Das Verzeichnisdienstkonzept für die PKI-1-Verwaltung

Volker Hammer (Secorvo, hammer.@secorvo.de),[1]
Dörte Neundorf (Secorvo, neundorf.@secorvo.de),[1]
Albrecht Rosenhauer (BMI, albrecht.rosenhauer@kbst.bund.de),[2]
Andreas Schmidt (BSI, andreas.schmidt@bsi.bund.de)[3]

[1] Secorvo Security Consulting GmbH, Albert Nestler-Str. 9, D-76131 Karlsruhe
[2] Bundesministerium des Innern, Alt-Moabit 101 D, D-10559 Berlin
[3] Bundesamt für Sicherheit in der Informationstechnik,
Godesberger Allee 185-189, D-53175 Bonn

Zusammenfassung: Public Key Infrastrukturen (PKI) erschließen ihren Nutzen für die Anwender erst dann in vollem Umfang, wenn abgegrenzte PKI-Realisierungen (*Domänen*), z. B. in Unternehmen, zu einer Domänen-übergreifenden Infrastruktur zusammengefügt werden. Dazu ist die Bereitstellung von Zertifikaten und Sperrlisten über die Grenzen der einzelnen PKI-Domänen hinaus erforderlich. Die Veröffentlichung dieser Informationen über ein gemeinsames Directory stößt jedoch auf vielfältige technische, rechtliche und organisatorische Probleme und muss Sicherheitsanforderungen genügen. Der Beitrag beschreibt übertragbare Konzepte, auf deren Basis ein Verzeichnisdienst für die PKI für die Einrichtungen der öffentliche Verwaltung (*PKI-1-Verwaltung*) aufgebaut wird. Dadurch wird der letzte Baustein dieser Infrastruktur realisiert.

1. Einführung

Public Key Infrastrukturen (PKI) entstehen in der Regel zunächst innerhalb von abgegrenzten Domänen, z. B. in einem Unternehmen oder für die Verwaltung eines Bundeslandes. Um den vollen Nutzen zu erschließen, müssen diese PKIs aber verknüpft werden. Dazu sind zwei Aufgaben zu lösen: die Einrichtung einer gemeinsame Wurzel-CA oder die gegenseitige Anerkennung der öffentlichen Schlüssel der Wurzel-Zertifizierungsinstanzen (siehe z. B. [HaPe 01]) und der Austausch von Zertifikaten und Sperrlisten. Der Beitrag zeigt die praktischen Probleme für den Austausch und die Veröffentlichung von Zertifikaten und Sperrlisten auf und beschreibt Konzepte für den Lösungsweg, der für die PKI-1-Verwaltung gewählt wurde. Die Konzepte sind weitgehend verallgemeiner- und übertragbar. Die zu Grunde liegenden Fragestellungen und Ansätze können daher auch als Checkliste bzw. Anregungen für andere übergreifende Verzeichnisdienste genutzt werden.

1.1 Vorgeschichte

Im Februar 2001 wurde beim Bundesamt für Sicherheit in der Informationstechnik (BSI) die Wurzel-Zertifizierungsinstanz der PKI-1-Verwaltung [PKI-1-V] in Betrieb genommen. Diese Wurzel-Zertifizierungsinstanz wird im weiteren kurz als PCA bezeichnet. Sie zertifiziert nachgeordnete Certification Authorities (CA) für abgegrenzte Zuständigkeitsbereiche, die im weiteren als Domänen bezeichnet werden. Beispiele für Domänen sind der Bundestag, einzelne Bundesländer, Behörden oder Kommunen. Mit Hilfe der PKI-1-Verwaltung können die Einrichtungen der öffentlichen Verwaltung untereinander und mit Bürgern und Unternehmen gesichert kommunizieren, z. B. durch verschlüsselte oder signierte E-Mails oder mittels SSL-Verbindungen. Als "Business Cases" für diese PKI werden alle Anwendungszwecke gesehen, die durch Grundschutz ausreichend abgesichert werden können. Dazu gehören neben E-Mail- und Datei-Sicherung z. B. die Authentisierung für e-Government-Anwendungen oder der Aufbau von VPNs. Schlüssel und Zertifikate der PKI-1-Verwaltung werden den Mitarbeitern der Verwaltung künftig auch über den digitalen Dienstausweis bereitgestellt. Aus der Sicht des Signaturbündnisses können die CAs der PKI-1-Verwaltung Zertifikate für „allgemeine PKI-Anwendungen" bereitstellen [SigBü]. Gegenwärtig sind 11 Domänen der PKI-1-Verwaltung beigetreten [PKI-1V]. Weitere Domänen mit einem Potential von jeweils über 100.000 Zertifikaten haben Verhandlungen über den Beitritt aufgenommen.

