



# SLOVENSKI STANDARD

## SIST EN 14890-1:2009

01-april-2009

---

**Uporabniški vmesnik za pametne kartice, ki se uporabljajo kot naprave za izdelovanje varnega podpisa - 1. del: Osnovne storitve**

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

Anwendungsschnittstelle für Chipkarten, die zur Erzeugung gesicherter Signaturen verwendet werden — Teil 1: Basis-Anforderungen

Interfaces applicatives des cartes à puce utilisées pour le création de signatures électroniques sécurisées - Partie 1: Services de base

<https://standards.iteh.ai/catalog/standards/sist/67862784-9b17-41c3-a187-7ce6a337b157/sist-en-14890-1-2009>

**Ta slovenski standard je istoveten z: EN 14890-1:2008**

---

**ICS:**

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices
-----------	---	--

**SIST EN 14890-1:2009**

**en,de**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

SIST EN 14890-1:2009

<https://standards.iteh.ai/catalog/standards/sist/67862784-9b17-41c3-a187-7ce6a337b157/sist-en-14890-1-2009>

EUROPEAN STANDARD  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

**EN 14890-1**

December 2008

ICS 35.240.15

Supersedes CWA 14890-1:2004

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.

[SIST EN 14890-1:2009](https://standards.iteh.ai/catalog/standards/sist/67862784-9b17-41c3-a187-7ce6a337b157/sist-en-14890-1-2009)

<https://standards.iteh.ai/catalog/standards/sist/67862784-9b17-41c3-a187-7ce6a337b157/sist-en-14890-1-2009>



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 $K_{ED,ICC}$ .....	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

## EN 14890-1:2008 (E)

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 <sub>IFD</sub> .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

14.9.2	Self-descriptive certificates.....	147
14.9.3	Self-descriptive certificates for elliptic curve cryptography.....	147
14.10	Steps of CVC verification.....	150
14.10.1	First round: CVC verification from a Root PuK.....	151
14.10.2	Subsequent round(s) .....	152
14.11	Commands to handle the CVC .....	152
14.12	C_CV.IFD.AUT (non self-descriptive) .....	152
14.13	C_CV.CA.CS-AUT (non self-descriptive).....	154
14.14	C.ICC.AUT.....	155
14.15	Self-descriptive CV Certificate (Example).....	155
14.15.1	Public Key .....	156
15	Files.....	157
15.1	File structure .....	157
15.2	File IDs .....	158
15.3	EF.DIR.....	158
15.4	EF.SN.ICC.....	158
15.5	EF.DH .....	159
15.6	EF.ELC .....	159
15.7	EF.C.ICC.AUT .....	160
15.8	EF.C.CA <sub>icc</sub> .CS-AUT .....	160
15.9	EF.C_X509.CH.DS.....	161
15.10	EF.C_X509.CA.CS (DF.ESIGN) .....	161
15.11	EF.DM.....	161
16	Cryptographic Information Application .....	162
16.1	ESIGN cryptographic information layout example .....	163
16.1.1	EF.CIAInfo .....	164
16.1.2	EF.AOD .....	165
16.1.3	EF.PrKD .....	168
16.1.4	EF.PuKD .....	170
16.1.5	EF.CD .....	171
16.1.6	EF.DCOD..... <a href="https://standards.iteh.ai/catalog/standards/sist/67862784-9b17-41c3-a187-7ce6a337b157/sist-en-14890-1-2009">https://standards.iteh.ai/catalog/standards/sist/67862784-9b17-41c3-a187-7ce6a337b157/sist-en-14890-1-2009</a>	172
Annex A	(informative) Device authentication — Cryptographic view .....	175
A.1	Algorithms for authentication with key exchange or key negotiation.....	175
A.2	Device authentication with key transport .....	175
A.2.1	Conformance to ISO/IEC 11770-3 .....	175
A.2.2	Using min(SIG, N-SIG) for the signature token .....	177
A.3	Device authentication with key negotiation.....	178
A.3.1	Diffie-Hellman Key Exchange.....	179
A.4	Device authentication with privacy protection.....	181
A.4.1	The authenticity of the public DH parameters.....	183
A.5	Device authentication with non traceability .....	185
A.5.1	Diffie-Hellman Key Exchange.....	185
A.6	The “Grandmaster Chess Attack” .....	187
Annex B	(informative) Personalization scenarios .....	189
Annex C	(informative) Build scheme for mEAC Object Identifiers .....	191
Bibliography	.....	193

