X.509 Zertifikatserweiterungen für die Verwaltung

2003-02-18

Konvention
X509ext – 1.0.2
Entwurf öffentlich

Bezeichnung	X.509 Zertifikatserweiterungen für die Verwaltung
Kurzbezeichnung	X.509 Erweiterungen
Version	1.0.2
Datum	2003-02-18
Dokumentenklasse	Konvention
Dokumentenstadium	Entwurf öffentlich
Kurzbeschreibung	X.509 Zertifikate erlauben die Aufnahme von zusätzlichen Attributen in Form von Zertifikkats-erweiterungen (Extensions). Diese Konvention beschreibt spezielle Erweiterungen für die Verwaltung.
Autor	Arno Hollosi, arno.hollosi@cio.gv.at
Arbeitsgruppe	BMöLS Stabsstelle IKT-Strategie des Bundes Operative Unit – Technik

Inhalt

Dieses Dokument verwendet die Schlüsselwörter MUSS, DARF NICHT, ERFORDERLICH, SOLLTE, SOLLTE NICHT, EMPFOHLEN, DARF, und OPTIONAL zur Kategorisierung der Anforderungen. Diese Schlüsselwörter sind analog zu ihren englischsprachigen Entsprechungen MUST, MUST NOT, REQUIRED, SHOULD, SHOULD NOT, RECOMMENDED, MAY, und OPTIONAL zu handhaben, deren Interpretation in RFC 2119 festgelegt ist.

1 Einleitung

Sowohl beim Schutz von Kommunikationswegen, als auch beim Einsatz der (sicheren) Signatur finden elektronische Zertifikate nach der X.509 Spezifikation breiten Einsatz [RFC3280]. Solche Zertifikate werden von einer vertrauenswürdigen Instanz (z.B. Zertifizierungsdiensteanbietern) ausgestellt und bestätigen den Zusammenhang zwischen einem kryptographischen Schlüsselpaar einerseits und Attributen (z.B. Verwendungszwecke, Name, Kennzeichen, etc.) andererseits.

In diesem Kontext bietet es sich an, Zertifikate die von einer Verwaltungsorganisation eingesetzt werden mit verwaltungsrelevanten Attributen zu versehen, unabhängig vom gewählten Zertifizierungsdiensteanbieter. Die so gekennzeichneten Zertifikate erlauben ein leichteres Management von Identitäten und Rollen.

2 X.509 Extension-Mechanismus

RFC3280 legt die Struktur für X.509 Zertifikate, so wie sie im Zusammenhang mit Internet-Anwendungen Verwendung finden fest. X.509 Zertifikate verwenden die binäre ASN.1 DER Kodierung, um Daten zu speichern. Neben Kerndaten wie Subjekt und Aussteller des Zertifikates, gibt es die Möglichkeit, weitere Attribute in Form von so genannten Extensions ins Zertifikat aufzunehmen.

Die ASN.1 Spezifikation der Extensions sieht wie folgt aus:

```
Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension
Extension   ::=  SEQUENCE  {
     extnID      OBJECT IDENTIFIER,
     critical    BOOLEAN DEFAULT FALSE,
     extnValue   OCTET STRING  }
```

Jede Extension hat also einen eindeutigen Bezeichner `extnID`, ein Flag ob diese Extension kritisch ist und den eigentlichen Wert der Extension `extnValue`.

Kritische Extensions sind jene, die von Applikationen behandelt werden müssen, bzw. falls diese unbekannt sind und nicht berücksichtigt werden können, muss die gesamte Verarbeitung abgebrochen werden. Aus RFC3280, Kapitel 4.2:

> The extensions defined for X.509 v3 certificates provide methods for associating additional attributes with users or public keys and for managing a certification hierarchy. The X.509 v3 certificate format also allows communities to define private extensions to carry information unique to those communities. Each extension in a certificate is designated as either critical or non-critical. A certificate using system MUST reject the certificate if it encounters a critical extension it does not recognize; however, a non-critical extension MAY be ignored if it is not recognized.

Die in weiterer Folge beschriebenen Zertifikatserweiterungen für die Verwaltung SOLLEN ausschließlich als „non-critical Extensions“ markiert werden, damit eine Verarbeitung mit Standardkomponenten möglich ist. Eine Verwendung von „critical Extensions“ SOLL nur nach genauer Prüfung des Einsatzszenarios erfolgen.