Allerdings wurde mit dem Aufsetzen der PCA noch kein Konzept für einen übergreifenden Verzeichnisdienst festgelegt. In der Infrastruktur stehen daher die Zertifikate und Sperrlisten nachgeordneter CAs und die Teilnehmer-Zertifikate einer Domäne nicht ohne weiteres zum Abruf durch Nutzer anderer Domänen bereit. Der Austausch dieser Informationen kann deshalb großen Aufwand verursachen. Zwar haben die einzelnen Zertifizierungsinstanzen lokale Verzeichnisdienste, die Zertifikate und Sperrlisten bereitstellen, diese sind aber von den individuellen Strategien der CAs geprägt und nur teilweise öffentlich zugreifbar. Sie bieten auch keine einheitliche Struktur, so dass ein Austausch zwischen ihnen nicht ohne weiteres möglich ist und Aufwand für eine spezifische Konfiguration der PKI-Clients anfallen kann.

Diese Ausgangssituation ist typisch für Insel-PKIs und erhöht den Aufwand für die Teilnehmer so, dass erhebliche Akzeptanzprobleme zu erwarten sind. Letztlich kann sogar der Zweck der PKI in Frage gestellt werden. Für die PKI-1-Verwaltung wird deshalb ein übergreifender Verzeichnisdienst realisiert. Übergreifend meint, dass in diesem Verzeichnisdienst die Zertifikate und Sperrlisten verschiedener Domänen abrufbar sind. Gewinner dieses Dienstes sind jeweils alle Nutzer der PKI, die außerhalb der jeweiligen Domäne angesiedelt sind. Je größer die Nutzerzahlen der PKI werden, desto größer wird auch die Bedeutung der Verzeichnisdienste. Aber auch: je leichter Zertifikate und Sperrlisten über ein Verzeichnis abzurufen sind, desto eher wächst die Zahl der aktiven Teilnehmer der PKI. Übergreifende Verzeichnisdienste tragen deshalb wesentlich dazu bei, das „Henne-Ei-Problem" von PKIs zu lösen.

1.2 Anforderungen übergreifende Verzeichnisdienste

Die Einrichtung eines übergreifenden Verzeichnisdienstes stößt in aller Regel auf vielfältige, typische Probleme. Lokale Verzeichnisdienste haben *unterschiedliche Einsatzzwecke*. Sie dienen etwa der Berechtigungsverwaltung und Administration einer ganzen technischen Infrastruktur, dem Informationsaustausch zwischen Bundesbehörden (IVBB-Directory) oder als reines PKI-Directory. Die Auswahl von Directory-Produkten, der unterschiedliche Aufbau der Directories und der Datenstrukturen ist wesentlich von solchen Zwecken und Entscheidungen innerhalb der Organisationen und von der Organisation des Betriebs des jeweiligen Verzeichnisdienstes bestimmt. Die Vorgaben der PKI haben dagegen oft nur geringen Einfluss. Eine Harmonisierung ist nicht zu erwarten. Ein übergreifender Verzeichnisdienst muss deshalb in der Lage sein, Datenquellen in einer großen Variantenbreiten zu berücksichtigen. Außerdem ergaben sich aus der Vielfalt der lokalen Verzeichnisdienste *technische Probleme*, weil nicht ohne weiteres interoperable Mechanismen für den Datenaustausch zur Verfügung stehen. In den Domänen sind außerdem unterschiedliche Technik- und Organisationsentwicklungen zu erwarten. Diese dürfen aber das übergreifende Verzeichnis nicht beeinflussen, weil der praktische Betrieb sonst kontinuierlich die lokalen Änderungen nachvollziehen müsste. Diese Hürden müssen durch geeignete Austauschprozesse überwunden werden.

Der übergreifende Verzeichnisdienst soll ein dem IT-Grundschutz vergleichbares *Sicherheitsniveau* erreichen. Außerdem kann erwartet werden, dass künftig viele Anwender auf die Infrastrukturkomponente zurückgreifen. Störungen können deshalb ein hohes Schadenspotential aufweisen. Deshalb sind eine Reihe von Sicherheitsmaßnahmen notwendig. Daneben werden die Daten aus eigenständigen Domänen über Aktualisierungsprozesse bereitgestellt. Deshalb müssen auch die Sicherheitsbedürfnisse der Domänen berücksichtigt werden.

Schließlich müssen *rechtliche Vereinbarungen* und *organisatorische Regelungen* die Pflichten zwischen den verschiedenen beteiligten Organisationen verteilen, damit ein reibungsloser Betrieb mit einer Mindest-Service-Qualität erreicht wird.

Technische Konzepte für den übergreifenden Verzeichnisdienst der PKI-1-Verwaltung werden im weiteren vorgestellt. Ausgewählte Sicherheitsmaßnahmen werden unter 2.5 kurz skizziert, für rechtliche und organisatorische Regelungen muss auf [VDK] verwiesen werden.

