

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 Zugriffskontrolle

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.

© Český normalizační institut, 1997

51599

ČSN ISO/IEC 10181-3

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 k 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

2

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

Předmluva.....	6
Úvod	7
1 Předmět normy	8
2 Normativní odkazy.....	9
2. 1 Identická doporučení mezinárodní normy.....	9
2. 2 Odpovídající doporučení mezinárodní normy se shodným technickým obsahem.....	9
3 Definice	9
4 Zkratky.....	11
5 Obecná diskuse o řízení přístupu.....	12
5. 1 Cíl řízení přístupu.....	12
5. 2 Základní aspekty řízení přístupu.....	12
5. 2. 1 Výkon funkcí řízení přístupu.....	13

5. 2. 2	Ostatní činnosti při řízení přístupu.....	14
5. 2. 3	PředáváníACI	16
5. 3	Distribuce komponent řízení přístupu.....	17
5. 3. 1	Příchozí řízení přístupu.....	17
5. 3. 2	Odchozí řízení přístupu.....	17
5. 3. 3	Vložené řízení přístupu.....	18
5. 4	Distribuce komponent řízení přístupu přes více bezpečnostních domén.....	18
5. 5	Hrozby vůči řízení přístupu.....	18
6	Politiky řízení přístupu.....	19
6. 1	Vyjádření politiky řízení přístupu.....	19
6. 1. 1	Kategorie politiky řízení přístupu.....	19
6. 1. 2	Skupiny a role	19
6. 1. 3	Bezpečnostní návěští.....	19
6. 1. 4	Politiky řízení přístupu v případě vícenásobného iniciátora.....	20
3		

ČSN ISO/IEC 10181-3

6. 2	Management politiky.....	20
6. 2. 1	Pevně stanovené politiky.....	20
6. 2. 2	Administrativně vyhlášené politiky.....	20
6. 2. 3	Uživatелеm zvolené politiky	20
6. 3	Granularita a omezení.....	20
6. 4	Pravidla dědičnosti.....	20
6. 5	Priorita pravidel politiky řízení přístupu	21
6. 6	Standardně nastavená pravidla politiky řízení přístupu.....	21
6. 7	Mapování politiky spolupracujícími bezpečnostními doménami	21
7	Informace a prostředky řízení přístupu.....	21
7. 1	ACI.....	21

7. 1. 1	ACI iniciátora.....	22
7. 1. 2	ACI cíle.....	22
7. 1. 3	ACI žádosti o přístup.....	22
7. 1. 4	ACI operandu.....	22
7. 1. 5	Kontextová informace	23
7. 1. 6	ACI svázaná s iniciátorem.....	23
7. 1. 7	ACI svázaná s cílem.....	23
7. 1. 8	ACI svázaná s žádostí o přístup.....	23
7. 2	Ochrana ACI.....	23
7. 2. 1	Certifikáty řízení přístupu.....	23
7. 2. 2	Tokeny řízení přístupu	24
7. 3	Prostředky pro řízení přístupu.....	24
7. 3. 1	Prostředky pro management.....	25
7. 3. 2	Prostředky týkající se činností.....	25
8	Klasifikace mechanismů řízení přístupu.....	28
8. 1	Úvod.....	28
8. 2	Schéma ACL.....	29
8. 2. 1	Základní rysy.....	29
8. 2. 2	ACI.....	29
8. 2. 3	Podpůrné mechanismy.....	29
8. 2. 4	Varianty schématu.....	30
8. 3	Schéma schopností.....	31
8. 3. 1	Základní vlastnosti.....	31
8. 3. 2	ACI.....	31
8. 3. 3	Podpůrné mechanismy.....	31
8. 3. 4	Varianty schématu - Schopnosti bez specifických operací.....	32
8. 4	Schéma založené na návěštích.....	32
8. 4. 1	Základní vlastnosti.....	32

8. 4. 2	ACI.....	33
8. 4. 3	Podpůrné mechanismy.....	33
4		
<hr/>		
ČSN ISO/IEC 10181-3		
8. 4. 4	Kanály s návěštím v roli cíle	33
8. 5	Schéma založené na kontextu.....	34
8. 5. 1	Základní vlastnosti.....	34
8. 5. 2	ACI.....	34
8. 5. 3	Podpůrné mechanismy.....	34
8. 5. 4	Varianty schématu.....	34
9	Interakce s jinými bezpečnostními službami a mechanismy.....	35
9. 1	Autentizace.....	35
9. 2	Integrita dat.....	35
9. 3	Důvěrnost dat	35
9. 4	Audit.....	35
9. 5	Ostatní služby týkající se přístupu.....	36
Příloha A	Výměna certifikátů řízení přístupu mezi komponentami.....	37
A. 1	Úvod.....	37
A. 2	Předávání certifikátů řízení přístupu.....	37
A. 3	Předávání vícenásobných certifikátů řízení přístupu	37
A. 3. 1	Příklad	37
A. 3. 2	Zevšeobecnění.....	37
A. 3. 3	Zjednodušení.....	38
Příloha B	Řízení přístupu v referenčním modelu OSI	39
B. 1	Všeobecně.....	39
B. 2	Použití řízení přístupu v rámci OSI vrstev.....	39
B. 2. 1	Použití řízení přístupu na úrovni síťové vrstvy.....	39

B. 2. 2 Použití řízení přístupu na úrovni transportní vrstvy	39
B. 2. 3 Použití řízení přístupu na úrovni aplikační vrstvy	39
Příloha C Nejednoznačnost identit řízení přístupu.....	40
Příloha D Distribuce komponent řízení přístupu.....	41
D. 1 Uvažované aspekty	41
D. 2 Umístění AEC a ADC.....	41
D. 3 Interakce mezi komponentami řízení přístupu.....	42
Příloha E Politika založená na pravidlech versus politika založená na identitě.....	44
Příloha F Mechanismus podpory předávání ACI prostřednictvím iniciátora.....	45
Příloha G Přehled bezpečnostních služeb řízení přístupu.....	46
Národní příloha NA (informativní)	47
NA. 1 Vysvětlivky k textu převzaté normy	47
NA. 2 Slovník použitých výrazů.....	47

5

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 k 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.

6

ČSN ISO/IEC 10181-3

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.

7

ČSN ISO/IEC 10181-3

1 Předmět normy

Bezpečnostní struktury jsou určeny k 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 mechanismů.

Bezpečnostní struktury se zabývají datovými prvky a posloupnostmi operací (ale nikoliv prvky protokolů), které jsou používány k 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 k systému (tj. k 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 CCITX. 800 | ISO 7498-2 jsou popsány některé všeobecně známé hrozby typické pro prostředí OSI, společně s bezpečnostními službami a mechanismy, které mohou být použity k 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 mechanismy pro řízení přístupu;
- c) definuje tyto služby a odpovídající mechanismy řízení přístupu;
- d) identifikuje funkční požadavky na protokoly s cílem podpořit tyto služby a mechanismy řízení přístupu;
- e) identifikuje požadavky na správu s cílem podpořit tyto služby a mechanismy řízení přístupu;
- f) zabývá se interakcí služeb a mechanismů řízení přístupu s jinými bezpečnostními službami a mechanismy.

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 nspecifikuje 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.