ČESKA TECHNICKÁ NORMA

ICS 35. 100. 01

Březen 1998

# Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura řízení přístupu

ČSN

ISO/IEC 10181-3

36 9694

Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework

Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadre pour la sécurité dans les systèmes ouverts: Cadre général de contrôle d'accès

Informationstechnik - Kommunikation Offener Systeme - Rahmenrichtlinien für IT Sicherheit in Offener Systemen - Teil 3: Rahmenrichtlinien für die Zugriffskontrole

Tato norma je českou verzí mezinárodní normy ISO/IEC 10181 -3: 1996. Mezinárodní norma ISO/IEC 10181 -3: 1996 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 10181-3: 1996. The International Standard ISO/IEC 10181-3: 1996 has the status of a Czech Standard.



51599

---



Národní předmluva

Citované normy

ISO/IEC 7498-1: 1994 zavedena v ČSN EN ISO/IEC 7498-1 Informační technologie - Základní referenční model - Základní model (36 9614)

ISO/IEC 10181-1: 1996 zavedena v ČSN ISO/IEC 10181-1 Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Přehled (36 9694)

ISO/IEC 10181-2: 1996 zavedena v ČSN ISO/IEC 10181-2 Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura autentizace (36 9694)

ISO/IEC 13712-1: 1995 dosud nezavedena

Upozornění na národní přílohu

Do této normy byla doplněna národní příloha NA, která obsahuje vysvětlivky к textu a slovník použitých termínů.

Vypracování normy

Zpracovatel normy: Ing. Vladimír Pračke, IČO 40654419 Technická normalizační komise: TNK 20 Informační technologie Pracovník Českého normalizačního institutu: Ing. Jitka Procházková



---

ČSN ISO/IEC 10181-3

MEZINÁRODNÍ NORMA

Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura řízení přístupu

ISO/IEC 10181-3

První vydání 1996-09-15

ICS 35. 100. 01

Deskriptory: data processing, information interchange, network interconnection, open systems interconnection, communication procedure, protection of information, security techniques, access.

Obsah

Strana

---

---

---

ČSN ISO/IEC 10181-3

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 společnou technickou komisí se rozesílají členům ISO к hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % z hlasujících členů.

Mezinárodní norma ISO/IEC 10181-3 byla připravena společnou technickou komisí ISO/IEC JTC 1, Informační technologie, subkomise SC 21 Propojení otevřených systémů, správa dat a otevřené distribuované zpracování, ve spolupráci s ITU-T. Identický text je publikován jako Doporučení ITU-T X. 812.

ISO/IEC 10181 se skládá z následujících částí se společným názvem Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů:

Část 1: Přehled

Část 2: Struktura autentizace

Část 3: Struktura řízení přístupu

Část 4: Struktura nepopiratelnosti

Část 5: Struktura důvěrnosti

Část 6: Struktura integrity

Část 7: Struktura bezpečnostního auditu

Přílohy A až G této části ISO/IEC 10181 jsou pouze informativní.



---



Úvod

Toto doporučení | mezinárodní norma definuje obecnou architekturu pro zajištění řízení přístupu. Prvotním cílem řízení přístupu je čelit hrozbě neautorizovaných činností týkajících se počítačů nebo komunikačních systémů; tyto hrozby jsou často dále děleny do tříd známých jako neautorizované použití, odhalení, modifikace, zničení a odmítnutí služby.



---



1 Předmět normy

Bezpečnostní struktury jsou určeny κ zajištění aplikace bezpečnostních služeb v prostředí otevřených systémů, přičemž termín Otevřené systémy zahrnuje takové oblasti jako databáze, distribuované aplikace, ODP a OSI. Bezpečnostní struktury se zabývají definováním způsobů zajišťování ochrany pro systémy a objekty uvnitř systémů a interakcemi mezi systémy. Bezpečnostní struktury se nezabývají metodologií konstruování systémů nebo mechanizmů.

