Object Identifier der öffentlichen Verwaltung (Teil 1 – Hauptdokument)	Konvention OID-T1 – 1.0.0 Ergebnis der AG	
Kurzbeschreibung	Object Identifier sind weltweit eindeutige Kennungen für Objekte und sind in ISO/IEC 9834-1 normiert. Objekte sind persistente, wohldefinierte Informationen, Definitionen oder Spezifikationen. Dieses Dokument beschreibt den Aufbau des OID-Baums für die österreichische Verwaltung und die damit einher gehenden Prozesse. Neben diesem Hauptdokument ist die taxative Auflistung vergebener OID zu beachten [OID-T2].	
Autor(en):	Thomas Rössler, EGIZ / BKA	Projektteam / Arbeitsgruppe AG-Bürgerkarte (Q-BK) / AG-II
Beiträge von:	P. Pfläging, Wien H. Pacnik, L.Stmk.	

Vorgelegt am **XX.XX.XXXX**

Abgelehnt von:
Zur Kenntnis genommen von:
Anregungen von:
Angenommen von: *(mit der Option von allen bzw. allen übrigen Ländern bei ablehnenden Stellungnahmen)*

1

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.

Historie

Version:	**Datum:**	**Kommentar:**
1.0.0D	11.11.2008	- Erstellt. - Auf Basis Workshop mit Wien/Stmk. - Fußnote bei Use-Case 1
Autor:		
Thomas Rössler, EGIZ		
Version:	**Datum:**	**Kommentar:**
1.0.0	27.02.2009	- Abgeschlossen zur Vorlage (1.0.0D → 1.0.0)
Autor:		
Version:	**Datum:**	**Kommentar:**
Autor:		

1 Einleitung / Motivation

Object Identifier (OID) bieten einen hierarchisch organisierten, standardisierten Ordnungsbegriff, deren Verwaltung dezentral erfolgt. OID sind weltweit eindeutige Kennungen für Objekte auf Basis der ISO-Norm ISO/IEC 9834-1. Dieser Mechanismus eignet sich daher zur standardisierten Beschreibung von Objekten anhand von international normierten Identifikatoren. Die Interpretation des Terms „Objekt“ ist hier nicht näher spezifiziert. Dem Objekt kann folglich eine beliebige semantische Bedeutung hinterlegt werden. Im Sinne dieser Spezifikation drückt ein Objekt eine besondere Eigenschaft aus oder steht für ein bestimmtes Attribut dessen Inhabers.

Zum Beispiel: das Objekt „Verwaltungseigenschaft“ drückt konkret aus, dass dessen Träger der österreichischen Verwaltung zugehört. Dank der international standardisierten Ausdrucksform von OIDs kann dieser Umstand auf normierte Weise beschrieben werden.

Die Verwendung von OIDs ist letztlich offen und breit. So zum Beispiel eignen sich OIDs aufgrund ihrer syntaktischen Struktur auch zur Einbettung in X.509-Zertifikaten. Konkret sollen anhand von OIDs in X.509-Zertifikaten besondere für die öffentliche Verwaltung relevante Eigenschaften auf normierte Art im Zertifikat ausgedrückt werden.

Wieder am Beispiel der „Verwaltungseigenschaft“ skizziert: der Ausdruck einer „Verwaltungseigenschaft“ in einem X.509-Serverzertifikat, das heißt das Vorkommen des entsprechenden OIDs im Zertifikat, zeichnet den Inhaber des Zertifikates als Teil der öffentlichen Verwaltung aus. In weiterer Folge ist der mit einem solchen SSL/TLS-Zertifikat ausgestattete Server zum Auslesen von Personendaten (Personenbindung) aus der Bürgerkarte berechtigt, oder aber sind Personen, die diese Eigenschaft in ihrem Signaturzertifikat besitzen, berechtigt damit Amtssignaturen zu erstellen. Die Überprüfung dieser Eigenschaft wird bspw. durch die Bürgerkartensoftware auf Basis von OIDs durchgeführt.

1.1 Zusammenfassung

Dieses Dokument beschreibt in weiterer Folge die wichtigsten Anwendungsfälle von OIDs in der öffentlichen Verwaltung. Zudem wird die grundlegende Struktur von OIDs beschrieben und der für die öffentliche Verwaltung reservierte und stellvertretend durch das Bundeskanzleramt verwaltete OID-Teilbaum definiert. Abschnitt 6 legt zudem die Prozedur zur Vergabe von OID durch Zertifizierungsdiensteanbieter fest.

