

# ČESKÁ TECHNICKÁ NORMA

ICS 35.240.15 **Březen 2010**

## **Aplikační rozhraní pro čipové karty používané jako zařízení pro vytváření bezpečného podpisu - Část 2: Další služby**

**ČSN**  
**EN 14890-2**  
36 9710

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

Interface applicative des cartes a puces utilisées comme dispositifs de création de signature  
numérique sécurisés -  
Partie 2: Services additionels

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

Tato norma je českou verzí evropské normy EN 14890-2:2008. Překlad byl zajištěn Úřadem pro  
technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN 14890-2:2008. It was translated by  
Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN 14890-2 (36 9710) z června 2009.

Národní předmluva

Změny proti předchozím normám

Proti předchozí normě dochází ke změně způsobu převzetí EN 14890-2:2008 do soustavy norem ČSN.  
Zatím co ČSN EN 14890-2 z června 2009 byla převzata schválením k přímému používání jako ČSN  
oznámením ve Věstníku, tato norma ji přejímá překladem.

Informace o citovaných normativních dokumentech

ISO/IEC 7816-4:2005 zavedena v ČSN ISO/IEC 7816-4:2006 (36 9205) Identifikační karty - Karty  
s integrovanými obvody - Část 4: Organizace, bezpečnost a příkazy pro výměnu

ISO/IEC 7816-8:2004 dosud nezavedena

ISO/IEC 7816-9:2004 zavedena v ČSN ISO/IEC 7816-9:2005 (36 9205) Identifikační karty - Karty

s integrovanými obvody – Část 9: Příkazy pro správu karet

EN 14890-1:2008 zavedena v ČSN EN 14890-1:2010 (36 9710) Aplikační rozhraní pro čipové karty používané jako zařízení pro vytváření bezpečného podpisu – Část 1: Základní služby

ISO/IEC 15946 dosud nezavedena

Vysvětlivky k textu převzaté normy

Soubory norem ISO/IEC, např. ISO/IEC 7816 atp., jsou v anglickém originálu nepřesně citovány, např. ISO 7816.

<b>Anglický termín</b>	<b>Používané termíny</b>	<b>Použitý český termín</b>
crypto algorithm	<ul style="list-style-type: none"><li>• šifrovací algoritmus</li><li>• kryptoalgoritmus</li></ul>	šifrovací algoritmus
<ul style="list-style-type: none"><li>• data field – empty</li><li>• data field – absent</li></ul>	<ul style="list-style-type: none"><li>• datové pole – prázdné</li><li>• datové pole – nevyskytuje se</li></ul>	<ul style="list-style-type: none"><li>• datové pole – prázdné</li><li>• datové pole – nevyskytuje se</li></ul>
elliptic curves over prime fields	<ul style="list-style-type: none"><li>• eliptické křivky nad prvočíselnými poli</li><li>• eliptické křivky nad prvočíselnými tělesy</li></ul>	eliptické křivky nad prvočíselnými poli
padding	<ul style="list-style-type: none"><li>• výplň, vyplňování</li><li>• vycpávka</li></ul>	výplň, vyplňování
discretionary data	<ul style="list-style-type: none"><li>• volně použitelná data</li><li>• data podle uvážení</li></ul>	volně použitelná data
features	<ul style="list-style-type: none"><li>• vlastnosti</li><li>• prvky</li></ul>	vlastnosti
flag	<ul style="list-style-type: none"><li>• flag</li><li>• příznak</li></ul>	flag
hash	<ul style="list-style-type: none"><li>• hash (název operace)</li><li>• hašování (název činnosti)</li><li>• výsledek operace hašování</li></ul>	<ul style="list-style-type: none"><li>• hash (název operace)</li><li>• hašování (název činnosti)</li></ul>
hash code	<ul style="list-style-type: none"><li>• hašový kód</li><li>• haš</li><li>• výsledek operace hašování</li></ul>	hašový kód
hash value	<ul style="list-style-type: none"><li>• hodnota hash</li><li>• (hodnota) digitálního otisku</li><li>• výsledek operace hašování</li></ul>	hodnota hash
<ul style="list-style-type: none"><li>• KE certificate</li><li>• key encipherment certificate</li></ul>	<ul style="list-style-type: none"><li>• KE certifikát</li><li>• certifikát k zašifrování klíče</li></ul>	KE certifikát
key seed	<ul style="list-style-type: none"><li>• výchozí materiál klíče</li><li>• počáteční klíč</li></ul>	výchozí materiál klíče
master key	<ul style="list-style-type: none"><li>• master klíč</li><li>• hlavní klíč</li></ul>	master klíč
mode	<ul style="list-style-type: none"><li>• režim</li><li>• mód</li></ul>	režim
X.509 certificate	<ul style="list-style-type: none"><li>• certifikát podle X.509</li><li>• certifikát X.509</li></ul>	certifikát podle X.509