1.3 Aufbau von Directories

Directories sind als hierarchische Datenbank organisiert. Jedes Objekt, zu dem Informationen in einem Directory gespeichert werden, erhält im Verzeichnisdienst als eindeutigen Schlüssel einen "Directory Namen", den sogenannten *Distinguished Name* (DN). Objekte sind z. B. ein Teilnehmer, eine Zertifizierungsinstanz oder eine Organisationseinheit. 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. 2). Das "unterste" Attribut, das den Namen des Entries von den anderen Entries auf der gleichen Ebene unterscheidet, wird auch als namensgebendes Attribut bezeichnet. In Abbildung 2 wäre dies für den Teilnehmer-Entry das Attribut cn.

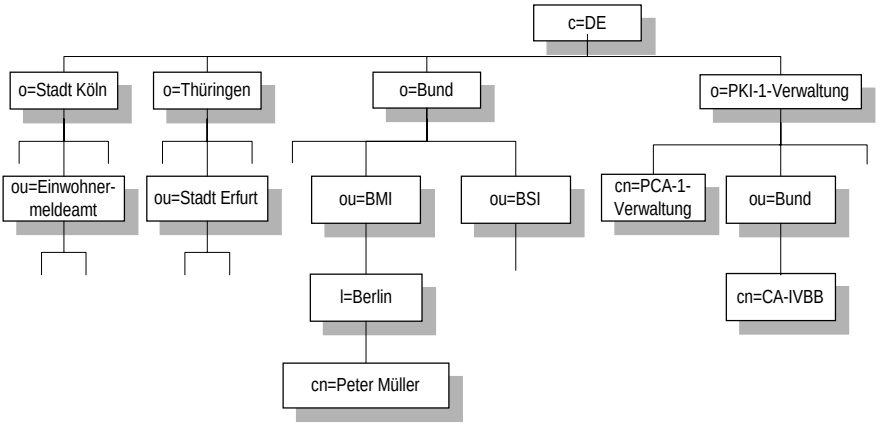

Abbildung 1: Beispiel für einen Directory Information Tree.
Ein Teilnehmer-Entry und eine CA sind als Beispiele aufgeführt. .

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.

In diesem Dokument ist der DIT-DN zu unterscheiden von den Namen im Zertifikat. Diese werden ebenfalls als Distinguished Names bezeichnet und müssen auch eindeutig gewählt werden. Die Namen im Zertifikat werden in diesem Dokument als *Subject-DN* (Name des Zertifikat-Inhabers) und *Issuer-DN* (Name des Zertifikat-Ausstellers) bezeichnet. DIT-DN und Subject-DN können übereinstimmen, müssen dies für Teilnehmer aber nicht unbedingt.

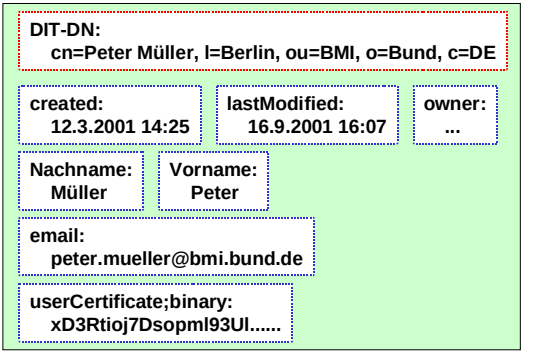

Abbildung 2: Ein Teilnehmer-Entry als Container für unterschiedliche Attribute.
Die eindeutige "Adresse" ist der DIT-DN

Ein Entry enthält verschiedene Daten zum Objekt. Die Speicherplätze für die einzelnen Daten im Entry werden als *Attribute* bezeichnet. Der Entry umfasst quasi als "Container" mehrere unterschiedliche Attribute (vgl. Abb. 2). 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* festgelegt.

2. Zentrale Elemente eines übergreifenden Verzeichnisdienstes

Zweck eines übergreifenden Verzeichnisdienstes für eine Public Key Infrastruktur ist die Bereitstellung von CA-Zertifikaten, Sperrlisten und Teilnehmer-Zertifikaten (kurz *PKI-Informationen*).

Im Falle der PKI-1-Verwaltung sind zwei Zielgruppen für die PKI-Informationen zu unterscheiden:

- Zum einen sollen PKI-Informationen organisationsübergreifend allen Teilnehmern innerhalb der öffentlichen Verwaltung zur Verfügung stehen. Dazu zählen die Mitarbeiter aus den Einrichtungen des Bundes, der Länder und der Kommunen.
- Außerdem sollen auch Externe die Zertifikate von Verwaltungsmitarbeitern abrufen und prüfen können. Der Umfang der sichtbaren Informationen für diese Zielgruppe soll jedoch gegenüber der internen Sicht für Verwaltungsmitarbeiter reduziert werden können.