Ein als Zusatz zu diesem Dokument verfasstes Dokument [OID-T2] enthält die taxative Definition und Auflistung aller bislang vergebener (Sub-)OIDs sowie deren Inhaber/Bestandsgeber. Diese Aufteilung der Dokumente soll vor allem die Wartbarkeit und besonders auch die Vergabe weiterer (Sub-)OIDs erleichtern. Das Dokument [OID-T2] definiert die einzelnen OIDs, sowie deren Einsatzbereich, Eigenschaften und zulässiger Werte im Detail.

2 Object Identifier (OID)

Object Identifier sind weltweit eindeutige Kennungen für Objekte und sind in ISO/IEC 9834-1 normiert. Objekte sind persistente, wohldefinierte Informationen, Definitionen oder Spezifikationen.

Für eine umfassende Einführung wird auf die referenzierten Standards und existierende Fachlektüre verwiesen. Um den Begriff einleitend zu beschreiben, wird die zusammenfassende Beschreibung aus [WA-OID] zitiert:

In der Informatik ist ein Object Identifier oder kurz OID ein weltweit eindeutiger Bezeichner, der benutzt wird um ein Informationsobjekt zu benennen (vgl. URN). Ein OID stellt einen Knoten in einem hierarchisch zugewiesenen Namensraum dar, der durch den ASN.1-Standard definiert ist. Jeder Knoten ist durch eine Folge von Nummern eindeutig gekennzeichnet, die seine Position beginnend an der Wurzel des Baumes angibt. Neue Knoten zur eigenen Verwendung können bei den entsprechenden Autoritäten des übergeordneten Knotens beantragt werden. Die Regeln für die Vergabe und Registrierung von OIDs sind festgelegt in den Normen ISO/IEC 9834 und DIN 66334. Die Verwaltung des OID-Baumes und die Sicherstellung der Eindeutigkeit von OIDs beruhen auf der Übertragung der Zuständigkeit für die untergeordneten Knoten an den Besitzer einer OID. [WA-OID]

3 Anwendungsszenarien (Use-Cases)

Das Anwendungsfeld von OIDs ist grundsätzlich ein breites. Beabsichtigt ist jedoch vor allem die Verwendung von OIDs innerhalb von X.509 Zertifikaten, um eine besondere Eigenschaft des Zertifikatsinhabers auf standardisierte Art auszudrücken. Dies ist auch klares Ziel und die Motivation für die vorliegende Spezifikation.

Auf Basis von derart ausgestatteter X.509 Zertifikaten werden folgende abgeleitete Anwendungsszenarien (Use-Cases) realisiert:

- Use-Case 1: Identifikation von Servern der öffentlichen Verwaltung
- Use-Case 2: Identifikation von Signaturzertifikaten der öffentlichen Verwaltung
- Use-Case 3: Erkennung berufsmäßiger Parteienvertreter

In den nachfolgenden Abschnitten werden diese Aspekte überblicksmäßig dargestellt. Aufbauend darauf wird in Abschnitt 4 die Verwendung von OIDs in X.509-Zertifikaten im Detail spezifiziert.

Obschon diese Spezifikation die Einbettung von OIDs in X.509-Zertifikaten vordergründig vorsieht, ist die Anwendung von OID auch außerhalb von X.509-Zertifikaten möglich und sinnvoll, zum Beispiel zur Repräsentation von Eigenschaften im Rahmen von Kommunikationsprotokollen, etc. Es können die selben Eigenschaften und Attribute – wie im taxativen Zusatzteil [OID-T2] dieser Spezifikation definiert – auch in anderen Anwendungsfällen über die definierten OIDs referenziert und formuliert werden.

3.1 UC1: Identifikation von Servern der öff.Verw.

Zusammenfassung: *Server und Services der öffentlichen Verwaltung müssen als solche automatisiert erkennbar sein. Der Betreiber – generell der Ursprung – solcher Server/Services wird anhand des Server-Zertifikates erkennbar. Das Zertifikat wird dazu von einer vertrauenswürdigen Stelle (Zertifizierungsdienst) ausgestellt und enthält Angaben zum Betreiber. Um anhand eines solchen Zertifikats einfach und zweifelsfrei die Services/Server der öffentlichen Verwaltung erkennen zu können, wird ein definiertes OID in diese Zertifikate eingebracht (konkret die sog. „Verwaltungseigenschaft").*

Ein vordringlicher Anwendungsfall hinter der Einführung von OID ist die Identifikation von Servern – bzw. Server-Applikationen – der öffentlichen Verwaltung. Dazu muss der Server der öffentlichen Verwaltung mit einem TLS/SSL-Serverzertifikat betrieben werden, das in seiner Form als X.509-

Zertifikat eine entsprechende OID enthält[1].

