Zertifikatserweiterungen der öffentlichen Verwaltung

Version 1.0.0

1 Motivation

Immer mehr Organisationen der öffentlichen Verwaltung planen den Einsatz von Public Key Zertifikaten nach dem Standard X.509. Dabei entsteht vielfach auch die Frage, wie bestimmte Eigenschaften oder Rollen eines Zertifikatinhabers in einem Zertifikat zum Ausdruck gebracht werden können.

Für zwei solcher Eigenschaften (Verwaltungseigenschaft, Dienstleistereigenschaft) wurden vom Bereich IKT-Strategie im Bundeskanzleramt bereits österreich-spezifische Zertifikatserweiterungen normiert. Der dafür verwendete Mechanismus soll auch für die Festlegung weiterer Eigenschaften herangezogen werden und soll in diesem Papier erklärt werden. Durch diese Strategie wird neben der internationalen Absicherung, dass die resultierenden Bezeichner für Österreich reserviert sind, auch sichergestellt, dass innerhalb Österreich die Subbezeichner nur für eine Eigenschaft zugeordnet werden.

2 Begriffsbestimmungen

Rund um die Diskussion der Zertifikatserweiterungen wird mit unterschiedlichen Begriffen hantiert, die nicht immer korrekt verwendet werden und daher meist zu Unklarheiten und Missverständnissen führen. Als Einführung zu diesem Papier werden daher zunächst die wichtigsten dieser Begriffe erläutert.

Zertifikatserweiterung

Ein Mechanismus, um in ein X.509-Zertifikat Eigenschaften aufzunehmen, die nicht zum Standardumfang eines Zertifikats (z.B. Name, Organisationszugehörigkeit, Emailadresse) gehören. Eine Zertifikatserweiterung hat einen eindeutigen Bezeichner und einen frei definierbaren Inhalt. Siehe auch Punkt 4.

OID

Technischer Fachbegriff für den eindeutigen Bezeichner (also den Namen) einer Zertifikatserweiterung. In X.509-Zertifikaten wird für die Bezeichnung der Erweiterung nicht Text (z.B. "Verwaltungseigenschaft") verwendet, sondern eine hierarchisch aufgebaute Folge von Ganzzahlen (z.B. "1.2.40.0.10.1.1.1"). Eine solche Ganzzahl-Folge wird Object Identifier oder OID genannt. Häufig wird der Begriff OID inkorrekter Weise als Synonym für den Begriff Zertifikatserweiterung verwendet. Im Normalfall wird im österrecihischen E-Government nur der Bezeichner normiert.

3 Zertifikatsinhalte

In ein X.509-Zertifikat können eine Reihe von Standard-Eigenschaften zur näheren Beschreibung des Zertifikatinhabers aufgenommen werden. Sehr häufig werden für

Personen die Eigenschaften Vorname (z.B. Max), Nachname (z.B. Mustermann), Emailadresse (z.B. max.mustermann@asf.gv.at), Organisation (z.B. Amt für schwierige Fragen) oder Staat (z.B. AT) vewendet. Für Maschinen sind häufig verwendete Standard-Eigenschaften beispielsweise IP-Adresse (z.B. 193.154.247.38) oder Domänenname (z.B. www.asf.gv.at).

4 Zertifikatserweiterungen

Sollen in ein X.509-Zertifikat Eigenschaften des Zertifikatinhabers aufgenommen werden, die sich nicht durch Standard-Eigenschaften ausdrücken lassen, steht der Mechanismus der Zertifikatserweiterung zur Verfügung. Im Sinne der Kompatibilität sollen in die Standard-Eigenschaften nicht implizit Erweiterungen codiert werden

Eine Zertifikatserweiterung besteht aus einem eindeutigen Bezeichner (also einem Namen) sowie einem zugehörigen, in der Regel frei definierbaren Inhalt.

4.1 Bezeichner

Kodiert wird der eindeutige Bezeichner in Form eines sogenannten Object Identifiers (OID), das ist eine hierarchisch aufgebaute Folge von Ganzzahlen (für die Zertifikatserweiterung "Verwaltungseigenschaft" lautet der OID z.B. "1.2.40.0.10.1.1.1").

