ČESKÁ NORMA

ICS 03.060;35.240.40

Leden 1996

Bankovnictví
ŘÍZENÍ A BEZPEČNOST OSOBNÍCH IDENTIFIKAČNÍCH ČÍSEL
Část 1: Principy a techniky ochrany PIN

ČSN
ISO 9564-1

97 9007

Banking - Personal Identification Number management and security Part 1: PIN protection principles and techniques

Banque - Gestion et sécurité du numéro personnel d'identification Partie 1: Principes et techniques de protection du PIN

Bankwesen: PIN-Ausgabe und -Verwaltung und PIN-Sicherheit Teil 1: Grundsätze und Verfahren zum Schutz der PIN

Tato norma je identická s ISO 9564-1:1991

Národní předmluva

Citované normy

ISO 7812:1987 dosud nezavedena

ISO 8583:1987 dosud nezavedena

ISO 8908:1993 dosud nezavedena

ISO 9807:1991 zavedena v ČSN ISO 9807 Bankovnictví - Požadavky na autentizaci zpráv (bankovní služby pro drobnou klientelu) (97 9005)

Vypracování normy

Zpracovatel normy: Česká národní banka, Ing.Hönigová Alena IČO 48136450

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Bankovnictví
ŘÍZENÍ A BEZPEČNOST OSOBNÍCH IDENTIFIKAČNÍCH ČÍSEL
Část 1: Principy a techniky ochrany PIN

ISO 9564-1
První vydání
1991-12-15

MDT 336.717:351.755.6:003.26

Deskriptory: banking, bank accounts, identification methods, registration number, protection of information, coded representation, algorithms.

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 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 9564-1 byla připravena technickou komisí ISO/TC 68, *Bankovnictví a související finanční služby*, SC 6, *Karty pro finanční transakce, související media and operace.*

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

1. část: Principy a techniky ochrany PIN

2. část: Schválené algoritmy pro šifrování PIN

Přílohy A a B jsou integrální součástí této části ISO 9564. Přílohy C, D, E, F, G a H mají pouze informativní charakter.

Úvod

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

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

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

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

Úroveň bezpečnosti, které by mělo být dosaženo, je nutné vztahovat k určitému počtu faktorů, včetně citlivosti dotyčných dat a pravděpodobnosti, že dojde k zachycení dat, praktičnosti předpokládaného šifrovacího procesu, nákladů na poskytnutí a prolomení zvláštního prostředku na zajištění bezpečnosti. Je proto nezbytné, aby se každý akceptor, zpracovatel a vydavatel karty dohodli na rozsahu a podrobnostech postupů bezpečnosti a řízení PIN. Absolutní bezpečnost není prakticky možné dosáhnout; proto by měly postupy pro řízení PIN implementovat preventivní opatření ke snížení příležitosti k prolomení bezpečnosti a usilovat o „vysokou" pravděpodobnost zjištění jakéhokoliv nelegálního přístupu nebo změny k materiálům PIN, důsledkem čehož by mohla tato preventivní opatření selhat. To se vztahuje na všechny etapy generování, výměny a použití PIN, včetně těch procesů, které se vyskytují v kryptografickém zařízení a těch, které souvisí s komunikací PIN.

Tato část ISO je navržena tak, aby si vydavatelé mohli být jednoznačně jisti, že i když PIN bude pod kontrolou jiných institucí, bylo řádně spravováno. Jsou stanoveny techniky pro ochranu procesu

autentizace zákazníka, založeného na PIN, fyzickou ochranou PIN proti neautorizovanému odhalení v průběhu celého životního cyklu PIN.

Tato část ISO 9564 určuje techniky pro ochranu PIN proti neautorizovanému odhalení v průběhu jeho životního cyklu a zahrnuje následující přílohy:

a) příloha A uvádí postup pro schválení šifrovacího algoritmu;

b) příloha B pokrývá obecné zásady správy klíčů;

c) příloha C pokrývá techniky pro ověření PIN;

d) příloha D se zabývá koncepty implementace pro vstupní zařízení PIN;

e) příloha E identifikuje příklad pseudonáhodného generování PIN;

f) příloha F určuje další návody pro návrh klávesnice PIN;

g) příloha G specifikuje vymazání záznamových médií používaných pro ukládání klíčových materiálů;

h) příloha H uvádí informace pro zákazníky.

V ISO 9564-2 jsou specifikovány schválené šifrovací algoritmy určené k použití pro ochranu PIN. Aplikace požadavků této části ISO 9564 vyžaduje uzavření dvojstranných dohod včetně volby algoritmů, specifikovaných v ISO 9564-2.

Tato část ISO 9564 je jednou ze série norem, dále uvedených, popisujících požadavky na bezpečnost v prostředí bankovních služeb pro drobnou klientelu:

ISO 9564-1:1991, *Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel - 1. část: Principy a techniky ochrany PIN.*

ISO 9564-2:1991, *Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel - 2. část: Schválený*(é) *algoritmus(-y) pro šifrování PIN.*

ISO 9807:1991, *Bankovnictví - Požadavky na autentizaci zpráv (bankovní služby pro drobnou klientelu).*

Požadavky ISO 9564 jsou kompatibilní s požadavky na úpravu dat vztahujících se k bezpečnosti, uvedenými v ISO 8583.

1 Předmět normy

Tato část ISO 9564 specifikuje minimální bezpečnostní opatření požadovaná pro efektivní mezinárodní řízení PIN. Poskytuje standardní prostředek pro výměnu dat PIN. Tato část ISO 9564 také specifikuje pravidla vztahující se ke schválení algoritmů na šifrování PIN. Tuto část ISO 9564 mohou aplikovat instituce, které jsou odpovědné za implementaci technik pro řízení a ochranu PIN pro transakce vytvářené pomocí bankovních karet. Ustanovení této části ISO 9564 nemají za cíl řešit

- ochranu PIN před ztrátou nebo úmyslným zneužitím zákazníkem nebo autorizovanými zaměstnanci vydavatele karet;

- privátní charakter transakčních dat, která nemají charakter PIN;

- ochranu zpráv transakce před změnou nebo substitucí, např. autorizační odpověď na ověření PIN;

- ochranu před opakovaným přenosem PIN nebo transakce;

- specifické techniky správy klíčů;

- řízení a bezpečnost PIN u transakcí řízených pomocí čipových karet (ICC);

- použití asymetrických šifrovacích algoritmů pro řízení PIN.

-- Vynechaný text --