



NSAI
Standards

Irish Standard
I.S. EN 14890-1:2008

Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services

I.S. EN 14890-1:2008

Incorporating amendments/corrigenda issued since publication:

<i>This document replaces:</i> S.R. CWA 14890-1:2004	<i>This document is based on:</i> EN 14890-1:2008 CWA 14890-1:2004	<i>Published:</i> 3 December, 2008 18 March, 2007
This document was published under the authority of the NSAI and comes into effect on: 2 February, 2009		ICS number: 35.240.15
NSAI 1 Swift Square, Northwood, Santry Dublin 9	T +353 1 807 3800 F +353 1 807 3838 E standards@nsai.ie W NSAI.ie	Sales: T +353 1 857 6730 F +353 1 857 6729 W standards.ie
		Price Code: AF
Údarás um Chaighdeáin Náisiúnta na hÉireann		

English Version

Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services

Interface applicative des cartes à puces utilisées comme
dispositifs de création de signature numérique sécurisés -
Partie 1 : Services de bases

Anwendungsschnittstelle für Chipkarten, die zur Erzeugung
qualifizierter elektronischer Signaturen verwendet werden -
Teil 1: Allgemeine Dienste

This European Standard was approved by CEN on 27 September 2008.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Contents

Foreword.....	6
1 Scope	7
2 Normative references	8
3 Terms and definitions	8
4 Symbols and abbreviations	11
5 Signature application	13
5.1 Application Flow	13
5.2 Trusted environment versus untrusted environment	16
5.3 Selection of E-SIGN application	16
5.3.1 General.....	16
5.3.2 Exceptions for Secure Messaging	17
5.4 Selection of cryptographic information application	17
5.5 Concurrent usage of signature applications	17
5.5.1 General.....	17
5.5.2 Methods of channel selection	17
5.5.3 Security issues on multiple channels	17
5.6 Security environment selection	18
5.7 Key selection.....	18
5.8 Basic Security Services	18
6 User verification.....	19
6.1 General.....	19
6.2 Knowledge based user verification	19
6.2.1 General.....	19
6.2.2 Explicit user verification	20
6.2.3 Password related mechanisms	20
6.2.4 Presentation formats	21
6.2.5 Retry counters.....	21
6.2.6 Password Change.....	21
6.2.7 Reset of RC and setting a new password	22
6.3 Biometric user verification	23
6.3.1 General.....	23
6.3.2 Retrieval of the Biometric Information Template	24
6.3.3 Performing the biometric user verification	25
6.3.4 Reset of RC.....	27
7 Digital Signature Service	28
7.1 Signature generation algorithms	28
7.2 Activation of digital signature service.....	28
7.3 General aspects	29
7.4 Signature Generation	30
7.4.1 No hashing in Card	30
7.4.2 Partial hashing	31
7.4.3 All hashing in Card	32
7.5 Selection of different keys, algorithms and input formats	33
7.5.1 Restore an existing SE.....	34
7.5.2 Modify the HT of a current SE	34
7.5.3 Modify the DST of a current SE	35
7.6 Read certificates and certificate related information.....	36
7.6.1 Read certificate related CIOs.....	36
7.6.2 Read signer's certificate from ICC	36
7.6.3 Retrieval of the signer's certificate from a directory service	37

8	Device authentication	38
8.1	Certification authorities and certificates.....	38
8.1.1	Certificate chains.....	38
8.1.2	Usage of cross certificates.....	39
8.2	Authentication environments.....	40
8.2.1	SCA in trusted environment.....	40
8.2.2	SCA in untrusted environment	41
8.2.3	Specification of the environment.....	41
8.2.4	Display message mechanism	41
8.2.5	Additional authentication environments.....	41
8.3	Key transport and key agreement mechanisms	41
8.4	Key transport protocol based on RSA	42
8.4.1	Authentication Steps.....	43
8.4.2	Session Key creation	52
8.5	Device authentication with privacy protection.....	52
8.5.1	Authentication steps	53
8.6	Privacy constrained Modular EAC (mEAC) protocol with non-traceability feature (based on elliptic curves)	70
8.6.1	Example for traceability case	70
8.6.2	Notation	70
8.6.3	Authentication steps	71
8.7	Asymmetric Authentication summary.....	82
8.8	Symmetric authentication scheme	83
8.8.1	Authentication steps	83
8.8.2	Session Key creation	86
8.9	Compute Session keys from key seed $K_{IFD/ICC}$	87
8.9.1	Compute TDES session keys	87
8.9.2	Compute AES-128 session keys for CBC mode and EMAC	88
8.9.3	Compute AES-128 session keys for CBC mode and CMAC	88
8.10	Compute send sequence counter SSC	89
8.11	Post-authentication phase.....	89
8.12	Ending the secure session	89
8.12.1	Example for ending a secure session	89
8.12.2	Rules for ending a secure session	89
8.13	Reading the Display Message	90
8.14	Updating the Display Message	92
9	Secure messaging	93
9.1	CLA byte	93
9.2	TLV coding of command and response message	93
9.3	Treatment of SM-Errors	94
9.4	Padding for checksum calculation	94
9.5	Send sequence counter (SSC)	94
9.6	Message structure of Secure Messaging APDUs	95
9.6.1	Cryptograms	95
9.6.2	Cryptographic Checksums.....	97
9.6.3	Final command APDU construction	100
9.7	Response APDU protection.....	101
9.8	Use of TDES and AES	107
9.8.1	TDES/AES encryption/decryption.....	107
9.8.2	CBC mode	108
9.8.3	Retail MAC with TDES.....	108
9.8.4	EMAC with AES	109
9.8.5	CMAC with AES	110
10	Key Generation	111
10.1	Key generation and export using PrK.ICC.AUT	111
10.2	Key generation and export with dynamic or static SM.....	111
10.3	Write certificates.....	112
10.4	Setting keys in static secure messaging	112
11	Key identifiers and parameters	112

