ČESKÁ TECHNICKÁ NORMA

ICS 35.040; 35.240.15; 35.240.40 **Říjen 2004**

	Bankovnictví - Bezpečná kryptografická zařízení (bankovní služby pro drobnou klientelu) - Část 2: Kontrolní seznamy shody bezpečnosti pro zařízení používaná v systémech karet s magnetickým proužkem	ČSN ISO 13491-2 97 9121

Banking - Secure cryptographic devices (retail) - Part 2: Security compliance checklists for devices used in magnetic
stripe card systems

Banque - Dispositifis cryptographiques de sécurité (services aux particuliers) - Partie 2: Listes de contrôle de conformité
de sécurité pour les dispositifs utilisés dans les systèmes de cartes à bande magnétique

Tato norma je českou verzí mezinárodní normy ISO 13491-2:2000. Mezinárodní norma ISO 13491-2:2000 má status české technické normy.

This standard is the Czech version of the International Standard ISO 13491-2:2000. The International Standard ISO 13491-2:2000 has the status of a Czech Standard.

71086

Národní předmluva

Citované normy

ISO 7498-2 zavedena v ČSN ISO 7498-2:1993 Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). Základný referenčný model. Část 2: Bezpečnostná architektúra

ISO 8908 zavedena v ČSN ISO 8908:1997 Bankovnictví a související finanční služby - Slovník a datové prvky, zrušena 2001-01

ISO 9564-1 zavedena v ČSN ISO 9564-1:1996 Bankovnictví. Řízení a bezpečnost osobních identifikačních čísel. Část 1: Principy a techniky ochrany PIN, nahrazena ISO 9564-1:2002

ISO 9564-2 zavedena v ČSN ISO 9564-2:1996 Bankovnictví. Řízení a bezpečnost osobních identifikačních čísel. Část 2: Schválené algoritmy pro šifrování PIN

ISO 9807 zavedena v ČSN ISO 9807:1996 Bankovnictví. Požadavky na autentizaci zpráv (bankovní služby pro drobnou klientelu), nahrazena ISO 16609:2004

ISO 11568 zavedeny v ČSN EN ISO 11568:1997 Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu)

ISO 13491-1 dosud nezavedena

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA
Bankovnictví - Bezpečná kryptografická zařízení (bankovní služby pro drobnou klientelu) -
Část 2: Kontrolní seznamy shody bezpečnosti pro zařízení používaná v systémech karet s magnetickým proužkem

ISO 13491-2
První vydání
2000-11-01

Obsah

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů (členů ISO). Příprava mezinárodních norem je obyčejně uskutečňována prostřednictvím technických komisí ISO. Každý členský orgán, který se zajímá o předmět, pro který byla ustavena technická komise, má právo být v této komisi reprezentován. Ve spolupráci s ISO se práce rovněž zúčastňují vládní i nevládní mezinárodní organizace. ISO úzce spolupracuje s Mezinárodní

elektrotechnickou komisí (IEC) ve všech otázkách elektrotechnické normalizace.

Mezinárodní normy jsou navrhovány v souladu s pravidly obsaženými v části 3 Směrnic ISO/IEC.

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

Pozornost je nutno věnovat možnosti, že by některé prvky této části ISO 13491 mohly být předmětem patentových práv. ISO nelze považovat za odpovědné za identifikování některých nebo všech takových patentových práv.

Mezinárodní norma ISO 13491-2 byla připravena Technickou komisí ISO/TC 68, *Bankovnictví, cenné papíry a ostatní finanční služby,* subkomise SC 6, *Finanční služby pro drobnou klientelu.*

ISO 13491 je tvořena následujícími částmi, pod společným názvem *Bankovnictví - Bezpečná kryptografická zařízení (bankovní služby pro drobnou klientelu)*:

- *Část 1: Pojetí, požadavky a metody hodnocení*
- *Část 2: Kontrolní seznamy shody bezpečnosti pro zařízení používaná v systémech karet s magnetickým proužkem*

Přílohy A až G tvoří nedílnou součást této části ISO 13491. Příloha H je pouze informativní.