Um bspw. den Ursprung „öffentliche Verwaltung“ in Form eines OID erkennen zu können, wird nachfolgend die OID „Verwaltungseigenschaft“ definiert. Die Existenz dieser OID ist ein technisches Synonym für das Attribut der Verwaltungseigenschaft. Ein jedes X.509-Zertifikat, das einen solchen OID als Erweiterung enthält, zeichnet den Inhaber des Zertifikates (Subjekt) als Teil der öffentlichen Verwaltung aus.

Auf Basis des OID kann bspw. ein Verbund von Web-Services der öffentlichen Verwaltung etabliert werden, in dem ohne zentrale Registratur oder Zugriffs-/Rechteverwaltung alle Teilnehmer als Teil der öffentlichen Verwaltung identifiziert werden können, alleine anhand des zum Verbindungsaufbaus verwendeten SSL/TLS-Zertifikates. Dieses Prinzip ist aber nicht nur auf die Eigenschaft und OID der öffentlichen Verwaltung beschränkt zu sehen, sondern kann auch unter Anwendung eines beliebigen Attributs – und des dementsprechenden OIDs – etabliert werden.

Eine konkrete Anwendung von anhand von OIDs identifizierten Servern ist das Konzept Bürgerkarte. Um zu prüfen, ob eine Bürgerkartenapplikation (Web-Applikation, Portal) dazu berechtigt ist die Personendaten (Personenbindung) einer Bürgerkarte auszulesen, prüft die Bürgerkartensoftware das von der Bürgerkartenapplikation zur Identifikation vorgewiesene SSL/TLS-Zertifikat. Dieses muss dazu eine Verwaltungseigenschaft ausweisen, wozu der entsprechende OID in Form einer X.509-Zertifikatserweiterung im SSL/TLS-Zertifikat der Bürgerkartenapplikation vorhanden sein muss. Ist die Bürgerkartenapplikation etwa ein Stammportal im Portalverbund, könnte dasselbe SSL/TLS-Zertifikat mit OID gleichzeitig dazu verwendet werden, um das Portal gegenüber einem Anwendungsportal als Portal der Verwaltung zu identifizieren.

In den hier skizzierten Szenarien wurde aus Gründen der Übersichtlichkeit auf die Beschreibung der in Verbindung mit SSL/TLS-Zertifikaten obligatorischen Zertifikatsprüfung verzichtet. Neben dem Vorhandensein einer OID muss das betreffende SSL/TLS-Zertifikat natürlich auch von einem vertrauenswürdigen Zertifizierungsdiensteanbieter ausgestellt und nicht widerrufen sein. Hier gibt es einerseits eine Reihe von kommerziellen Zertifizierungsdiensteanbieter; andererseits kann im Rahmen einer geschlossenen Benutzergruppe – vgl. Beispiel des Verbunds von Web-Services – eine eigene Zertifizierungsinstanz herangezogen werden. In diesem Bezug macht die vorliegende Spezifikation keine weiterführenden Vorgaben, da dies stark vom konkreten Anwendungsfall und den damit begründeten Kontext abhängig ist.

3.2 UC2: Identifikation von Signatur-Eigenschaften (z.B. Amtssignatur)

Zusammenfassung: *Besondere Eigenschaften elektronischer Signaturen – bzw. Eigenschaften, die durch den Signator bzw. dessen Rolle zur Entfaltung gelangen – werden ebenfalls im Signaturzertifikat anhand von OIDs ausgedrückt. Zum Beispiel ist eine Amtssignatur technisch erst durch das OID „Verwaltungseigenschaft“ im Signaturzertifikat des Signators erkennbar.*

Ähnlich geartet – wie in Abschnitt 3.1 skizziert – stellt sich auch der zweite Anwendungsfall für OID

[1] Für BürgerInnen ist als nachvollziehbarer und lesbarer Nachweis, dass sie es mit einem Server der öffentlichen Verwaltung zu tun haben, auch und vor allem die Verwaltungsdomäne *.gv.at relevant (z.B. in Verbindung mit Web-Servern). Die für solche Server ausgestellten X.509 Zertifikate enthalten somit auch den qualifizierten Namen des Servers (samt *.gv.at-Domäne) womit der Ursprung „öffentliche Verwaltung“ menschlich lesbar erkennbar wird. Granularere Unterscheidungen sind damit jedoch nicht möglich.

im Rahmen von X.509-Zertifikaten dar. Bei elektronischen Signaturen wird ebenfalls als Nachweis des Ursprungs – zum Beispiel Ursprung „öffentliche Verwaltung“ – der Signatur ein Zertifikat verwendet, das weitestgehend als X.509-Zertifikat repräsentiert wird.

