ČESKÁ NORMA

MDT 336.719.2:355.405.2:681.3.04

Leden 1996

BANKOVNICTVÍ - Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu) - Část 1: Obecné zásady

ČSN ISO 10126-1

97 9001

Banking - Procedures for message encipherment (wholesale) - Part 1: General principles

Banque - Procédures de chiffrement de messages (service aux entreprise) - Partie 1: Principes généraux

Bankwesen - Verfahren für Berichteenzifferung für Firmenkunden l. Teil: Allgemeine Grundsätze

Tato norma je identická s ISO 10126-1:1991, první vydání.

Národní předmluva

Citované normy

ISO 646:1983 zavedena v ČSN ISO/IEC 646 Informační technika - 7-bitový kódovaný soubor znaků ISO (36 9104)

ISO 8730:l991 zavedena v ČSN ISO 8730 Bankovnictví - Požadavky na autentizaci zprávy (bankovní služby pro velkou klientelu) (97 9008)

ISO 8731-1:1987 zavedena v ČSN ISO 8731-1 Bankovnictví - Schválené algoritmy pro autentizaci zprávy - 1. část: DEA (97 9003)

ISO 8731-2:1987 zavedena v ČSN ISO 8731-2 Bankovnictví - Schválený algoritmus pro autentizaci zprávy - 2. část: Algoritmy pro autentikátor zprávy (97 9003)

ISO 8732:1988 dosud nezavedena

ISO 10126-2:1991 zavedena v ČSN 10126-2 Bankovnictví - Postupy pro šifrování správ (bankovní služby pro velkou klientelu) (97 9001)

Vypracování normy

Zpracovatel: Ing. Dagmar Jírová, IČO 18651399

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

18194

BANKOVNICTVÍ - POSTUPY PRO ŠIFROVÁNÍ ZPRÁV (BANKOVNÍ SLUŽBY PRO VELKOU KLIENTELU)
Část 1: Obecné zásady

ISO 10126-1
První vydání
1991-11-01

Obsah strana

1	Předmět normy	3
2	Odkazy na normy	3
3	Definice	4
4	Použití	5
5	Šifrování a dešifrování celých zpráv a prvků, určených pro šifrování	5
6	Transparentní přenos zašifrovaných dat	7
7	Pořadí zpracování	11
8	Schválený postup pro šifrovací algoritmy	12
	Přílohy	
	A Postup pro kontrolu alternativních šifrovacích algoritmů	13
	B Příklady filtrování	15
	C Filtrování - Rozšiřující faktory pro vybrané filtry	18
	D Příklady ilustrující šifrování a dešifrování prvků, určených pro šifrování	19

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 organizace, vládní i nevládní, s nimiž ISO navázalo pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech

záležitostech normalizace v elektrotechnice.

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 10126-1 byla připravena technickou komisí ISO/TC 68, *Bankovnictví a souvisící finanční služby, subkomise SC 2 Činnosti a postupy.*

ISO 10126 obsahuje následující části s obecným názvem Bankovnictví - Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu):

- 1. část: Obecné zásady
- 2. část: Algoritmus DEA

ISO 10126 vychází z práce vykonané v ANSI a je vývojovým stupněm ANSI X9.23 (1988), *Finanční instituce: Šifrování finančních zpráv u bankovních služeb pro velkou klientelu*, přičemž zůstává s touto normou kompatibilní.

Cílem čtyř příloh k této části ISO 10126 je usnadnit její implementaci.

a) Příloha A uvádí postup pro kontrolu alternativních šifrovacích algoritmů.

b) Příloha B uvádí příklady různých filtrovacích technik, popsaných v této části ISO 10126.

c) Příloha C provádí srovnání účinků filtrů popsaných v této části ISO 10126 a s použitím faktoru rozšíření ukazuje vztah mezi počtem přenášených a vytvořených bitů.

---

d) Příloha D uvádí příklady tří metod šifrování a dešifrování prvků, určených pro šifrování uvnitř zprávy, popsaných v této části ISO 10126.

Příloha A je nedílnou součástí této části ISO 10126. Přílohy B, C a D mají pouze informativní charakter.

Úvod

Tato část ISO 10126 specifikuje metodu pro šifrování a dešifrování celých (nebo částí) finančních zpráv u bankovních služeb pro velkou klientelu využitím šifrování na aplikační úrovni s cílem zajistit důvěrnost.

Úroveň bezpečnosti zajišťovaná touto částí ISO 10126 je závislá

a) na bezpečnosti spojené s algoritmem používaným pro šifrování a na implementaci tohoto algoritmu v postupech stanovených v této části ISO 10126 a

b) na operaci bezpečného systému správy klíčů.

Zvláštní algoritmy, vhodné pro použití u této části ISO 10126 jsou popsány v ISO 10126-2. Vhodný mezinárodní standard pro správu klíčů je popsán v ISO 8732.

1 Předmět normy

Definované postupy jsou navrženy na ochranu finančních zpráv (celých zpráv nebo prvků, určených pro šifrování), vyměňovaných prostřednictvím jakékoliv komunikační architektury, pomocí šifrování. Tyto architektury zahrnují střádačový systém předávání zpráv a telexové prostředí, libovolný počet uzlů a veřejné nebo privátní sítě.

Protože šifrovaný text může interferovat s komunikačními procesy v existujících finančních sítích služeb pro velkou klientelu, zajišťuje tato část ISO 10126 prostředky umožňující přenos šifrovaných zpráv mnoha sítěmi, aniž by byly chybně interpretovány jako informace komunikačního protokolu [např. STX (začátek textu), EOT (konec textu)].

Použitím této části ISO 10126 je chráněna důvěrnost dat finančních zpráv ve strukturované i nestrukturované formě.

Popsané techniky nezajišťují ochranu integrity (t. j. ochranu proti modifikaci, substituci nebo opakovanému přenosu). Ochrana integrity dat je předmětem ISO 8730 a ISO 8731. Formáty zpráv jsou rovněž mimo rozsah této části ISO 10126.

-- Vynechaný text --