3 Definierte Zertifikatserweiterungen

Im Folgenden werden die im Kontext von X.509 Zertifikaten definierten Erweiterungen beschrieben. Derzeit ist nur eine Erweiterung definiert.

3.1 Verwaltungseigenschaft

Um ein Zertifikat als einer Verwaltungsorganisation zugehörig auszuweisen, kann die Verwaltungseigenschaft als Extension aufgenommen werden. Der zugehörige Object Identifier ist in „Object Identifier der öffentlichen Verwaltung“[OID] definiert.

Folgende ASN.1 Struktur wird angewandt:

```
Extension ::= SEQUENCE {
   extnID = 1.2.40.0.10.1.1.1
   critical = false
   extnValue ::= CHOICE  {
        isPublicAuthority   alwaysTrue,
                     code   DirectoryString }
}
alwaysTrue BOOLEAN ::= TRUE
```

Ist kein Verwaltungskennzeichen bekannt bzw. soll bloß die Verwaltungseigenschaft im Zertifikat ausgedrückt werden, wird die erste Option verwendet.

Ist ein Kennzeichen bekannt [VKZ], kann diese mit der zweiten Möglichkeit spezifiziert werden. Der Typ *DirectoryString* ist im RFC3280 wie folgt definiert:

```
DirectoryString ::= CHOICE {
      teletexString           TeletexString (SIZE (1..MAX)),
      printableString         PrintableString (SIZE (1..MAX)),
      universalString         UniversalString (SIZE (1..MAX)),
      utf8String              UTF8String (SIZE (1..MAX)),
      bmpString               BMPString (SIZE (1..MAX)) }
```

```
The DirectoryString type is defined as a choice of PrintableString,
TeletexString, BMPString, UTF8String, and UniversalString.  The
UTF8String encoding [RFC 2279] is the preferred encoding, and all
certificates issued after December 31, 2003 MUST use the UTF8String
encoding of DirectoryString (...).  Until that date, conforming CAs
MUST choose from the following options when creating a distinguished
name, including their own:

   (a)  if the character set is sufficient, the string MAY be
   represented as a PrintableString;

   (b)  failing (a), if the BMPString character set is sufficient the
   string MAY be represented as a BMPString; and

   (c)  failing (a) and (b), the string MUST be represented as a
   UTF8String.  If (a) or (b) is satisfied, the CA MAY still choose
   to represent the string as an UTF8String.
```

Durch die Verwendung des *DirectoryString* Typs ist eine größtmögliche Kompatibilität im Hinblick auf bestehende Applikationen gewährleistet[1].

[1] Dieser Typ wird unter anderem auch für Stringwerte in den Datentypen für Subject und Issuer DN verwendet.

Referenzen

RFC3280

R. Housley, W. Polk, W. Ford, D. Solo: RFC 3280 Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile, IETF Request for Comment, April 2002

ASN1

ITU-T Recommendation X.680 (1997), ISO/IEC 8824-1: 1998, Information Technology – Abstract Syntax Notation One (ASN.1), Specification of Basic Notation

DER

ITU-T Recommendation X.690 (1997), ISO/IEC 8825-1: 1998, Information Technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encodig Rules (CER) and Distinguished Encoding Rules (DER)

OID

Hollosi A.: Object Identifier der öffentlichen Verwaltung, OID 1.0.2, 2003-02-13

VKZ

Grandits F., Wiesner H.: Kennzeichen für Organisationseinheiten von Gebietskörperschaften bzw. Körperschaften öffentlichen Rechts (Verwaltungskennzeichen), VKZ 1.0, 2002-12-13

Historie

Version 1.0.2, 2003-02-18

- Dokument aufgeteilt in OID-1.0.2 und X509ext-1.0.2
- Behördenkennzeichen umbenannt in Verwaltungskennzeichen

Version 1.0.1, 2002-08-06

- ASN.1 Struktur von BOOLEAN DEFAULT TRUE auf alwaysTrue umgestellt
- Angaben über Subject und SubjectAlternativeName entfernt