



**Informační technologie - Propojení
otevřených systémů - Bezpečnostní
struktury otevřených systémů:
Přehled**

**ČSN
ISO/IEC 10181-1**

36 9694

Information technology - Open Systems Interconnection - Security frameworks for open systems:
Overview

Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadre pour la sécurité
dans les systèmes ouverts: Présentation

Informationstechnik - Kommunikation Offener Systeme - Rahmenrichtlinien für IT Sicherheit in
Offenen Systemen - Übersicht

Tato norma je českou verzí mezinárodní normy ISO/IEC 10181-1:1996. Mezinárodní norma ISO/IEC
10181-1:1996 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 10181-1:1996. The
International Standard ISO/IEC 10181-1:1996 has the status of a Czech standard.

© Český normalizační institut, 1997

51306

Strana 2

Národní předmluva

Citované normy

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

ISO 7498-2:1989 zavedena v ČSN ISO 7498-2 Systémy na spracovanie informácií - Prepojenie

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Jitka Procházková

Strana 3

MEZINÁRODNÍ NORMA **Informační technologie - Propojení otevřených** **systémů - Bezpečnostní struktury otevřených** **systémů: Přehled**

ISO/IEC 10181-1
První vydání
1996-08-01

ICS 35.100

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

Obsah	strana
Předmluva	5
Úvod	5
1 Předmět normy	5
2 Normativní odkazy	6
2.1 Identická doporučení mezinárodní normy	6
2.2 Dvojice doporučení mezinárodních norem se shodným technickým obsahem	6
3 Definice	6
3.1 Definice základního referenčního modelu	6
3.2 Definice bezpečnostní architektury	6
3.3 Doplnující definice	7
4 Zkratky	9
5 Notace	9
6 Organizace	9
6.1 1. část - Přehled	9
6.2 2. část - Autentizace	10
6.3 3. část - Řízení přístupu	10
6.4 4. část - Nepopiratelnost	10
6.5 5. část - Důvěrnost	11
6.6 6. část - Integrita	11

6.7	7. část - Bezpečnostní audit a alarmy	11
6.8	Správa klíčů	11
7	Společné pojmy	12
7.1	Bezpečnostní informace	12
7.2	Bezpečnostní doména	12
7.2.1	Bezpečnostní politika a pravidla bezpečnostní politiky	12
7.2.2	Autorita bezpečnostní domény	13
7.2.3	Vzájemné vztahy mezi bezpečnostními doménami	13
7.2.4	Ustavení pravidel bezpečné interakce	14
7.2.5	Transfer bezpečnostních informací mezi doménami	15
7.3	Význam bezpečnostní politiky pro specifické bezpečnostní služby	15
7.4	Důvěryhodné entity	15
7.5	Důvěra	16
7.6	Důvěryhodné třetí strany	16

Strana 4

8	Generické bezpečnostní informace	16
8.1	Bezpečnostní návěští	16
8.2	Kryptografické kontrolní hodnoty	17
8.3	Bezpečnostní certifikáty	17
8.3.1	Úvod do bezpečnostních certifikátů	17
8.3.2	Ověření a řetězení bezpečnostních certifikátů	18
8.3.3	Revokace bezpečnostních certifikátů	18
8.3.4	Opakované použití bezpečnostních certifikátů	18
8.3.5	Struktura bezpečnostních certifikátů	18
8.4	Bezpečnostní tokeny	19
9	Generické bezpečnostní prostředky	20
9.1	Prostředky souvisící s managementem	20
9.1.1	Instalace SI	20
9.1.2	Deinstalace SI	20
9.1.3	Změna SI	20
9.1.4	Validace SI	20
9.1.5	Zrušení validace SI	20
9.1.6	Aktivace/Deaktivace bezpečnostní služby	20
9.1.7	Zaprotokolování	20
9.1.8	Zrušení zaprotokolování	20
9.1.9	Distribuce SI	20
9.1.10	Vytisknutí seznamu SI	20
9.2	Prostředky souvisící s provozem	20
9.2.1	Identifikace důvěryhodných bezpečnostních autorit	20
9.2.2	Identifikace pravidel bezpečné interakce	21
9.2.3	Získání SI	21
9.2.4	Generování SI	21
9.2.5	Ověření SI	21
10	Interakce mezi bezpečnostními mechanismy	21
11	Odmítnutí služby a dostupnost	22
12	Jiné požadavky	22
	Příloha A - Některé příklady ochranných mechanismů pro bezpečnostní certifikáty	23
	A.1 Ochrana používající bezpečnostní službu komunikací OSI	23
	A.2 Ochrana používající parametr umístěný v bezpečnostním certifikátu	23
	A.2.1 Metoda autentizace	23