Eine solche Zweiteilung der Zielgruppe kann sich auch in anderen Bereichen wiederfinden, beispielsweise, wenn eine Gruppe von Unternehmen ein übergreifendes internes und ein eingeschränktes externes PKI-Verzeichnis betreiben will. Im Falle des Verzeichnisdienstkonzepts wird die Zugangsbegrenzung zu den unterschiedlichen Datenbeständen mit Hilfe der Systemarchitektur erreicht werden.

2.1 Architektur

Aus den genannten Zielgruppen und den bestehenden Netzwerk-Strukturen im Bereich der öffentlichen Verwaltung wurde die in Abbildung 3 dargestellte zweistufige Architektur der übergreifenden Verzeichnisdienste abgeleitet. Neben den lokalen Verzeichnisdiensten der Domänen werden zwei zusätzliche Verzeichnisdienste betrieben. Ein sogenannter "Verzeichnisdienst der Verwaltung" (VDV) ist im gemeinsamen Intranet der Verwaltungen, dem TESTA D Netz, angesiedelt. Auf den VDV haben alle Mitarbeiter der öffentlichen Verwaltung Zugriff, denen der Zugang zum gemeinsamen Intranet erlaubt ist. Externe Teilnehmer erreichen dagegen nur den im öffentlichen Internet eingerichteten "Veröffentlichungsdienst" (VöD). Die beiden Dienste werden im weiteren zusammenfassend auch als *Dienste des Verzeichnisdienstkonzepts* bezeichnet.

Zugeliefert werden die PKI-Informationen von der PCA sowie den direkt nachgeordneten CAs. Jede dieser der PCA direkt nachgeordneten CAs bildet im Verständnis des Verzeichnisdienstkonzepts eine PKI-Domäne. Den nachgeordneten CAs steht es frei, weitere CAs innerhalb ihrer Domäne einzurichten. Es wird angenommen, dass die CAs einer Domäne ihre Daten zunächst an einen lokalen Verzeichnisdienst übermitteln.

Die Übertragung von den Domänen zu den Diensten des Verzeichnisdienstkonzepts muss in speziellen Prozessen erfolgen und wird unten dargestellt.. Der Client-Zugriff aller internen und externen Teilnehmer erfolgt prinzipiell über LDAP (Lightweight Directory Access Protocol). Zusätzlich kann ein Datei-Download per HTTP für CA-Zertifikate und Sperrlisten unterstützt werden.

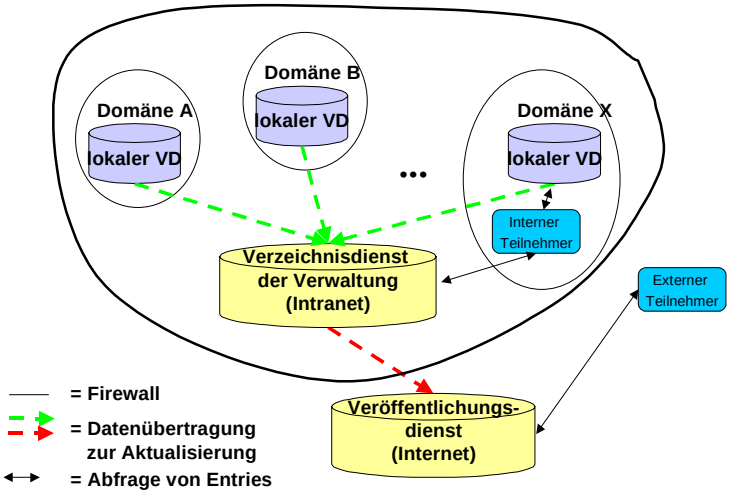

Abb. 3: Logische Architektur der Verzeichnisdienste im Verzeichnisdienstkonzept

2.2 Inhalte der Verzeichnisdienste im Verzeichnisdienstkonzept

Welche Daten sollen in einem übergreifenden Verzeichnisdienst einer PKI bereitgestellt werden? Zunächst sind die Entries relevant, die PKI-Informationen enthalten: CA-, CRL Distribution Point- und Teilnehmer-Entries. Für die Auswahl von einzelner Entries dieser drei Typen sind mehrere Kriterien zu berücksichtigen. Für die gewählten Entries werden dann die Daten bestimmt, die in den Verzeichnisdiensten veröffentlicht werden. Für beide Aspekte sind Datenschutz und andere Vertraulichkeitsaspekte wichtig.