Auch hier müssen Signaturen von Stellen der öffentlichen Verwaltung – zum Beispiel Amtssignaturen – als solche erkennbar sein, ganz den Vorgaben des E-Government Gesetzes folgend.

Um dies technisch zu erreichen, werden entsprechende OIDs innerhalb der zur Verifikation von Signaturen verwendeten X.509-Zertifikate eingeführt. Letztlich soll anhand dessen zumindest eine technische, automatisierte Prüfeinrichtung (Prüfsoftware) den Ursprung eines amtssignierten Dokumentes auf standardisierte Weise verifizieren können, in Verbindung mit allen anderen zur Verifikation von Zertifikaten erforderlichen Schritten (z.B. Überprüfung des Ausstellers des Zertifikates, Widerrufsprüfung, etc.).

Analog zur Amtssignatur verhält es sich beispielsweise mit Signaturen von berufsmäßigen Parteienvertretern, wie bspw. Rechtsanwälte, Ziviltechniker oder Notare. Auch in deren Signaturzertifikate kann ein entsprechender OID aufgenommen werden, der die besondere Eigenschaft des Zertifikatsinhabers – bspw. die Eigenschaft eines Notars – standardisiert ausdrückt (siehe auch Use-Case 3). Dessen Signatur bzw. deren Eigenschaft als bspw. „offizielle Signatur eines Notars“ ist somit auch automatisiert erkennbar. Die Festlegung der konkreten OIDs erfolgt ebenfalls in [OID-T2].

3.3 UC3: Einschreiten von berufsmäßigen Parteienvertretern/Organwaltern

Zusammenfassung: *Berufsmäßige Parteienvertreter und Organwalter, die im Namen anderer Rechtsgeschäfte tätigen und E-Government Services bedienen dürfen, werden als solche ebenfalls über definierte OIDs im Signaturzertifikat erkannt. So kann bspw. nach Authentifizierung über Bürgerkartenfunktionen zweifelsfrei ein Vertreter dieser Berufsgruppen erkannt und ihm entsprechend weiterführende Rechte eingeräumt werden (so zum Beispiel bei E-Government Anwendungen).*

Bei berufsmäßigen Parteienvertretern muss nach § 5 Abs. 2 E-Government-Gesetz [EGovG] deren *„[..] generelle Befugnis zur Vertretung aus der nach den berufsrechtlichen Vorschriften erfolgenden Anmerkung der Berufsberechtigung im Signaturzertifikat ersichtlich [..]*“ [EGovG] sein. Diese „Anmerkung“ erfolgt ebenfalls über definierte OIDs, die im zweiten Teil dieser Spezifikation [OID-T2] festgelegt werden, wie zum Beispiel die OIDs für Notare, Anwälte oder Ziviltechniker. Sinngemäß analog wird auch die Eigenschaft des „Organwalter“, gemäß den Vorgaben § 5 Abs. 3 [EGovG], in Form eines OID im Signaturzertifikat ausgedrückt.

Aufgrund dieser besonderen Eigenschaften der Signaturzertifikate von berufsmäßigen Parteienvertretern und Organwaltern können diese anhand der Vorlage einer von ihnen erzeugten elektronischen Signatur als solche gesichert authentisiert werden.

Letztlich ist dieser Anwendungsfall auf die Erkennung besonderer, verwaltungsrelevanter Eigenschaften anhand eines Signaturzertifikates reduzierbar. Es gelten somit die selben Maßgaben wie in Abschnitt 3.2 beschrieben. Aufgrund der konkreten Anwendung als Nachweis einer besonderen Vertretungsmacht und der damit verbundenen besonderen Relevanz ist dieser Anwendungsfall jedoch gesondert zu sehen.

4 OID in X.509 Zertifikaten

Sowohl beim Schutz von Kommunikationswegen als auch beim Einsatz der elektronischen Signatur finden Zertifikate nach der X.509 Spezifikation breiten Einsatz [RFC3280]. Solche Zertifikate werden von einer vertrauenswürdigen Instanz (z.B. Zertifizierungsdiensteanbieter) ausgestellt und bestätigen den Zusammenhang zwischen einem kryptographischen Schlüsselpaar und Attributen des Inhaber (z.B. Verwendungszwecke, Name, Kennzeichen, etc.). In diesem Kontext bietet es sich an Zertifikate, die von einer Verwaltungsorganisation eingesetzt werden, mit verwaltungsrelevanten Attributen zu versehen, unabhängig vom gewählten Zertifizierungsdiensteanbieter. Die Formulierung von verwaltungsrelevanten Attributen soll anhand der in dieser Spezifikation definierten OIDs erfolgen. Die Existenz von OIDs in X.509 Zertifikaten wird in üblichen Zertifikatsdarstellungen gängiger Betriebssysteme/Applikationen (zum Beispiel Microsoft Windows, etc.) zwar angezeigt, jedoch nur in ihrer numerischen Repräsentation (z.B. als 1.2.40.0.10.1.1.1). Daher zielen OIDs eher auf die maschinelle Prüfbarkeit durch entsprechende Prüfsoftware ab, als auf eine lesbare Darstellung gegenüber den BürgerInnen.

