ČESKÁ TECHNICKÁ NORMA
ICS 35.100.70 **Duben 2004**

Informační technologie – Propojení otevřených systémů – Adresář: Základní struktury certifikátu veřejného klíče a certifikátu atributu

ČSN ISO/IEC 9594-8 ed. 4 **OPRAVA 1**
36 9671

idt ISO/IEC 9594-8:2001/Cor.1:2002-09

Corrigendum

Tato oprava je českou verzí opravy ISO/IEC 9594-8:2001/Cor.1:2002-09.

This Corrigendum is the Czech version of the Corrigendum ISO/IEC 9594-8:2001/Cor.1:2002-09.

Oprava 1 mezinárodní normy ISO/IEC 9594-8:2001 byla připravena společnou technickou komisí ISO/IEC JTC 1 *Informační technologie,* subkomisí SC 6, *Telekomunikace a výměna informací mezi systémy*.

ČSN ISO/IEC 9594-8 ed. 4 (36 9671) Informační technologie - Propojení otevřených systémů - Adresář: Základní struktury certifikátu veřejného klíče a certifikátu atributu z dubna 2003 se opravuje takto:

Technická oprava 1

(zahrnuje usnesení týkající se chybových hlášení 272, 273, 274, 275, 276, 277 278 a 279)

1) Oprava chyb uvedených v chybovém hlášení č. 272

V článku 8.4.2.1 přidejte následující text na konec odstavce, který začíná slovy „Složka **pathLenConstraint** bude přítomna pouze tehdy, …“

Omezení nabývá platnosti počínaje dalším certifikátem v cestě. Omezení omezuje délku segmentu certifikační cesty mezi certifikátem, obsahujícím toto prodloužení (extension) a certifikátem koncové entity (end-entity certificate). Nemá žádný vliv na počet certifikátů CA v certifikační cestě mezi důvěryhodným ukotvením a certifikátem obsahujícím toto prodloužení. Proto délka kompletní certifikační cesty může překročit maximální délku segmentu omezeného tímto prodloužením. Omezení řídí počet certifikátů nikoliv vydaných CA pro svou potřebu mezi certifikátem CA obsahujícím omezení a certifikátem koncové entity. Proto celková délka tohoto segmentu cesty, s výjimkou certifikátů, vydaných CA pro svou potřebu, může překročit hodnotu omezení až o dva certifikáty. (Toto zahrnuje certifikáty ve dvou koncových bodech segmentu a certifikáty CA mezi dvěma koncovými body, které jsou omezeny hodnotou tohoto prodloužení.)

*V článku 15.5.2.1, v odstavci, který začíná slovy „Složka **pathLenConstraint** je smysluplná pouze tehdy, je-li…“, nahraďte poslední dvě věty tohoto odstavce následujícím*:

Omezení omezuje délku segmentu delegované cesty (delegation path) mezi certifikátem obsahujícím toto prodloužení a certifikátem koncové entity. Nemá žádný vliv na počet certifikátů AA v delegované cestě mezi důvěryhodným ukotvením a certifikátem obsahujícím toto prodloužení. Proto délka kompletní delegované cesty může překročit maximální délku segmentu omezeného tímto prodloužením. Omezení řídí počet certifikátů AA mezi certifikátem AA obsahujícím omezení a certifikátem koncové entity. Proto celková délka tohoto segmentu cesty může překročit hodnotu omezení až o dva certifikáty. (Toto zahrnuje certifikáty ve dvou koncových bodech segmentu plus certifikáty AA mezi dvěma koncovými body, které jsou omezeny hodnotou tohoto prodloužení.)

2) Oprava chyb uvedených v chybovém hlášení č. 273

Nahraďte článek 8.4.2.2 následujícím:

8.4.2.2 Rozšíření omezení jména

Toto pole, které se bude používat pouze v certifikátu CA, označuje místo pro jméno, v rámci kterého musí být umístěna všechna jména subjektů v následujících certifikátech v certifikační cestě. Toto pole je definováno takto:

```
nameConstraints EXTENSION ::= {
        SYNTAX          NameConstraintsSyntax
        IDENTIFIED BY   id-ce-nameConstraint }


NameConstraintsSyntax ::= SEQUENCE {
        permittedSubtrees       [0]     GeneralSubtrees OPTIONAL,
        excludedSubtrees        [1]     GeneralSubtrees OPTIONAL,
        requiredNameForms       [2]     NameForms OPTIONAL }


GeneralSubtrees ::=SEQUENCE SIZE (1..MAX) OF GeneralSubtree


GeneralSubtree ::=SEQUENCE {
        base                    GeneralName,
        minimum         [0]     BaseDistance DEFAULT 0
        maximum         [1]     BaseDistance OPTIONAL }


BaseDistance ::=INTEGR (0..MAX)


NameForms ::=SEQUENCE {
        basicNameForms      [0]     BasicNameForms OPTIONAL,
        otherNameForms      [1]     SEQUENCE SIZE (1..MAX) OF SUBJECT IDENTIFIER OPTIONAL }
(ALL EXCEPT ({--žádná; tj. alespoň jedna složka bude přítomna--}))


BasicNameForms ::= BIT STRING {
        rfc822Name                  (0)
        dNSName                     (1)
        x400Address                 (2)
        directoryName               (3)
        ediPartyName                (4)
        uniformResourceIdentifier   (5)
        iPAddress                   (6)
        registeredID                (7) } (SIZE (1..MAX))
```

Pokud jsou přítomny, každý z **permittedSubtrees** (povolené podstromy) a **excludedSubtrees** (vyloučené podstromy) specifikuje jeden nebo více pojmenovávacích podstromů, každý je definován jménem kořenu podstromu a volitelně, v rámci tohoto podstromu, také oblastí, která je ohraničená horní a/nebo spodní úrovní. Je-li přítomen **permittedSubtrees**, jména subjektů v tomto podstromu jsou přijatelná. Pokud je přítomen **excludedSubtrees**, jakýkoli certifikát vydaný subjektem CA nebo následnými CAs v certifikační cestě, který má jméno subjektu v rámci těchto podstromů, je nepřijatelný. Pokud jsou přítomny oba **permittedSubtreees** i **excludedSubtrees** a prostory pro jméno se překrývají, prohlášení o vyloučení má přednost před jmény v tomto překrytí. Pokud ani povolené ani vyloučené podstromy nejsou specifikovány jako forma jména, pak je přijatelné jakékoli jméno v rámci této formy jména. Pokud je přítomen **requiredNameForms**, všechny následné certifikáty v certifikační cestě musí zahrnovat jméno aspoň jedné z požadovaných forem jména.

Pokud je přítomen **permittedSubtrees**, následující se vztahuje na všechny certifikáty v cestě. Jestliže jakýkoli certifikát obsahuje jméno subjektu (v poli pro subjekt nebo v prodloužení **subjectAltNames**) formy jména, pro který jsou specifikovány povolené podstromy, jméno musí odpadnout v rámci aspoň jednoho ze specifikovaných podstromů. Jestliže jakýkoli certifikát obsahuje pouze jména subjektu forem jména, jiných než pro jaké jsou specifikované povolené podstromy, jména subjektů nemusí odpadnout v žádném ze specifikovaných podstromů. Například předpokládejme, že dva povolené podstromy jsou specifikovány, jeden pro formu jména DN a jeden pro rfc822, žádné vyloučené podstromy nejsou specifikované, ale **requiredNameForms** jsou specifikovány přítomnými bity **directoryName** a **rfc822Name**. Certifikát, který obsahoval pouze jiná jména, než je jméno adresáře nebo jméno rfc822, nebude přijatelný. Pokud **requiredNameForms** nebyly specifikovány, nebude takový certifikát přijatelný. Například předpokládejme, že dva povolené podstromy jsou specifikovány, jeden pro formu jména DN a jeden pro rfc822, žádné vyloučené podstromy nejsou specifikovány, a **requiredNameForms** nejsou přítomny. Certifikát, který obsahoval pouze DN a kde DN je ve specifikovaném, povoleném podstromu, bude přijatelný. Certifikát, který obsahoval DN i rfc822 a kde pouze jeden z nich je ve specifikovaném, povoleném podstromu, bude nepřijatelný. Certifikát, který obsahoval pouze jiná jména, než DN nebo rfc822, bude také přijatelný.

