

DIN EN 419212-3:2017-11 (E)

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 3: Device authentication protocols; English version EN 419212-3:2017

Contents	Page
European foreword.....	5
Introduction	6
1 Scope.....	7
2 Normative references.....	7
3 Terms and definitions	7
4 Symbols and abbreviations	15
5 Management Summary	18
5.1 Motivation.....	18
5.2 What is in behind?.....	19
5.3 Use Cases	20
5.4 Privacy and Security.....	21
5.5 Overview - EU Directive and Regulation.....	21
5.6 Facts and Figures.....	22
Annex A (normative) Algorithm Identifiers — Coding and specification	23
Table A.1 — AlgIDs.....	24
Table A.2 — Coding of byte 3 and 4 (for hash calculation - byte 2 = '01' to '0F').....	24
Table A.3 — Coding of byte 3 (for digital signature computation - byte 2 = '1x')	25
Table A.4 — Coding of byte 4 (for digital signature computation - byte 2 = '1x')	25
Table A.5 — Coding of byte 3 (for C/S authentication - byte 2 = '2x').....	25
Table A.6 — Coding of byte 4 (for C/S authentication - byte 2 = '2x').....	25
Table A.7 — Coding of byte 3 (for key decipherment - byte 2 = '3x').....	26
Table A.8 — Coding of byte 4 (for key decipherment - byte 2 = '3x').....	26
Table A.9 — Coding of byte 3 (for authentication protocol - byte 2 = '4x').....	26
Table A.10 — Coding of byte 4 (for authentication protocol - byte 2 = '4x')	28
Table A.11 — Coding of byte 3 (for digital signature verification - byte 2 = '9x').....	28
Table A.12 — Coding of byte 4 (for digital signature verification - byte 2 = '9x').....	28
Table A.13 — Coding of byte 3 (for role authentication - byte 2 = 'Ax').....	29
Table A.14 — Coding of byte 3 (for privacy features - byte 2 = 'Cx')	29
Table A.15 — Coding of byte 4 (for role authentication - byte 2 = 'Ax').....	29
Table A.16 — Coding of byte 4 (for privacy feature - byte 2 = 'Cx')	29
Table A.17 — 1-byte Algorithm-ID coding.....	30
Annex B (informative) OID values.....	32
B.1 OIDs for certificate signatures.....	32
Table B.1 — Object identifier values related to a public key in a certificate.....	32
B.2 OIDs for key transport protocol.....	32

Table B.2 — Object identifier values for the key transport protocol.....	33
B.3 OIDs for device authentication with privacy	33
Table B.3 — Object identifier values for device authentication with privacy	33
B.4 OIDs for password based mechanisms	34
Table B.4 — PACE OIDs	34
B.5 OIDs for mEAC protocol.....	34
B.5.1 OIDs for Chip Device Authentication	34
Table B.5 — Chip Device Authentication (DES/AES).....	34
B.5.2 OIDs for Terminal Device Authentication.....	35
Table B.6 — Terminal Authentication (RSA/ECDSA).....	35
B.6 OIDs for privacy protocols.....	36
B.6.1 OIDs for Restricted Identification.....	36
Table B.7 — OIDs for Restricted Identification.....	36
Table B.8 — OIDs for use in certificate extension.....	36
B.6.2 OIDs for Restricted Identification.....	36
Table B.9 — OIDs for use in auxiliary data verification.....	36
B.7 OIDs for mEAC based eServices - OIDs for Terminal Device Authentication in mEAC- based eServices	36
Table B.10 — OID values for the mEAC Terminal Authentication.....	36
B.8 OIDs for the PCA mechanism	37
Table B.11 — OID for the PCA mechanism.....	37
Annex C (informative) Build scheme for object identifiers defined by EN 419212	38
Figure C.1 — Build scheme for mEAC OIDs.....	39
Annex D (informative) Tutorial on Signature Technology	40
D.1 General	40
D.2 Signatures and keys	41
Table D.1 — Generating RSA keys.....	42
D.3 Signing documents	42
D.4 About certificates.....	43
D.5 The “chain of trust”	44
D.6 Multi step signature generation.....	44
D.6.1 General	44
D.6.2 Device authentication protocols	44
D.6.3 Secure Messaging.....	45
D.6.4 Password based device authentication	45
D.6.5 PIN entry	45
D.7 Signing the document.....	46

Annex E (informative) Guide to the EN 419212	47
E.1 From EN 14890 to EN 419212.....	47
E.2 The EU Regulation 910/2014 and the Directive 1999/93/EU.....	48
E.3 Secure Elements (SE)	48
E.4 Specific protection required for contactless integrated circuits	49
E.4.1 General.....	49
E.4.2 Eavesdropping attacks	49
E.4.3 Skimming attack.....	49
E.4.4 Relay attack.....	49
E.4.5 Denial of Service (DoS) attack	49
E.4.6 Countermeasures.....	50
E.5 The Human-Machine Interface.....	50
E.6 Communications with the ICC and with the user	50
E.7 Information that should be initially communicated by the ICC to the IFD	51
E.8 User agreement using PINs.....	51
E.9 PIN unlocking.....	52
E.10 PIN change	52
E.11 User agreement using biometric information	52
E.12 User control using a local display and a local keyboard	52
E.13 Card applications	53
E.13.1 General.....	53
E.13.2 eSign card application	53
E.13.3 Device authentication mechanisms.....	53
E.13.4 Document Decryption mechanisms	53
E.14 Signature-/Seal functions.....	53
E.14.1 General.....	53
E.14.2 Digital signature/seal creation	54
E.14.3 Digital signature verification.....	54
E.14.4 Identification and authentication service.....	54
Bibliography.....	56