Bezpečnostní struktury se zabývají datovými prvky a posloupnostmi operací (ale nikoliv prvky protokolů), které jsou používány κ dosažení určitých bezpečnostních služeb. Tyto bezpečnostní služby se mohou aplikovat na komunikující entity systémů stejně tak jako na data vyměňovaná mezi systémy a na data spravovaná systémy.

V případě řízení přístupu, přístupy mohou být buďto κ systému (tj. κ entitě, která představuje komunikující část systému) nebo uvnitř systému. Informační položky, které je nutno poskytnout pro získání přístupu, i posloupnost operací při žádostech o přístup a při oznamování výsledků přístupu jsou v rozsahu působnosti bezpečnostních struktur. Avšak jakékoliv informační položky a operace, závislé výlučně na konkrétní aplikaci a úzce zaměřené na lokální přístup uvnitř systému, spadají mimo rozsah působnosti těchto bezpečnostních struktur.

Mnoho aplikací obsahuje požadavky na bezpečnost z důvodu ochrany zdrojů proti hrozbám, včetně informací, které vyplývají ze vzájemného propojování otevřených systémů. V Doporučení CCITTX. 800 | ISO 7498-2 jsou popsány některé všeobecně známé hrozby typické pro prostředí OSI, společně s bezpečnostními službami a mechanismy, které mohou být použity к ochraně proti těmto hrozbám.

Řízením přístupu je nazýván proces určování, jaké použití zdrojů v prostředí otevřených systémů je povoleno, a případné zamezení neautorizovaného přístupu tam, kde je to vhodné. Toto doporučení mezinárodní norma definuje obecný rámec pro zajištění služeb řízení přístupu.

Tato bezpečnostní struktura:

a) definuje základní pojetí řízení přístupu;

b) ukazuje způsob, jak mohou být základní pojmy řízení přístupu konkretizovány, aby podporovaly některé obecně uznávané služby a mechanizmy pro řízení přístupu;

c) definuje tyto služby a odpovídající mechanismy řízení přístupu;

d) identifikuje funkční požadavky na protokoly s cílem podpořit tyto služby a mechanizmy řízení přístupu;

e) identifikuje požadavky na správu s cílem podpořit tyto služby a mechanizmy řízení přístupu;

f) zabývá se interakcí služeb a mechanizmů řízení přístupu s jinými bezpečnostními službami a mechanizmy.

Řízení přístupu, stejně jako jiné bezpečnostní služby, může být zajištěno pouze v kontextu definované bezpečnostní politiky pro konkrétní aplikaci. Stanovení politiky řízení přístupu je mimo oblast působnosti tohoto doporučení | mezinárodní normy; přesto jsou zde některé charakteristiky politiky řízení přístupu předmětem diskuse.

Specifikace výměn v rámci protokolu, jejichž provedení může být nezbytné pro zajištění služeb řízení přístupu, není předmětem tohoto doporučení | mezinárodní normy.

Toto doporučení | mezinárodní norma nespecifikuje ani konkrétní mechanismy, které podporují tyto služby řízení přístupu, ani podrobnosti služeb a protokolů pro management bezpečnosti.

Tuto strukturu může použít řada různých typů norem, včetně:

a) norem, které začleňují toto pojetí řízení přístupu;

b) norem, které specifikují abstraktní služby zahrnující řízení přístupu;

c) norem, které specifikují používání služby řízení přístupu;

d) norem, které specifikují prostředky poskytování řízení přístupu v prostředí otevřených systémů; a

e) norem, které specifikují mechanismy řízení přístupu.

Takovéto normy mohou používat tuto strukturu následovně:

- normy typu a, b, c, d, a e mohou používat terminologii této struktury;

- normy typu b, c, d a e mohou používat prostředky definované v článku 7 této struktury; a

- norma typu e může být založena na třídách mechanismu definovaného v článku 8.

9