ČESKÁ TECHNICKÁ NORMA

ICS 35.240.15 **Červen**
2005

Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 5: Použití algoritmů	ČSN ISO 10202-5 36 9736

idt ISO 10202-5:1998

Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards -
Part 5: Use of algorithms

Cartes de transactions financières - Architecture de sécurité des systèmes de transactions financières utilisant des
cartes à circuit intégré -
Partie 5: Utilisation des algorithmes

Bankkarten - Sicherheitsarchitektur in Zahlungsverkehrssystemen für Karten mit integrierten Schaltkreisen -
Teil 5 : Anwendung der Algorithmen

Tato norma je českou verzí mezinárodní normy ISO 10202-5:1998. Mezinárodní norma ISO 10202-5:1998 má
status české technické normy.

This standard is the Czech version of the International Standard ISO 10202-5:1998. The International Standard ISO 10202-5:1998 has the status of a Czech Standard.

Národní předmluva

Citované normy

ISO 4909 zavedena v ČSN ISO 4909 (36 9727) Bankovní karty - Obsah dat magnetického proužku pro stopu 3

ISO 9564-1 zavedena v ČSN ISO 9564-1 (97 9007) Bankovnictví. Řízení a bezpečnost osobních identifikačních čísel. Část 1: Principy a techniky ochrany PIN

ISO/IEC 9796 zavedena v souboru ČSN ISO/IEC 9796 (36 9736) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy

ISO 10202-1 zavedena v ČSN ISO 10202-1 (36 9736) Identifikační karty - Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 1: ®ivotní cyklus karty

ISO 10202-2 zavedena v ČSN ISO 10202-2 (36 9736) Identifikační karty - Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 2: Proces transakce

ISO 10202-3 zavedena v ČSN ISO 10202-3 (36 9736) Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 3: Vztahy mezi kryptografickými klíči

ISO 10202-4 zavedena v ČSN ISO 10202-4 (36 9736) Identifikační karty - Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 4: Bezpečné aplikační moduly

ISO 10202-6 zavedena v ČSN ISO 10202-6 (36 9736) Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 6: Ověření držitele karty

ISO 10202-7 zavedena v ČSN ISO 10202-6 (36 9736) Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 7: Správa klíčů

ISO 10202-8 zavedena v ČSN ISO 10202-8 (36 9736) Identifikační karty - Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 8: Všeobecné zásady a přehled

Vysvětlivky k textu převzaté normy

V anglickém originálu jsou často odkazy na čísla obrázků posunuty o 1.

Anglický termín	**Český termín**	**Použitý termín**
Hash (function)	• Hašovací funkce • Digitální otisk	Hašovací (funkce)
Plain text	• Nezašifrovaný text • Čitelný text	• Nezašifrovaný text • Čitelný text

	• Otevřený text	
Application data file, ADF	• Soubor aplikačních dat • Soubor dat aplikace	Soubor aplikačních dat
Common data file, CDF	• Soubor společných dat • Soubor základních dat	Soubor společných dat

Upozornění na národní poznámky

Do normy byla k článku 3.21 doplněna informativní národní poznámka.

Vypracování normy

Zpracovatel: Anna Juráková, Praha, IČO 61278386, Dr. Karel Jurák

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 5: Použití algoritmů

ISO 10202-5

První vydání

1998-07

ICS 35.240.15

Obsah

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětovou federací národních normalizačních orgánů

(členů ISO). Mezinárodní normy obvykle připravují technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala 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 % hlasujících členů.

Mezinárodní norma ISO 10202-5 byla vypracována technickou komisí ISO/TC 68, *Bankovnictví, cenné papíry a ostatní finanční služby*, subkomisí SC 6, *Finanční služby v drobném bankovnictví.*

ISO 10202 sestává z následujících částí se společným názvem *Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody*:

– *Část 1: ®ivotní cyklus karty*

– *Část 2: Proces transakce*

– *Část 3: Vztahy mezi kryptografickými klíči*

– *Část 4: Bezpečné aplikační moduly*

– *Část 5: Použití algoritmů*

– *Část 6: Ověření držitele karty*

– *Část 7: Správa klíčů*

– *Část 8: Všeobecné zásady a přehled*

Přílohy A až H této části ISO 10202 jsou pouze informativní.

Úvod

Normalizace bezpečnostní architektury systémů finančních transakcí, které používají karty s integrovanými obvody (ICC), je rozdělena do následujících částí:

Část 1: ®ivotní cyklus karty

Část 2: Proces transakce

Část 3: Vztahy mezi kryptografickými klíči

Část 4: Bezpečné aplikační moduly

Část 5: Použití algoritmů

Část 6: Ověření držitele karty

Část 7: Správa klíčů

Část 8: Všeobecné zásady a přehled

Tato část ISO 10202 popisuje kryptografické procesy, které jsou k dispozici pro splnění bezpečnostních funkcí definovaných v částech 2, 4 a 6, které vyžadují kryptografické algoritmy.

ISO 10202 umožňuje provádění všech bezpečnostních funkcí se symetrickým nebo asymetrickým typem algoritmu. ISO 10202 se nezabývá technikami s nulovou znalostí, které mohou být zahrnuty v dalších etapách.

Všechny uzly, které se účastní v daném kryptografickém procesu, musí být schopny provádět požadované kryptografické funkce.

Kryptografické procesy, které jsou nutné pro provedení bezpečnostní funkce, jsou specifikovány ve volbách. Pro každý kryptografický proces je specifikována samostatná volba pro každý typ algoritmu. Rovněž je specifikována samostatná volba pro každou variantu kryptografického procesu, která vyžaduje další komunikační kroky.

Kapitola 5 mapuje bezpečnostní funkce na kryptografické procesy, které jsou k dispozici pro jejich dosažení.

Kapitola 6 specifikuje podrobnosti kryptografických procesů. Tato část ISO 10202 není implementační specifikací, avšak vyznačuje datové prvky požadované v obou uzlech pro zajištění, že kryptografický proces je prováděn ve shodě s požadovanými bezpečnostními postupy.

1 Předmět normy

Tato část ISO 10202 platí pro kryptografické výměny, kde alespoň jeden uzel je ICC nebo SAM. Výměny mezi dalšími uzly systému jsou mimo předmět této části ISO 10202.

Použití libovolné bezpečnostní funkce je volitelné v závislosti na požadavcích systému. Pokud se požaduje specifická funkce, musí se provádět zde popsaným způsobem.

-- Vynechaný text --