

DIN EN 419212-5:2018-06 (E)

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 5: Trusted eService; English version EN 419212-5:2018

Contents	Page
European foreword.....	4
Introduction	5
1 Scope.....	6
2 Normative references.....	6
3 Terms and definitions	6
4 Abbreviations and notation.....	6
5 Additional Service Selection.....	6
6 Client/Server Authentication	10
6.1 General.....	10
6.2 Client/Server protocols	10
6.3 Steps preceding the client/server authentication	11
6.4 Padding format	11
6.4.1 PKCS #1 v 1-5 Padding.....	11
6.4.2 PKCS #1 V 2.x (PSS) Padding.....	12
6.4.3 Building the DSI on ECDSA	13
6.5 Client/Server protocol	13
6.5.1 General.....	13
6.5.2 Step 1 — Read certificate	14
6.5.3 Step 2 — Set signing key for client/server internal authentication	15
6.5.4 Step 3 — Internal authentication	16
6.5.5 Client/Server authentication execution flow.....	18
6.5.6 Command data field for the client server authentication	19
7 Role Authentication.....	20
7.1 Role Authentication of the card	20
7.2 Role Authentication of the server	20
7.3 Symmetrical external authentication.....	20
7.3.1 Protocol	20
7.3.2 Description of the cryptographic mechanisms	24
7.3.3 Role description.....	25
7.4 Asymmetric external authentication	25
7.4.1 Protocol based on RSA.....	25
8 Symmetric key transmission between a remote server and the ICC.....	28
8.1 Steps preceding the key transport.....	28
8.2 Key encryption with RSA	28
8.2.1 General.....	28
8.2.2 PKCS#1 v1.5 padding.....	30
8.2.3 OAEP padding.....	30
8.2.4 Execution flow	31
8.3 Diffie-Hellman key exchange for key encipherment.....	33
8.3.1 General.....	33
8.3.2 Execution flow	35

9	Signature verification	37
9.1	General.....	37
9.2	Signature verification execution flow.....	37
9.2.1	General	37
9.2.2	Step 1: Receive Hash.....	37
9.2.3	Step 2: Select verification key	39
9.2.4	Step 3: Verify digital signature	39
10	Certificates for additional services	40
10.1	File structure.....	40
10.2	File structure.....	41
10.3	EF.C_X509.CH.DS.....	41
10.4	EF.C.CH.AUT	41
10.5	EF.C.CH.KE.....	42
10.6	Reading Certificates and the public key of CAs.....	42
11	APDU data structures.....	42
11.1	Algorithm Identifiers.....	42
11.2	General	42
11.3	CRTs.....	43
11.3.1	General	43
11.3.2	CRT DST for selection of ICC's private client/server auth. key	43
11.3.3	CRT AT for selection of ICC's private client/server auth. key.....	43
11.3.4	CRT CT for selection of ICC's private key.....	44
11.3.5	CRT DST for selection of IFD's public key (signature verification)	44
	Annex A (informative) Security Service Descriptor Templates.....	45
	Annex B (informative) Example of DF.CIA	51
	Bibliography	58