**EN 14890-1:2008 (E)****Foreword**

This document (EN 14890-1:2008) has been prepared by Technical Committee CEN/TC 224 “xxx”, the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 2009, and conflicting national standards shall be withdrawn at the latest by June 2009.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes CWA 14890-1:2004.

This standard additionally provides generic **Identification, Authentication and Digital Signature (IAS)** services and thereby contains all additional cryptographic services specified in CWA 14890-2.

The standard will enable the development of interoperable cards issued by any card industry sector. The standard will describe an application interface and behavior of the SSCD i.e. it should be possible to implement on e.g. native and interpreter based cards.

The standard is compliant with other European standards developed in the framework of the European Directive 1999/93.

This standard *Application Interface for smart cards used as Secure Signature Creation Devices* consists of two parts:

- Part 1: “Basic Services” describes the mandatory specifications for an SSCD as part of generic IAS Services to be used in compliance to requirements of Article 5.1 of the Electronic Signature Directive,
- Part 2: “Additional Services” describes remaining services for IAS.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: 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 the United Kingdom.



## 1 Scope

Part 1 of this series specifies the application interface to Smart Cards during the usage phase, used as Secure Signature Creation Devices (SSCD) according to the Terms of the European Directive on Electronic Signature 1999/93 to enable interoperability and usage as SSCD on a national or European level.

This document describes the mandatory services for the usage of Smart Cards as SSCDs based on CEN CWA 14890 (all parts). This covers the signing function, storage of certificates, the related user verification, establishment and use of trusted path and channel, requirements for key generation and the allocation and format of resources required for the execution of those functions and related cryptographic token information.

Thereby the functionality of CWA 14890-1 is enhanced in the following areas:

- Device authentication with Elliptic Curves (ELC) for existing asymmetric authentication protocols (RSA Transport, Privacy Protocol),
- Enhancement of existing asymmetric authentication protocols due to privacy and non-traceability constraints,
- **Card Verifiable (CV) Certificate Formats** (self descriptive) with ELC for all types of authentication and authorization protocols,
- Secure Messaging Tags and use of commands with Odd-INS Code in compliance to the actual ISO/IEC 7816-4,
- Further hash algorithms (SHA2-family) with corresponding Object identifier and Algorithm references,
- Use of AES in authentication protocols,
- Use of AES for secure messaging.

The following items are out of scope:

- 1) The physical, electrical and transport protocol characteristics of the card,
- 2) The external signature creation process and signature environment,
- 3) The elements required to verify an electronic signature produced by a card used as a SSCD,
- 4) The error handling process.

**EN 14890-1:2008 (E)****2 Normative references**

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE For future implementations refer to the latest versions of the referenced documents; the following list refers to documents relevant at publication of this standard EN 14890.

EN ISO 3166-1, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes (ISO 3166-1:2006)*

ISO/IEC 7816-4:2005, *Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-6, *Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange*

ISO/IEC 7816-8:2004, *Identification cards – Integrated circuit cards – Part 8: Commands for security operations*

ISO/IEC 7816-11:2004, *Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods*

ISO/IEC 7816-15:2004, *Identification cards – Integrated circuit cards with contacts – Part 15: Cryptographic information application*

ISO/IEC 9796-2:2008, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms*

ISO 11568-2:2005, *Banking – Key management (retail) – Part 2: Symmetric ciphers, their key management and life cycle*

ISO/IEC 14888-2:2008, *Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms*

ISO/IEC 15946-1, *Information Technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General*

ISO/IEC 18033-3, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*

**3 Terms and definitions**

For the purposes of this document, the terms and definitions given in ISO/IEC 7816-4:2005 and the following apply.

