ČESKÁ TECHNICKÁ NORMA

ICS 35.240.40 **Březen**
2005

Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel (PIN) - Část 1: Základní principy a požadavky na online zacházení s PIN v systémech ATM a POS	ČSN ISO 9564-1 97 9007

Banking - Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements
for online PIN handling in ATM and POS systems

Banque - Gestion et sécurité du numéro personnel d'identification (PIN) - Partie 1: Principes et exigences de base
pour la gestion du PIN en ligne dans les systémes ATM et POS

Bankwesen - PIN-Management und Sicherheit - Teil 1: Grundsätze und Verfahren zum Schutz der PIN bei Online-PIN-Prüfung in- ATM und POS-Systemen

Tato norma je českou verzí mezinárodní normy ISO 9564-1:2002. Mezinárodní norma ISO 9564-1:2002 má status české technické normy.

This standard is the Czech version of the International Standard ISO 9564-1:2002. The International Standard ISO 9564-1:2002 has the status of a Czech Standard.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN 9564-1 (97 9007) z ledna 1996.

72036

Národní předmluva

Změny proti předchozí normě

Tato norma zpřísňuje zásady pro řízení a bezpečnost PIN.

Citované normy

ISO 9564-2:1991 zavedena v ČSN ISO 9564-2:1996 (97 9007) Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel (PIN) - Část 2: Schválené algoritmy pro šifrování PIN

ISO 11568 (všechny části) zavedena v ČSN ISO 11568:1997 Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu)

ISO 13491 (všechny části) zavedena v ČSN ISO 13491 (97 9121) Bankovnictví - Bezpečná kryptografická zařízení (bankovní služby pro drobnou klientelu)

ISO/IEC 7812 (všechny části) zavedena v ČSN ISO/IEC 7812 (36 9732) Identifikační karty - Identifikace vydavatelů karet

ISO/IEC 7813:2001 zavedena v ČSN ISO/IEC 7813:2002 (36 9733) Identifikační karty - Karty pro finanční transakce

ISO/IEC 7816 (všechny části) zavedena v ČSN ISO/IEC 7816 (36 9205) Identifikační karty - Karty s integrovanými obvody s kontakty

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42, Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel (PIN) - Část 1: Základní principy a požadavky na online zacházení s PIN v systémech ATM a POS

ISO 9564-1

Druhé vydání

2002-04

ICS 35.240.40

ISO copyright office
Case postale 56, CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

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

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

Hlavním úkolem technických komisí je příprava mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členským orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % z hlasujících členů.

Je třeba upozornit, že některé prvky této části ISO 9564 mohou být předmětem patentových práv. ISO nepřejímá odpovědnost za identifikaci některých nebo všech patentových práv.

ISO 9564-1 byla připravena technickou komisí ISO/TC 68, *Bankovnictví, cenné papíry a ostatní finanční služby*, subkomise SC 6, *Finanční služby v drobném bankovnictví*.

Toto druhé vydání ruší a nahrazuje první vydání (ISO 9564-1:1991), které bylo technicky revidováno.

ISO 9564 se skládá z následujících částí se společným názvem *Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel (PIN):*

– *Část 1: Základní principy a požadavky na online zacházení s PIN v systémech ATM a POS*

– *Část 2: Schválený(é) algoritmus(y) pro zašifrování PIN*

– *Část 3: Požadavky na ochranu PIN pro offline zacházení s PIN v systémech ATM a POS*

Přílohy A až G této části ISO 9564 mají pouze informativní charakter.

Úvod

Osobní identifikační číslo (PIN) je prostředek pro ověření identity zákazníka v systému elektronického převodu finančních fondů (EFT).

Cílem řízení PIN je chránit PIN před neautorizovaným odhalením, kompromitováním a nesprávným použitím v průběhu jeho životního cyklu a minimalizovat tak riziko podvodu, které se může vyskytnout v systémech EFT. Utajení PIN je nutné zajistit v průběhu celého životního cyklu, který sestává z výběru, vydání, aktivace, uložení, vstupu, přenosu, validace, deaktivace a jakéhokoliv dalšího použití PIN.

Bezpečnost PIN také závisí na řádné správě klíčů. Udržování kryptografických klíčů v tajnosti má zásadní význam, protože kompromitace kteréhokoliv klíče umožňuje kompromitaci každého PIN, zašifrovaného pod tímto klíčem.

