ČESKÁ TECHNICKÁ NORMA

ICS 35. 100. 01

Červen 1999

Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura nepopiratelnosti

ČSN

ISO/IEC 10181-4

36 9694

idt ITU-T X. 813: 1996

Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework

Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadres de sécurité pour les systèmes ouverts: Cadre de non-répudiation

Informationstechnik - Kommunikation Offener Systeme - Rahmenrichtlinien für IT Sicherheit in Offenen Systemen: Nicht Verweigerung

Tato norma je českou verzí mezinárodní normy ISO/IEC 10181-4: 1997. Mezinárodní norma ISO/IEC 10181-4: 1997 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 10181-4: 1997. The International Standard ISO/IEC 10181-4: 1997 has the status of a Czech Standard.

56081

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 otvorených systémov (OSI). Základný referenčný model. Časť 2: Bezpečnostná architektúra (36 9615)

ISO/IEC 9594-8: 1995 zavedena v ČSN ISO/IEC 9594-8 Informační technologie - Propojení otevřených

systémů - Adresář: Struktura autentizace (36 9671)

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

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Jitka Procházková

2

ČSN ISO/IEC 10181-4

MEZINÁRODNÍ NORMA

Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura nepopiratelnosti

ISO/IEC 10181-4

První vydání 1997-04-01

ICS 35. 100. 01

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

Obsah

Strana

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 a IEC 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 národním orgánům ke schvalování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Mezinárodní norma ISO/IEC 10181-4 byla připravena Společnou technickou komisí ISO/IEC JTC 1 Informační technologie, subkomisí 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. 813.

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 až F této části ISO/IEC 10181 jsou pouze pro informaci.

Úvod

Cílem služby nepopiratelnosti je shromažďovat a udržovat nevyvratitelné důkazy, týkající se údajné události nebo činnosti, zajistit jejich dostupnost a validaci, aby bylo možné řešit spory o tom, zda se událost nebo činnost vyskytla či nikoliv. Služba nepopiratelnosti může být aplikována v mnoha různých kontextech a situacích. Služba může být aplikována na generování dat, jejich uchovávání nebo přenos. Nepopiratelnost zahrnuje generování důkazu, který může být použit κ tomu, aby se prokázalo, že se některý typ události nebo činnosti uskutečnil, takže tato událost nebo činnost nemůže být později odmítnuta.

V prostředí OSI (viz Doporučení CCITT X. 800 a ISO 7498-2) má služba nepopiratelnosti dvě formy:

- nepopiratelnost s průkazem původu, která je používána proti nepravdivému popření ze strany odesilatele, že data nebo jejich obsah byly odeslány

- nepopiratelnost s průkazem doručení, která je používána proti nepravdivému popření ze strany příjemce, že data nebo jejich obsah (tj. informace, které data reprezentují) byly přijaty.

Aplikace, které využívají protokoly OSI, mohou požadovat jiné formy služby nepopiratelnosti, specifické pro konkrétní třídy aplikací. Např. MHS (Doporučení ITU-T X. 402 | ISO 10021-2) definuje službu nepopiratelnosti podání, zatímco systém předávání zpráv EDI (viz Doporučení X. 435) definuje služby nepopiratelnosti vyhledávání a nepopiratelnosti předání.

Pojetí této struktury není omezeno na komunikace OSI, ale může být interpretováno siřeji, aby obsáhlo např. vytváření a uchovávání dat pro pozdější použití.

Toto doporučení | mezinárodní norma definuje obecnou strukturu pro poskytnutí služby nepopiratelnosti.

Tato struktura:

- rozšiřuje pojetí služeb nepopiratelnosti, popsaných v Doporučení CCITT X. 800 a ISO 7498-2 a popisuje, jak mohou být aplikovány v otevřených systémech;

- popisuje alternativy pro poskytnutí těchto služeb; a

- vysvětluje vztah těchto služeb κ ostatním bezpečnostním službám. Služby nepopiratelnosti mohou požadovat:

- rozhodci, kteří budou rozhodovat spory, vzniklé jako důsledek popřených událostí nebo činností; a

- důvěryhodné třetí strany, které zaručí autenticitu a integritu dat, určených κ použití pro ověření důkazu.

1 Předmět normy

Toto doporučení I mezinárodní norma se zabývá aplikací bezpečnostních služeb v prostředí otevřených systémů, kde termín "otevřené systémy" zahrnuje takové oblasti jako jsou databáze, distribuované aplikace, otevřené distribuované zpracování a OSI. Bezpečnostní struktury se zabývají definováním prostředků poskytování ochrany pro systémy a objekty uvnitř systémů a interakcí mezi systémy. Bezpečnostní struktury se nezabývají metodologií konstrukce systémů nebo mechanismů.

Bezpečnostní struktury se zabývají datovými prvky a posloupnostmi operací (ne však prvky protokolů), které jsou používány κ získání specifických bezpečnostních služeb. Tyto bezpečnostní služby se mohou použít jak u komunikujících entit systémů tak u dat vyměňovaných mezi systémy a spravovaných systémy.

Toto doporučení | mezinárodní norma:

- definuje základní pojetí nepopiratelnosti;

- definuje obecné služby nepopiratelnosti;

- identifikuje možné mechanismy κ poskytnutí služeb nepopiratelnosti;

- identifikuje obecné požadavky managementu na řízení služeb a mechanismů nepopiratelnosti.

Služba nepopiratelnosti, stejně jako jiné bezpečnostní služby, může být zajištěna pouze v kontextu definované bezpečnostní politiky pro danou aplikaci. Definice bezpečnostní politiky je mimo rozsah působnosti tohoto doporučení | mezinárodní normy.

Specifikace podrobností výměn v rámci protokolu, jejichž provedení může být nezbytné pro dosažení nepopiratelnosti, není předmětem tohoto doporučení | mezinárodní normy.

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

Některé postupy popsané v této struktuře dosahují bezpečnost aplikací kryptografických technik. Tato struktura je nezávislá na použití konkrétních kryptografických nebo jiných algoritmů nebo konkrétních kryptografických technik (např. symetrických nebo asymetrických), ačkoliv určité třídy mechanismů nepopiratelnosti mohou záviset na vlastnostech konkrétních algoritmů. V praxi je však

pravděpodobné, že bude použito několik různých algoritmů. Dvě entity, které si přejí použít kryptograficky chráněná data, musí podporovat stejný kryptografický algoritmus.

[POZNÁMKA - Ačkoliv ISO nenormalizuje kryptografické algoritmy, normalizuje v ISO/IEC 9979 postupy používané pro jejich registraci.]

Tuto strukturu může použít řada různých typů norem, včetně:

1) norem, které začleňují toto pojetí nepopiratelnosti;

2) norem, které specifikují abstraktní služby zahrnující nepopiratelnost;

3) norem, které specifikují používání služby nepopiratelnosti;

4) norem, které specifikují prostředky poskytování nepopiratelnosti v architektuře otevřených systémů; a

5) norem, které specifikují mechanismy nepopiratelnosti. Takovéto normy mohou používat strukturu nepopiratelnosti následovně:

- normy typu 1), 2), 3), 4) nebo 5) mohou používat terminologii této struktury;

- normy typu 2), 3), 4) nebo 5) mohou používat dílčí služby definované v článku 7 této struktury; a

- normy typu 5) mohou být založeny na třídách mechanismu definovaného v článku 8.