ČESKÁ TECHNICKÁ NORMA

ICS 35.100.01 **Duben**
2003

	Informační technologie - Propojení otevřených systémů - Adresář: Základní struktury certifikátu veřejného klíče a certifikátu atributu	ČSN ISO/IEC 9594-8 ed. 4 36 9671

idt ITU-T X.509:2000

Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

Technologies de l’information - Interconnexion de systèmes ouverts (OSI) - L’annuaire: Cadres de clé publique et de
certificat d’attribut

Tato norma je českou verzí mezinárodní normy ISO/IEC 9594-8 ed. 4:2001. Mezinárodní norma ISO/IEC 9594-8 ed.4:2001 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 9594-8 ed. 4:2001. The International Standard ISO/IEC 9594-8 ed. 4:2001 has the status of a Czech Standard.

Upozornění

ČSN ISO/IEC 9594-8:1999 je dočasně ponechána v platnosti, aby podporovala na ní založené implementace. Po určité době však nebude nadále podporována. Doporučuje se proto, aby se implementace přizpůsobily tomuto čtvrtému vydání.

66177

Národní předmluva

Změny proti předchozí normě

Toto čtvrté vydání ISO/IEC 9594-8 je technickou revizi třetího vydání (ISO/IEC 9594-8:1998), které je dočasně ponecháno, aby podporovalo implementace založené na třetím vydání. Toto vydání zahrnuje také Technickou opravu 1:2000 a Technickou opravu 2:2002

Citované normy

ISO/IEC 10021-4:1999 dosud nezavedena

ISO/IEC 9594-1:2001 dosud nezavedena

ISO/IEC 9594-2:2001 dosud nezavedena

ISO/IEC 9594-3:2001 dosud nezavedena

ISO/IEC 9594-4:2001 dosud nezavedena

ISO/IEC 9594-5:2001 dosud nezavedena

ISO/IEC 9594-6:2001 dosud nezavedena

ISO/IEC 9594-7:2001 dosud nezavedena

ISO/IEC 9594-9:2001 dosud nezavedena

ISO/IEC 9594-10:2001 dosud nezavedena

ISO/IEC 9834-1:1993 zavedena v ČSN ISO/IEC 9834-1:1997 (36 9674) Informační technologie. Propojení otevřených systémů. Procedury pro činnost registračních orgánů OSI. Část 1: Všeobecné procedury

ISO/IEC 8824-1:1998 dosud nezavedena

ISO/IEC 8824-2:1998 dosud nezavedena

ISO/IEC 8824-3:1998 dosud nezavedena

ISO/IEC 8824-4:1998 dosud nezavedena

ISO/IEC 8825-1:1998 dosud nezavedena

ISO/IEC 8825-2:1998 dosud nezavedena

ISO/IEC 10181-3:1996 zavedena v ČSN ISO/IEC 10181-3:1998 (36 9694) Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura řízení přístupu

ISO/IEC 10181-4:1997 zavedena v ČSN ISO/IEC 10181-4:1999 (36 9694) Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura nepopíratelnosti

ISO/IEC 13712-1:1995 dosud nezavedena

ISO/IEC 13712-2:1995 dosud nezavedena
ISO 7498-2:1989 zavedena v ČSN ISO 7498-2:1994 (36 9615) Systémy na spracovanie informácií.

Prepojenie otvorených systémov (OSI). Základný referenčný model. Čas» 2: Bezpečnostná architektúra

Upozornění na národní poznámky

Do normy byly doplněny v kapitolách 3, 5 a 17 informativní národní poznámky.

Upozornění na národní přílohu

Do této normy byla doplněna národní příloha NA (informativní), která obsahuje slovník použitých termínů.

Vypracování normy

Zpracovatel: TTC TESLA TELEKOMUNIKACE, s.r.o., IČ 41194403, Ing. Zdeněk ®ilka, CSc.

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

---

MEZINÁRODNÍ NORMA
Informační technologie - Propojení otevřených systémů - Adresář: Základní struktury certifikátu klíče veřejného a certifikátu atributu

ISO/IEC 9594-8
Čtvrté vydání
2001-08-01

ICS 35.100.01

Obsah

Strana

Strana

Strana

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí

na vypracování mezinárodních norem prostřednictvím technických komisí zřízených příslušnou organizací, aby se zabývaly určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společného zájmu. Práce se zúčastňují i jiné mezinárodní organizace, vládní a nevládní, s nimiž ISO a IEC navázaly pracovní styk.

Mezinárodní normy jsou navrhovány v souladu s částí 3 Směrnic ISO/IEC.

