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.

Anglický termín	Používané termíny	Použitý český termín
crypto algorithm	• šifrovací algoritmus • kryptoalgoritmus	šifrovací algoritmus
• data field – empty • data field – absent	• datové pole – prázdné • datové pole – nevyskytuje se	• datové pole – prázdné • datové pole – nevyskytuje se
elliptic curves over prime fields	• eliptické křivky nad prvočíselnými poli • eliptické křivky nad prvočíselnými tělesy	eliptické křivky nad prvočíselnými poli
padding	• výplň, vyplňování • vycpávka	výplň, vyplňování
discretionary data	• volně použitelná data • data podle uvážení	volně použitelná data
features	• vlastnosti • prvky	vlastnosti
flag	• flag • příznak	flag
hash	• hash (název operace) • hašování (název činnosti) • výsledek operace hašování	• hash (název operace) • hašování (název činnosti)
hash code	• hašový kód • haš • výsledek operace hašování	hašový kód
hash value	• hodnota hash • (hodnota) digitálního otisku • výsledek operace hašování	hodnota hash
• KE certificate • key encipherment certificate	• KE certifikát • certifikát k zašifrování klíče	KE certifikát
key seed	• výchozí materiál klíče • počáteční klíč	výchozí materiál klíče
master key	• master klíč • hlavní klíč	master klíč
mode	• režim • mód	režim
X.509 certificate	• certifikát podle X.509 • certifikát X.509	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

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, Švédska 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, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Španělska, Švédska a Švýcarska.

Obsah

Strana

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.