ČESKÁ TECHNICKÁ NORMA

ICS 35.240.40

Červen 1998

	Bankovnictví - Správa klíčů pomocí asymetrických algoritmů - Část 2: Schválené algoritmy používající kryptosystém RSA	ČSN ISO 11166-2 97 9118

Banking **-** Key management by means of asymmetric algorithms - Part 2: Approved algorithms using the RSA cryptosystem

Banque - Gestion de clés au moyen d,algorithmes asymétriques - Partie 2: Algorithmes approuvés utilisant le système de chiffrement RSA

Bankwesen - Schlüsselverwaltung durch asymmetrische Algorithmen - Teil 2: Erlaubte Algorithmen bei der Benutzung des RSA - Verschlüsselungssystems

Tato norma je českou verzí mezinárodní normy ISO 11166-2:1994. Mezinárodní norma ISO 11166-2:1994 má status české technické normy.

This standard is the Czech version of the International Standard ISO 11166-2. The International Standard ISO 11166-2:1994 has the status of a Czech Standard.

52046

Národní předmluva

Citované normy

ISO/IEC 646:1991 zavedena v ČSN ISO/IEC 646 Informační technika - 7-bitový kódovaný soubor znaků ISO pro výměnu informací (36 9104)

ISO 9362:1994 Bankovnictví - Bankovní telekomunikační zprávy - Bankovní identifikační kódy, dosud nezavedena

ISO 11166-1:1994 zavedena v ČSN ISO 11166-1 Bankovnictví - Správa klíčů pomocí asymetrických algoritmů - Část 1: Zásady, postupy a formáty (97 9118)

Vypracování normy

Zpracovatel normy: Ing. Hana Pačesová, IČO 7919

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

---

MEZINÁRODNÍ NORMA	
Bankovnictví	ISO 11166-2
Správa klíčů pomocí asymetrických algoritmů -	První vydání
Část 2: Schválené algoritmy používající	1994-11-15
kryptosystém RSA	

MDT 35.240.40

Deskriptory: banking, banking documents, financial documents, data processing, messages, inter-bank payment messages, protection of information, key management, security techniques, authentication, message authentication codes, algorithms.

Obsah

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětovou federací národních normalizačních organizací (členů ISO). Na mezinárodních normách obvykle pracují technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být zastoupen v této technické komisi. Práce se zúčastňují i mezinárodní komise, vládní i nevládní, s nimiž ISO navázalo pracovní styk. ISO úzce spolupracuje ve všech záležitostech technické normalizace s Elektrotechnickou komisí (IEC).

Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členům ISO k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% z hlasujících členů.

Mezinárodní norma ISO 11166-2 byla připravena technickou komisí ISO/TC 68, *Bankovnictví a souvisící finanční služby,* Subkomise 2, *Činnosti a postupy.*

ISO 11166 se skládá z následujících částí se společným názvem

Bankovnictví - Správa klíčů pomocí asymetrických algoritmů:

- Část 1: Zásady, postupy a formáty
- Část 2: Schválené algoritmy používající kryptosystém RSA.

Příloha A je nedílnou součástí této části ISO 11166. Přílohy B a C jsou pouze pro informaci.

Úvod

ISO 11166-1 specifikuje ty aspekty správy klíčů v bankovnictví, využívající asymetrické algoritmy, které jsou nezávislé na použitých algoritmech. Další části normy specifikují asymetrické algoritmy, schválené pro použití v postupech Části 1.

Tato část ISO 11166 specifikuje schválené algoritmy používající kryptosystém RSA. Poskytuje také spojení mezi specifikací algoritmu a značením použitým v Části 1 k označení základních kryptografických procesů používaných při správě klíčů v bankovnictví.

V dalších částech normy budou dle plánu specifikovány alternativní schválené algoritmy, přičemž žádný jednotlivý algoritmus nebude povinný.

Úroveň bezpečnosti, kterou je možné dosáhnout použitím kryptografického algoritmu, závisí, kromě dalších faktorů, na parametrech definujících algoritmus a na aktuálním stavu technologie zpracování informací. Z těchto důvodů neimplikuje všeobecné schválení algoritmu pro použití, provedené v postupech 1.části normy, konkrétní úroveň bezpečnosti.

Příloha A specifikuje přiřazené hodnoty Kódu formátů a funkcí (FFC), které by měly být použité v případě, že certifikáty jsou podepsané provedením transformace textu.

1 Předmět normy

Tato část ISO 11166 specifikuje asymetrické algoritmy, t.j. algoritmy, které jsou určené pro asymetrické zašifrování a pro digitální podpis, využívající kryptosystém RSA, a které jsou schválené pro použití normou 11166-1.

Tato část ISO 11166 specifikuje specifické používání metody RSA. Nepopisuje kryptosystém RSA v jeho obecném tvaru. Specifikuje také módy činnosti pro digitální podpis RSA. Tyto algoritmy a módy činnosti jsou pouze pro účely Části 1 této mezinárodní normy.

-- Vynechaný text --