RFC3280 legt die Struktur für sogenannte X.509 Zertifikate fest, so wie sie im Zusammenhang mit Internet-Anwendungen Verwendung finden. 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 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.

Um ein X.509-Zertifikat mit einem Attribut der öffentlichen Verwaltung zu versehen SOLLEN die in dieser Spezifikation definierten OIDs der öffentlichen Verwaltung“ verwendet werden. Diese OIDs MÜSSEN als Extension dem X.509 beigefügt werden. Dazu wird die folgende ASN.1 Struktur angewandt:

```
Extension ::= SEQUENCE {
    extnID = oidIdentifier
    critical = false
    extnValue ::= OCTET STRING -- CONTAINING oidValue
}

oidValue ::= CHOICE {
    alwaysTrue  BOOLEAN(true)
    null        NULL
    value       DirectoryString
}
```

Dabei gilt:

`oidIdentifier` = Identifier der angewandten OID laut dieser Spezifikation.

`oidValue` = Wert der OID laut dieser Spezifikation.

Bei welchem OID (festgelegt durch den numerischer Identifier `oidIdentifier`) welche Werte (`oidValue`) zulässig sind, wird im Zuge der taxativen Definition von vergebenen OIDs im Rahmen des Zusatzteils [OID-T2] dieser Spezifikation festgelegt.

Sind zu einem OID auch Werte definiert (`oidValue`) so MUSS zur Kodierung des Wertes der Typ `DirectoryString` gem. RFC3280 verwendet werden. Dieser Typ 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.

5 OID-Teilbaum der öffentlichen Verwaltung

OIDs werden in Delegation verwaltet und sind in dieser Hinsicht mit Internet Domänen vergleichbar. In diesem Sinne wurde analog zum etablierten URI-Teilbaum der öffentlichen Verwaltung – `*.gv.at` – ein OID-Teilbaum – `gv-at` – für die OIDs der öffentlichen Verwaltung eingeführt (gv-at-OID-Teilbaum). Alle unter dieser OID definierten OIDs repräsentieren Eigenschaften der österreichischen öffentlichen Verwaltung oder Eigenschaften die im Interesse der öffentlichen Verwaltung liegen.

Den OID-Teilbaum der öffentlichen Verwaltung hat das Bundeskanzleramt stellvertretend für die öffentliche Verwaltung beim österreichischen Normierungsinstitut ÖNORM beantragt und zur Verwaltung übertragen bekommen (analog der Verwaltung der *gv.at – Domäne). Die Wurzel-OID des Teilbaums ist

`1.2.40.0.10`

bzw. in ASN.1 Syntax [ASN1]:

```
gv-at OBJECT IDENTIFIER ::= { iso (1) member-body (2)
                              austria (40) (0) (10) }
```

Die Vergabe von OIDs unmittelbar unterhalb dieser Wurzel-OID erfolgt nach Abstimmung im

Kooperationsgremium BLSG[2]. Anträge auf OIDs unmittelbar unterhalb dieser Wurzel-OID MÜSSEN zur Weiterbehandlung an die mit der operativen Verwaltung beauftragte Arbeitsgruppe gerichtet werden.

Object Identifier DÜRFEN nur für Organisationskategorien der öffentlichen Verwaltung oder Kategorien von Verwaltungshandelnden definiert werden. Im Sinne einer durchgängigen Policy sind jedenfalls jene Organisationen berechtigt die Definition eines OID im `gv-at` Teilbaum zu beantragen, die auch ein Recht auf Zuteilung und Verwendung einer `gv.at` Domäne haben. Die Feststellung, ob die die OID beantragende Person berechtigt ist im Namen ihrer Organisation tätig zu werden, erfolgt analog zum Vergabeprozess von `gv.at` Domänen [GVAT].