Auswahl von Entries zur Replikation

Die Entscheidung über die Sensitivität und Freigabe von Entries zur Veröffentlichung kann nur innerhalb der jeweiligen Domäne geregelt und getroffen werden. Dabei können beispielsweise Betriebsvereinbarungen, individuelle Einwilligungen oder Policies der Organisation eine Rolle spielen. So könnten Funktionszertifikate generell veröffentlich werden, Mitarbeiter-Zertifikate aber nur bei bestimmten Aufgaben und bei Zustimmung des Mitarbeiters. In einem zweistufigen übergreifenden Verzeichnisdienst wird es dabei regelmäßig vorkommen, dass die Bereitstellung von Teilnehmer-Entries für den inneren Kreis zulässig ist, nicht aber die externe Veröffentlichung. Daraus ergaben sich zwei Konsequenzen:

- Zum einen müssen die Domänen die Bereitstellung der Entries vollständig steuern können, da nur sie über die entsprechenden Freigabe-Informationen verfügen und die zugehörigen Prozesse lokal definieren.
- Zum anderen wurden im Verzeichnisdienstkonzept Steuerungsmöglichkeiten realisiert, durch die wiederum die Entries ausgewählt werden, die in den Veröffentlichungsdienst repliziert werden. Die jeweilige Domäne muss diese Steuerinformation liefern.

Die Veröffentlichung von Entries für CAs und CRL Distribution Points (CDP) sollte in der Regel keine Probleme aufwerfen, sondern vielmehr erwünscht sein. Entscheidungen über Veröffentlichungen sind primär für die Entries von Teilnehmern zu treffen.

Datenumfang von Entries

Es muss entschieden werden, welche Informationen in den Entries enthalten sein müssen und welche optional enthalten sein können. Auch dafür müssen mehrere Aspekte berücksichtigt werden. Damit die Dienste des Verzeichnisdienstkonzepts ihren Zweck erfüllen können, müssen die PKI-Informationen bereitgestellt werden. In den Teilnehmer-Entries sind dies die Teilnehmer-Zertifikate, für Zertifizierungsinstanzen die CA-Zertifikate und die Sperrlisten. In Entries vom Typ CDP werden ebenfalls Sperrlisten eingetragen. Zu beachten ist, dass mit den Zertifikaten implizit auch die in ihnen enthaltenen Informationen veröffentlicht werden.

Die Informationen müssen so bereitgestellt werden, dass die existierenden Clients sie verarbeiten können. Viele gängige Clients haben zur Zeit noch Probleme, wenn in einem Teilnehmer-Entry mehrere Zertifikate enthalten sind. Sie wählen dann aus den abgerufenen Zertifikaten unter Umständen eines mit falschem keyUsage oder ausgelaufenem Gültigkeitszeitraum aus. Im Verzeichnisdienstkonzept wurde deshalb bis auf Weiteres festgelegt, dass nur ein Zertifikat im Teilnehmer-Entry repliziert wird. Dieses muss zur Verschlüsselung zugelassen sein. Auf Teilnehmer-Zertifikate zur Prüfung eines Signaturschlüssels kann im Verzeichnis verzichtet werden, weil sie in allen gängigen E-Mail-Sicherheitsprodukten mit der signierten Nachricht mitgeschickt werden.

Außerdem müssen Informationen vorhanden sein, anhand derer Zertifikate und Sperrlisten gesucht und ausgewählt werden können. Für CA-Entries wurde dazu im Verzeichnisdienstkonzept gemäß [X.509 2001] festgelegt, dass der Subject DN mit dem DIT-DN übereinstimmen muss und damit implizit auch als suchbares Attribut zur Verfügung steht (siehe auch unten DIT). Für Teilnehmer-Entries wird im Kontext von E-Mail-Verschlüsselung die E-Mail-Adresse das häufigste Suchkriterium sein. Daneben sind aber auch der Vor- und Nachname und die Organisationsbezeichnung Suchkriterien, die von Teilnehmern verwendet werden. Diese Attribute werden in den Entries der Teilnehmer vorgehalten.

Schließlich soll das Schema der Verzeichnisdienste möglichst stabil sein, um den Aufwand für die Administration niedrig zu halten. Für eine effiziente Realisierung einer ersten Ausbaustufe ist es deshalb sinnvoll, je Entry-Typ nur eine sehr begrenzte Auswahl von Attributen vorzusehen. Diese Strategie vermindert außerdem das Risiko, dass verse-

hentlich sensitive Informationen aus dem lokalen Verzeichnisdienst außerhalb sichtbar werden, beispielsweise Zugriffsrechte oder Passworte.

2.3 DIT und Schema

Stabile Aktualisierungsprozesse und der effiziente Betrieb eines übergreifenden Verzeichnisdienstes können nur erreicht werden, wenn sich die unterschiedlichen Ausgangsdaten der Domänen auf stabile Namensregeln und ein einheitliches Directory-Schema abbilden lassen. Für CA- und CDP-Entries einerseits und für Teilnehmer-Entries andererseits sind unterschiedliche Strategien geeignet, um dieses Ziel zu erreichen.