Pokud je přítomen **excludedSubtrees** (vyloučené podstromy), žádný certifikát vydaný subjektem CA nebo následnými CAs v certifikační cestě, který má jméno subjektu (v poli pro **subjekt** nebo v prodloužení **subjectAltNames**) v rámci tohoto podstromu není přijatelný. Například předpokládejme, že dva vyloučené podstromy jsou specifikovány, jeden pro formu jména DN a jeden pro rfc822. Certifikát, který obsahoval pouze DN a kde DN je v rámci specifikovaného vyloučeného podstromu, bude nepřijatelný. Certifikát, který obsahoval jména DN i rfc822 a kde alespoň jeden z nich je ve specifikovaném, vyloučeném podstromu, bude nepřijatelný.

Když má certifikační subjekt více jmen pro stejnou formu jména (včetně případu, kdy u formy jména **directoryName** je jméno v subjektovém poli certifikátu nenulový), pak budou všechna jména porovnávána kvůli přesnosti se jménem omezení této formě jména.

Pokud jsou přítomny **requiredNameForms**, všechny následné certifikáty v certifikační cestě musí obsahovat jméno subjektu aspoň jedné z požadovaných forem jména.

Co se týče formy jména dostupných přes typ **GeneralName**, pouze ty formy jména, které mají jasně definovanou hierarchickou strukturu, mohou být použity v poli **permittedSubtrees** a **excluded Subtrees**. Forma jména **directoryName** tento požadavek splňuje; při použití formy jména se pojmenovávací podstrom shoduje s podstromem DIT.

Minimální pole specifikuje horní hranici oblasti v rámci podstromu. Všechna jména, jejichž koncová složka jména je specifikována nad touto úrovní, nejsou obsažena v této oblasti. **Minimální** hodnota rovnající se nule (chyba) odpovídá základně, tj. vrchnímu uzlu podstromu. Když je například **minimum** nastavené na 1, potom pojmenovávací podstrom (naming subtree) vylučuje základnový uzel, ale zahrnuje podřízené uzly.

Maximální pole specifikuje spodní hranici oblasti v rámci podstromu. Žádná jména, jejichž poslední složka je specifikována pod touto úrovní, nejsou obsaženy v této oblasti. **Maximální** hodnota rovnající se nule odpovídá základně, tj. vrcholu podstromu. Chybějící **maximální** složka indikuje, že v rámci tohoto podstromu by neměl být zaveden žádný spodní limit. Když je například **maximum** nastavené na 1, potom pojmenovávací podstrom vylučuje všechny uzly kromě základny podstromu a jeho přímé podřízené.

Toto rozšíření může být podle volby vydavatele certifikátu kritické nebo nekritické. Doporučuje se, aby bylo označeno jako kritické, jinak by uživatel certifikátu nemusel zjistit, že následující certifikáty v certifikační cestě jsou umístěny v prostoru pro jméno, určeném vydáním CA.

Implementace shody nejsou potřeba k rozpoznání všech možných forem jména.

Pokud je rozšíření přítomné a je označeno příznakem, implementace používající certifikát (certificate-using implementation) musí rozpoznat a zpracovat všechny formy jména, pro která je zde jak specifikace podstromu (povoleného nebo vyloučeného) v rozšíření, tak i odpovídající hodnota v **subjektovém** poli nebo v prodloužení **subjectAltNames** jakéhokoli následujícího certifikátu v certifikační cestě. Pokud se nerozpoznaná forma jména objeví ve specifikaci podstromu i v následném certifikátu, bude se s takovým certifikátem nakládat jako kdyby to bylo setkání s nerozpoznaným kritickým rozšířením. Pokud jakékoli jméno subjektu v certifikátu v rámci vyloučeného podstromu odpadne, certifikát je nepřijatelný. Pokud je podstrom specifikován pro formu jména, která není obsažena v žádném následném certifikátu, může být takový podstrom ignorován. Pokud složka **requiredNameForms** specifikuje pouze nerozpoznané formy, jména, bude se s takovým certifikátem zacházet jako kdyby šlo o setkání s nerozpoznaným kritickým rozšířením. Jinak se alespoň jedna z rozpoznaných forem jména musí objevit ve všech následujících certifikátech v cestě.