V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC1. Návrhy mezinárodních norem přijaté společnou technickou komisí se rozesílají k hlasováním národním orgánům. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Uživatelé a implementátoři by měli věnovat pozornost existenci postupu „řešení vad“ v ISO/IEC, aby identifikovali a opravili chyby v mezinárodních normách publikováním Technických oprav (Technical Corrigenda). Identické korektury se provádějí v odpovídajících doporučeních ITU-T pomocí Oprav (Corrigenda) a mohou být provedeny také prostřednictvím Příručky implementátora. Podrobnosti o Technických opravách v mezinárodních normách jsou k dispozici na webové stránce ISO; publikované Technické opravy lze získat z archivu na webové stránce ISO nebo od národních orgánů ISO a IEC. Opravy a příručky implementátora k doporučením ITU-T lze získat z webové stránky ITU-T.

Mezinárodní norma ISO/IEC 9594-8 byla připravena společnou technickou komisí ISO/IEC JTC1, *Informační technologie,* subkomisí SC6, *Telekomunikace a výměna informací mezi systémy*, ve spolupráci s ITU-T. Identický text je publikován jako Doporučení ITU-T X.509.

Toto čtvrté vydání ISO/IEC 9594-8 je technickou revizi třetího vydání (ISO/IEC 9594-8:1998), které je dočasně ponecháno, aby podporovalo implementace založené na třetím vydání. Toto vydání zahrnuje také Technickou opravu 1:2000.

ISO/IEC 9594 sestává z následujících částí pod obecným názvem *Informační technologie - Propojení otevřených systémů - Adresář*:

– *Část 1: Přehled pojmů, modelů a služeb*

– *Část 2: Modely*

– *Část 3: Definice abstraktní služby*

– *Část 4: Procedury pro distribuovanou operaci*

– *Část 5: Specifikace protokolů*

– *Část 6: Vybrané typy atributů*

– *Část 7: Vybrané třídy objektů*

– *Část 8: Základní struktury certifikátu veřejného klíče a certifikátu atributu*

– *Část 9: Replikace*

– *Část 10: Použití managementu systémů pro správu Adresáře*

Příloha A, B a F tvoří normativní část této části ISO/IEC 9594. Přílohy C, D, E, G, H a I jsou pouze informativní.

Úvod

Toto doporučení | tato mezinárodní norma spolu s jinými doporučeními | mezinárodními normami byly vytvořeny k usnadnění propojení systémů zpracování informací pro poskytování služeb Adresáře. Na množinu těchto systémů spolu s adresářovými informacemi, které obsahují, lze pohlížet jako na integrovaný celek zvaný *Adresář.* Informace obsažené v Adresáři, souhrnně známé jako informační báze Adresáře (DIB), se používají k usnadnění komunikace mezi objekty, s objekty nebo o objektech, jako jsou aplikační entity, lidé, terminály a rozdělovníky.

Adresář sehrává význačnou roli v propojení otevřených systémů, jehož cílem je přitom omezit na minimum rozsah technických dohod nad rámec samotných norem propojení a umožnit propojování systémů zpracování informací:

– od různých výrobců;

– pod různými managementy;

– různé úrovně složitosti a

– různého stáří.

Mnohé aplikace obsahují požadavky na bezpečnost k ochraně před hrozbami narušení přenosu informací. V podstatě jsou všechny bezpečnostní služby závislé na spolehlivé znalosti identity účastníků komunikace, tj. na autentizaci.

Toto doporučení | mezinárodní norma obsahuje definice základní struktury certifikátů veřejného klíče. Tato základní struktura zahrnuje specifikaci datových objektů, které se používají k reprezentaci samotných certifikátů a rovněž oznámení o revokaci vydaných certifikátů, které by už neměly být důvěryhodné. Pokud základní struktura certifikátu veřejného klíče definovaná v této specifikaci definuje některé kritické části Infrastruktury veřejného klíče (PKI), nedefinuje PKI v celém rozsahu. Tato specifikace ovšem poskytuje základ, na kterém by mohly být vybudovány úplné PKI a jejich specifikace.

Podobně toto doporučení | tato mezinárodní norma obsahuje definice základní struktury certifikátů atributu. Tato základní struktura zahrnuje specifikace datových objektů používaných pro reprezentování samotných certifikátů a rovněž oznámení o revokaci vydaných certifikátů, které by už neměly být důvěryhodné. Pokud základní struktura certifikátu atributu definovaná v této specifikaci definuje některé kritické složky infrastruktury managementu privilegia (PMI), nedefinuje PMI v celém rozsahu.Tato specifikace ovšem poskytuje základ, na kterém by mohly být vybudovány úplné PMI a jejich specifikace.