A.2.2 Metoda tajného klíče	23
A.2.3 Metoda veřejného klíče	24
A.2.4 Metoda jednosměrné funkce	24
A.3 Ochrana vnitřních a vnějších parametrů během přepravy	24
A.3.1 Transfer vnitřních parametrů k vydávající bezpečnostní autoritě	24
A.3.2 Transfer vnějších parametrů mezi entitami	24
A.4 Použití bezpečnostních certifikátů jednotlivými entitami nebo skupinami entit	25
A.5 Spojování bezpečnostního certifikátu s přístupy	25
Příloha B - Literatura	26

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% z hlasujících členů.

Mezinárodní norma ISO/IEC 10181-1 byla připravena společnou technickou komisí ISO/IEC JTC1, *Informační technologie*, subkomise SC 21, *Propojení otevřených systémů, řízení dat a otevřené distribuované zpracování*, ve spolupráci s ITU-T. Identický text je publikován jako Doporučení ITU-T X.810.

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

- 1. část: *Přehled*
- 2. část: *Struktura autentizace*
- 3. část: *Struktura řízení přístupu*
- 4. část: *Struktura nepopiratelnosti*
- 5. část: *Struktura důvěrnosti*
- 6. část: *Struktura integrity*
- 7. část: *Struktura bezpečnostního auditu a alarmů*

Přílohy A a B této části ISO/IEC 10181 jsou pouze pro informaci.

Úvod

Mnoho aplikací má požadavky na bezpečnost, aby byla zajištěna ochrana proti hrozbám vyskytujícím se při komunikaci informací. Některé obecně známé hrozby, spolu s bezpečnostními službami a mechanismy, které mohou být použity k ochraně proti těmto hrozbám, jsou popsány v Doporučení CCITT X.800 | ISO 7498-2.

Toto doporučení | mezinárodní norma definuje strukturu, ve které jsou specifikovány bezpečnostní služby pro otevřené systémy.

1 Předmět normy

Bezpečnostní struktury se zabývají aplikací bezpečnostních služeb v prostředí otevřených systémů, přičemž termín *Otevřené systémy* zahrnuje takové oblasti jako databáze, distribuované aplikace, ODP a OSI. Bezpečnostní struktury se zaměřují na definování prostředků pro ochranu systémů a objektů uvnitř systémů a na interakce mezi systémy. Bezpečnostní struktury se nezabývají metodologií konstrukce systémů nebo mechanismů.

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

Bezpečnostní struktury poskytují základ pro další normalizaci tím, že poskytují odpovídající názvosloví a definice rozhraní generických abstraktních služeb pro specifické bezpečnostní požadavky. Kategorizují rovněž mechanismy, které je možné použít k dosažení těchto požadavků.

Jedna bezpečnostní služba často závisí na jiných bezpečnostních službách, v důsledku čehož je obtížné izolovat jednu část bezpečnosti od jiných částí. Bezpečnostní struktury se zabývají specifickými bezpeč-

Strana 6

nostními službami, popisují okruh mechanismů, které mohou být použity k poskytnutí bezpečnostních služeb a identifikují vzájemné závislosti mezi službami a mechanismy. Popis těchto mechanismů může zahrnovat využití a spolehnutí se na různé bezpečnostní služby; tímto způsobem popisují bezpečnostní struktury využití a důvěru jedné bezpečnostní služby v jinou bezpečnostní službu.

Tato část bezpečnostních struktur:

- popisuje organizaci bezpečnostních struktur;

- definuje bezpečnostní pojmy, které jsou vyžadovány ve více než jedné části bezpečnostních struktur;
- popisuje vzájemný vztah služeb a mechanismů identifikovaných v dalších částech struktur.

-- Vynechaný text --