

DIN EN 419212-1:2015-03 (E)

Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services; English version EN 419212-1:2014

Contents		Page
Foreword		7
Introduction		9
1	Scope	10
2	Normative references	10
3	Terms and definitions	11
4	Symbols and abbreviations	15
5	Signature application	18
5.1	Application Flow	18
5.2	Trusted environment versus untrusted environment	22
5.3	Selection of E-SIGN application	22
5.3.1	General	22
5.3.2	Exceptions for Secure Messaging	23
5.4	Selection of cryptographic information application	23
5.5	Concurrent usage of signature applications	24
5.5.1	General	24
5.5.2	Methods of channel selection	24
5.5.3	Security issues on multiple channels	24
5.6	Security environment selection	24
5.7	Key selection	25
5.8	Security Services	25
6	User verification	26
6.1	General	26
6.2	Knowledge based user verification	26
6.2.1	General	26
6.2.2	Explicit user verification	27
6.2.3	Password based mechanisms	28
6.2.4	Presentation formats	28
6.2.5	Retry and Usage counters	28
6.2.6	Password Change	29
6.2.7	Reset of RC and setting a new password	29
6.3	Biometric user verification	30
6.3.1	General	30
6.3.2	Retrieval of the Biometric Information Template	31
6.3.3	Performing the biometric user verification	32
6.3.4	Reset of RC	34
7	Digital Signature Service	34
7.1	General	34
7.2	Signature generation algorithms	35
7.3	Activation of digital signature service	35
7.4	General aspects	36
7.5	Signature Generation	37
7.5.1	General	37
7.5.2	No hashing in Card	37

7.5.3	Partial hashing	38
7.5.4	All hashing in ICC	39
7.6	Selection of different keys, algorithms and input formats	40
7.6.1	General	40
7.6.2	Restore an existing SE	41
7.6.3	Setting the Hash Template (HT) of a current Security Environment (SE)	42
7.6.4	Modify the Digital Signature Template (DST) of a current Security Environment (SE)	42
7.7	Read certificates and certificate related information	43
7.7.1	General	43
7.7.2	Read certificate related CIOs	43
7.7.3	Read signer's certificate from ICC	44
7.7.4	Retrieval of the signer's certificate from a directory service	44
8	Device authentication	45
8.1	General	45
8.2	Asymmetric Authentication introduction	46
8.3	Certification authorities and certificates	46
8.3.1	Certificate chains	46
8.3.2	Usage of link certificates	47
8.4	Authentication environments	48
8.4.1	General	48
8.4.2	SCA in trusted environment	48
8.4.3	SCA in untrusted environment	48
8.4.4	Specification of the environment	49
8.4.5	Display message mechanism	49
8.4.6	Additional authentication environments	49
8.5	Key transport and key agreement mechanisms	49
8.6	Key transport protocol based on RSA	50
8.6.1	General	50
8.6.2	Authentication Steps	52
8.6.3	Session Key creation	62
8.7	Device authentication with privacy protection	63
8.7.1	General	63
8.7.2	Authentication steps	63
8.8	Privacy constrained Modular EAC (mEAC) protocol with non-traceability feature	82
8.8.1	General	82
8.8.2	Example for traceability case	83
8.8.3	Notation	83
8.8.4	Authentication steps	84
8.8.5	Unlinkability Mechanism with individual private keys	99
8.9	Symmetric authentication scheme	108
8.9.1	General	108
8.9.2	Authentication steps	108
8.9.3	Session Key creation	112
8.10	Compute Session keys from key seed KIFD/ICC	113
8.10.1	General	113
8.10.2	Generation of key data	113
8.10.3	Partitioning of the key data	113
8.10.4	Algorithm and method specific definition for key derivation	113
8.10.5	Key derivation from passwords	116
8.11	Compute send sequence counter SSC	118
8.12	Post-authentication phase	118
8.13	Ending the secure session	119
8.13.1	General	119
8.13.2	Example for ending a secure session	119
8.13.3	Rules for ending a secure session	119
8.14	Reading the Display Message	119
8.15	Updating the Display Message	122
9	Password-based authentication protocols	123
9.1	General	123
9.2	Notation	123

