


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.

Národní předmluva

Změny proti předchozí normě

Toto čtvrté vydání ISO/IEC 9594-8 je technickou revizí 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

Strana 3

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

Předmluva

.....
..... 8

Úvod

.....
..... 9

ODDÍL 1

V©EOBECNÉ

.....
11

1 Předmět
normy

.....
11

2 Normativní

odkazy	12
2.1 Identická doporučení mezinárodní normy	12
2.2 Párová doporučení mezinárodní normy ekvivalentní v technickém obsahu	13
3 Definice	13
3.1 Definice bezpečnostní architektury referenčního modelu OSI	13
3.2 Definice modelu Adresáře	14
3.3 Definice	14
4 Zkratky	19
5 Úmluvy	19
6 Přehled základních struktur	20
6.1 Digitální podpisy	21
ODDÍL 2 ZÁKLADNÍ STRUKTURA CERTIFIKÁTU VEŘEJNÉHO KLÍČE	24
7 Veřejné klíče a certifikáty veřejného klíče	24
7.1 Generování dvojic klíčů	28
7.2 Vytvoření certifikátu veřejného	

klíče.....	29
7.3 Platnost certifikátu.....	29
8 Certifikát veřejného klíče a rozšíření CRL.....	32
8.1 Vedení politiky.....	32
8.1.1 Certifikační politika.....	32
8.1.2 Křížová certifikace.....	33
8.1.3 Mapování politiky.....	34
8.1.4 Zpracování certifikační cesty.....	34
8.1.5 Samovydané certifikáty.....	35
8.2 Rozšíření informací o klíči a politice.....	35
8.2.1 Požadavky.....	35
8.2.2 Pole rozšíření certifikátu veřejného klíče a CRL.....	36
8.3 Rozšíření informace o subjektu a vydavateli.....	40
8.3.1 Požadavky.....	40

8.3.2	Pole rozšíření certifikátu a CRL.....	41
8.4	Rozšíření omezení certifikační cesty.....	43
8.4.1	Požadavky	43
8.4.2	Pole rozšíření certifikátu.....	44
8.5	Základní rozšíření CRL.....	46
8.5.1	Požadavky	46
8.5.2	CRL a pole rozšíření záznamu CRL.....	47
8.6	Rozšíření distribučních bodů CRL a CRL delta.....	53
8.6.1	Požadavky	53
8.6.2	Pole rozšíření distribučních bodů CRL a CRL delta.....	54
9	Vztah přírůstkového seznamu CRL delta k základnímu CRL.....	58
10	Procedura zpracování certifikační cesty.....	59
10.1	Vstupy zpracování cesty.....	59
10.2	Výstupy zpracování cesty.....	59

10.3	Proměnné zpracování cesty.....	60
10.4	Inicializační krok.....	60
10.5	Zpracování certifikátu.....	61
10.5.1	Základní kontroly certifikátu.....	61
10.5.2	Zpracování mezilehlých certifikátů.....	61
10.5.3	Zpracování indikátoru explicitní politiky.....	62
10.5.4	Závěrečné zpracování.....	62
11	Schéma adresáře PKI.....	63
11.1	Třídy objektů adresáře PKI a tvary jmén.....	63
11.1.1	Třída objektu uživatele PKI.....	63
11.1.2	Třída objektu CA PKI.....	63
11.1.3	Třída objektu distribučních bodů CRL a tvar jména.....	63
11.1.4	Třída objektu delta CRL.....	64
11.1.5	Třída objektu certifikační politiky & CPS.....	64
11.1.6	Třída objektu certifikační cesty PKI.....	64
11.2	Atributy adresáře PKI.....	64
11.2.1	Atribut certifikátu	

