

2005

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

Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards -
Part 2: Transaction process

Cartes de transactions financières - Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré - Partie 2: Processus de transaction

Bankkarten - Sicherheitsarchitektur in Zahlungsverkehrssystemen für Karten mit integrierten Schaltkreisen -
Teil 2: Transaktionsprozess

Tato norma je českou verzí mezinárodní normy ISO 10202-2:1996. Mezinárodní norma ISO 10202-2:1996 má status české technické normy.

This standard is the Czech version of the International Standard ISO 10202-2:1996. The International Standard ISO 10202-2:1996 has the status of a Czech Standard.

	© Český normalizační institut, 2005 73638 Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.
--	--

Národní předmluva

Citované normy

ISO 7812-1:1993 zrušena¹

ISO 7812-2:1993 zrušena²

ISO/IEC 7816-3:1989 nahrazena ISO/IEC 7816-3:1997 zavedenou jako ČSN ISO/IEC 7816-3:2004 (36 9205) Identifikační karty - Karty s integrovanými obvody s kontakty - Část 3: Elektronické signály a protokoly přenosu

ISO/IEC 7816-4:1995 zavedena v ČSN EN ISO/IEC 7816-4:1997 (36 9205) Identifikační karty - Karty s integrovanými obvody s kontakty - Část 4: Meziobvodové příkazy pro vzájemnou výměnu

ISO/IEC 7816-5:1994 zavedena v ČSN EN ISO/IEC 7816-5:1996 (36 9734) Identifikační karty - Karty s integrovanými obvody s kontakty - Část 5: Systém číslování a registrační postup identifikátorů aplikací

ISO 10202-1:1991 zavedena v ČSN ISO 10202-3:1994 (36 9736) Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - @ivotní cyklus karty

ISO 10202-3:1998 zavedena v ČSN ISO 10202-3:1999 (36 9736) Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Vztahy mezi kryptografickými klíči

ISO 10202-4:1996 zavedena v ČSN ISO 10202-4:2005 (36 9736) Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 4: Bezpečné aplikační moduly

ISO 10202-5:1998 zavedena v ČSN ISO 10202-5:2005 (36 9736) Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 5: Použití algoritmů

ISO 10202-6:1994 zavedena v ČSN ISO 10202-6:1996 (36 9736) Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 6: Ověření držitele karty

ISO 10202-7:1998 zavedena v ČSN ISO 10202-7:2005 (36 9736) Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody - Část 7: Správa klíčů

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

- ¹ ISO 7812-1:1993 nahrazena ISO/IEC 7812-1:2000 zavedena v ČSN ISO/IEC 7812-1:2002 (36 9732) Identifikace vydavatelů karet – Část 1: Systém číslování
- ² ISO 7812-2:1993 nahrazena ISO/IEC 7812-2:2000 zavedena v ČSN ISO 7812-2:2002 (36 9732) Identifikace vydavatelů karet – Část 2: Aplikační a registrační postupy

Odmítavé stanovisko k manipulaci s PDF souborem

Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe lze tento soubor tisknout nebo prohlížet, ale nesmí být editován, ledaže by typy písma, které jsou vloženy, byly používány na základě licence a instalovány v počítači, na němž se editace provádí. Při stažení tohoto souboru přejímají jeho uživatelé odpovědnost za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřijímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytváření tohoto souboru PDF, lze najít ve Všeobecných informacích, které jsou k souboru připojeny; parametry, pomocí kterých byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členské organizace ISO mohly používat. V málo pravděpodobném případě, tj. když vznikne problém, který se týká souboru, informujte o tom na níže uvedené adrese Ústřední sekretariát ISO.

Všechna práva vyhrazena. Není-li uvedeno jinak, nesmí být žádná část této publikace reprodukována nebo zpracována jakoukoli jinou formou, jako jsou například elektronické nebo mechanické prostředky, včetně fotokopíí a mikrofilmu, bez písemného povolení ISO; povolení lze vyžádat na níže uvedené adrese nebo u členské národní organizace v zemi žadatele.

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

MEZINÁRODNÍ NORMA

Karty pro finanční transakce - Bezpečnostní architektura systémů
 finančních transakcí využívající karty s integrovanými obvody -
 Část 2: Proces transakce