Definovány jsou také informační objekty pro uchování objektů PKI a PMI v Adresáři a pro porovnání zadaných hodnot s hodnotami uloženými.

Toto doporučení | tato mezinárodní norma také obsahuje definice základní struktury pro poskytování autentizačních služeb Adresářem jeho uživatelům.

Toto doporučení | tato mezinárodní norma poskytuje základní struktury, na kterých mohou být jinými skupinami norem a průmyslovými komunitami definovány průmyslové profily. Mnohé z rysů, které jsou definované v těchto základních strukturách jako volitelné se mohou prostřednictvím profilů stát závaznými pro použití v určitých prostředích. Toto čtvrté vydání technicky reviduje a zdokonaluje, ale

nenahrazuje třetí vydání tohoto doporučení | této mezinárodní normy. Implementace mohou stále ještě požadovat shodu se třetím vydáním. Po určité době však nebude třetí vydání podporováno (tj. oznámené vady již nebudou řešeny). Doporučuje se, aby se implementace co nejdřív přizpůsobily tomuto čtvrtému vydání.

Toto čtvrté vydání specifikuje verzi 1 a 2 protokolů Adresáře.

První a druhé vydání specifikuje pouze verzi 1. Většina služeb a protokolů specifikovaných v tomto vydání je navržena tak, aby pracovala ve verzi 1. Avšak některé rozšířené služby a protokoly, například podepsané chyby, nebudou fungovat, pokud všechny entity Adresáře zahrnuté v operaci nebudou mít dohodnutou verzi 2. A» byla dojednána kterákoli verze, lze rozdíly mezi službami a mezi protokoly definovanými ve čtyřech vydáních, s výjimkou těch, které byly specificky určeny pro verzi 2, uspokojit použitím pravidel rozšiřitelnosti definovaných v tomto vydání Doporučení ITU-T X.519 | ISO/IEC 9594-5.

Příloha A, která je nedílnou částí tohoto doporučení | této mezinárodní normy, poskytuje modul ASN.1, který obsahuje všechny definice, které jsou spojené se základními strukturami.

Příloha B, která je nedílnou částí tohoto doporučení | této mezinárodní normy, poskytuje pravidla pro generování a zpracování seznamů revokovaných certifikátů.

Příloha C, která není nedílnou částí tohoto doporučení | této mezinárodní normy, poskytuje příklady vydávání přírůstkového seznamu revokovaných certifikátů delta-CRL.

Příloha D, která není nedílnou částí tohoto doporučení | této mezinárodní normy, poskytuje příklady syntaxe politiky privilegia a privilegovaných atributů.

Příloha E, která není nedílnou částí tohoto doporučení | této mezinárodní normy, je úvodem do kryptografie s veřejným klíčem.

Příloha F, která je nedílnou částí tohoto doporučení | této mezinárodní normy, definuje identifikátory objektu přidělené algoritmům autentizace a šifrování bez formálního registru.

Příloha G, která není nedílnou částí tohoto doporučení | této mezinárodní normy, obsahuje příklady používání omezení certifikační cesty.

Příloha H, která není nedílnou částí tohoto doporučení | této mezinárodní normy, obsahuje abecední seznam definic informačních položek v této specifikaci.

Příloha I, která není nedílnou částí tohoto doporučení | této mezinárodní normy, uvádí dodatky a zprávy o vadách, které byly začleněny do tohoto vydání tohoto doporučení | této mezinárodní normy.

Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) upozorňuje na to, že se prohlašuje, že by vyhovění této části ISO/IEC 9594 mohlo zahrnovat použití patentu týkajícího se technického prostředku distribuční bod CRL.

ISO a IEC nezaujímají stanovisko k důkazu, platnosti a rozsahu tohoto patentového práva.

Držitel tohoto patentového práva ujistil ISO a IEC, že je ochoten dohodnout s uživateli na celém světě

licence za rozumných a nediskriminačních okolností a podmínek. V tomto ohledu je ustanovení držitele tohoto patentového práva registrováno u ISO a IEC. Informace lze získat u:

Entrust Technologies

Mr. Mike Morgan, Senior Legal Counsel

750 Heron Road, Suite E08

Ottawa, Ontario K1V 1A7

Canada

Je třeba věnovat pozornost možnosti, že některé z prvků této části ISO/IEC 9594 mohou být subjektem jiných patentových práv než těch, které byly uvedeny výše. ISO a IEC nesmí být činěny zodpovědnými za identifikaci některých nebo všech takových patentových práv.