Vypracování normy

Zpracovatel: Anna Juráková, Praha, IČ 61278386, Dr. Karel Jurák

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

**EVROPSKÁ NORMA EN 14890-2**  
**EUROPEAN STANDARD**  
**NORME EUROPÉENNE**  
**EUROPÄISCHE NORM** Listopad 2008

ICS 35.240.15 Nahrazuje CWA 14890-2:2004

**Aplikační rozhraní pro čipové karty používané jako zařízení pro vytváření bezpečného podpisu -  
Část 2: Další služby**

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

Interface applicative des cartes a puces utilisées comme dispositifs de création de signature numérique sécurisés - Partie 2: Services additionels	Anwendungsschnittstelle für Chipkarten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden - Teil 2: Zusätzliche Dienste
---	--

Tato evropská norma byla schválena CEN 2008-10-5.

Členové CEN jsou povinni splnit Vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se musí této evropské normě bez jakýchkoliv modifikací dát status národní normy. Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru nebo u kteréhokoliv člena CEN.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce přeložená členem CEN do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Řídicímu centru, má stejný status jako oficiální verze.

**CEN**

**Evropský výbor pro normalizaci**  
**European Committee for Standardization**  
**Comité Européen de Normalisation**  
**Europäisches Komitee für Normung**

**Řídicí centrum: rue de Stassart 36, B-1050 Brusel**

© 2008 CEN Veškerá práva pro využití v jakékoli formě a jakýmkoli prostředky Ref. č.  
EN 14890-2:2008 E  
jsou celosvětově vyhrazena národním členům CEN.

Členy CEN jsou národní normalizační orgány Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Španělska, Švédsko a Švýcarska.

**Předmluva**

Tento dokument (EN 14890-2:2008) byl vypracován v technické komisi CEN/TC 224 „Identifikace osob, elektronický podpis a karty a příslušné systémy a operace“, jejíž sekretariát je při AFNOR.

Této evropské normě musí být udělen status národní normy buď publikováním identického textu nebo vyhlášením nejpozději do května 2009 a národní normy, které jsou s ní v rozporu, musí být zrušeny nejpozději do května 2009.

Je třeba upozornit na to, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CEN neodpovídá za identifikování jednotlivých nebo všech souvisejících patentových práv.

Tento dokument nahrazuje CWA 14890-2:2004.

Tato evropská norma má podporovat stabilní implementaci evropského právního rámce pro elektronické podpisy. Norma zapracovává CEN CWA 14890, Části 1 a 2, které definují funkční a bezpečnostní požadavky na čipové karty určené pro používání jako zařízení pro vytváření bezpečného podpisu (SSCD). Toto je ve shodě s podmínkami Evropské směrnice o elektronickém podpisu 1999/93. Karta odpovídající této normě musí být schopna vytvářet „Kvalifikovaný elektronický podpis“, který splňuje požadavky 5.1 Směrnice o elektronickém podpisu, který má tímto ekvivalentní status jako ručně psaný podpis.

Tato norma dále poskytuje všeobecný popis služeb identifikace, autentizace a digitálního podpisu (IAS) a obsahuje všechny další kryptografické služby specifikované v CEN CWA 14890 Část 2.

Norma umožňuje vývoj interoperabilních karet určených pro libovolnou oblast kartového podnikání. Norma rovněž popisuje aplikační rozhraní a chování SSCD, které lze implementovat do nativních karet nebo do karet vyžadujících interpreter.

Norma je ve shodě s dalšími evropskými normami vypracovanými v rámci Evropské směrnice 1999/93.

Tato evropská norma *Aplikační rozhraní pro čipové karty používané jako zařízení pro vytváření bezpečného podpisu* sestává ze dvou částí:

- Část 1: „Základní služby“ popisuje povinné specifikace pro SSCD jako část obecných služeb IAS, které se mají používat ve shodě s požadavky 5.1 Směrnice o zásadách Společenství pro elektronické podpisy [5].
- Část 2: „Další služby“ popisuje zbývající služby IAS.