ISO 10202-2

První vydání

1996-02-01

Obsah

Strana

1	Předmět normy	7
2	Normativní odkazy	7
3	Definice	8
4	Všeobecné zásady bezpečnosti	9
5	Bezpečnostní funkce procesu transakce	9
5.1	Inicializace kartové relace	10
5.2	Přístup k CDF	10
5.3	Autentizace a ověření specifické pro CDF	10
5.3.1	Statická autentizace CDF	10
5.3.2	Dynamická autentizace CDF	10
5.3.3	Autentizace CAD, SAM nebo hostitelského systému	10
5.3.4	Ověření držitele	

karty.....	11
5.3.5 Aktualizace parametrů	
CDF.....	11
5.4 Přístup k	
ADF	
.....	
... 11	
5.5 Autentizace a ověření specifické pro	
ADF.....	11
5.5.1 Statická autentizace	
ADF.....	11
5.5.2 Dynamická autentizace	
ADF.....	11
5.5.3 Autentizace CAD, SAM nebo hostitelského	
systemu.....	11
5.5.4 Ověření držitele	
karty.....	11
5.5.5 Aktualizace parametrů	
ADF.....	12
5.6 Zacházení s	
transakcemi	
.....	12
5.6.1 Autorizace	
transakce	
.....	12
5.6.2 Určení akceptace držitele	
karty.....	12
5.6.3 Certifikace	
transakcí	
.....	12
5.6.4 Zaznamenávání	
transakcí.....	12
5.7 Ukončení kartové	
relace.....	12
Příloha A (informativní) Příklad funkcí	

transakce.....	13
Příloha B (informativní) Příklady situací, kdy by CAD mělo provést on-line autorizaci.....	24
Příloha C (informativní) Vztahy v procesu transakce.....	25
Příloha D (informativní) Bibliografie.....	26

Strana 6

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.

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

Mezinárodní norma ISO 10202-2 byla připravena technickou komisí ISO/TC 68, *Bankovníctví, cenné papíry a ostatní finanční služby*, subkomise SC 6, *Finanční služby v drobném bankovníctví*.

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: *Životní 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, B, C a D této části ISO 10202 mají pouze informativní charakter.

Strana 7

1 Předmět normy

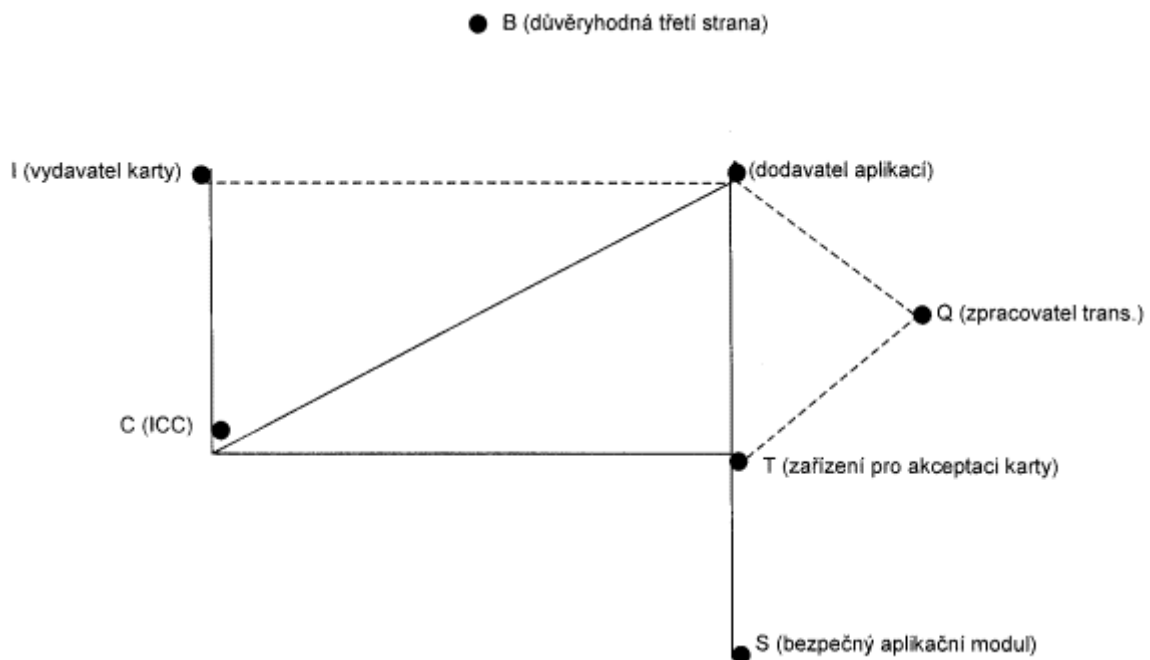
Tato část ISO 10202 specifikuje minimální úroveň bezpečnosti požadovanou pro výměnu a poskytuje bezpečnostní volby, z kterých může vydavatel karty nebo dodavatel aplikace vybrat odlišné úrovně bezpečnosti v souladu s aplikací a politikou řízení rizika.

POZNÁMKA 1 Kdykoliv je v této části ISO 10202 odkaz na vydavatele karty nebo dodavatele aplikace, tyto výrazy zahrnují agenty jmenované některými z nich.

Vztahy, na které se tato část ISO 10202 uplatňuje, jsou ukázány na obrázku 1 a vysvětleny v ISO 10202-3.

Zprávy, které nejsou autentizovány nebo kódovány kartou s integrovanými obvody ICC, jsou mimo předmět této části ISO 10202.

Vztahy zobrazené přerušovanými čarami jsou mimo rozsah této části ISO 10202.



-- Vynechaný text --