DuD
Datenschutz und Datensicherheit

Directory

Volker Hammer

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

Als *Directory* oder Verzeichnisdienst werden besonders strukturierte Datenbanken bezeichnet. Die Bezeichnung *Directory* wurde in den 80er Jahren durch die Standardisierungsarbeiten für große, verteilte elektronische Verzeichnisse für die Telekommunikation geprägt.[1] Lokale Directories finden heute häufig z. B. auch im Rahmen von Single-Sign-On Verfahren oder für die Administration ganzer IT-Infrastrukturen Anwendung.

In Directories werden Informationen zu Objekten abgelegt. Objekte sind z. B. ein Teilnehmer, eine Zertifizierungsinstanz oder eine Organisationseinheit. Oft werden im Verzeichnis die organisatorischen Strukturen einer Hierarchie abgebildet.

Jedes Objekt, zu dem Informationen gespeichert werden, erhält im Verzeichnis einen sogenannten Distinguished Name (DN). Der DN ist der eindeutige Schlüssel im Directory. Jeder Name kennzeichnet einen sogenannten *Entry* (siehe unten), in dem die Informationen zum Objekt abgelegt werden. Der Distinguished Name ergibt sich dann aus der Folge der relativen Namen (der sogenannten Relative Distinguished Names) vom Teilnehmer-Knoten bis zur Wurzel, z. B. „cn=Peter Müller, l=Berlin, ou=BMI, o=Bund, c=DE" (vgl. Abb. 3). Das „unterste" Attribut, das den Namen des Entries von den anderen Entries auf der gleichen Ebene unterscheidet, wird auch als *namensgebendes Attribut* bezeichnet. Dieses Attribut bildet den relativen Namen (Relative Distinguished Name) dieser Ebene. In Abbildung 3 wäre dies für den Teilnehmer-Entry das Attribut *cn*.

Die Entries der sich ergebenden Struktur bilden einen Baum, den sogenannten *Directory Information Tree* oder *DIT*. Um den Namen, der die Platzierung eines Entries im DIT bestimmt, von anderen Namen unterscheiden zu können, wird er im weiteren als *DIT-DN* (Directory Information Tree Distinguished Name) bezeichnet.

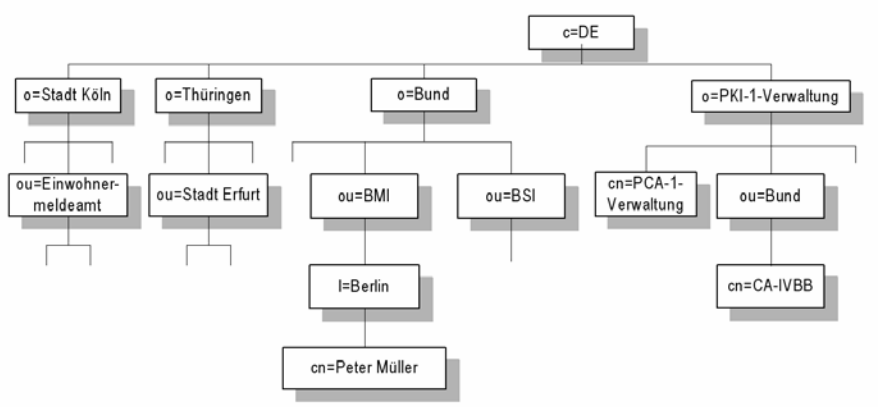

Abb. 3: Beispiel für einen Directory Information Tree. Ein Teilnehmer-Entry und eine CA sind als Beispiele aufgeführt.

Jeder Entry enthält Daten zum entsprechenden Objekt. Die Speicherplätze für die einzelnen Daten im Entry werden als *Attribute* bezeichnet. Der Entry umfasst quasi als „Container" mehrere unterschiedliche Attribute. In den Attributen werden dann die einzelnen Werte abgelegt, die dem Objekt zugeordnet sind, beispielsweise die E-Mail-Adresse, der Nachname oder das Zertifikat eines Teilnehmers (vgl. Abb. 2).

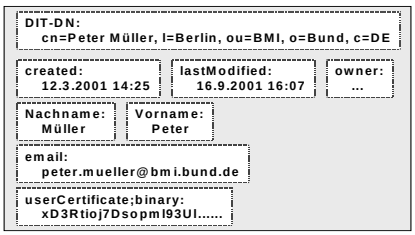

Abb. 4: Ein Teilnehmer-Entry als Container für unterschiedliche Attribute. Die eindeutige „Adresse" ist der DIT-DN

Um den Aufbau eines Directories und seinen Inhalt im Betrieb automatisch kontrollieren zu können, wird nicht nur die zulässige Namensstruktur (DIT) sondern auch der zulässige Inhalt der Entries im *Directory-Schema* konfiguriert. Wie die Werte in Attributen abzulegen sind und welche Semantik sie haben, wird über sogenannte *Attribut-Typen* festgelegt. Mehrere Attribut-Typen können zu einer *Objektklasse* gruppiert werden. Der Aufbau jedes Entries wird dann durch eine oder mehrere solcher Objektklassen definiert. Im Directory-Schema wird schließlich auch festgelegt, auf welcher Ebene des DIT welche Typen von Entries zulässig sind.

Im Kontext von Public Key Infrastrukturen ist der Distinguished Name in Zertifikaten zu unterscheiden von dem Distinguished Name des Entries im Directory, in dem das Zertifikat bereitgestellt wird. Auch die Namen in Zertifikaten werden als Distinguished Names bezeichnet und müssen eindeutig gewählt werden. In der Praxis können sie mit denen im Directory übereinstimmen, müssen dies aber nicht unbedingt.

[1] Siehe insbesondere International Telecommunication Union – Telecommunication Sector: ITU-T Recommendation X.500 ff – Information Technology - Open Systems Interconnection – The Directory. Einfachere Techniken werden in LDAP-Directories realisiert, siehe RFC 2251: Lightweight Directory Access Protocol (v3), IETF, December 1997.