CA- und CDP-Entries

Für CA- und CDP-Entries gelten besondere Anforderungen. Sie müssen im DIT an den Stellen platziert werden, auf die bestimmte Angaben in Zertifikaten verweisen. Um dieser Anforderung bei stabilem DIT Rechnung zu tragen, wurden im Rahmen des Projekts für CA-Entries die Namensregeln für Subject DNs und für CDPs die DIT-DNs verbindlich festgelegt. Beide Attribute definieren den Platz der jeweiligen Entries im DIT der übergreifenden Verzeichnisdienste. Soweit CAs in der PKI-1-Verwaltung mit abweichenden Subject DNs eingerichtet waren, mussten sie auf konsistente Namen migrieren.

In bestimmten Fällen können in den lokalen Verzeichnisse der Domänen andere abweichende DIT-DNs gewählt werden, beispielsweise in Windows 2000 PKIs. Die DIT-Namen dieser Entries werden in den Aktualisierungsprozessen, ähnlich wie die Entries für Teilnehmer (siehe unten), für die übergreifenden Verzeichnisdienste auf die vorgegebenen Namen umgesetzt.

Teilnehmer-Entries

Für die Behandlung von Teilnehmer-Entries bestehen größere Spielräume. Für sie gibt es keine Vorgaben für die Ablage im DIT. Zur Suche werden automatische oder manuelle Prozesse verwendet, die sich auf die E-Mail-Adresse oder Kenntnisse über Namen und Organisation des Teilnehmers stützen.

Für Teilnehmer-Entries wurde entschieden, dass ihre DIT-Namen im Aktualisierungsprozess auf ein einheitliches Format abgebildet werden. Die Namensgebung im Zertifikat (Subject DN) ist davon nicht betroffen. Abbildung 4 zeigt beispielhaft, wie unterschiedliche Namensformate umgesetzt werden. Als namensgebendes Attribut für Teilnehmer-Entries wird im Verzeichnisdienstkonzept die E-Mail-Adresse verwendet. Sie muss als Attribut in den lokalen Verzeichnissen vorhanden sein, denn es soll ja die Sicherung von E-Mails unterstützt werden. Diese Namensform ist zwar etwas ungewöhnlich, bietet aber für die Aktualisierungsprozesse die notwendige Eindeutigkeit. Die Entscheidung erlaubt eine sehr einfache Realisierung und vermeidet zusätzliche Maßnahmen in den Domänen.

Austausch-DIT und Namensregeln

Die Namensregeln für CAs und für Teilnehmer bilden gemeinsam den sogenannten *Austausch-DIT*, auf dem der Verzeichnisdienst der Verwaltung und der Veröffentlichungsdienst basieren. Die Anforderungen an die Domänen bestehen dabei hauptsächlich im Bereich der CA- und CDP-Namen. Für Teilnehmer-Entries sind die Vorgaben minimal und dürften in der Praxis keine Einschränkungen aufwerfen. Die harmonisierten Namensregeln sind in [NR] festgelegt. Sie sind verbindlich für die PKI-1-Verwaltung.

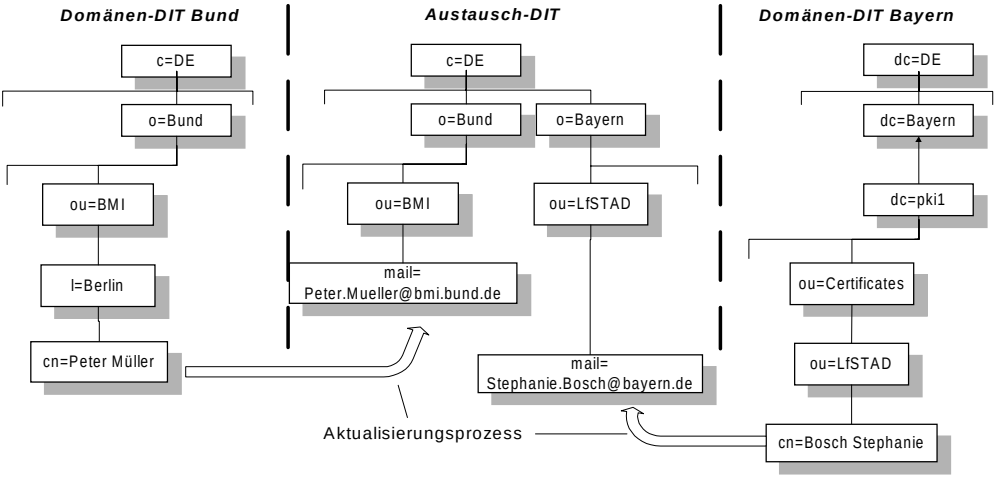

Abbildung 4: Umsetzung von Teilnehmer-Entries aus zwei Domänen (links und rechts) in den Austausch-DIT (Mitte) für Teilnehmer aus dem BMI und aus Bayern

Directory Schema

Das Directory-Schema beschreibt, welche Informationen die Entries der einzelnen Objekttypen enthalten. Im Falle des Austausch-DITs betrifft dies die Definitionen für die Entries von Teilnehmern, CAs und CDPs in den übergreifenden Diensten.