Úvod

Tato mezinárodní norma specifikuje jak fyzické, tak i logické charakteristiky a správu bezpečných kryptografických zařízení (Secure Cryptographic Devices, SCDs), používaných pro ochranu zpráv, kryptografických klíčů a dalších citlivých informací používaných v prostředí drobného bankovnictví.

Bezpečnost drobného bankovnictví je ve velké míře závislá na bezpečnosti těchto kryptografických zařízení. Požadavky na bezpečnost jsou založeny na předpokladu, že k souborům uloženým na počítači lze přistupovat, lze s nimi manipulovat, komunikační linky mohou být „napíchnuty“ a autorizovaná data nebo kontrolní vstupy do systémového zařízení mohou být nahrazena neautorizovanými vstupy. Zatímco některá kryptografická zařízení (např. hostitelské bezpečnostní moduly) jsou umístěna ve zpracovatelských centrech s relativně vysokou bezpečností, velký podíl kryptografických zařízení používaných v drobném bankovnictví (např. PIN klávesnice, ATM atd.) je nyní umístěn v prostředích, která nejsou bezpečná. Proto když jsou těmito zařízeními zpracovávána citlivá data jako PIN, MAC, kryptografické klíče a jiná, existuje zde riziko, že tato zařízení mohou být narušena nebo jinak kompromitována, aby tato data byla odhalena nebo modifikována.

Prostřednictvím vhodného použití kryptografických zařízení, která mají patřičné charakteristiky fyzické a logické bezpečnosti a jsou náležitě spravována, musí být zajištěno omezení rizika finanční ztráty. Pro tato zařízení je vyžadováno hodnocení, aby bylo zajištěno, že mají správné vlastnosti z hlediska fyzické a logické bezpečnosti.

Tato část ISO 13491 poskytuje kontrolní seznamy shody bezpečnosti pro vyhodnocování bezpečných

kryptografických zařízení používaných v systémech s magnetickým proužkem v souladu s ISO 13491-1.

Vhodné charakteristiky zařízení jsou nezbytné pro zajištění, že zařízení má náležité provozní schopnosti a poskytuje přiměřenou ochranu datům, která uchovává. Nezbytná je náležitá správa zařízení, aby bylo zaručeno, že zařízení je legitimní, že nebylo neautorizovaným způsobem modifikováno a že jakákoliv citlivá data vložená do zařízení (např. kryptografické klíče) nebyla prozrazena nebo změněna.

Absolutní bezpečnost není prakticky dosažitelná. Kryptografická bezpečnost závisí na každé fázi životního cyklu bezpečného kryptografického zařízení a doplňující se kombinaci náležitých postupů pro správu zařízení a bezpečných kryptografických vlastností. Tyto postupy pro správu implementují ochranná opatření pro omezení příležitosti k narušení bezpečnosti kryptografického zařízení. Cílem těchto opatření je vysoká pravděpodobnost detekce jakéhokoliv nedovoleného přístupu k citlivým nebo důvěrným datům v případě, že charakteristiky zařízení nezabránily kompromitaci bezpečnosti nebo selhaly při její detekci.

---

1 Předmět normy

Tato část ISO 13491 specifikuje kontrolní seznamy pro použití při hodnocení bezpečných kryptografických zařízení (Secure Cryptographic Devices, SCD) včetně kryptografických procesů v prostředí karet s magnetickým proužkem, dle specifikace v ISO 9564, ISO 9807 a ISO 11568. Nespecifikuje kontrolní seznamy pro SCD použitá v prostředí čipových karet.

Tato část ISO 13491 se nezabývá problematikou vyplývající z odmítnutí služby SCD.

V kontrolních seznamech uvedených v přílohách A až H je termín „neproveditelný“ určen pro vyjádření názoru, že ačkoliv specifický útok může být technicky proveditelný, byl by ekonomicky nerozumný, protože provést útok by stálo mnohem více než by činil prospěch z úspěšného útoku. Kromě útoků s čistě ekonomickým zájmem je nutné zvažovat i zlomyslné útoky zaměřené na poškození reputace.

-- Vynechaný text --