SLOVENSKI STANDARD
SIST EN 14890-2:2009

01-april-2009

Uporabniški vmesnik za pametne kartice, ki se uporabljajo kot naprave za izdelovanje varnega podpisa - 2. del: Dodatne storitve

Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

Anwendungsschnittstelle für Smartcards als sichere Signaturerstellungseinheiten - Teil 1: Basisdienste

Interfaces applicatives des cartes à puce utilisées pour le création de signatures électroniques sécurisées - Partie 2: Services additionels

Ta slovenski standard je istoveten z: **EN 14890-2:2008**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST EN 14890-2:2009 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 14890-2

November 2008

ICS 35.240.15

Supersedes CWA 14890-2:2004

English Version

Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

Interface d'application des cartes intelligentes utilisées comme dispositifs sûrs de création de signature - Partie 2 : Services complémentaires

Anwendungsschnittstelle für Chipkarten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden - Teil 2: Zusätzliche Dienste

This European Standard was approved by CEN on 5 October 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

Ref. No. EN 14890-2:2008: E

Contents

Page

Foreword

This document (EN 14890-2:2008) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by DIN.

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 May 2009, and conflicting national standards shall be withdrawn at the latest by May 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 14890-2:2004.

This European Standard is to support the robust implementation of the European legal framework for electronic signatures. It incorporates CEN CWA 14890 Parts 1 and 2, defining the functional and security requirements for a smart card intended to be used as a Secure Signature Creation Device. This is in accordance with the Terms of the European Directive on Electronic Signature 1999/93, whereby a card compliant to the standard shall be able to produce a 'Qualified electronic signature' that fulfils the requirements of Article 5.1 of the Electronic Signature Directive, therefore giving it the equivalent status of a hand-written signature.

This standard additionally provides generic **I**dentification, **A**uthentication and Digital **S**ignature (IAS) services and contains all additional cryptographic services specified in CEN CWA 14890 Part 2.

The standard enables the development of interoperable cards issued by any card industry sector. The standard also describes an application interface and behaviour of the SSCD that should be possible to be implemented on native and interpreter based cards.

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

This European 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 [5].

— 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 2 of this series contains **I**dentification, **A**uthentication and **D**igital Signature (IAS) services in addition to the SSCD services already described in Part 1 to enable interoperability and usage for IAS on a national or European level.

This part describes additional functionality to support generic Identification, Authentication and Digital Signature (IAS) services. It contains the functionality of Part 2 of CEN CWA 14890. This covers key decipherment and client (card holder) server authentication, signature verification and related cryptographic token information.

— Additionally this document is enhanced in respect to

— **C**lient-**S**erver (C/S) Authentication Protocols with ELC and their description in DF.CIA

— Identity management on base of C/S Authentication

— Card capability description and Application Capability Description

The following items are out of scope:

1. The physical, electrical and transport protocol characteristics of the card,

2. 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.

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

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

ISO/IEC 7816-9:2004, *Identification cards —- Integrated circuit cards —- Part 9: Commands for card management*

EN 14890-1:2008, *Application Interface for smart cards used as Secure Signature Creation Devices — Basic Services*

ISO/IEC 15946, *Information Technology — Security techniques — Cryptographic techniques based on elliptic curves*

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
C/S external authentication
authentication of the server by the client. The client is regarded as the combination of the PC and the ICC. This external authentication is out of the scope of this specification

3.2
C/S internal authentication
authentication of the client by the server. The client is regarded as the combination of the PC and the ICC

3.3
IFD
device or entity that belongs to the external world (outside the ICC)

3.4
Secured channel
communication link between the ICC and a security module (possibly also an ICC) that provides authenticity and/or integrity and/or secrecy

4 Abbreviations and notation

The abbreviations and notation is in accordance with those given in [1].

APDU	Application protocol data unit
ARR	Access Rule Record
AT	CRT for Authentication
C/S	Client-Server
CA	Certificate authority
CC	Cryptographic checksum
CCT	Cryptographic checksum template
CIA	Cryptographic information application
CMS	Card Management System
CRT	Control Reference Template
CT	Confidentiality Template
D[key](msg)	Decipherment of <msg> with <key>
DES-3	Data Encryption Standard (Triple DES)
DF	Dedicated File
DH	Diffie-Hellman
DO	Data Object
DS	Digital Signature
DSI	Digital Signature Input
DST	CRT for Digital Signature
E[key](msg)	Encipherment of <msg> with <key>
EF	Elementary File
FCI	File Control Information
FCP	File Control Parameters
H_<id>	Hash function using <id> algorithm
ICC	Integrated Circuit(s) Card
ID	Identifier
IFD	Interface Device
INS	Instruction byte
KE	Key Encipherment
KEI	Key Encipherment Input Format
KID	Key Identifier
MD5	Message Digest 5 (hash algorithm)
MF	Master File
OAEP	Optimal Asymmetric Encryption Padding
P1-P2	Parameter bytes
PI	Padding Indicator

PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standards
PrK	Private Key
PSO	PERFORM SEC. OPERATION
PSS	Probabilistic Signature Scheme
PuK	Public Key
RCA	RootCA
RFU	Reserved for Future Use
RND	Random number
SE	Security Environment
SFI	Short File Identifier
SHA	Secure Hash Algorithm
SK	Secret Key
SM	Secure Messaging
SN	Serial Number
SSCD	Secure Signature Creation Device
SSD	Secure Service Descriptor
UQB	Usage Qualifier

5 Additional Service Selection

Additional services are typically used in the context of applications that use digital signatures.

A well known additional service is the **client/server authentication**. In this case, the ICC is used as a crypto toolbox, e.g. in order to encrypt a challenge with a private key, being stored in the ICC. This is particularly helpful in applications, where a tamper resistant device is required for client/server authentication. An ICC does have the tamper resistant quality and may therefore be used efficiently to support the application in this context.

A **document decryption** is another known service which may be performed by the IFD. A terminal application receives a document, typically encrypted with a symmetric key. The symmetric key is also encrypted with another public key. The ICC contains the appropriate private key, deciphers the symmetric key and returns it to the terminal application.

While the typical usage of a signature card is the generation of a digital signature, an application might want to verify a signature with a public key, being stored in the ICC. In this case an additional service is invoked for the **signature verification**.

Additional services provided in the ICC mandate the existence of an appropriate security environment. Associated security environments are described in Annex C.

In addition to the descriptive information found in DF.CIA (refer to EN 14890-1:2008, Clause 16) information might be required that can be presented in Security Service Descriptors. The concept of security service descriptors is described in Annex A.

User verification may be required prior to the usage of additional services. The password for this user verification shall be different from the password used for the signature generation. This is to maintain the purpose of the signature generation password for the sole purpose of a ‘declaration of will’ in the case of a signature generation.

