

DIN EN 419212-3:2016-11 (E)

Application Interface for Secure Elements for Electronic Identification,
Authentication and Trusted Services - Part 3: Device authentication protocols;
English version FprEN 419212-3:2016

Contents

Page

European foreword.....	5
Introduction	6
1 Scope.....	7
2 Normative references.....	7
3 Device authentication.....	7
3.1 General.....	7
3.2 Asymmetric Authentication introduction	8
3.3 Certification authorities and certificates	9
3.3.1 Certificate chains.....	9
3.3.2 Usage of link certificates.....	9
3.4 Authentication environments	10
3.4.1 SCA in trusted environment	10
3.4.2 SCA in untrusted environment.....	10
3.4.3 Specification of the environment	11
3.4.4 Display message mechanism	11
3.4.5 Additional authentication environments.....	11
3.5 Key transport and key agreement mechanisms	11
3.6 Device authentication with privacy protection.....	12
3.6.1 General.....	12
3.6.2 Authentication steps	12
3.7 Privacy constrained Modular EAC (mEAC) protocol with non-traceability feature	29
3.7.1 General.....	29
3.7.2 Example for traceability case.....	30
3.7.3 Notation	30
3.7.4 Authentication steps	31
3.7.5 Unlinkability Mechanism with individual private keys	45
3.8 Symmetric authentication scheme	52
3.8.1 General.....	52
3.8.2 Authentication steps	53
3.8.3 Session Key creation	56
3.9 Key transport protocol based on RSA.....	57
3.9.1 General.....	57
3.9.2 Authentication Steps.....	59
3.9.3 Session Key creation	67
3.10 Compute Session keys from key seed $K_{IFD/ICC}$	67
3.10.1 General.....	67
3.10.2 Generation of key data	67
3.10.3 Partitioning of the key data.....	68
3.10.4 Algorithm and method specific definition for key derivation	68
3.10.5 Key derivation from passwords.....	70
3.11 Compute send sequence counter SSC.....	71
3.12 Post-authentication phase	72

3.13	Ending the secure session.....	72
3.13.1	General	72
3.13.2	Example for ending a secure session.....	72
3.13.3	Rules for ending a secure session	73
3.14	Reading the Display Message	73
3.15	Updating the Display Message	75
4	Data structures	76
4.1	General	76
4.2	CRTs.....	76
4.2.1	General	76
4.2.2	CRT AT for the selection of internal private authentication keys.....	76
4.2.3	CRT AT for selection of internal authentication keys.....	77
4.2.4	CRT for selection of IFD's PuK.CA _{IFD} .CS_AUT	77
4.2.5	CRT for selection of IFD's PuK.IFD.AUT	78
4.2.6	CRT AT for selection of the public DH / ECDH key parameters	78
4.2.7	GENERAL AUTHENTICATE DH key parameters used by the Privacy Protocol	78
4.2.8	CRT AT for selection of ICC's private authentication key.....	79
4.2.9	CRT for selection of IFD's PuK.IFD.AUT	79
4.2.10	CRT for selection of PrK.ICC.KA.....	79
4.3	Key transport device authentication protocol.....	80
4.3.1	EXTERNAL AUTHENTICATE	80
4.3.2	INTERNAL AUTHENTICATE	81
4.4	Privacy device authentication protocol.....	81
4.4.1	EXTERNAL AUTHENTICATE (DH case)	81
4.4.2	EXTERNAL AUTHENTICATE (ECDH case)	82
4.4.3	INTERNAL AUTHENTICATE (DH case).....	83
4.4.4	INTERNAL AUTHENTICATE (ECDH case).....	83
5	CV_Certificates and Key Management	84
5.1	General	84
5.2	Level of trust in a certificate	84
5.3	Key Management.....	84
5.4	Certificate types	85
5.4.1	Card Verifiable Certificates	85
5.4.2	Signature-Certificates	86
5.4.3	Authentication Certificates	86
5.5	Use of the public key extracted from a CV-certificate.....	86
5.6	Validity of the key extracted from a CV-certificate.....	86
5.7	Structure of CVC.....	87
5.7.1	General	87
5.7.2	Non-self-descriptive certificates	87
5.7.3	Self-descriptive certificates	88
5.8	Certificate Content.....	88
5.8.1	General	88
5.8.2	CAR-Certification Authority Reference DO.....	90
5.8.3	CHR-Certificate Holder Reference DO.....	91
5.8.4	CHA-Certificate Holder Authorization Data Object (CHA-DO).....	92
5.8.5	Role identifier specifications.....	93
5.8.6	User and service provider authentication.....	95
5.8.7	CHAT-Certificate Holder Authorization Template (CHAT).....	96
5.8.8	OID — Object identifier	96
5.8.9	CEDT — Certificate Effective Date Template	96
5.8.10	CXDT — Certificate Expiration date Template.....	96

5.9	Certificate signature.....	97
5.9.1	General.....	97
5.9.2	Non self-descriptive certificates.....	97
5.9.3	Self-descriptive certificates.....	98
5.10	Coding of the certificate content.....	98
5.10.1	Non self-descriptive certificates.....	98
5.10.2	Self-descriptive certificates.....	99
5.10.3	Self-descriptive certificates for elliptic curve cryptography.....	99
5.11	Steps of CVC verification	103
5.11.1	General.....	103
5.11.2	First round: CVC verification from a Root PuK.....	104
5.11.3	Subsequent round(s)	104
5.12	Commands to handle the CVC	105
5.13	C_CV.IFD.AUT (non self-descriptive)	105
5.14	C_CV.CA.CS-AUT (non self-descriptive).....	106
5.15	C.ICC.AUT	107
5.16	Self-descriptive CV Certificate (Example)	108
5.16.1	General.....	108
5.16.2	Public Key	108
5.16.3	Certificate Holder Authorization Template.....	109
5.16.4	Certificate Extension	109
5.16.5	ECDSA Signature	110
	Annex A (informative) Device authentication Protocol Properties.....	111
	Bibliography.....	113