.....	90
12.2.4	CRT DST for selection of IFD's public key (signature verification).....	90
Annex A	(normative) Security Service Descriptor Templates.....	91
A.1	Security Service Descriptor Concept.....	91
A.2	SSD Data Objects.....	92
A.2.1	DO Extended Header List, tag '4D'.....	92
A.2.2	DO Instruction set mapping (ISM), tag '80'.....	92
A.2.3	DO Command to perform (CTP), tag '52' (refer to ISO/IEC 7816-6).....	92
A.2.4	DO Algorithm object identifier (OID), tag '06' (refer to ISO/IEC 7816-6).....	92
A.2.5	DO Algorithm reference, tag '81'.....	92
A.2.6	DO Key reference, tag '82'.....	93
A.2.7	DO FID key file, tag '83'.....	93
A.2.8	DO Key group, tag '84'.....	93
A.2.9	DO FID base certificate file, tag '85'.....	93
A.2.10	DO FID adjoined certificate file, tag '86'.....	93
A.2.11	DO Certificate reference, tag '87'.....	93
A.2.12	DO Certificate qualifier, tag '88'.....	93
A.2.13	DO FID for file with public key of the certification authority PK(CA), tag '89'.....	93
A.2.14	DO PIN usage policy, tag '5F2F'.....	93
A.2.15	DO PIN reference, tag '8A'.....	94
A.2.16	DO Application identifier (AID), tag '4F' (refer to ISO/IEC 7816-6).....	94
A.2.17	DO CLA coding, tag '8B'.....	94
A.2.18	DO Status information (SW1-SW2), tag '42' (refer to ISO/IEC 7816-6).....	94
A.2.19	DO Discretionary data, tag '53' (refer to ISO/IEC 7816-6).....	94
A.2.20	DO SE number, tag '8C'.....	94
A.2.21	DO SSD profile identifier, tag '8D'.....	95
A.2.22	DO FID mapping, tag '8E'.....	95
A.3	Location of the SSD templates.....	95
A.4	Examples for SSD templates.....	95
Annex B	(informative) Security environments.....	97
B.1	Definition of CRTs (examples).....	98
B.1.1	CRT for Authentication (AT).....	99
B.1.2	CRT for Cryptographic Checksum (CCT).....	100
B.1.3	CRT for Digital Signature (DST).....	101
B.1.4	CRT for confidentiality (CT).....	102
B.2	Security Environments (example).....	103
B.2.1	Security Environment #10.....	103
B.2.2	Security Environment #11.....	104
B.3	Coding of access conditions (example).....	104

B.3.1	Access Conditions	105
B.3.2	Access rule references	106
B.3.3	Access conditions for EF.ARR	107
B.3.4	EF.ARR records	107
Annex C	(normative) Algorithm Identifiers — Coding and specification	110
Annex D	(informative) Example of DF.CIA	117
Annex E	(informative) Build scheme for object identifiers defined by EN 14890	122
Bibliography	124

This document is a preview generated by EVS

Foreword

This document (EN 419212-2:2014) has been prepared by Technical Committee 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 June 2015 and conflicting national standards shall be withdrawn at the latest by June 2015.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN 14890-2:2008.

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

EN 419212, *Application Interface for smart cards used as Secure Signature Creation Devices*, consists of two parts:

- *Part 1: Basic services* which describes the specifications for IAS based services on smart cards to be used in compliance to the requirements of Article 5.1 of the Electronic Signature Directive; and
- *Part 2: Additional services* [the present document] which describes other services that may be used in conjunction with all, some or none of the services described in Part 1.

This standard supports services in the context of IAS Identification, **A**uthentication and Electronic **S**ignature (IAS) services, as well as other services.

In EN 419212-1, the standard allows to support the implementation of the European legal framework for electronic signatures, defining the functional and security features for a smart card intended to be used as a Secure Signature Creation Device according to the Terms of the European Directive on Electronic Signature 1999/93/EC. A card compliant to the standard will be able to produce a "Qualified Electronic Signature (QES)" that fulfils the requirements of Article 5.1 of the Electronic Signature Directive and therefore can be considered equivalent to hand-written signatures.

In EN 419212-2, the standard specifies mechanisms to support other services like generic Identification, Authentication, confidentiality, signature verification services and privacy features.

EN 419212 defines a set of services that will enable the development of interoperable cards issued by any card industry sector. The standard will describe an application interface and behavior of the SSCD, i.e. it should be possible to implement it on native and interpreter based cards.

Compared with the 2008 versions of EN 14890, the following broad change has been made:

The scope of the standard was enhanced through new mechanisms in the field of password based mechanisms and privacy.

Regarding EN 419212-1, the most significant technical changes that have been made are the following ones:

- new algorithms added to device authentication protocols (e.g. AES, ELC);
- added AES to secure messaging;

- introduced password based mechanisms (PACEv2);
- updating references to their latest releases;
- algorithm Identifier coding;
- recommendation for making best use of device authentication protocols.

Regarding EN 419212-2, the most significant technical changes that have been made are the following ones:

- a) Added privacy services including:
 - 1) anonymity and pseudonymity services;
 - 2) auxiliary data transmission e.g. for Age verification;
 - 3) e-Services with trusted third party;
 - 4) e-Services with 2-parties.

According to the CEN-CENELEC Internal Regulations, the national standards organizations 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, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

1 Scope

This European Standard contains Identification, Authentication and Digital Signature (IAS) services in addition to the SSCD mechanisms already described in EN 419212-1 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.

EN 419212-1:2014, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 1: Basic services*

ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit(s) cards with contacts — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-6:2006, *Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements for interchange*

ISO/IEC 7816-8:2004, *Integrated circuit(s) cards with contacts — Part 8: Commands for security operations*

ISO/IEC 9796 (all parts), *Information technology — Security techniques — Digital signature schemes giving message recovery*

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

3 Terms and definitions

For the purposes of this document, 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

anonymity

assurance in which a user may use a resource or service without disclosing the user's identity

3.2

anonymization

process that removes the association between an identifying data set and a data subject

3.3

anonymized data

data that was once linked to an individual but can now no longer be related to them

3.4

anonymous data

data that cannot be linked to a specific individual

3.5

C/S external authentication

authentication of the server by the client