Pokud je rozšíření přítomné a je označeno jako nekritické a implementace používající certifikát nerozpozná formu jména použitou v jakékoli **základní** složce, potom taková specifikace podstromu může být ignorována. Pokud je rozšíření označeno jako nekritické a jakákoli forma jména specifikovaná ve složce **requiredNamesForms** nejsou rozpoznány realizací používající certifikát, potom se s certifikátem bude zacházet tak, jako kdyby složka **requiredNameForms** nebyla přítomna.

V článku 10.3 přidejte novou proměnnou zpracování cesty, jak je uvedeno a následující proto přečíslujte:

d) *požadované-formy-jmen*: (možná prázdný) soubor sestav forem jména. Pro každou sestavu forem jmen musí všechny následující certifikáty obsahovat jméno jedné z forem jmen v souboru.

V článku 10.4 přidejte nový inicializační krok, jak je uvedeno a následující proto přečíslujte:

d) Inicializovat *požadované-formy-jmen* do prázdného souboru;

V článku 10.5.1 přidejte krok ke kontrole, aplikovaný na všechny certifikáty následovně:

h) Pokud certifikát není mezilehlý vydaný vlastním CA, a pokud *požadované-formy-jména* není prázdný soubor, v každé sadě forem jména v *požadovaných-formách-jména* zkontrolujte, zda v certifikátu jedné z forem jména v sadě je jméno subjektu.

V článku 10.5.2 přidejte krok k omezení zaznamenávající kroky aplikované na zprostředkující certifikáty takto:

c) Pokud je rozšíření **nameConstraint** se složkou **requiredNameForms** v certifikátu přítomno, nastavte proměnnou *požadované-formy-jména* do spojení její předchozí hodnoty a souboru složeného ze sady forem jména specifikovaného v certifikačním rozšíření. Pokud složka **requiredNameForms** obsahuje více než jednu formu jména, proměnná *požadované-formy-jména* signalizuje, že jméno aspoň jedné z indikovaných forem jména v rozšíření bude přítomno ve všech následných certifikátech. Spojení předchozí hodnoty proměnné *požadované-formy-jména* s hodnotou aktuálního rozšíření certifikátu je soubor sestav signalizujících požadavky pro všechny následné certifikáty. Když je například aktuální *požadované-formy-jména* nastaveno na požadavek, že buď jméno DN nebo rfc822 musí být přítomno v certifikátech a že aktuální rozšíření ve zpracovávaném certifikátu indikuje, že jsou požadována buď jména rfc822 nebo DNS, výsledné spojení, které je novou *požadovanou-formou-jména* indikuje, že každý z následných certifikátů musí mít buď jméno rfc822 nebo obě jména DN a DNS.

V příloze A modul **certificateExtensions** *aktualizuje ASN.1 pro rozšíření* **nameConstraint,** *jak je uvedeno výše.*

V příloze A modul **certificateExtensions**, *přidejte následující*:

id-cenameConstraint OBJECT IDENTIFIER ::= {id-ce 30 1}

V příloze A modul **certificateExtensions**, *vymažte následující:*

id-cenameConstraints OBJECT IDENTIFIER ::= {id-ce 30}

V příloze A modul **certificateExtensions**, *přidejte následující do souborů OIDs neužívaných v této specifikaci:*

id-ce 30

3) Oprava chyb uvedených v chybovém hlášení č. 274

V příloze A nahraďte **AttCertVersion** *ASN.1 tímto*:

AttCertVersion ::= INTEGER {v2(1)}

V 12.1 nahraďte první odstavec, který následuje po ASN.1 tímto:

version rozlišuje mezi různými verzemi atributového certifikátu. Pro atributové certifikáty vydané v souladu se syntaxí ve specifikaci, **version** musí být **v2**.

