ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Květen 1998

	Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 1: Struktura	ČSN ISO/IEC 11770-1 36 9785

Information technology - Security techniques - Key Management - Part 1: Framework

Technologies de l'information - Techniques de sécurité - Partie 1: Cadre général

Informationstechnik - Sicherheitstechniken - Schlüsselmanagement - Teil 1: Rahmenrechtlinien

Tato norma je českou verzí mezinárodní normy ISO/IEC 11770-1:1996. Mezinárodní norma ISO/IEC 11770-1:1996 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 11770-1:1996. The International Standard ISO/IEC 11770-1:1996 has the status of a Czech Standard.

52103

Národní předmluva

Citované normy

ISO 7498-2:1989, zavedena v ČSN ISO 7498-2:1993 Systémy zpracování informací - Propojení otevřených systémů - Základní referenční model - Část 2: Bezpečnostní architektura (36 9615)

ISO/IEC 9798-1:1991, zavedena v ČSN ISO/IEC 9798-1:1997 Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 1: Všeobecný model (36 9743)

ISO/IEC 10181-1:1996, zavedena v ČSN ISO/IEC 10181-1:1997 Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury pro otevřené systémy: Část 1: Přehled (36 9694)

Vypracování normy

Zpracování normy: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

---

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 1: Struktura	ISO/IEC 11770-1 První vydání 1996-12-15

MDT 35.040

Deskriptory: data processing, information interchange, protection of information, security techniques, key management, cryptography.

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i mezinárodní komise, vládní i nevládní, s nimiž ISO navázalo pracovní styk.

ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členům ISO k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% hlasujících členů.

Mezinárodní norma ISO/IEC 11770-1 byla připravena společnou technickou komisí ISO/IEC JTC1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT.*

ISO/IEC 11770-1 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Správa klíčů:*

- *1. část: Struktura*

- *2. část: Mechanismy používající symetrické techniky*
- *3. část: Mechanismy používající asymetrické techniky*

Mohou následovat další části.

Přílohy A až E této části ISO/IEC 11770 jsou pouze pro informaci.

Obsah

Strana

Úvod

V oblasti informačních technologií neustále vzrůstá potřeba používat kryptografické mechanismy na ochranu dat před neautorizovaným odhalením nebo manipulací, pro autentizaci entit a pro zajištění nepopiratelnosti. Bezpečnost a spolehlivost těchto mechanismů je přímo závislá na správě a ochraně bezpečnostního parametru, klíče. Bezpečná správa těchto klíčů je kritická při integraci kryptografických funkcí do systému, neboť i nejpracnější koncept bezpečnosti bude neefektivní v případě slabé správy klíčů. Účelem správy klíčů je poskytnout postupy pro práci s materiálem správy klíčů používaných v symetrických nebo asymetrických kryptografických mechanismech.

Základním problémem je ustavit materiál klíče, jehož původ, integrita, včasnost a (v případě tajných klíčů) důvěrnost by mohly být zaručeny jak přímým tak nepřímým uživatelům. Správa klíčů zahrnuje funkce jako je generování, ukládání, vymazávání a archivace materiálu klíče v souladu s bezpečnostní politikou (ISO 7498-2).

Tato část normy 11770 má speciální vztah ke strukturám bezpečnosti otevřených systémů (ISO/IEC 10181). Všechny tyto struktury, včetně této části, identifikují základní pojetí a charakteristiky mechanismů, pokrývajících různé aspekty bezpečnosti. Tato část ISO/IEC 11770 uvádí všeobecné modely správy klíčů, které jsou podstatné pro symetrické a asymetrické kryptografické mechanismy.

1 Předmět normy

Tato část ISO/IEC 11770:

1. identifikuje cíl správy klíčů;
2. popisuje všeobecný model, na kterém jsou založeny mechanismy správy klíčů;
3. definuje základní pojmy správy klíčů společné všem částem této normy;
4. definuje služby správy klíčů;
5. identifikuje charakteristiky mechanismů správy klíčů;

6. specifikuje požadavky na správu materiálu klíče v průběhu jeho životního cyklu; a

7. popisuje strukturu správy materiálu klíče v průběhu jeho životního cyklu.

Tato struktura definuje obecný model správy klíčů, nezávislý na použití jakéhokoliv konkrétního kryptografického algoritmu. Avšak některé mechanismy distribuce klíčů mohou záviset na konkrétních vlastnostech algoritmu, např. na vlastnostech asymetrických algoritmů.

Specifické mechanismy správy klíčů jsou předmětem jiných částí ISO/IEC 11770. Symetrickými mechanismy se zabývá část 2 (ISO/IEC 11770-2, *Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 2: Mechanismy používající symetrické techniky).* Asymetrickými mechanismy se zabývá část 3 (ISO/IEC 11770-3, *Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky).* Tato část ISO/IEC 11770 obsahuje materiál nutný pro základní pochopení *části* 2 a 3. Příklady použití mechanismů správy klíčů jsou obsaženy v ISO 8732 a ISO 11166. Jestliže je pro správu klíčů požadována nepopiratelnost, měla by se využít norma ISO/IEC 13888.

Tato část ISO/IEC 11770 se zabývá jak automatickými tak manuálními aspekty správy klíčů, včetně přehledu datových prvků a posloupností operací, které jsou používány k získání služeb správy klíčů. Nespecifikuje však podrobnosti týkající se výměn protokolů.

Správa klíčů může být poskytnuta, stejně jako je tomu u jiných bezpečnostních služeb, pouze v kontextu definované bezpečnostní politiky. Definice bezpečnostní politiky je mimo rámec této normy o více částech.

-- Vynechaný text --