Gemäß dem Prinzip der Übertragung (Delegation) der Zuständigkeit zur Vergabe von untergeordneten Sub-OIDs an den Inhaber einer OID, können OIDs im OID-Teilbaum der öffentlichen Verwaltung auch weiter unterteilt werden. Das Recht zur weiteren Unterteilung einer OID KANN dem Inhaber einer OID zugesprochen werden. Dieses Recht MUSS im Zuge der Beantragung der OID bereits ausgesprochen werden oder KANN nachträglich gesondert durch den OID-Inhaber beantragt werden. Das Recht zur weiteren Unterteilung einer zugeteilten OID durch dessen Inhaber MUSS in der veröffentlichten taxativen Auflistung [OID-T2] vergebener OIDs vermerkt sein. Jede durch den Inhaber einer OID weiter vergebenen Sub-OID MUSS innerhalb des durch seine OID aufgespannten Teilbaums erfolgen und im Einklang mit dieser Spezifikation stehen. Derart vergebene Sub-OIDs MÜSSEN der mit der Verwaltung des gv-at-OID-Teilbaums beauftragten Arbeitsgruppe – und in weiterer Folge dem Kooperationsgremium BLSG – bekannt gegeben und zur Kenntnis gebracht werden. Nach erfolgter Kenntnisnahme seitens des Kooperationsgremiums BLSG MUSS die vergebene Sub-OID in die Liste der vergebenen OIDs [OID-T2] aufgenommen und veröffentlicht werden.

Soweit dieses Dokument keine weiteren Kategorien in einem Teilbaum definiert, erfolgt die Verwaltung des Teilbaums unter der vergebenen OID durch den Inhaber der OID bzw. der Organisation der entsprechenden Vertretung (z.B. Gemeindebund, Notariatskammer, etc.) selbstständig – ohne notwendige Mitwirkung der Verwaltungsinstanz des gv-at-OID-Teilbaums. Bei übergreifender Bedeutung kann die Koordination der zur Verwaltung des gv-at-OID-Teilbaums beauftragten Arbeitsgruppe in Anspruch genommen werden.

Soweit die OIDs durch die mit der Verwaltung des gv-at-OID-Teilbaums beauftragte Arbeitsgruppe koordiniert werden, wählt diese die OID-Nummer, wobei Vorschläge übernommen werden, sofern diese zu keinem Konflikt führen. Zu den OID-Nummern wird jeweils eine Textbezeichnung festgelegt.

Einmal zugewiesen wird ein OID nicht zurückgenommen (ein Widerrufsverfahren ist technisch nicht möglich) und bleibt ein gültiger Bezeichner für die betroffene Kategorie. Es KANN lediglich in der taxativen Auflistung vergebener OIDs [OID-T2] vermerkt werden, dass ein OID obsolet – also nicht länger im Gebrauch – ist bzw. sein sollte.

Die Nummern und Bezeichnungen für Knoten MÜSSEN im Rahmen des Dokumentes [OID-T2] auf der Webseite der mit der Verwaltung des gv-at-OID-Teilbaums beauftragten Arbeitsgruppe veröffentlicht werden. Soweit Sub-OIDs und Sub-OID-Teilbäume im Sinne der Delegation von anderen Organisationen verwaltet werden, MÜSSEN die Sub-OIDs an die Arbeitsgruppe zur Veröffentlichung mitgeteilt werden.

---

[2] Bund, Länder, Städte und Gemeinden

5.1 Wurzel Object Identifier

Der Wurzel-OID für die österreichische Verwaltung ist **1.2.40.0.10**:

```
OID 1            International Standards Organisation (ISO)
OID 1.2          ISO Member Body
OID 1.2.40       Austria (ÖNorm-Institut)
OID 1.2.40.0.10  Österreichische Verwaltung
```

In ASN.1 Syntax [ASN1]:

```
ASN.1:
gv-at OBJECT IDENTIFIER ::= { iso (1) member-body (2)
                              austria (40) (0) (10) }
```

5.2 Vergabe von OIDs (Kontakt)

Als Kontakt für die Vergabe von Object Identifiern dient primär folgende E-Mailadresse bzw. die folgende Postanschrift des Bundeskanzleramt:

E-Mailadresse: numbering@bka.gv.at

Postanschrift: OID Vergabe
Bundeskanzleramt
Abteilung I/11
Ballhausplatz 2
A-1014 Wien

5.3 Grundstruktur des OID-Baums

Um eine Strukturierung der in der öffentlichen Verwaltung benützten OIDs vorzunehmen, wird der OID-Baum der öffentlichen Verwaltung die in Abbildung 1 dargestellte Grundstruktur unterlegt.