4) Oprava chyb uvedených v chybovém hlášení č. 275

V8.2.2.4 přidejte toto jako nový druhý odstavec následující za ASN.1 pro rozšíření **extKeyUsage**:

CA může prosazovat užití any-extended-key-usage (použití-jakéhokoli-prodlouženého-klíče) použitím identifikátoru **anyExtendedKeyUsage**. To umožňuje CA vydat certifikát, který obsahuje OIDs pro užití prodlouženého klíče, který může být aplikací požadován, bez omezení certifikátu použít pouze tyto klíče. Pokud by použití prodlouženého klíče použití klíče omezovalo, potom zařazení tohoto OID omezení odstraní.

anyExtendedKeyUsage OBJECT IDENTIFIER ::= {2 5 29 37 0}

5) Oprava chyb uvedených v chybovém hlášení č. 276

V 8.1.5.:

V poslední větě zaměňte „a indikátory *nevyřízené-explicitní-politiky*“ *za* „*indikátory nevyřízené-explicitní-politiky* a *zábranu-jakékoliv-politiky“.*

V článku 8.4.2.4. v první větě:

Nahraďte výraz „pro všechny certifikáty v certifikační cestě“ *slovy* „pro všechny certifikáty v certifikační cestě kromě samovydaných“.

V článku 10.5.1. e):

Nahraďte „nebo je-li nastaven *indikátor-jakékoli-politiky-zamezení,* potom se vymazává“ *výrazem* „nebo je-li nastaven *indikátor-jakékoli-politiky-zamezení* a certifikát není zprostředkující samovydaný, potom ho vymažte“.

6) Oprava chyb uvedených v chybovém hlášení č. 277

V 8.4.2.3 v poslední větě druhého odstavce:

Nahraďte „která je subjektem následujícího certifikátu“ *slovy* „která je vydavatelem následujícího certifikátu“.

7) Oprava chyb uvedených v chybovém hlášení č. 278

V 8.6.2.6 v první větě:

Nahraďte „se musí používat pouze jako rozšíření certifikátu a může se…“ *slovy* „může se používat buď jako certifikát nebo jako rozšíření CRL. V těchto certifikátech může být rozšíření…“

8) Oprava chyb uvedených v chybovém hlášení č. 279

V 7 přidejte následující ihned za ***CrossCertificates***:

PkiPath ::= SEQUENCE OF Certificate

PkiPath se používá jako zástupce certifikační cesty. V takové větě je pořadí certifikátů takové, že subjekt prvního certifikátu je vydavatelem druhého certifikátu atd.

V 11.1.6:

Nahraďte „třídy objektu **pkiCA**“ *výrazem* „**pkiCA** nebo **pkiUser**“.

V poslední větě posledního odstavce v 7:

Nahraďte „**CertPath**“ výrazem „**CertPath** nebo hodnotou **Certificate** v **PkiPath**“.

V 11.2.10:

Vymažte **PkiPath** *v notaci ASN.1*:

V první větě 11.2.10:

Nahraďte „křížových-certifikátů“ *výrazem* „certifikátů“.

V 11.2.10 nahraďte text následující za notaci ASN.1 tímto:

Tento atribut může být uložen ve vstupu do adresáře objektové třídy **pkiCA** nebo **pkiUser**.

Pokud je uložen ve vstupech **pkiCA**, hodnoty tohoto atributu obsahují certifikační cesty vylučující certifikáty koncové entity. Takový atribut se používá k uložení certifikačních cest, které se často používají jako záložní části spojené s touto CA. Hodnota tohoto atributu se může užít společně s jakýmkoli certifikátem koncové entity vydaným posledním certifikačním subjektem v atributové hodnotě.

Pokud je uložen ve vstupech **pkiUser**, hodnoty tohoto atributu obsahují certifikační cesty, které zahrnují certifikáty koncové hodnoty. V takovém případě je koncovou entitou uživatel, jehož vstup obsahuje tento atribut. Hodnoty tohoto atributu reprezentují kompletní certifikační cesty pro certifikáty vydané pro tohoto uživatele.

V 11.3.9 v poslední větě prvního odstavce:

Nahraďte „vydaným autoritě CA, která vydává certifikáty koncové entity, který se validuje“ *slovy „*vydaný pro specifický subjekt“.

U p o z o r n ě n í : Změny a doplňky, jakož i zprávy o nově vydaných normách jsou uveřejňovány ve Věstníku Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN ISO/IEC 9594-8 ed. 4 OPRAVA 1

Vydal: ČESKÝ NORMALIZAČNÍ INSTITUT, Praha
Vytiskl: XEROX CR, s.r.o.
Rok vydání 2004, 8 stran
Distribuce: Český normalizační institut, Hornoměcholupská 40, 102 04 Praha 10

69993 Cenová skupina 408