9.3	Authentication steps	124
9.3.1	General	124
9.3.2	Step 1 -- Reading the protocol relevant public parameters	125
9.3.3	Step 2 -- Set PBM parameters and generate blinding point	127
9.3.4	Step 3 -- Get encrypted nonce	128
9.3.5	Step 4.1 -- Map nonce and compute generator point for generic mapping	129
9.3.6	Step 4.2 -- Map nonce and compute generator point for integrated mapping	130
9.3.7	Step 5 -- Generate session keys	133
9.3.8	Step 6 -- Explicit key authentication	134
10	Secure Messaging	135
10.1	General	135
10.2	CLA byte	135
10.3	TLV coding of command and response message	135
10.4	Treatment of SM-Errors	136
10.5	Padding for checksum calculation	136
10.6	Send sequence counter (SSC)	136
10.7	Message structure of Secure Messaging APDUs	136
10.7.1	Cryptograms	136
10.7.2	Cryptographic Checksums	139
10.7.3	Final command APDU construction	143
10.8	Response APDU protection	143
10.9	Use of TDES and AES	150
10.9.1	TDES/AES encryption/decryption	150
10.9.2	CBC mode	151
10.9.3	Retail MAC with TDES	151
10.9.4	EMAC with AES	152
10.9.5	CMAC with AES	154
11	Key Generation	155
11.1	General	155
11.2	Key generation and export using PrK.ICC.AUT	155
11.3	Key generation and export with SM	155
11.4	Write certificates	156
12	Key identifiers and parameters	156
12.1	General	156
12.2	Key identifiers (KID)	156
12.2.1	General	156
12.2.2	Secret and private keys	156
12.3	Public Key parameters	156
12.3.1	General	156
12.3.2	RSA public key parameters	157
12.4	Diffie-Hellman key exchange parameters	157
12.5	Authentication tokens in the protocols mEACv2 and PCA	157
12.5.1	General	157
12.5.2	TDES	157
12.5.3	AES	157
12.5.4	Ephemeral Public Key Data Object	157
12.6	The compression function Comp()	158
12.7	DSA with ELC public key parameters	158
12.7.1	General	158
12.7.2	The plain format of a digital signature	159
12.7.3	The uncompressed encoding	159
12.8	ELC key exchange public parameters	160
13	Data structures	160
13.1	CRTs	160
13.1.1	CRT AT for the selection of internal private authentication keys	160
13.1.2	CRT AT for selection of internal authentication keys	161
13.1.3	CRT for selection of IFD's PuK.CAIFD.CS_AUT	161
13.1.4	CRT for selection of IFD's PuK.IFD.AUT	162

