ČESKÁ TECHNICKÁ NORMA

ICS 35.240.15

Listopad

2003

	Bankovnictví - Bezpečný přenos souborů (drobné obchody)	ČSN ISO 15668 97 9120

Banking - Secure file transfer (retail)

Banque - Transfert de fichier de sécurité (services aux particuliers)

Bankwesen - Sichere Dateienübertragung (Einzelhandel)

Tato norma je českou verzí mezinárodní normy ISO 15668:1999. Mezinárodní norma ISO 15668:1999 má status české technické normy.

This standard is the Czech version of the International Standard ISO 15668:1999. The International Standard ISO 15668:1999 has the status of a Czech Standard.

68311

Národní předmluva

Citované normy

ISO 8372:1987 zavedena v ČSN ISO 8372:1998 (97 9117) Zpracování informací - Módy činnosti pro

algoritmus 64-bitové blokové šifry

ISO 8583:1993 zavedena v ČSN ISO 8583:1999 (36 9740) Zprávy vytvořené na bázi karet pro finanční transakce - Specifikace pro výměnu zpráv

ISO 8731-1:1987 zavedena v ČSN ISO 8731-1:1996 (97 9003) Bankovnictví - Schválené algoritmy pro autentizaci zprávy - Část 1: DEA

ISO 9564-1:1991 zavedena v ČSN ISO 9564-1:1996 (97 9007) Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel - Část 1: Zásady a techniky ochrany PIN, nahrazena ISO 9564-1:2000

ISO/IEC 9796:1991 dosud nezavedena, nahrazena ISO/IEC 9796-3:2000

ISO/IEC 9796-2:1997 zavedena v ČSN ISO/IEC 9796-2:1999 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy - Část 2: Mechanismy používající hašovací funkci, nahrazena ISO/IEC 9796-2:2002

ISO/IEC 9797:1994 zavedena v ČSN ISO/IEC 9797:1997 (36 9782) Informační technologie - Bezpečnostní techniky - Mechanismus integrity dat používající kryptografickou kontrolní funkci s využitím algoritmu blokové šifry, nahrazena ISO/IEC 9797-1:1999 a ISO/IEC 9797:2002

ISO/IEC 9798-1:1991 zavedena v ČSN ISO/IEC 9798-1:1997 (36 9743) Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 1: Všeobecný model, nahrazena ISO/IEC 9798-1:1997

ISO/IEC 9798-2:1994 nahrazena ISO/IEC 9798-2:1999, zavedena v ČSN ISO/IEC 9798-2:2000 (36 9743) Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 2: Mechanismy používající symetrické šifrovací algoritmy

ISO/IEC 9798-3:1993 zavedena v ČSN ISO/IEC 9798-3:1997 (36 9743) Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 3: Autentizace entit používající algoritmus s veřejným klíčem, nahrazena ISO/IEC 9798-3:1998

ISO/IEC 9798-4:1995 zavedena v ČSN ISO/IEC 9798-4:2001 (36 9743) Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 4: Mechanismy používající kryptografickou kontrolní funkci, nahrazena ISO/IEC 9798-4:1999

ISO 9807:1991 zavedena v ČSN ISO 9807:1996 (97 9005) Bankovnictví a související finanční služby - Požadavky na autentizaci zpráv (drobné obchody)

ISO/IEC 10116:1997 zavedena v ČSN ISO/IEC 10116:2000 (36 9742) Informační technologie - Módy činnosti pro algoritmus n-bitové blokové šifry

ISO/IEC 10118-1:1994, nahrazena ISO/IEC 10118-1:2000, zavedena v ČSN ISO/IEC 10118-1:2002 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 1: Všeobecně

ISO/IEC 10118-2:1994, nahrazena ISO/IEC 10118-2:2002 zavedena v ČSN ISO/IEC 10118-2:2002 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 2: Hašovací funkce používající algoritmus n-bitové blokové šifry

ISO 11568 (všechny části) zavedena v ČSN ISO 11568:1997 (97 9114) Bankovnictví - Správa klíčů (drobné bankovnictví)

ISO/IEC 13888-2:1998 zavedena v ČSN ISO/IEC 13888-2:2001 (36 9787) Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 2: Mechanismy používající symetrické techniky

ISO/IEC 13888-3:1997 zavedena v ČSN ISO 13888-3:2001 (36 9787) Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 3: Mechanismy používající asymetrické techniky

NIST FIPS PUB 180-1, Bezpečný hašovací standard (Bezpečný hašovací algoritmus SHA-1)

Národní poznámky

1) V normě byly při převzetí opraveny formální chyby, zjištěné v originálním dokumentu. Oprava se týká číslování článků pod A.1.1 a A.1.3 v příloze A.

2) Pro účely této normy je anglický výraz download překládán jako zavádění nebo zavedení, upload jako nahrávání jako nahrání.

3) V anglickém originálu normy nejsou uvedeny samostatně zkratky, ale vysvětlení méně obvyklých zkratek je umístěno průběžně v textu (např. EPOS, AVM, ATM) nebo v definicích (např. MAC). BIN je označení extenze souboru.

