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

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

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.

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

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

Contents

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 **I**dentification, **A**uthentication and Digital **S**ignature (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,
- **C**ard **V**erifiable (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.

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

3.10
file identifier
2-bytes binary value used to address a file

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.

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

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

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

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

5 Signature application

5.1 Application Flow

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