ČESKÁ TECHNICKÁ NORMA

ICS 35.240.15 **Srpen**
2005

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

Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards -
Part 7: Key management

Cartes de transactions financières - Architecture de sécurité des systèmes de transactions financières utilisant des
cartes à circuit intégré - Partie 7: Gestion de clé

Bankkarten - Sicherheitsarchitektur in Zahlungsverkehrssystemen für Karten mit integrierten Schaltkreisen -
Teil 7: Schlüsselverwaltung

Tato norma je českou verzí mezinárodní normy ISO 10202-7:1998. Mezinárodní norma ISO 10202-7:1998 má status české technické normy.

This standard is the Czech version of the International Standard ISO 10202-7:1998. The International Standard ISO 10202-7:1998 has the status of a Czech Standard.

Národní předmluva

Citované normy

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

ISO 7816-3 zavedena v ČSN ISO 7816-3 (36 9205) Informační technologie - Identifikační karty - Karty s integrovanými obvody s kontakty - Část 3: Elektronické signály a protokoly přenosu

ISO/IEC 7816-4 zavedena v ČSN EN ISO/IEC 7816-4 (36 9205) Informační technologie - Identifikační karty - Karty s integrovanými obvody s kontakty - Část 4: Mezioborové příkazy pro výměnu

ISO/IEC 7816-5 zavedena v ČSN EN ISO/IEC 7816-5 (36 9734) Identifikační karty - Karty s integrovanými obvody s kontakty - Část 5: Systém číslování a registrační postup identifikátorů aplikací

ISO 8732 zavedena v ČSN ISO 8732 (97 9117) Bankovnictví - Správa klíčů (bankovní služby pro velkou klientelu)

ISO 8908 zavedena v ČSN ISO 8908 (97 9116) Bankovnictví a související finanční služby - Slovník a datové prvky

ISO/IEC 9796 zavedena v ČSN ISO/IEC 9796 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy

ISO 9992-1 zavedena v ČSN ISO 9992-1 (36 9735) Identifikační karty. Karty pro finanční transakce. Zprávy mezi kartou s integrovanými obvody a zařízením akceptujícím kartu. Část 1: Pojmy a struktury

ISO 9992-2 dosud nezavedena

ISO 10202 (všechny části) soubor postupně zaváděn v ČSN ISO 10202 (36 9736) Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody

ISO 11568 zavedena v ČSN EN ISO 11568 (97 9114) (všechny části), Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu)

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

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

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 7: Správa klíčů

ISO 10202-7

První vydání

1998-07-15

ICS 35.240.15

Obsah

Strana

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.

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

Mezinárodní norma ISO 10202-7 byla připravena technickou komisí ISO/TC 68, *Bankovnictví, cenné papíry a ostatní finanční služby*, SC 6, *Finanční služby v drobném bankovnictví*.

ISO 10202 se skládá 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 principy a přehled*

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

1 Předmět normy

Tato část ISO 10202 specifikuje požadavky na správu klíčů pro systémy finančních transakcí používající karty s integrovanými obvody. Definuje postupy a procesy pro bezpečnou správu kryptografických klíčů použitých během životního cyklu karty a zpracování transakcí v prostředí karty s integrovaným obvodem. Jsou popsána schémata správy jak symetrických, tak i asymetrických klíčů. Jsou specifikovány minimální požadavky na správu klíčů.

Správa klíčů představuje proces, pomocí něhož jsou kryptografické klíče poskytovány pro použití mezi autorizovanými komunikujícími stranami a tyto klíče dále podléhají bezpečným postupům, dokud nejsou zničeny. Bezpečnost šifrovaných dat závisí na tom, zda je zabráněno odhalení, neautorizované modifikaci, substituci, vložení nebo vymazání klíčů. Správa klíčů se tudíž zabývá postupy generování, uchovávání, distribuce, použití a zničení klíčů. Formalizací takových postupů jsou rovněž vytvořeny

podmínky pro zřízení auditních záznamů.

Tuto část ISO 10202 lze aplikovat pro prostředí jak on-line tak i off-line zpracování transakcí mezi ICC a SAM a v on-line prostředí (end-to-end) mezi ICC a SAM nebo bezpečnostním modulem hostitelského systému.

-- Vynechaný text --