uživatele.....	64
11.2.2 Atribut certifikátu CA.....	64
11.2.3 Atribut dvojice křížových certifikátů.....	64
11.2.4 Atribut seznamu revokovaných certifikátů.....	65
11.2.5 Atribut revokačního seznamu autority.....	65
11.2.6 Atribut revokačního seznamu delta.....	65
11.2.7 Atribut podporovaných algoritmů.....	65
11.2.8 Atribut prohlášení certifikační praxe.....	66
11.2.9 Atribut certifikační politiky.....	66
11.2.10 Atribut cesty PKI	66
11.3 Pravidla porovnávání adresáře PKI.....	67
11.3.1 Exaktní shoda certifikátu.....	67
Strana 5	
Strana	
11.3.2 Shoda certifikátu	67
11.3.3 Exaktní shoda dvojice certifikátů.....	68

11.3.4 Shoda dvojice certifikátů.....	69
11.3.5 Exaktní shoda seznamu certifikátů.....	69
11.3.6 Shoda seznamu certifikátů.....	69
11.3.7 Shoda identifikátoru algoritmu.....	70
11.3.8 Shoda politiky	70
11.3.9 Shoda cesty PKI	70
ODDÍL 3 ZÁKLADNÍ STRUKTURA CERTIFIKÁTU ATRIBUTU.....	71
12 Certifikáty atributu	71
12.1 Struktura certifikátu atributu.....	71
12.2 Cesty certifikátu atributu.....	74
13 Vztah autority atributu, SOA a certifikační autority.....	74
13.1 Privilegia v certifikátech atributu.....	75
13.2 Privilegium v certifikátech veřejného klíče.....	75
14 Modely PMI	75
14.1 Obecný model	

.....	. 75
14.1.1 PMI v kontextu řízení přístupu.....	77
14.1.2 PMI v kontextu nepopíratelnosti.....	77
14.2 Model řízení	77
14.3 Model delegování	78
14.4 Model rolí	79
14.4.1 Atribut role	79
15 Rozšíření certifikátu managementu privilegia.....	80
15.1 Rozšíření základního managementu privilegia.....	80
15.1.1 Požadavky	80
15.1.2 Pole rozšíření základního managementu privilegia.....	81
15.2 Rozšíření revokace privilegia.....	83
15.2.1 Požadavky	83
15.2.2 Pole rozšíření revokace	

privilegia.....	83
15.3 Rozšíření zdroje autority.....	84
15.3.1 Požadavky	84
15.3.2 Pole rozšíření SOA	84
15.4 Rozšíření role	85
15.4.1 Požadavky	85
15.4.2 Pole rozšíření role	86
15.5 Rozšíření delegování	87
15.5.1 Požadavky	87
15.5.2 Pole rozšíření delegování.....	87
16 Procedura zpracování cesty privilegia.....	90
16.1 Základní procedura zpracování.....	90
16.2 Procedura zpracování role.....	91

16.3 Procedura zpracování delegování.....	91
16.3.1 Ověřit integritu pravidla dominance.....	92
16.3.2 Ustanovit platnou cestu delegování.....	92
16.3.3 Ověřit delegování privilegií.....	92
16.3.4 Určení úspěš/neúspěš	93
17 Schéma adresáře PMI.....	93
17.1 Třídy objektu Adresáře PMI.....	93
17.1.1 Třída objektu uživatele PMI.....	93
17.1.2 Třída objektu AA PMI.....	93
17.1.3 Třída objektu SOA PMI.....	93
17.1.4 Distribuční bod třídy objektů certifikátu atributu CRL.....	93
17.1.5 Cesta delegování PMI.....	94
17.1.6 Třída objektu politiky privilegia.....	94
17.2 Atributy Adresáře PMI.....	94
17.2.1 Atribut certifikátu atributu.....	94
17.2.2 Certifikát atributu AA.....	