ODDÍL 1 - V©EOBECNÉ

1 Předmět normy

Toto doporučení | tato mezinárodní norma řeší některé z bezpečnostních požadavků v oblasti autentizace a jiných bezpečnostních služeb poskytnutím množiny základních struktur, na nichž mohou být založeny úplné služby. Toto doporučení | tato mezinárodní norma definuje speciálně tyto základní struktury:

– certifikáty veřejného klíče;

– certifikáty atributu;

– autentizační služby.

Základní struktura certifikátu veřejného klíče definovaná v tomto doporučení | v této mezinárodní normě zahrnuje definici informačních objektů pro infrastrukturu veřejného klíče (PKI) včetně certifikátů veřejného klíče a seznamu revokovaných certifikátů (CRL). Základní struktura certifikátu atributu zahrnuje definici informačních objektů pro infrastrukturu managementu privilegia (PMI), včetně certifikátů atributu a seznamu revokovaných certifikátů atributu (ACRL). Tato specifikace poskytuje také základní strukturu pro vydávání, správu, používání a revokování certifikátů. V definovaných formátech jak pro typy certifikátů, tak pro všechna schémata revokačního seznamu je zahrnut mechanismus rozšiřitelnosti. Toto doporučení | tato mezinárodní norma zahrnuje také množinu standardních rozšíření pro každý formát, u něhož se předpokládá, že bude obecně užitečný v mnoha aplikacích PKI a PMI. Do tohoto doporučení | této mezinárodní normy jsou zahrnuty složky schématu včetně tříd objektů, typů atributů a pravidel porovnávání pro ukládání objektů PKI a PMI do Adresáře. Předpokládá se, že jiné prvky PKI a PMI mimo tyto základní struktury, jako protokoly managementu klíče a certifikátu, operační protokoly, dodatečné certifikáty a rozšíření CLR jsou definovány jinými normalizačními orgány (například ISO TC 68, IETF atd.).

Autentizační schéma definované v tomto doporučení | této mezinárodní normě je generické a může se použít na různé aplikace a prostředí.

Adresář využívá certifikáty veřejného klíče a certifikáty atributu a v tomto doporučení | této

mezinárodní normě se definuje také základní struktura pro využívání těchto prostředků Adresářem. Aby umožnil silnou autentizaci, podepsané a/nebo zašifrované operace a pro ukládání podepsaných nebo zašifrovaných dat do Adresáře, používá Adresář technologii veřejného klíče včetně certifikátů. Aby se umožnilo řízení přístupu založené na pravidlech, může Adresář používat certifikáty atributu. I když se základní struktura pro ně uvádí v této specifikaci, úplná definice používání těchto struktur Adresářem a používání asociovaných služeb poskytovaných Adresářem a jeho složkami je uvedena v úplné množině specifikací Adresáře.

V základní struktuře autentizačních služeb toto doporučení | tato mezinárodní norma:

– specifikuje formu autentizačních informací uchovaných v Adresáři;

– popisuje, jak lze z Adresáře získat autentizační informace;

– stanovuje předpoklady o tom, jak se autentizační informace vytvářejí a umis»ují do Adresáře;

– definuje tři způsoby, jak mohou aplikace tyto autentizační informace používat k provádění autentizace a popisuje, jak mohou být jiné bezpečnostní služby podporovány autentizací.

Toto doporučení | tato mezinárodní norma popisuje dvě úrovně autentizace: jednoduchou autentizaci používající heslo pro ověření deklarované identity a silnou autentizaci obsahující charakteristické hodnoty (credentials) vytvořené použitím kryptografických technik. Zatímco jednoduchá autentizace nabízí nějakou omezenou ochranu proti neoprávněnému přístupu, jako základ pro poskytnutí bezpečnostních služeb by se měla používat pouze silná autentizace. Není záměrem to stanovit jako obecnou základní struktury pro autentizaci, ale může se to obecně používat v aplikacích, které tyto techniky považují za adekvátní.

Autentizace (a jiné bezpečnostní služby) se mohou poskytovat pouze v kontextu definované bezpečnostní politiky. Je věcí uživatelů aplikace, aby definovali vlastní bezpečnostní politiku, která může být omezena službami poskytovanými normou.

Je záležitostí aplikací, které definující normy a používají základní strukturu autentizace, aby specifikovaly výměny protokolu, které je třeba provádět tak, aby se dosáhlo autentizace založené na autentizační informaci získané z Adresáře. Protokol používaný aplikacemi k získání charakteristických hodnot (credentials) z Adresáře je přístupový protokol Adresáře (DAP) specifikovaný v Doporučení ITU-T X.519 | ISO/IEC 9594-5.

-- Vynechaný text --