Die lokalen Verzeichnisdienste müssen die Daten bereitstellen, die in den übergreifenden Verzeichnisdiensten benötigt werden. Dazu sind mindestens die folgenden Informationen erforderlich:

- die Attribute, die den DIT Distinguished Name im Austausch-DIT bilden. Dies sind für Teilnehmer-Entries die E-Mail-Adresse, die Bezeichnung der Organisation, die Bezeichnung der Domäne und „c=DE“.
- Attribute, die der Suche des Entries dienen, wie die E-Mail-Adresse, den Namen des Teilnehmers oder eine Organisationseinheit,
- die PKI-Attribute in den Objektklassen nach [X.509 2001] und
- das Steuerungsattribut, das über die Replikation in den VöD entscheidet.

Diese Attribute und einige weitere Steuerinformationen, z. B. das Datum der letzten Aktualisierung eines Entries, müssen lokal vorhanden sein. Das zugehörige lokale Schema kann jedoch sehr flexibel definiert sein. Die lokal vorhandenen Attribute werden

dann im Rahmen des Aktualisierungsprozesses noch innerhalb der Domäne auf die Attribute umgesetzt, die für das Schema des Austausch-DITs festgelegt sind.

2.4 Aktualisierungsverfahren

Wegen der unterschiedlichen Produkte in den Domänen kann kein standardisierter Replikationsmechanismus verwendet werden, wie er z. B. in [X.525] festgelegt ist. Das Verzeichnisdienstkonzept stellt deshalb Skripte zur Verfügungen, die die Replikation durchführen. Für die Implementierung wird auf Standards zurückgegriffen.

Für die Übergabe von Daten an den VDV wird von allen Domänen ein einheitliches Datenformat verwendet. Es basiert auf LDIF-Dateien (LDAP Data Interchange Format, [LDIF]). Alle gängigen Verzeichnisdienst-Produkte unterstützen LDAP-Abfragen, mit denen LDIF-Dateien erzeugt werden können Die LDIF-Dateien können daher einfach erstellt werden. Soweit CA-Produkte direkt LDIF-Dateien erzeugen können, kann sogar auf einen lokalen Verzeichnisdienst verzichtet werden. Jede Datei erhält einen speziellen Datei-Header, in dem Verwaltungsinformationen für die Prozesse des Verzeichnisdienstkonzepts abgelegt werden. Diese Verwaltungsinformationen enthalten z. B. das Kennzeichen der Quell-Domäne und den Typ der Aktualisierung. Sie werden insbesondere auch für Sicherheitsmaßnahmen genutzt.

Die Aktualisierungsdaten werden periodisch von den Domänen an den VDV geliefert. Die Domänen veranlassen die Übertragung der Daten und haben dabei die volle Kontrolle über die Bereitstellung der Aktualisierungsdaten. Sie kontrollieren insbesondere, welche Entries repliziert werden. Für die Auswahl wird auf Steuerinformationen zurückgegriffen, die oft in den Domänen-Verzeichnissen schon vorhanden sind. Welche Bedingungen für die Auswahl auszuwerten sind, kann konfiguriert werden. Das Verzeichnisdienstkonzept greift daher in die Pflegeprozesse für die Steuerinformationen nicht ein. Die Domänen kontrollieren auch den Umsetzungsprozess für die Attribute der Entries auf das Schema des Austausch-DIT. Es werden also nur die Daten an den VDV geliefert, die dort in das Verzeichnis eingestellt werden dürfen.

Für eine gute Skalierbarkeit werden die Entries von CAs und die von Teilnehmern grundsätzlich in getrennten Dateien übertragen. Außerdem kann zwischen Vollabgleichen und Differenzialabgleichen unterschieden werden. In der Regel werden nur die seit der letzten Aktualisierung geänderten Entries übermittelt. Nur in zeitlich größeren Abständen oder für ein Recovery werden alle freigegebenen Entries übertragen.

Die Aktualisierung der Entries im Veröffentlichungsdienst wird über einen bilateralen Prozess direkt aus dem VDV vorgenommen. Welche Entries übertragen werden dürfen, wird anhand einer von den Domänen zugelieferten Steuerinformation entschieden.

Löschen von Entries

Neue Entries oder Änderungen bestehender Entries können in den lokalen Verzeichnisdiensten anhand des letzten Änderungsdatums leicht identifiziert werden. Eine entspre-

chende Information für gelöschte Entries ist aber oft nur mit erheblichem Aufwand verfügbar. Im VDV wird deshalb regelmäßig mit Hilfe eines Vollabgleichs festgestellt, welche Einträge im lokalen Verzeichnisdienst noch vorhanden sind. Alle anderen werden auch im VDV gelöscht.

