

# DIN EN 419212-2:2015-03 (E)

## Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional services; English version EN 419212-2:2014

---

<b>Contents</b>		<b>Page</b>
Foreword .....		5
1	Scope .....	7
2	Normative references .....	7
3	Terms and definitions .....	7
4	Abbreviations and notation .....	9
5	Additional Service Selection .....	11
6	Client/Server Authentication .....	14
6.1	Client/Server protocols .....	14
6.2	Steps preceding the client/server authentication .....	15
6.3	Padding format .....	15
6.3.1	PKCS #1 v 1-5 Padding .....	15
6.3.2	PKCS #1 V 2.x (PSS) Padding .....	16
6.3.3	Building the DSI on ECDSA .....	17
6.4	Client/Server protocol .....	18
6.4.1	Step 1 -- Read certificate .....	18
6.4.2	Step 2 -- Set signing key for client/server internal authentication .....	19
6.4.3	Step 3 -- Internal authentication .....	20
6.4.4	Client/Server authentication execution flow .....	22
6.4.5	Command data field for the client server authentication .....	24
7	Role Authentication .....	25
7.1	Role Authentication of the card .....	25
7.2	Role Authentication of the server .....	25
7.3	Symmetrical external authentication .....	25
7.3.1	Protocol .....	25
7.3.2	Description of the cryptographic mechanisms .....	30
7.3.3	Role description .....	30
7.4	Asymmetric external authentication .....	31
7.4.1	Protocol based on RSA .....	31
7.4.2	Protocol based on modular Enhanced Role Authentication (mERA) .....	34
8	Symmetric key transmission between a remote server and the ICC .....	49
8.1	Steps preceding the key transport .....	49
8.2	Key encryption with RSA .....	49
8.2.1	PKCS#1 v1.5 padding .....	50
8.2.2	OAEP padding .....	50
8.2.3	Execution flow .....	51
8.3	Diffie-Hellman key exchange for key encipherment .....	54
8.3.1	Execution flow .....	56
9	Signature verification .....	58
9.1	Signature verification execution flow .....	58
9.1.1	Step 1: Receive Hash .....	59
9.1.2	Step 2: Select verification key .....	60
9.1.3	Step 3: Verify digital signature .....	61

10	Certificates for additional services .....	62
10.1	File structure .....	63
10.2	EF.C_X509.CH.DS .....	63
10.3	EF.C.CH.AUT .....	63
10.4	EF.C.CH.KE .....	63
10.5	Reading Certificates and the public key of CAs .....	64
11	Privacy Context functions .....	65
11.1	Introduction .....	65
11.2	Auxiliary Data Comparison .....	65
11.2.1	Presentation of the auxiliary data .....	66
11.2.2	Age Verification .....	68
11.2.3	Document Validation .....	69
11.3	Restricted Identification .....	70
11.3.1	Command APDU for Step RI:1 .....	73
11.3.2	Command APDU for Step RI:2 .....	74
11.4	eServices with trusted third party protocol .....	77
11.4.1	mERA-based eServices with trusted third party protocol .....	78
11.4.2	mEAC-based eServices with trusted third party .....	83
11.5	eServices with two party protocols .....	86
11.5.1	mEAC-based eServices with on-line two party protocol .....	86
11.5.2	mEAC-based eServices with off-line two party protocol .....	87
12	APDU data structures .....	89
12.1	Algorithm Identifiers .....	89
12.2	CRTs .....	89
12.2.1	CRT DST for selection of ICC's private client/server auth. key .....	89
12.2.2	CRT AT for selection of ICC's private client/server auth. key .....	89
12.2.3	CRT CT for selection of ICC's private key .....	90
12.2.4	CRT DST for selection of IFD's public key (signature verification) .....	90
Annex A (normative) Security Service Descriptor Templates .....		91
A.1	Security Service Descriptor Concept .....	91
A.2	SSD Data Objects .....	92
A.2.1	DO Extended Header List, tag `4D' .....	92
A.2.2	DO Instruction set mapping (ISM), tag `80' .....	92
A.2.3	DO Command to perform (CTP), tag `52' (refer to ISO/IEC 7816-6) .....	92
A.2.4	DO Algorithm object identifier (OID), tag `06' (refer to ISO/IEC 7816-6) .....	92
A.2.5	DO Algorithm reference, tag `81' .....	92
A.2.6	DO Key reference, tag `82' .....	93
A.2.7	DO FID key file, tag `83' .....	93
A.2.8	DO Key group, tag `84' .....	93
A.2.9	DO FID base certificate file, tag `85' .....	93
A.2.10	DO FID adjoined certificate file, tag `86' .....	93
A.2.11	DO Certificate reference, tag `87' .....	93
A.2.12	DO Certificate qualifier, tag `88' .....	93
A.2.13	DO FID for file with public key of the certification authority PK(CA), tag `89' .....	93
A.2.14	DO PIN usage policy, tag `5F2F' .....	93
A.2.15	DO PIN reference, tag `8A' .....	94
A.2.16	DO Application identifier (AID), tag `4F' (refer to ISO/IEC 7816-6) .....	94
A.2.17	DO CLA coding, tag `8B' .....	94
A.2.18	DO Status information (SW1-SW2), tag `42' (refer to ISO/IEC 7816-6) .....	94
A.2.19	DO Discretionary data, tag `53' (refer to ISO/IEC 7816-6) .....	94
A.2.20	DO SE number, tag `8C' .....	94
A.2.21	DO SSD profile identifier, tag `8D' .....	95
A.2.22	DO FID mapping, tag `8E' .....	95
A.3	Location of the SSD templates .....	95
A.4	Examples for SSD templates .....	95
Annex B (informative) Security environments .....		97

<b>B.1</b>	<b>Definition of CRTs (examples)</b> .....	<b>98</b>
<b>B.1.1</b>	<b>CRT for Authentication (AT)</b> .....	<b>99</b>
<b>B.1.2</b>	<b>CRT for Cryptographic Checksum (CCT)</b> .....	<b>100</b>
<b>B.1.3</b>	<b>CRT for Digital Signature (DST)</b> .....	<b>101</b>
<b>B.1.4</b>	<b>CRT for confidentiality (CT)</b> .....	<b>102</b>
<b>B.2</b>	<b>Security Environments (example)</b> .....	<b>103</b>
<b>B.2.1</b>	<b>Security Environment #10</b> .....	<b>103</b>
<b>B.2.2</b>	<b>Security Environment #11</b> .....	<b>104</b>
<b>B.3</b>	<b>Coding of access conditions (example)</b> .....	<b>104</b>
<b>B.3.1</b>	<b>Access Conditions</b> .....	<b>105</b>
<b>B.3.2</b>	<b>Access rule references</b> .....	<b>106</b>
<b>B.3.3</b>	<b>Access conditions for EF.ARR</b> .....	<b>107</b>
<b>B.3.4</b>	<b>EF.ARR records</b> .....	<b>107</b>
<b>Annex C (normative) Algorithm Identifiers -- Coding and specification</b> .....		<b>110</b>
<b>Annex D (informative) Example of DF.CIA</b> .....		<b>117</b>
<b>Annex E (informative) Build scheme for object identifiers defined by EN 14890</b> .....		<b>122</b>
<b>Bibliography</b> .....		<b>124</b>