Tato část ISO 9564 specifikuje požadavky v absolutních podmínkách, kdekoliv je to možné. V některých případech prakticky není možno se vyhnout určité úrovni subjektivity, zejména při diskusi o stupni požadované nebo dosažené bezpečnosti.

Úroveň bezpečnosti, které by mělo být dosaženo, je nutné vztahovat k určitému počtu faktorů, včetně citlivosti dotyčných dat a pravděpodobnosti, že data budou zachycena, reálnosti předpokládaného šifrovacího procesu a nákladů na poskytnutí a prolomení konkrétních prostředků na zajištění bezpečnosti. Je proto nezbytné, aby se každý akceptor, zpracovatel a vydavatel karty dohodli na rozsahu a podrobnostech bezpečnosti a řízení PIN. Absolutní bezpečnost není prakticky možné dosáhnout; postupy pro řízení PIN by proto měly implementovat preventivní opatření, aby se snížila příležitost k prolomení bezpečnosti, a usilovat o „vysokou“ pravděpodobnost detekce jakéhokoliv nezákonného přístupu nebo změny materiálu PIN v případě, že by tato preventivní opatření selhala. To se vztahuje na všechny fáze generování, výměny a použití PIN, včetně procesů, které se vyskytují v kryptografickém zařízení nebo souvisí s komunikací PIN.

Tato část ISO 9564 je navržena tak, aby vydavatelé mohli jednoznačně zajistit, do jakého stupně je praktické, aby PIN, i když bude pod kontrolou jiných institucí, byl náležitě řízen. Jsou stanoveny techniky na ochranu procesu autentizace zákazníka, založeného na PIN, ochranou PIN proti neautorizovanému odhalení v průběhu celého životního cyklu PIN. Budou publikovány další části, které budou obsahovat principy a techniky ochrany PIN, elektronický obchod a další prostředí, identifikovaná při tvorbě tohoto dokumentu.

V ISO 9564-2 jsou specifikovány schválené šifrovací algoritmy, které mají být použity při ochraně PIN. Aplikace požadavků této části ISO 9564 vyžaduje, aby byly realizovány dvoustranné dohody, včetně volby algoritmů specifikovaných v ISO 9564-2.

Tato část ISO 9564 je jednou ze série dále uvedených norem, které popisují požadavky na bezpečnost v prostředí drobného bankovnictví:

ISO 9564-2:1991 *Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel (PIN) - Část 2: Schválené algoritmy pro šifrování PIN*

ISO 9564-3:-[1)] *Banking - Personal Identification Number (PIN) management and security - Part 3: PIN protection requirements for offline PIN handling in ATM and POS systems*

ISO 10202 (všechny části) *Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody*

ISO 11568 (všechny části) *Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu)*

ISO 13491 (všechny části) *Bankovnictví - Bezpečná kryptografická zařízení (bankovní služby pro*

drobnou klientelu)

ISO 15668 *Bankovnictví - Bezpečný přenos souborů (drobné obchody)*

[1)] Bude publikována.

---

1 Předmět normy

Tato část ISO 9564 specifikuje základní principy a techniky, poskytující minimální bezpečnostní opatření požadovaná pro efektivní mezinárodní řízení PIN. Tato opatření mohou aplikovat instituce, které jsou odpovědné za implementaci technik pro řízení a ochranu PIN.

Tato část ISO 9564 rovněž specifikuje techniky ochrany PIN aplikovatelné na transakce vytvářené pomocí karet pro finanční transakce v online prostředí a normalizované prostředky pro výměnu PIN dat. Tyto techniky mohou použít instituce, odpovědné za implementaci technik pro řízení a ochranu PIN v bankomatech (ATM) a terminálech v místě prodeje (POS) sponzorovaných zpracovatelem.

Ustanovení této části ISO 9564 nemají za cíl řešit:

a) řízení a bezpečnost PIN v offline PIN prostředí, což je řešeno v ISO 9564-3;

b) řízení a bezpečnost PIN v prostředí elektronického obchodu, což má být popsáno v další části ISO 9564;

c) ochranu PIN před ztrátou nebo úmyslným nesprávným použitím zákazníkem nebo autorizovanými zaměstnanci vydavatele;

d) soukromí transakčních dat, která nemají charakter PIN;

e) ochranu zpráv transakce před změnou nebo substitucí, například autorizační odezva na ověření PIN;

f) ochranu před opakovaným přenosem PIN nebo transakce;

g) specifické techniky správy klíčů.

-- Vynechaný text --