V souladu s Vnitřními předpisy CEN/CENELEC se národní normalizační organizace následujících zemí zavazují, že zavedou tuto evropskou normu: Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunsko, Řecko, Slovensko, Slovinsko, Spojeného království, Španělsko, Švédsko a Švýcarsko.

Obsah

Strana

Předmluva 6

**1** Předmět normy 10

**2** Citované normativní dokumenty 10

**3** Termíny a definice 10

**4** Zkratky a zápis 11

**5** Volba další služby 12

**6** Autentizace klient/server 14

- 6.1** Všeobecně 14
- 6.2** Protokoly klient/server 14
- 6.3** Kroky předcházející autentizaci klient/server 14
- 6.4** Formát výplně 14
  - 6.4.1** PKCS #1 v 1-5 14
  - 6.4.2** DSI podle PKCS #1 V 2.x (PSS) 15
- 6.5** Protokol klient/server 16
  - 6.5.1** Všeobecně 16
  - 6.5.2** Krok 1 - Čtení certifikátu 17
  - 6.5.3** Krok 2 - Ustavení podpisového klíče pro interní autentizaci klient/server 17
  - 6.5.4** Krok 3 - Interní autentizace 18
  - 6.5.5** Průběh provádění autentizace klient/server 19
  - 6.5.6** Datové pole příkazu pro autentizaci klient/server 20
- 7** Autentizace role 21
  - 7.1** Autentizace role karty 21
  - 7.2** Autentizace role serveru 21
  - 7.3** Symetrická externí autentizace 22
    - 7.3.1** Protokol 22
    - 7.3.2** Popis role 24
  - 7.4** Asymetrická externí autentizace 24
    - 7.4.1** Protokol založený na RSA 24
    - 7.4.2** Popis role 26
- 8** Dešifrování šifrovacího klíče 26
  - 8.1** Kroky předcházející dešifrování klíče 27
  - 8.2** Správa klíčů pomocí RSA 27
    - 8.2.1** Všeobecně 27
    - 8.2.2** Výplň OAEP 28
    - 8.2.3** Průběh provádění 29

