

DIN EN 419212-2:2016-11 (E)

Application Interface for Secure Elements for Electronic Identification,
Authentication and Trusted Services - Part 2: Signature and Seal Services; English
version FprEN 419212-2:2016

Contents

Page

European foreword.....	6
Introduction	7
1 Scope.....	8
2 Normative references.....	8
3 Terms and definitions	9
4 Symbols and abbreviations	9
5 Signature application.....	9
5.1 Application Flow.....	9
5.2 Trusted environment versus untrusted environment	11
5.3 Selection of E-SIGN application.....	12
5.3.1 General.....	12
5.3.2 Exceptions for Secure Messaging.....	13
5.4 Selection of cryptographic information application	13
5.5 Concurrent usage of signature applications.....	13
5.5.1 General.....	13
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	14
5.8 Security Services.....	14
6 User verification	15
6.1 General.....	15
6.2 Knowledge based user verification	15
6.2.1 General.....	15
6.2.2 Explicit user verification	16
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.....	27
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	29
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	31
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.....	33
8.1	General	33
8.2	Notation.....	34
8.3	Authentication steps.....	34
8.3.1	General	34
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.....	38
8.3.6	Step 4.2 — Map nonce and compute generator point for integrated mapping.....	39
8.3.7	Step 5 — Generate session keys	41
8.3.8	Step 6 — Explicit key authentication.....	42
9	Secure Messaging.....	43
9.1	General	43
9.2	CLA byte.....	43
9.3	TLV coding of command and response message	43
9.4	Treatment of SM-Errors	44
9.5	Padding for checksum calculation.....	44
9.6	Send sequence counter (SSC)	44
9.7	Message structure of Secure Messaging APDUs.....	45
9.7.1	Cryptograms	45
9.7.2	Cryptographic Checksums.....	46
9.7.3	Final command APDU construction	49
9.8	Response APDU protection	50
9.9	Use of TDES and AES	54
9.9.1	TDES/AES encryption/decryption.....	54
9.9.2	CBC mode	55
9.9.3	Retail MAC with TDES.....	55
9.9.4	EMAC with AES.....	56
9.9.5	CMAC with AES	57
10	Key Generation	57
10.1	General	57
10.2	Signature key and certificate generation.....	58
11	Key identifiers and parameters.....	59
11.1	General	59
11.2	Key identifiers (KID)	60

11.2.1	General.....	60
11.2.2	Secret and private keys.....	60
11.3	Public Key parameters.....	60
11.3.1	General.....	60
11.3.2	RSA public key parameters.....	60
11.4	Diffie-Hellman key exchange parameters.....	60
11.5	Authentication tokens in the protocols mEACv2 and PCA	61
11.5.1	General.....	61
11.5.2	TDES.....	61
11.5.3	AES.....	61
11.5.4	Ephemeral Public Key Data Object	61
11.6	The compression function Comp()	61
11.7	DSA with ELC public key parameters.....	62
11.7.1	General.....	62
11.7.2	The plain format of a digital signature.....	62
11.7.3	The uncompressed encoding.....	63
11.8	ELC key exchange public parameters	63
12	AlgIDs, Hash- and DSI Formats.....	63
12.1	General.....	63
12.2	Algorithm Identifiers and OIDs.....	64
12.3	Hash Input-Formats	64
12.3.1	General.....	64
12.3.2	PSO:HASH without command chaining	65
12.3.3	PSO:HASH with command Chaining	65
12.4	Formats of the Digital Signature Input (DSI).....	66
12.4.1	General.....	66
12.4.2	DSI according to ISO/IEC 14888-2 (scheme 2)	66
12.4.3	Digest Info for SHA-X Hash:Digest Info SHA:Digest Info.....	68
12.4.4	DSI according to PKCS #1 V 2.x MGF function	70
12.4.5	DSA with DH key parameters.....	71
12.4.6	Elliptic Curve Digital Signature Algorithm - ECDSA	71
13	Files	71
13.1	General.....	71
13.2	File structure	71
13.3	File IDs.....	72
13.4	EF.DIR.....	72
13.5	EF.SN.ICC.....	73
13.6	EF.DH	73
13.7	EF.ELC	74
13.8	EF.C.ICC.AUT.....	74
13.9	EF.C.CA _{ICC} .CS-AUT	75
13.10	EF.C_X509.CH.DS	75
13.11	EF.C_X509.CA.CS (DF.ESIGN)	75
13.12	EF.DM.....	76
14	Cryptographic Information Application	76
14.1	General.....	76
14.2	ESIGN cryptographic information layout example	79
14.2.1	General.....	79
14.2.2	EF.CIAInfo.....	79
14.2.3	EF.AOD.....	81
14.2.4	EF.PrKD	86
14.2.5	EF.PuKD	89

14.2.6 EF.CD.....	91
14.2.7 EF.DCOD.....	93
Annex A (normative) Security environments.....	98
A.1 General	98
A.2 Definition of CRTs (examples)	99
A.2.1 General	99
A.2.2 CRT for Authentication (AT).....	99
A.2.3 CRT for Cryptographic Checksum (CCT)	101
A.2.4 CRT for Digital Signature (DST).....	101
A.2.5 CRT for confidentiality (CT).....	102
A.3 Security Environments (example).....	103
A.3.1 General	103
A.3.2 Security Environment #10	104
A.3.3 Security Environment #11	104
A.4 Coding of access conditions (example).....	104
A.4.1 General	104
A.4.2 Access Conditions	105
Annex B (informative) Seals and Signatures.....	106
B.1 General	106
B.2 Example of a seal creation/verification	106
B.3 Definition of a Seal versus signature	106
B.4 Verifying a seal vs. signature	107
B.5 Seal creation specifications.....	107
B.5.1 General	107
B.5.2 User verification.....	107
B.5.3 Automated sealing.....	107
B.5.4 Delegated sealing.....	107
B.5.5 Operating conditions.....	108
Annex C (informative) Remote Signatures	109
C.1 Introduction.....	109
C.2 Architecture.....	109
C.2.1 General	109
C.2.2 Static view.....	110
C.2.3 Dynamic View.....	110
Bibliography	112