**3.1****Answer-to-Reset file**

elementary file which indicates operating characteristics of the card

**3.2****command-response pair**

set of two messages: a command followed by a response

**3.3****data element**

item of information seen at the interface for which are defined a name, a description of logical content, a format and a coding

**3.4****data object**

information seen at the interface which consists of a tag, a length and a value (i.e., a data element)

NOTE In this specification, data objects are referred to as BER-TLV data objects.

**3.5****data unit**

smallest set of bits which can be unambiguously referenced

**3.6****dedicated file**

file containing file control information and, optionally, memory available for allocation

NOTE It may be the parent of EFs and/or DFs.

**3.7****DF name**

string of bytes which uniquely identifies a dedicated file in the card

**3.8****elementary file**

set of data units or records which share the same file identifier

NOTE It cannot be the parent of another file.

**3.9****file control parameters**

logical, structural and security attributes of a file

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)

**3.10****file identifier**

2-bytes binary value used to address a file

[SIST EN 14890-1:2009](https://standards.iteh.ai/catalog/standards/sist/67862784-9b17-41c3-a187-736187b157/sist-en-14890-1-2009)

<https://standards.iteh.ai/catalog/standards/sist/67862784-9b17-41c3-a187-736187b157/sist-en-14890-1-2009>

**3.11****master file**

mandatory unique dedicated file representing the root of the file structure

**3.12****message**

string of bytes transmitted by the interface device to the card or vice-versa, excluding transmission-oriented characters as defined in ISO/IEC 7816-3

**3.13****parent file**

dedicated file immediately preceding a given file within the hierarchy

**3.14****password**

data which may be required by the application to be presented to the card by its user

NOTE A password in the context of this specification is a string of numbers and/or ASCII characters.

**3.15****path**

concatenation of file identifiers without delimitation

NOTE If the path starts with the identifier of the master file, it is an absolute path.

**EN 14890-1:2008 (E)****3.16****private key**

secret part of an asymmetric key pair e.g. signature creation data as specified in the EU directive for electronic signatures

**3.17****public key**

public part of an asymmetric key pair

**3.18****record**

string of bytes which can be handled as a whole by the card and referenced by a record number

**3.19****record number**

sequential number assigned to each record which uniquely identifies the record within its elementary file

**3.20****retry counter**

counter being used to count the number of erroneous usages of a related (security) object

NOTE If the object (e.g. password entry) was used correctly (correct password entered) then the retry counter is reset to its initial value. A typical value of a retry counter is 3.

**3.21****secret key**

either a symmetrical key or private part of a public key pair

**3.22****trusted channel**

means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP

**3.23****trusted environment**

operating environment that avoids the fraud with data that is seen at the communication interface by the definition of its physical location, physical security protection or physical access conditions or other measures to protect from tampering or intrusion of data

NOTE See 8.2.3.

**3.24****trusted path**

means by which a user and a TSF can communicate with necessary confidence to support the TSP

**3.25****untrusted environment**

operating environment that allows tampering and intrusion of data available at the communication interface

NOTE The decision whether an environment is trusted cannot always be made at the system level and therefore might have to be taken by the card holder.

**3.26****usage counter**

counter updated each time a related object is used

NOTE Opposite to retry counters, usage counters are not reset to their initial value after the object was successfully used.