11.1	Key identifiers (KID).....	112
11.2	Public Key parameters	112
11.3	DSA with ELC public key parameters.....	113
11.4	RSA Diffie-Hellman key exchange parameters.....	114
11.5	ELC key exchange parameters.....	114
12	Data structures.....	115
12.1	CRTs.....	115
12.1.1	CRT AT for selection of internal authentication keys	115
12.1.2	CRT for selection of IFD's PuK.CA _{IFD} .CS_AUT	115
12.1.3	CRT for selection of IFD's PuK.IFD.AUT	116
12.1.4	CRT AT for selection of the public DH key parameters	116
12.1.5	GENERAL AUTHENTICATE DH key parameters	116
12.1.6	CRT AT for selection of ICC's private authentication key	116
12.1.7	CRT for selection of IFD's PuK.IFD.AUT	117
12.1.8	CRT for selection of PrK.ICC.KA.....	117
12.2	Key transport device authentication protocol	117
12.2.1	EXTERNAL AUTHENTICATE	117
12.2.2	INTERNAL AUTHENTICATE.....	118
12.3	Privacy device authentication protocol.....	119
12.3.1	EXTERNAL AUTHENTICATE	119
12.3.2	INTERNAL AUTHENTICATE.....	120
13	AlgIDs, Hash- and DSI Formats.....	121
13.1	Algorithm Identifiers and OIDs.....	121
13.2	Hash Input-Formats	122
13.2.1	PSO:HASH without command chaining	123
13.2.2	PSO:HASH with command Chaining	124
13.3	Formats of the Digital Signature Input (DSI).....	124
13.3.1	DSI according to ISO/IEC 14888-2 (scheme 2).....	124
13.3.2	DSI according to PKCS #1 V 1.5.....	125
13.3.3	Digest Info for SHA-X	127
13.3.4	DSI according to PKCS #1 V 2.x.....	128
13.3.5	DSA with DH key parameters	130
13.3.6	Elliptic Curve Digital Signature Algorithm - ECDSA	130
14	CV_Certificates and Key Management	130
14.1	Level of trust in a certificate	130
14.2	Key Management	130
14.3	Card Verifiable Certificates	131
14.3.1	Signature-Certificates	132
14.3.2	Authentication Certificates	132
14.4	Use of the public key extracted from the certificate	132
14.5	Validity of the key extracted from a certificate	132
14.6	Structure of CVC	133
14.6.1	Non-self-descriptive certificates	133
14.6.2	Self-descriptive certificates	134
14.7	Certificate Content.....	134
14.7.1	CPI-Certificate Profile Identifier.....	135
14.7.2	CAR-Certification Authority Reference	136
14.7.3	CHR-Certificate Holder Reference	137
14.7.4	CHA-Certificate Holder Authorization (CHA)	138
14.7.5	Role identifier specifications	139
14.7.6	CHAT-Certificate Holder Authorization Template (CHAT)	142
14.7.7	OID — Object identifier	142
14.7.8	CED — Certificate Effective Date	144
14.7.9	CXD — Certificate Expiration date	144
14.8	Certificate signature	144
14.8.1	Non self-descriptive certificates	144
14.8.2	Self descriptive certificates	146
14.9	Coding of the certificate content.....	146
14.9.1	Non self-descriptive certificates	146

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- Looking for additional Standards? Visit Intertek Inform Infostore
 - Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation
-