

DIN EN 419212-2:2018-09 (E)

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 2: Signature and Seal Services; English version EN 419212-2:2017

Inhalt	Seite
European foreword	5
1 Scope	7
2 Normative references	7
3 Terms and definitions	8
4 Symbols and abbreviations	8
5 Signature application	8
5.1 Application Flow	8
5.2 Trusted environment versus untrusted environment	10
5.3 Selection of ESIGN application	11
5.3.1 General	11
5.3.2 Exceptions for Secure Messaging	12
5.4 Selection of cryptographic information application	12
5.5 Concurrent usage of signature applications	12
5.5.1 General	12
5.5.2 Methods of channel selection	13
5.5.3 Security issues on multiple channels	13
5.6 Security environment selection	13
5.7 Key selection	13
5.8 Security Services	14
6 User verification	14
6.1 General	14
6.2 Knowledge based user verification	15
6.2.1 General	15
6.2.2 Explicit user verification	15
6.2.3 Password-based mechanisms	17
6.2.4 Presentation formats	17
6.2.5 Retry and Usage counters	17
6.2.6 Password Change	18
6.2.7 Reset of RC and setting a new password	18
6.3 Biometric user verification	19
6.3.1 General	19
6.3.2 Retrieval of the Biometric Information Template	20
6.3.3 Performing the biometric user verification	21
6.3.4 Reset of RC	23
7 Digital Signature Service	23
7.1 General	23
7.2 Signature generation algorithms	24
7.3 Activation of digital signature service	24
7.4 General aspects	24
7.5 Signature Generation	26
7.5.1 General	26

7.5.2	No hashing in Card	26
7.5.3	Partial hashing	26
7.5.4	All hashing in ICC.....	28
7.6	Selection of different keys, algorithms and input formats.....	29
7.6.1	General.....	29
7.6.2	Restore an existing SE.....	30
7.6.3	Setting the Hash Template (HT) of a current Security Environment (SE)	30
7.6.4	Modify the Digital Signature Template (DST) of a current Security Environment (SE)	31
7.7	Read certificates and certificate related information	31
7.7.1	General.....	31
7.7.2	Read certificate related CIOs.....	32
7.7.3	Read signer's certificate from ICC	32
7.7.4	Retrieval of the signer's certificate from a directory service.....	33
8	Password-based authentication protocols	34
8.1	General.....	34
8.2	Notation	34
8.3	Authentication steps	35
8.3.1	General.....	35
8.3.2	Step 1 — Reading the protocol relevant public parameters	36
8.3.3	Step 2 — Set PBM parameters and generate blinding point.....	37
8.3.4	Step 3 — Get encrypted nonce.....	38
8.3.5	Step 4.1 — Map nonce and compute generator point for generic mapping.....	39
8.3.6	Step 4.2 — Map nonce and compute generator point for integrated mapping	40
8.3.7	Step 5 — Generate session keys.....	42
8.3.8	Step 6 — Explicit key authentication	42
9	Secure Messaging	43
9.1	General.....	43
9.2	CLA byte	44
9.3	TLV coding of command and response message.....	44
9.4	Treatment of SM-Errors.....	44
9.5	Padding for checksum calculation	45
9.6	Send sequence counter (SSC).....	45
9.7	Message structure of Secure Messaging APDUs	45
9.7.1	Cryptograms.....	45
9.7.2	Cryptographic Checksums	47
9.7.3	Final command APDU construction.....	50
9.8	Response APDU protection.....	51
9.9	Use of TDES and AES.....	55
9.9.1	TDES/AES encryption/decryption	55
9.9.2	CBC mode.....	56
9.9.3	Retail MAC with TDES	56
9.9.4	EMAC with AES	57
9.9.5	CMAC with AES	58
10	Key Generation.....	58
10.1	General.....	58
10.2	Signature key and certificate generation	59
11	Key identifiers and parameters	60
11.1	General.....	60
11.2	Key identifiers (KID).....	61
11.2.1	General.....	61
11.2.2	Secret and private keys.....	61
11.3	Public Key parameters	61
11.3.1	General.....	61

11.3.2	RSA public key parameters	61
11.4	Diffie-Hellman key exchange parameters	62
11.5	Authentication tokens in the protocols mEACv2 and PCA.....	62
11.5.1	General	62
11.5.2	TDES	62
11.5.3	AES	62
11.5.4	Ephemeral Public Key Data Object.....	62
11.6	The compression function Comp().....	62
11.7	DSA with ELC public key parameters	63
11.7.1	General	63
11.7.2	The plain format of a digital signature	64
11.7.3	The uncompressed encoding.....	64
11.8	ELC key exchange public parameters.....	64
12	AlgIDs, Hash- and DSI Formats	65
12.1	General	65
12.2	Algorithm Identifiers and OIDs	65
12.3	Hash Input-Formats.....	65
12.3.1	General	65
12.3.2	PSO:HASH without command chaining.....	66
12.3.3	PSO:HASH with command Chaining.....	66
12.4	Formats of the Digital Signature Input (DSI)	67
12.4.1	General	67
12.4.2	DSI according to ISO/IEC 14888-2 (scheme 2).....	68
12.4.3	DSI according to PKCS #1 V 1.5.....	68
12.4.4	Digest Info for SHA-X Hash:Digest Info SHA:Digest Info	70
12.4.5	DSI according to PKCS #1 V 2.x MGF function.....	72
12.4.6	DSA with DH key parameters	73
12.4.7	Elliptic Curve Digital Signature Algorithm - ECDSA.....	73
13	Files.....	73
13.1	General	73
13.2	File structure.....	73
13.3	File IDs	74
13.4	EF.DIR.....	74
13.5	EF.SN.ICC	75
13.6	EF.DH	75
13.7	EF.ELC.....	76
13.8	EF.C.ICC.AUT.....	76
13.9	EF.C.CA _{ICC} .CS-AUT	77
13.10	EF.C_X509.CH.DS.....	77
13.11	EF.C_X509.CA.CS (DF.ESIGN)	78
13.12	EF.DM	78
14	Cryptographic Information Application.....	78
14.1	General	78
14.2	ESIGN cryptographic information layout example.....	80
14.2.1	General	80
14.2.2	EF.CIAInfo	81
14.2.3	EF.AOD	83
14.2.4	EF.PrKD	87
14.2.5	EF.PuKD	91
14.2.6	EF.CD.....	92
14.2.7	EF.DCOD	94
Annex A (normative)	Security environments.....	99
Annex B (informative)	Seals and Signatures.....	107