17.2.3 Deskriptoru atributu certifikátu atributu *)	94	
17.2.4 Certifikát atributu revokačního seznamu atributu.....	95	
17.2.5 Atribut seznamu revokovaných certifikátů AA.....	95	
17.2.6 Atribut cesty delegování	95	
17.2.7 Atribut politiky privilegia	95	
17.3 Obecná pravidla porovnávání adresáře PMI.....	95	
17.3.1 Exaktní shoda certifikátu atributu.....	95	
17.3.2 Shoda certifikátu atributu.....	96	
17.3.3 Shoda vydavatele a držitele.....	96	
17.3.4 Shoda cesty delegování	96	
ODDÍL 4 ZÁKLADNÍ STRUKTURY POUŽÍVÁNÍ CERTIFIKÁTU VEŘEJNÉHO KLÍČE & CERTIFIKÁTU		
ATRIBUTU		
ADRESÁŘEM		97
18 Autentizace Adresáře	97	
18.1 Procedura jednoduché autentizace.....	97	
18.1.1 Generování chráněné identifikující informace.....	98	
18.1.2 Procedura pro chráněnou jednoduchou		

autentizaci.....	99
18.1.3 Typ atributu hesla uživatele.....	99
18.2 Silná autentizace	
100	
18.2.1 Získání certifikátů veřejného klíče z adresáře.....	100
18.2.2 Procedury silné autentizace.....	
102	
19 Řízení přístupu	
105	
20 Ochrana operací Adresáře.....	106
Příloha A (normativní) Základní struktury certifikátu veřejného klíče a certifikátu atributu.....	107
Příloha B (normativní) Generování CRL a pravidla zpracování.....	128
B.1 Úvod	
.....	128
B.1.1 Typy CRL	
.....	128
Strana 7	
<hr/>	
Strana	
B.1.2 Zpracování CRL	
129	
B.2 Určení parametrů pro seznamy CRL.....	129

B.3	Určení požadovaných seznamů	
CRL.....		130
B.3.1	Koncová entita s kritickým CRL	
DP.....		130
B.3.2	Koncová entita s nekritickým CRL	
DP.....		130
B.3.3	CA s kritickým CRL	
DP.....		131
B.3.4	CA s nekritickým CRL	
DP.....		131
B.4	Získání	
CRL		
.....		
..		131
B.5	Zpracování	
CRL		
.....		
		131
B.5.1	Validace pole působnosti základního	
CRL.....		132
B.5.2	Validace pole působnosti CRL	
delta.....		133
B.5.3	Kontrola platnosti a aktuálnosti základního	
CRL.....		134
B.5.4	Platnost a kontroly CRL	
delty.....		134
Příloha C (informativní) Příklady vydávání CRL		
delta.....		135
C.1	Úvod	
.....		
.....		135
Příloha D (informativní) Politika privilegia a příklady definice atributu privilegia		
privilegia.....		137
D.1	Úvod	
.....		
.....		137

D.2 Ukázkové syntaxe	137
D.2.1 První příklad	137
D.2.2 Druhý příklad	139
D.3 Příklad atributu privilegia	141
Příloha E (informativní) Úvod do kryptografie s veřejným klíčem	142
Příloha F (normativní) Definice odkazu identifikátorů objektu algoritmu	144
Příloha G (informativní) Příklady použití omezení certifikační cesty	145
G.1 Příklad 1: Použití základních omezení	145
G.2 Příklad 2: Použití omezení jména	145
G.3 Příklad 3: Použití mapování politiky a omezení politiky	145
Příloha H (informativní) Abecední seznam definic informačních položek	147
Příloha I (informativní) Změny a opravy	150
Národní příloha NA (informativní) Slovník použitých výrazů	151

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 webových stránkách ISO; publikované Technické opravy lze získat z archivu na webových stránkách 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 revizí třetího vydání (ISO/IEC 9594-8:1998), které je dočasně ponecháno, aby podporovalo implementaci 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 nejdříve 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.

Strana 10

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.

Strana 11

ODDÍL 1 - VŠEOBECNÉ

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 umisťují 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 strukturu 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 --