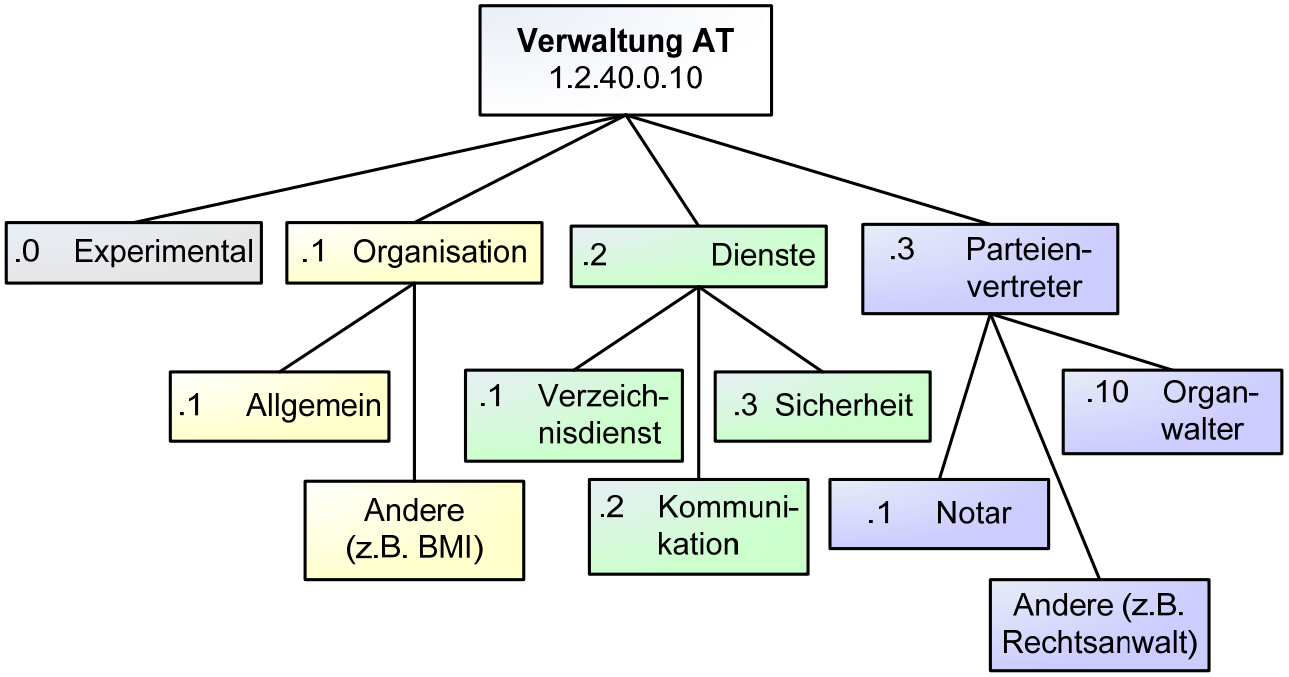

Abbildung 1: Grundstruktur des OID Baums der Verwaltung

Die Grundstruktur auf oberster Ebene wird nachfolgend definiert. Die taxative und detaillierte Definition einzelner OIDs erfolgt im taxativen zweiten Teil dieses Dokuments [OID-T2].

5.3.1 Teilbaum “Experimental” (1.2.40.0.10.0)

Die Experimental-OID und alle darunter liegenden OIDs sind für temporäre, experimentelle Verwendung reserviert. Applikationsentwickler DÜRFEN für Testumgebungen diese OIDs frei einsetzen – diese OIDs MÜSSEN NICHT bei der mit der Verwaltung des gv-at-OID-Teilbaums beauftragten Arbeitsgruppe registriert werden. Die gewählten OIDs haben nur im Kontext der Applikation eine Bedeutung, nicht jedoch außerhalb. Sie DÜRFEN NICHT in Produktionsumgebungen eingesetzt werden, sondern nur in Test- und Pilotumgebungen.

5.3.2 Teilbaum “Organisation” (1.2.40.0.10.1)

In diesem Teilbaum befinden sich OIDs, die sich auf Organisationen bzw. Organisatorisches beziehen. Neben einem „Allgemein“ - Teilbaum können Verwaltungsorganisationen eigene Teilbäume für ihre internen Anwendungen anfordern. Diese OIDs werden in diesem Teilbaum angesiedelt. Die Verwaltung der Teilbäume obliegt der Organisation, die diese OID angefordert hat.

5.3.3 Teilbaum „Dienste“ (1.2.40.0.10.2)

Die Dienste-OID enthält eine Aufgliederung nach Funktionen, in der die OID eingesetzt werden soll. Als nächste Knotenpunkte sind derzeit definiert eine OID für Verzeichnisdienste, Kommunikationsdienste, etc.

