ČESKÁ TECHNICKÁ NORMA

ICS 35.240.40 **Srpen**
2005

Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel - Část 3: Požadavky na off-line zacházení s PIN v systémech ATM a POS	ČSN ISO 9564-3 97 9007

Banking - Personal Identification Number management and security - Part 3: Requirements for offline PIN handling
in ATM and POS systems

Banque - Gestion et sécurité du numéro personnel d´identification - Partie 3: Exigences relatives à la protection du PIN
pour traitement du PIN hors ligne dans les systèmes ATM et POS

Bankwesen - PIN-Management und Sicherheit - Teil 3: Verfahren zum Schutz der PIN bei Offline-PI--Prüfung in ATM
und POS-Systemen

Tato norma je českou verzí mezinárodní normy ISO 9564-3:2003. Mezinárodní norma ISO 9564-3:2003 má status české technické normy.

This standard is the Czech version of the International Standard ISO 9564-3:2003. The International Standard ISO 9564-3:2003 has the status of a Czech Standard.

Národní předmluva

Citované normy

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

ISO 9564-1:2002 zavedena v ČSN ISO 9564-1:2005 (97 9007) 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 9564-2:1991 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 11568-2 zavedena v ČSN EN ISO 11568:1997 (97 9114) Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 2: Techniky správy klíčů pro symetrické šifry

EMV2000 nezavedeno

Národní poznámka

Pro potřeby této normy se anglické slovo „security“ překládá českým slovem „bezpečnost“.

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 - Část 3:Požadavky na offline zacházení s PIN v systémech ATM a POS

ISO 9564-3
První vydání
2003-11-15

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 2 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 tohoto dokumentu mohou být předmětem patentových práv. ISO nepřejímá odpovědnost za identifikaci některých nebo všech patentových práv.

ISO 9564-3 byla připravena technickou komisí ISO/TC 68, *Bankovnictví, cenné papíry a ostatní finanční služby,* subkomise SC 6, *Finanční služby v drobném bankovnictví*.

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

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

– *Část 2: Schválené algoritmy pro zašifrování PIN*

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

Část 4, Doporučené praktiky pro zacházení s PIN v otevřených sítích, je ve fázi přípravy.

Úvod

Karty pro finanční transakce s vloženými integrovanými obvody (IC) umožnily technicky snadno provádět offline ověření PIN s použitím karet IC. Vydavatelé karet mohou zvolit mezi online nebo offline způsobem ověření PIN. Tato část ISO 9564 stanovuje specifické požadavky pro offline zacházení s PIN.

Offline ověření PIN nevyžaduje, aby PIN držitele karty byl pro ověření posílán hostitelskému systému vydavatele, a z tohoto důvodu se nemusí mnoho bezpečnostních požadavků vztahujících se k ochraně PIN v sítích aplikovat. Mnoho všeobecných zásad a technik pro ochranu PIN je však možné použít i v případě, že je PIN ověřováno offline. Tato část ISO 9564 se omezuje na požadavky vztahující se specificky na podstatu offline zacházení s PIN a pokud to není explicitně vyloučeno, je možné aplikovat základní principy řízení PIN stanovené v ISO 9564.

ISO 10202[1] a zejména část 6 této mezinárodní normy definuje bezpečnostní požadavky na ověření držitele karty s použitím karet IC. Měli bychom si však povšimnout, že ISO 10202 definuje požadavky spíše na karty IC samotné než na akceptační systémy zpracovatele karet IC a může tak být považována za doplněk k ISO 9564.

1 Předmět normy

Tato část ISO 9564 specifikuje minimální bezpečnostní požadavky požadované při offline zacházení s osobním identifikačním číslem (PIN) a standardní prostředky vzájemné výměny dat PIN v offline prostředí.

Je aplikovatelná na finanční transakce, na transakce vytvářené pomocí karet vyžadující offline ověření PIN a na instituce, které jsou odpovědné za implementaci technik pro řízení a ochranu PIN v ATM a terminálech v místě prodeje (POS) podporovaných zpracovatelem.

Tuto část ISO 9564 *nelze* použít na

a) řízení a bezpečnost PIN v online prostředí PIN, kterým se zabývá ISO 9564-1,
b) schválené algoritmy pro šifrování PIN, kterými se zabývá ISO 9564-2,
c) použití PIN v otevřeném prostředí sítí, kterým se zabývá ISO 9564-4,
d) ochranu PIN před ztrátou nebo záměrným nesprávným použitím zákazníkem nebo autorizovanými zaměstnanci vydavatele nebo jejich agentů,
e) zajištění soukromí dat transakcí, nemajících charakter dat PIN,
f) ochranu zpráv transakcí před změnou nebo nahrazením, např. online odezvu autorizace,
g) ochranu před opakovaným přehráním PIN nebo transakce,
h) specifické techniky správy klíčů,
i) rozhodnutí, zda by měla karta IC přijmout PIN zašifrované,
j) bezkontaktní karty IC.

Základní principy řízení PIN popsané v kapitole 4 ISO 9564-1:2002 jsou pro tuto část ISO 9564 platné a normativní.

Požadavky spojené s kartami IC pro více aplikací jsou považovány za věc vydavatele a nejsou zde obsaženy.

Tato část ISO 9564 je zpracována na základě požadavků aplikovatelných v technologii karet IC, tím však není míněno omezení její použitelnosti pouze na technologii karet IC.

-- Vynechaný text --