## **8.3** Výměna klíče podle Diffie-Hellmana 30

### **8.3.1** Všeobecně 30

### **8.3.2** Průběh provádění 32

## **8.4** Identifikátor algoritmu pro DECIPHER 33

## **9** Ověřování podpisu 34

### **9.1** Průběh provádění ověřování podpisu 34

#### **9.1.1** Krok 1: Příjem dat pro hašování 34

#### **9.1.2** Krok 2: Volba ověřovacího klíče 35

#### **9.1.3** Krok 3: Ověření digitálního podpisu 36

Strana

## **10** Certifikáty pro další služby 37

### **10.1** Struktura souboru 37

### **10.2** EF.C.CH.AUT 37

### **10.3** EF.C.CH.KE 38

### **10.4** Čtení certifikátů a veřejných klíčů certifikačních autorit CA 38

## **11** Datové struktury jednotky APDU 38

### **11.1** Identifikátory algoritmů 38

#### **11.1.1** Identifikátory AlgID pro autentizaci klient/server 38

#### **11.1.2** Identifikátor algoritmu pro DECIPHER 39

### **11.2** Šablony CRT 39

#### **11.2.1** CRT DST pro volbu soukromého klíče karty ICC pro autentizaci klient/server 39

#### **11.2.2** CRT AT pro volbu soukromého klíče karty ICC pro autentizaci klient/server 40

#### **11.2.3** CRT CT pro volbu soukromého klíče karty ICC 40

#### **11.2.4** CRT CT pro volbu šifrovacího DH klíče karty ICC 40

#### **11.2.5** CRT DST pro volbu veřejného klíče zařízení IFD (ověřování podpisu) 40

## **Příloha A** (normativní) Šablony deskriptorů bezpečnostních služeb 42

### **A.1** Úvod 42

### **A.2** Koncept deskriptoru bezpečnostní služby 42

### **A.3** Datové objekty SSD 43

**A.3.1** DO rozšířeného seznamu záhlaví, tag '4D, 43

**A.3.2** DO mapování sady instrukcí (*Instruction set mapping – ISM*), tag '80, 43

**A.3.3** DO příkazu, který se má provést (*Command to perform – CTP*), tag '52, (viz ISO/IEC 7816-6) 43

**A.3.4** DO identifikátoru objektu algoritmu (*object identifier – OID*), tag '06, (viz ISO/IEC 7816-6) 43

**A.3.5** DO odkazu na algoritmus, tag '81, 43

**A.3.6** DO odkazu na klíč, tag '82, 43

**A.3.7** DO FID souboru klíče, tag '83, 43

**A.3.8** DO skupiny klíčů, tag '84, 43

**A.3.9** DO FID souboru základního certifikátu, tag '85, 43

**A.3.10** DO FID souboru s připojeným certifikátem, tag '86, 43

**A.3.11** DO odkazu na certifikát, tag '87, 44

**A.3.12** DO kvalifikátoru certifikátu, tag '88, 44

**A.3.13** DO FID pro soubor s veřejným klíčem certifikační autority PK(CA), tag '89, 44

**A.3.14** DO pravidel používání PIN, tag '5F2F, (viz ISO/IEC 7816-6) 44

**A.3.15** DO odkazu na PIN, tag '8A, 44

**A.3.16** DO identifikátoru aplikace (AID), tag '4F, (viz ISO/IEC 7816-6) 44

**A.3.17** DO kódování CLA, tag '8B, 44

**A.3.18** DO stavové informace (SW1-SW2), tag '42, (viz ISO/IEC 7816-6) 44

**A.3.19** DO volně použitelných dat, tag '53, (viz ISO/IEC 7816-6) 44

**A.3.20** DO čísla SE, tag '8C, 45

**A.3.21** DO identifikátoru profilu SSD, tag '8D, 45

**A.3.22** DO mapování FID, tag '8E, 45

**A.4** Umístění SSD šablon 45

**A.5** Příklady SSD šablon 45

**B.1** Všeobecně 46

**B.2** Parametry eliptické křivky 46

**B.3** Bod veřejného klíče 46

**B.4** Formát ECDSA podpisu 46

**Příloha C** (informativní) Bezpečnostní prostředí 48

**C.1** Úvod 48

**C.2** Definice šablon CRT (příklady) 49

**C.2.1** Všeobecně 49

**C.2.2** CRT pro autentizaci (AT) 49

**C.2.3** CRT pro kryptografický kontrolní součet (CCT) 50

**C.2.4** CRT pro digitální podpis (DST) 51

**C.2.5** CRT pro důvěrnost (CT) 52

**C.3** Bezpečnostní prostředí (příklad) 53

**C.3.1** Všeobecně 53

**C.3.2** Bezpečnostní prostředí #10 53

**C.3.3** Bezpečnostní prostředí #11 53

**C.4** Kódování podmínek přístupu (příklad) 54

**C.4.1** Všeobecně 54

**C.4.2** Podmínky přístupu 54

**C.4.3** Odkazy na pravidla přístupu 54

**C.4.4** Podmínky přístupu pro EF.ARR 56

**C.4.5** Záznamy EF.ARR 56

**Příloha D** (informativní) Aspekty interoperability 59

**D.1** Všeobecně 59

**D.2** Volba autentizace zařízení 59

**D.2.1** Všeobecně 59

**D.2.2** Průběh generování podpisu s možnými volbami zpracování 60

**D.3** Volba metody ověření uživatele 60



## **Příloha E** (informativní) Příklad souboru DF.CIA 61

### Bibliografie 65

#### 1 Předmět normy

Část 2 tohoto souboru popisuje služby identifikace, autentizace a digitálního podpisu (IAS). Navíc ke službám SSCD, které byly popsány v Části 1, aby umožňovaly interoperabilitu a používání pro IAS na národní nebo evropské úrovni.

Tato část popisuje další funkce pro podporu generických služeb identifikace, autentizace a digitálního podpisu (IAS). Obsahuje funkce Části 2 dokumentu CEN CWA 14890. Toto pokrývá dešifrování klíče a autentizaci klient (držitel karty)/server, ověřování podpisu a příslušnou kryptografickou informaci tokenu.

Tento dokument je tedy zesílen v následujících oblastech:

- Protokoly autentizace klient-server (C/S) založené na eliptických křivkách ELC a jejich popis v DF.CIA
- Správa identity na základě autentizace C/S
- Popis možností karty (*card capability*) a popis možností aplikace (*application capability*)

Následující položky přesahují předmět této normy:

1. Fyzikální a elektrické charakteristiky karty a charakteristiky protokolu přenosu,
2. Procesy pro ošetření chyb.

Konec náhledu - text dále pokračuje v placené verzi ČSN.