4) Anglické slovo "security" se pro účely této normy překládá českým slovem "bezpečnost".

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA
Bankovnictví - Bezpečný přenos souborů (drobné obchody) ISO 15668

První vydání
1999-12-01

ICS 35.240.15

Obsah

Strana

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 s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Mezinárodní normy jsou navrhovány v souladu s pravidly uvedenými v části 3 Směrnic ISO/IEC.

Návrhy mezinárodních norem, přijaté technickými komisemi, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Je třeba věnovat pozornost tomu, že některé části této mezinárodní normy mohou být předmětem patentových práv. ISO neodpovídá za identifikaci jakýchkoliv nebo všech takových patentových práv.

Mezinárodní norma ISO 15668 byla připravena technickou komisí ISO/TC 68, *Bankovnictví, cenné papíry a jiné finanční služby,* subkomise SC 6, *Finanční služby v oblasti drobných obchodů.*

Přílohy A až D této mezinárodní normy jsou pouze informativní.

Úvod

Tato mezinárodní norma popisuje, jak zabezpečit přenosy souborů v prostředí drobných bankovních obchodů. Typickým příkladem takových přenosů souborů jsou přenosy mezi zařízením akceptujícím karty a zúčtovací bankou, nebo mezi zúčtovací bankou a vydavatelem karet.

1 Předmět normy

Na rozdíl od přenosů souborů v prostředí velkého bankovnictví, které jsou charakterizované výměnami velkých objemů dat mezi velkými počítači v prostředí s relativně vysokou bezpečností („přenosy velkých souborů“) jsou přenosy v prostředí drobného bankovnictví, ve kterém se používají nástroje zavedené z počítače, charakterizovány malými objemy a menším stupněm spolehlivosti prostředí. Takovým zařízením může být například terminál v elektronickém místě prodeje (EPOS), automatické prodejní zařízení (AVM), bankomat (ATM) nebo server obchodníka při komunikaci s platebními branami.

Předpokládá se, že mezi entitami účastnícími se bezpečného přenosu souborů existuje předem stanovený vztah, který by měl zejména pokrýt právní a komerční aspekty vztahující se k odpovědnosti za přenos souborů.

Tato mezinárodní norma se aplikuje na různé druhy přenosu souborů použité v prostředí drobného bankovnictví, ale nepokrývá transakční zprávy identifikované v ISO 8583.

Přenos může vyžadovat včasnost a vyžaduje alespoň jednu z následujících bezpečnostních služeb:

– autentizaci původu zprávy;

– autentizaci příjemce;

– integritu;

– důvěrnost;

– nepopiratelnost původu;

– nepopiratelnost doručení;

– auditovatelnost.

Předpokládá se, že všechna data (pře)poslaná původcem musí být před uskutečněním přenosu potvrzena jako legitimní a správná.

Různé typy souborů určených k přenosu mohou obsahovat:

– software

– drobné transakce, které byly provedeny a registrovány, (nahrání)

– technická data vztahující se k zúčtovací bance (parametry přístupu...), (zavedení)

– aplikační data vztahující se k zúčtovací bance (seznam BIN, „horký seznam“ (hot list), ...), (zavedení).

Přenosy těchto souborů mají následující charakteristiky:

a) typem dat určených k přenosu mohou být

- neutajovaná data (kolekce drobných transakcí, technická data, aplikační data); nebo
- utajovaná data.

b) počet entit přijímajících dat může být:

- jedna
- více než jedna (vysílání i s tisíci příjemci)

c) komunikační kanály mohou sestávat z jednoho nebo z obou následujících příkladů:

- telekomunikace: veřejná sí», soukromá sí»

d) povaha přenosu může být:

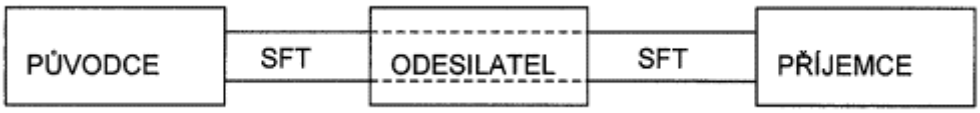
- přímo spojený, v reálném čase uskutečněný přenos (nazývaný také přepojování okruhů); nebo
- střádačový systém přenosu (nazývaný také přepojování zpráv).

POZNÁMKA Tato mezinárodní norma zohledňuje během přenosu bezpečnostní službu. Požadavky nutné k zajištění, že přenášené soubory nejsou po uskutečnění přenosu změněny, jsou mimo rozsah této mezinárodní normy.

Přípustné formy bezpečného přenosu souborů

Přenos zabezpečených souborů

Funkce přenosu neposkytuje žádné bezpečnostní služby, ale zahrnuje pouze komunikační služby. V tomto případě musí být soubor před uskutečněným přenosem zabezpečený. Bezpečnost je řízena samotným původcem a příjemcem. Nemusejí se tak spoléhat na nižší vrstvy. Komunikační vrstva (odesilatel a příjemce) nepřidává žádnou bezpečnost.



SFT = Bezpečný přenos souborů (Secure File Transfer)

-- Vynechaný text --