2.5 Kernaspekte für die Sicherheit

Auf einen Infrastrukturdienst greifen viele Anwender zurück. Es müssen deshalb Maßnahmen ergriffen werden, die die Qualität der Daten sicherstellen und Reaktionen in Notfällen unterstützen. Dazu wurden im Verzeichnisdienstkonzept der PKI-1-Verwaltung unter anderem die beiden folgenden Maßnahmen ergriffen.

Eine zentrale Maßnahme besteht im **Schutz der Entries jeder Domäne.** Andere Domänen oder gar Dritte dürfen sie nicht verändern oder löschen. Dies wird im Verzeichnisdienstkonzept erreicht, in dem sich die Domäne gegenüber dem VDV mit kryptographischen Verfahren authentisiert und die Übertragung der Daten in einer kryptographisch gesicherten Verbindung erfolgt. Vor dem Einstellen von Daten in den VDV wird außerdem geprüft, ob die zugelieferten Entries im Namensraum der Domäne liegen.

Für schwere Störungen wird außerdem ein **Notfall-Konzept** unterstützt, über das die Kerndienste weiter aufrecht erhalten können, gegebenenfalls mit geringerer Service-Qualität. Im Worst-Case könnten die Domänen ihre Daten damit sogar bilateral zwischen den lokalen Verzeichnisdiensten replizieren.

3 Status und Ausblick

Das Verzeichnisdienstkonzept wurde durch ein Editorial Board einstimmig verabschiedet. In diesem Board waren unter anderem die PCA, mehre Domänen, CA-Dienstleister und Betreiber von Verzeichnisdiensten vertreten. Dadurch, durch die geringen Anforderungen an die Domänen und die hohe Flexibilität trifft das Verzeichnisdienstkonzept auf große Akzeptanz.

Die beiden Dienste des Verzeichnisdienstkonzepts sind seit Ende 2002 mit dem definierten Schema im Rahmen des TESTA D Netzes im Wirkbetrieb. Der VDV und der VöD sind unter der Adresse "pki-directory.testa-de.net" zu ereichen, die im Intra- bzw. Internet entsprechend aufgelöst wird. Der VöD stellt die Zertifikate und Sperrlisten von mehreren CAs bereit. Teilnehmer-Zertifikate werden noch nicht eingestellt, weil dazu die Domänen erst die entsprechenden Freigaben einrichten müssen. Für die Implementierung der Replikationsskripte wird derzeit darauf gewartet, dass sich mindestens zwei Domänen mit unterschiedlicher Directory-Technik beteiligen. Die implementierten Replikationsskripte sollen dann in der PKI-1-Verwaltung als „Installations-Paket“ bereitgestellt werden. Dadurch wird auch der technische Aufwand für die Domänen sehr gering gehalten.

Das Verzeichnisdienstkonzept liefert alle Voraussetzungen für die Implementierung übergreifender Verzeichnisdienste in der PKI-1-Verwaltung. Die Konzepte sind in hohem Maße übertragbar. Voraussetzung ist allerdings ein minimaler Satz von Namensregeln.

Literaturverzeichnis

Aktuelle Informationen zum Verzeichnisdienstkonzept sind zu finden unter http://www.bsi.bund.de/aufgaben/projekte/sphinx/verwpki/struktur.htm

[HaPe 01] Hammer, V. / Petersen, H. (2001): Aspekte der Cross-Zertifizierung, in: Horster, P.: Kommunikationssicherheit im Zeichen des Internet, Wiesbaden, 2001, 192 ff.

[PKI-1V] *verschiedene Informationen zur PKI-1-Verwaltung*: auf http://www.bsi.bund.de/aufgaben/projekte/sphinx/verwpki/

[LDAPv3] RFC 2251 - Wahl, M. / Howes, T. / Kille, S.: Lightweight Directory Access Protocol (v3), IETF, December 1997.

[LDIF] The LDAP Data Interchange Format (LDIF) – Technical Specification, RFC 2849, IETF, June 2000.

[NR] BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Zertifizierungsinfrastruktur für die PKI-1-Verwaltung – Namensregeln und -formate, Bonn, 2002; http://www.bsi.bund.de/aufgaben/projekte/sphinx/verwpki/konzept.htm

[SigBu] Signaturbündnis: Vorgaben und Konvergenzziele für das Signaturbündnis, Version 1.2, Stand 19. März 2003, *http://www.iid.de/iukdg/esignatur6.html*

[VDK] BSI (Hrsg.): Zertifizierungsinfrastruktur für die PKI-1-Verwaltung – Verzeichnisdienstkonzept, Bonn, 2002; http://www.bsi.bund.de/aufgaben/projekte/sphinx/verwpki/konzept.htm

[X.509] ITU-T X.509 – International Telecommunication Union - Telecommunication Sector: – Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 2001.

[X.525] ITU-T X.525 - International Telecommunication Union - Telecommunication sector: Information Technology - Open Systems Interconnection - The Directory: Replication, 2001.