5.3.4 Teilbaum „Parteienvertreter“ (1.2.40.0.10.3)

Die Parteienvertreter-OID erfasst die berufsmäßigen Parteienvertretungen und enthält eine

Aufgliederung nach den Berufsgruppen. Als nächste Knotenpunkte sind derzeit OIDs definiert für Notare, Rechtsanwälte, Ziviltechniker und Organwalter.

6 Eintragung der OID durch Zertifizierungsdienste

6.1 Vergabeprozeß

Zertifizierungsdiensteanbieter (ZDA) MÜSSEN vor der Eintragung eines OID in ein Zertifikat eines Antragstellers (Antragsteller bzgl. Ausstellung des Zertifikates) beim jeweiligen Bestandsgeber die explizite Zustimmung dazu einholen. Der jeweilige zuständige Bestandsgeber ist der taxativen OID Definition in [OID-T2] zu entnehmen.

Gemäß den Pflichten und Aufgaben des Bestandsgebers MUSS der Bestandsgeber über die Vergabe der OID entscheiden, das heißt ob der gegenständliche Antragsteller berechtigt ist das angeforderte OID zu führen. Sollte der Bestandsgeber zur Entscheidungsfindung weitere Informationen vom Antragsteller benötigen, so ist der Bestandsgeber angehalten, diese über den Zertifizierungsdiensteanbieter oder direkt vom Antragssteller einzufordern. Im Zweifelsfall MUSS die Eintragung der OID verweigert werden.

Die Zustimmung zur Eintragung MUSS gegenüber dem Zertifizierungsdiensteanbieter nachvollziehbar erfolgen.

Im Zweifel über Zuständigkeiten, das heißt bei Unklarheit bzgl. des zuständigen Bestandsgebers, KANN der ihm hierarchisch übergeordnete Bestandsgeber kontaktiert werden. In letzter Instanz ist zur Klärung der Zuständigkeiten die in Abschnitt 5.2 festgelegte Stelle zu kontaktieren. In einem solchen Eskalationsszenario MUSS ein übergeordneter Bestandsgeber alle notwendigen und zumutbaren Schritte unternehmen, um den zuständigen Bestandsgeber zu ermitteln und zu kontaktieren. Ein übergeordneter Bestandsgeber DARF jedoch NICHT anstelle des zuständigen Bestandsgeber eine Entscheidung über die Vergabe des OID treffen. Im Zweifelsfall ist keine Aussage möglich und das OID DARF NICHT vergeben werden.

6.2 Anforderungen an den Zertifizierungsdienst

Die Vergabe von OID im Rahmen von Zertifikaten erfordert grundsätzlich keine besondere Eigenschaft seitens der Zertifizierungsdienste. Vielmehr KANN jedoch das Anwendungsfeld der einzelnen OID gewisse Zertifikatsqualitäten bedingen. Daher MÜSSEN im Rahmen der taxativen OID Festlegung [OID-T2] zu jedem OID die damit einher gehenden Zertifikatsqualitäten festgelegt sein. Die jeweilige (Mindest-)Qualität MUSS vom betreffenden Zertifizierungsdienst angeboten werden können.

Bei der Festlegung von Zertifikatsqualitäten MÜSSEN die Qualitäten laut Signaturgesetz beachtet werden, wo anwendbar und sinnvoll. Die letzte Entscheidungsgewalt KANN jedoch auch dem jeweiligen Bestandsgeber zugesprochen werden. Der Bestandsgeber KANN sich daher sowohl explizit für bestimmte Zertifikatseigenschaften aussprechen als auch die Letztentscheidung bezüglich eines Zertifizierungsdienstes für sich beanspruchen (zum Beispiel anhand der konkreten Zertifikats-Policies eines ZDAs).

Referenzen

ASN1

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

GVAT

FA Netzwerke: Naming Policy “gv.at”, Richtlinien zur Domänenverwaltung in den obersten Bundesbehörden, Version 3.1, 1998-07-24

OID-T2

AG Bürgerkarte: Object Identifier der öffentlichen Verwaltung (Teil 2 – Taxative Definition). OID-T2-1.0.0, Version 1.0.0 vom XX.XX.XXXX.

EGovG

Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (EGovG), BGBl. I Nr. 10/2004, idgF nach E-GovG-Novelle 2007.

WA-OID

Artikel zu Object-Identifier aus de.wikipedia.org. Abgerufen aus dem WWW am 8.9.2008 unter http://de.wikipedia.org/wiki/Object_Identifier .