Die gesamte Menge an festgelegten OID nennt man auch OID-Baum. Eine Teilfolge von Ganzzahlen einer OID (von links aus beginnend) nennt man auch Teilbaum (der Teilbaum "1" stellt z.B. den von der ISO verwalteten Teilbaum dar; der Teilbaum "1.2.40.0.10" stellt den Teilbaum der österreichischen Verwaltung im weitesten Sinn dar). Ein Teilbaum wird jeweils von einer bestimmten Organisation verwaltet (z.B. "1" von der ISO, "1.2.40.0.10" vom Bereich IKT-Strategie im Bundeskanzleramt).

Eine Organisation kann die Verwaltung von Teilen ihres eigenen Teilbaums an andere Organisationen delegieren (z.B. hat der Bereich IKT-Strategie im Bundeskanzleramt die Verwaltung des Teilbaums "1.2.40.0.10.1.2" – also eines Unterbaums von "1.2.40.0.10" - an das BMI delegiert.

Für eine detaillierte Darstellung des Teilbaums der österreichischen Verwaltung siehe [1]. In diesem Dokument findet sich auch die Kontaktadresse für die Koordination der Festlegung eines OID unterhalb dieses Teilbaums.

Existenz und Inhalte von Zertifikatserweiterungen sind als „Attribute“ im Sinne des Signaturgesetzes anzusehen. Durch die Zuordnung der Teilbaumverwaltung an eine Organisation wird sichergestellt, dass das mit der Verwendung des OID verbundene Widerrufsrecht des Machtgebers laut SigG auch effizient umgesetzt werden kann.

4.2 Inhalt

Für eine bestimmte Zertifikatserweiterung kann der Inhalt in der Regel beliebig festgelegt werden. Der Inhalt kann beispielsweise ein einfacher Wert wie ein Text, eine Zahl, oder ein Boolean-Wert (wahr oder falsch) sein, aber auch eine Struktur von mehreren Werten, z.B. eine Sequenz eines Texts und einer Zahl. Teil einer Sequenz kann wiederum eine Sequenz sein, sodass sich solche Inhalte beliebig tief schachteln lassen.

5 Existierende Zertifikatserweiterungen der öffentlichen Verwaltung

Dieser Abschnitt beschreibt die zwei bisher vom Bereich IKT-Strategie im Bundeskanzleramt normierten Zertifikatserweiterungen, die beide als Bezeichner eine OID aus dem Teilbaum der österreichischen Verwaltung aufweisen.

5.1 Verwaltungseigenschaft

Die Verwaltungseigenschaft bringt zum Ausdruck, dass der Zertifikatsinhaber einer Verwaltungsorganisation angehört.

Der als Bezeichner verwendete OID lautet "1.2.40.0.10.1.1.1".

Der Inhalt besteht entweder aus einem Boolean-Wert, der stets den Wert true annimmt, oder aus einem Text, der das Verwaltungskennzeichen der Verwaltungsorganisation enthält, welcher der Zertifikatsinhaber angehört. Die erste Variante kann verwendet werden, wenn das Verwaltungskennzeichen nicht bekannt ist, oder es nicht erwünscht ist, die genaue Organisation zu bezeichnen.

Für weitere Details siehe [2].

5.2 Dienstleistereigenschaft

Die Dienstleistereigenschaft bringt zum Ausdruck, dass der Zertifikatinhaber im Auftrag (als Dienstleister) einer öffentlichen Verwaltungsorganisation tätig ist. Zertifkate, die solchermaßen gekennzeichnet sind, dürfen ausschließlich für Dienste/Applikationen eingesetzt werden, die tatsächlich im Auftrag einer öffentlichen Verwaltungsorganisation erfolgen, nicht für z.B. privatwirtschaftliche Dienste des Zertifikatinhabers.

Der als Bezeichner verwendete OID lautet "1.2.40.0.10.1.1.2".

Der Inhalt der Dienstleistereigenschaft ist leer, d.h. die Semantik dieser Zertifikatserweiterung (Dienstleister) kommt allein durch ihre Existenz im Zertifikat zum Ausdruck.

Für weitere Details siehe [2].

6 Referenzen

[1]

Hollosi, Arno: Object Identifier der öffentlichen Verwaltung. Version 1.0.4 vom 21.02.2005. Abrufbar unter http://www.cio.gv.at/it-infrastructure/oid/OID-1.0.4-20050221.pdf.

[2]

Hollosi, Arno: X.509-Zertifikatserweiterungen für die Verwaltung. Version 1.0.3 vom 21.02.2005.
Abrufbar unter http://www.cio.gv.at/it-infrastructure/pki/X509ext-1.0.3-20050221.pdf.

Ing. Gerhard Schwarz
gerhard.schwarz@bka.gv.at