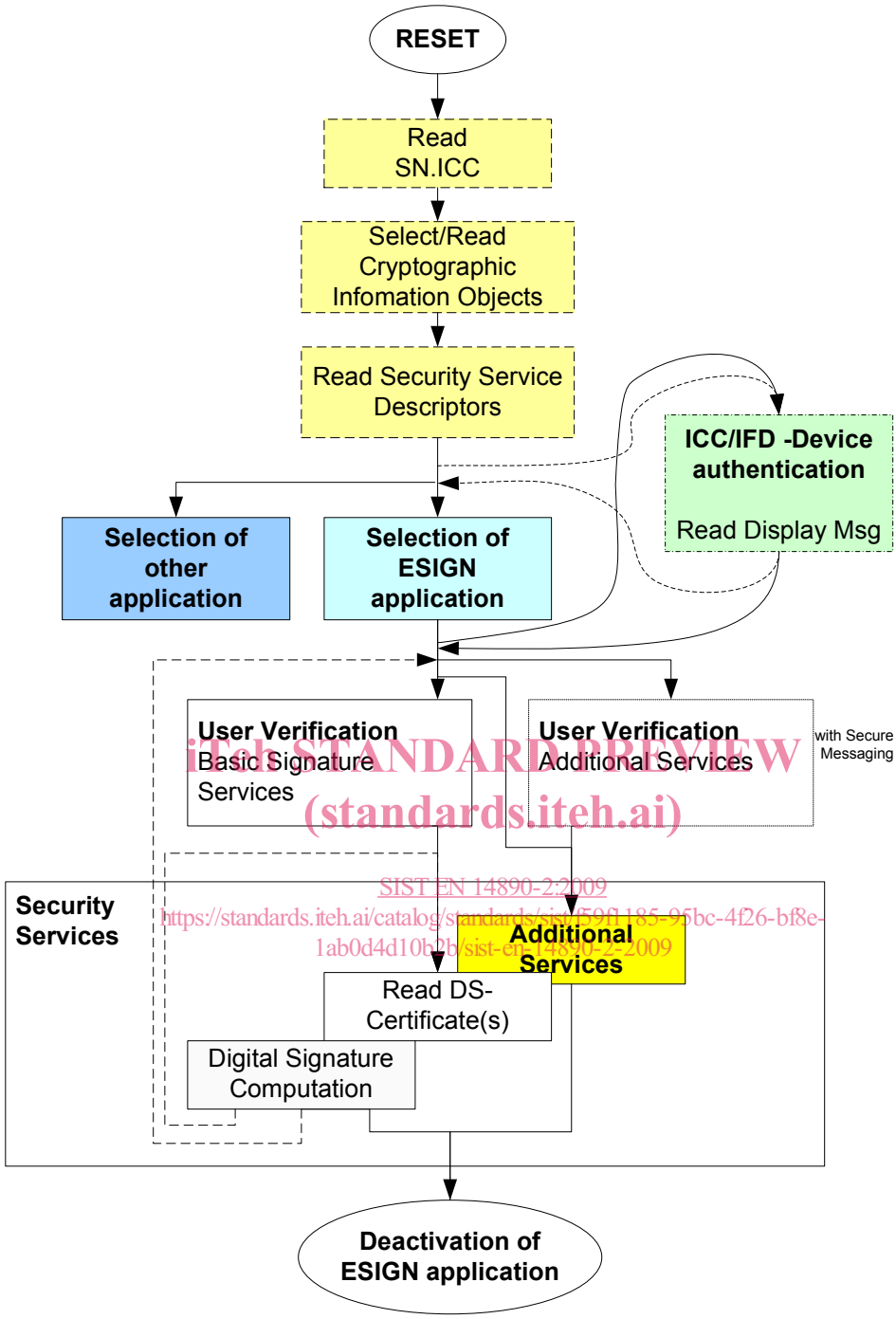

Figure 1 — Example of additional service selection

Figure 1 shows the selection of additional services in the context of the ESIGN application. User verification might be required for some of the additional services. The detailed access conditions are described in the appropriate security environments.

6 Client/Server Authentication

6.1 General

For proving access rights to components such as servers, a PK based authentication procedure has to be performed. Such client/server Authentication (See 3.2) is a process, being independent from the requirement of a device authentication.

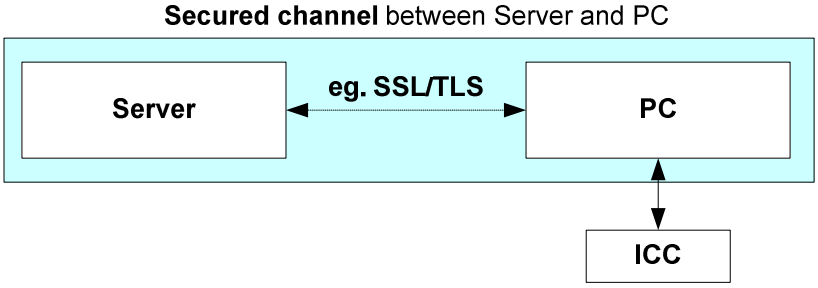

Figure 2 — Example of client/server authentication

In the above example client/server authentication establishes a secured channel between a remote server and a PC. The ICC will be used as a cryptographic toolbox in order to provide the cryptographic functionality to the PC.

This specification does not support the authentication of the server (See 3.1). The server's certificate as well as the server protocol is application specific and therefore out of the scope of this document.

6.2 Client/Server protocols

This specification covers only the case, where the card performs a digital signature computation applying the private key for authentication in an INTERNAL AUTHENTICATE (COMPUTE DIGITAL SIGNATURE) command to the authentication input contained in the data field of the command after formatting the input.

The key pair used for client/server authentication shall be different from the device authentication keys and signature generation keys respectively. The public part of this key pair, stored with the distinguished name of the cardholder is certified by a certificate (typically X.509 [7]. Such a certificate is not interpreted by the ICC.

Relevant authentication procedures are e.g.

— PK Kerberos protocol (for logon authentication)

— SSL/TLS protocol

— WTLS protocol.

All the above protocols base on the same cryptographic algorithms. In particular they are all using PKCS #1 padding format in the case of RSA. Therefore this specification describes only the PKCS #1 padding.

6.3 Steps preceding the client/server authentication

The steps preceding a client/server authentication are application specific. Hence this specification does not mandate the existence of those steps.

The access conditions proposed in Annex C specify user verification as a mandatory step prior to client/server authentication.