13.1.5	CRT AT for selection of the public DH / ECDH key parameters	162
13.1.6	CRT AT for selection of the PBM key parameters	162
13.1.7	GENERAL AUTHENTICATE DH key parameters used by the Privacy Protocol	163
13.1.8	CRT AT for selection of ICC's private authentication key	163
13.1.9	CRT for selection of IFD's PuK.IFD.AUT	164
13.1.10	CRT for selection of PrK.ICC.KA	164
13.2	Key transport device authentication protocol	164
13.2.1	EXTERNAL AUTHENTICATE	165
13.2.2	INTERNAL AUTHENTICATE	166
13.3	Privacy device authentication protocol	166
13.3.1	EXTERNAL AUTHENTICATE (DH case)	167
13.3.2	EXTERNAL AUTHENTICATE (ECDH case)	168
13.3.3	INTERNAL AUTHENTICATE (DH case)	169
13.3.4	INTERNAL AUTHENTICATE (ECDH case)	170
14	AlgIDs, Hash- and DSI Formats	171
14.1	Algorithm Identifiers and OIDs	171
14.2	Hash Input-Formats	172
14.2.1	PSO:HASH without command chaining	172
14.2.2	PSO:HASH with command Chaining	173
14.3	Formats of the Digital Signature Input (DSI)	173
14.3.1	DSI according to ISO/IEC 14888-2 (scheme 2)	174
14.3.2	DSI according to PKCS #1 V 1.5	175
14.3.3	Digest Info for SHA-X	176
14.3.4	DSI according to PKCS #1 V 2.x	178
14.3.5	DSA with DH key parameters	179
14.3.6	Elliptic Curve Digital Signature Algorithm - ECDSA	179
15	CV_Certificates and Key Management	180
15.1	Level of trust in a certificate	180
15.2	Key Management	180
15.3	Certificate types	181
15.3.1	Card Verifiable Certificates	181
15.3.2	Signature-Certificates	181
15.3.3	Authentication Certificates	181
15.4	Use of the public key extracted from a CV-certificate	181
15.5	Validity of the key extracted from a CV-certificate	182
15.6	CVC structure	183
15.6.1	Non-self-descriptive certificates	183
15.6.2	Self-descriptive certificates	183
15.7	Certificate Content	184
15.7.1	CPI-Certificate Profile Identifier	184
15.7.2	CAR-Certification Authority Reference DO	185
15.7.3	CHR-Certificate Holder Reference DO	186
15.7.4	CHA-Certificate Holder Authorization Data Object (CHA-DO)	187
15.7.5	Role identifier specifications	189
15.7.6	CHAT-Certificate Holder Authorization Template (CHAT)	192
15.7.7	OID -- Object identifier	192
15.7.8	CEDT -- Certificate Effective Date Template	192
15.7.9	CXDT -- Certificate Expiration date Template	192
15.8	Certificate signature	193
15.8.1	Non self-descriptive certificates	193
15.8.2	Self-descriptive certificates	194
15.9	Coding of the certificate content	194
15.9.1	Non self-descriptive certificates	194
15.9.2	Self-descriptive certificates	195
15.9.3	Self-descriptive certificates for elliptic curve cryptography	195
15.10	Steps of CVC verification	199
15.10.1	First round: CVC verification from a Root PuK	200
15.10.2	Subsequent round(s)	201
15.11	Commands to handle the CVC	201
15.12	C_CV.IFD.AUT (non self-descriptive)	201

15.13	C_CV.CA.CS-AUT (non self-descriptive)	203
15.14	C.ICC.AUT	204
15.15	Self-descriptive CV Certificate (Example)	204
15.15.1	Public Key	205
15.15.2	Certificate Holder Authorization Template	205
15.15.3	Certificate Extension	205
15.15.4	ECDSA Signature	206
16	Files	207
16.1	File structure	207
16.2	File IDs	208
16.3	EF.DIR	208
16.4	EF.SN.ICC	208
16.5	EF.DH	209
16.6	EF.ELC	209
16.7	EF.C.ICC.AUT	210
16.8	EF.C.CAICC.CS-AUT	211
16.9	EF.C_X509.CH.DS	211
16.10	EF.C_X509.CA.CS (DF.ESIGN)	212
16.11	EF.DM	212
17	Cryptographic Information Application	213
17.1	ESIGN cryptographic information layout example	214
17.1.1	EF.CIAInfo	215
17.1.2	EF.AOD	216
17.1.3	EF.PrKD	219
17.1.4	EF.PuKD	221
17.1.5	EF.CD	222
17.1.6	EF.DCOD	223
Annex A (normative) Algorithm Identifiers -- Coding and specification		226
Annex B (informative) Device authentication Protocol Properties		234
Annex C (informative) Personalization scenarios		236
Annex D (informative) OID values		238
D.1	OIDs for certificate signatures	238
D.2	OIDs for key transport protocol	239
D.3	OIDs for device authentication with privacy	239
D.4	OIDs for password based mechanisms	240
D.5	OIDs for mEAC protocol	241
D.5.1	OIDs for Chip Device Authentication	241
D.5.2	OIDs for Terminal Device Authentication	241
D.6	OIDs for privacy protocols	242
D.6.1	OIDs for Restricted Identification	242
D.6.2	OIDs for Restricted Identification	243
D.7	OIDs for mEAC based eServices	243
D.7.1	OIDs for Terminal Device Authentication in mEAC-based eServices	243
D.8	OIDs for the PCA mechanism	244
Annex E (informative) Build scheme for object identifiers defined by EN 14890		245
Bibliography		247