## 4 Symbols and abbreviations

<b>AES</b>	Advanced Encryption Standard
<b>AID</b>	Application Identifier
<b>AKI</b>	Authority Key Identifier
<b>AKP</b>	Asymmetric key pair
<b>APDU</b>	Application protocol data unit
<b>AT</b>	Authentication Template, CRT for Authentication
<b>AUT</b>	Authentication
<b>BCD</b>	Binary Coded Decimal
<b>BER</b>	Basic Encoding Rules
<b>C</b>	Certificate
<b>CA</b>	Certification Authority
<b>CAR</b>	CA Reference
<b>CC</b>	Cryptographic Checksum
<b>CG</b>	Cryptogram
<b>CH</b>	Cardholder
<b>CHA</b>	Certificate Holder Authorization
<b>CHR</b>	Certificate Holder Reference
<b>CIA</b>	Cryptographic Information Application
<b>CIO</b>	Cryptographic Information Object
<b>CLA</b>	Class byte
<b>CPI</b>	Certificate Profile Identifier
<b>CRT</b>	Control Reference Template
<b>CS</b>	CertSign, certificate containing the public part of a signature key pair
<b>CV</b>	Card Verifiable
<b>CWA</b>	CEN Workshop Agreement
<b>C/S</b>	Client/Server
<b>D[key](msg)</b>	Decipherment of <msg> with <key>
<b>DE</b>	Data Element
<b>DES</b>	Data Encryption Standard
<b>DF</b>	Dedicated File
<b>DH</b>	Diffie-Hellman
<b>DIR</b>	Directory
<b>DO</b>	Data Object
<b>DS</b>	Digital Signature
<b>DSA</b>	Digital Signature Algorithm
<b>DSI</b>	Digital Signature Input
<b>DST</b>	Digital Signature Template, CRT for DS
<b>E[key](msg)</b>	Encipherment of <msg> with <key>
<b>ECC</b>	European Citizen Card

## EN 14890-1:2008 (E)

<b>EDFB</b>	Encrypted Data Formatted Block
<b>EF</b>	Elementary File
<b>ELC</b>	Elliptic Curve Cryptography
<b>FCI</b>	File Control Information
<b>FID</b>	File Identifier
<b>h(msg)</b>	hash-code of <msg>
<b>HT</b>	CRT for hash code
<b>ICC</b>	Integrated Circuit(s) Card
<b>ID</b>	Identifier
<b>IFD</b>	Interface Device
<b>INS</b>	Instruction byte
<b>KE</b>	Key Encipherment
<b>KID</b>	Key Identifier
<b>MAC[key](msg)</b>	Message Authentication Code of <msg> built with <key>
<b>MF</b>	Master File
<b>MSE</b>	MANAGE SECURITY ENVIRONMENT
<b>OID</b>	Object Identifier
<b>PI</b>	Padding Indicator
<b>PIN</b>	Personal Identification Number
<b>PKCS</b>	Public Key Cryptography Standards
<b>PKI</b>	Public Key Infrastructure
<b>PrK</b>	Private Key
<b>PRND</b>	Padding Random Number
<b>PSO</b>	PERFORM SECURITY OPERATION
<b>PSS</b>	Probabilistic Signature Scheme
<b>PuK</b>	Public Key
<b>P1-P2</b>	Parameter bytes
<b>RC</b>	Retry Counter
<b>RCA</b>	RootCA
<b>RD</b>	Reference Data
<b>RFU</b>	Reserved for Future Use
<b>RID</b>	Registered application provider identifier
<b>RND</b>	Random number
<b>RSA</b>	Sig-Alg. of Rivest, Shamir, Adleman
<b>SCA</b>	Signature-Creation Application
<b>SE</b>	Security Environment
<b>SHA</b>	Secure Hash Algorithm
<b>SIG( )</b>	Signature of
<b>SK</b>	Secret Key
<b>SM</b>	Secure Messaging

<b>SN</b>	Serial Number
<b>SSC</b>	Send Sequence Counter
<b>SSCD</b>	Secure Signature Creation Device
<b>SW1-SW2</b>	Status bytes
<b>TDES</b>	Triple-DES
<b>TOE</b>	Target of evaluation
<b>TLV</b>	Tag, Length, Value
<b>TSF</b>	TOE Security Functions
<b>TSP</b>	TOE Security Policy

## 5 Signature application

### 5.1 Application Flow

The following diagrams demonstrate a typical application flow as described in CWA 14170 [3].

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN 14890-1:2009](https://standards.iteh.ai/catalog/standards/sist/67862784-9b17-41c3-a187-7ce6a337b157/sist-en-14890-1-2009)

<https://standards.iteh.ai/catalog/standards/sist/67862784-9b17-41c3-a187-7ce6a337b157/sist-en-14890-1-2009>