DuD
Datenschutz und Datensicherheit

Das Verzeichnisdienstkonzept der PKI-1-Verwaltung

Volker Hammer

Der Nutzen von Public Key Infrastrukturen erschließt sich für die Anwender erst dann in vollem Umfang, wenn abgegrenzte PKI-Domänen, z. B. in einzelnen Unternehmen, zu einer übergreifenden Infrastruktur zusammengefügt werden. Dazu ist u. a. die Bereitstellung von Zertifikaten und Sperrlisten über die Grenzen der einzelnen PKI-Domänen hinaus erforderlich. Der Beitrag beschreibt, mit welchen Konzepten dies im Verzeichnisdienst der PKI-1-Verwaltung des Bundes realisiert wird.[1]

Dr. Volker Hammer

Secorvo Security Consulting GmbH. Arbeitsschwerpunkt: Public Key Infrastrukturen, Anforderungsanalyse, Technikgestaltung, Datenschutz, Information Security Management.
E-Mail: hammer@secorvo.de

Einleitung

Public Key Infrastrukturen (PKI) werden in der Regel zunächst innerhalb von abgegrenzten Bereichen (*Domänen*) aufgebaut, z. B. für ein Unternehmen oder ein Bundesland. Um den vollen Nutzen von Public Key-Verfahren zu erschließen, müssen diese Domänen jedoch verknüpft werden. Für die Verknüpfung sind zwei Aufgaben zu lösen: die gegenseitige Anerkennung der öffentlichen Schlüssel der Wurzel-Zertifizierungsinstanzen [HaPe 01] und der Austausch von Zertifikaten und Sperrlisten.

Im Februar 2001 wurde beim Bundesamt für Sicherheit in der Informationstechnik (BSI) die Wurzel-Zertifizierungsinstanz der PKI-1-Verwaltung (PCA) in Betrieb genommen. 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 sollen die Einrichtungen der öffentlichen Verwaltung untereinander und mit Bürgern und Unternehmen gesichert kommunizieren können, z. B. durch verschlüsselte oder signierte E-Mails oder mittels SSL-Verbindungen. Das Sicherheitsniveau der PKI-1-Verwaltung soll IT-Grundschutz unterstützen. Allerdings wurde mit dem Aufsetzen der PCA noch kein Konzept festgelegt, wie Zertifikate und Sperrlisten (im folgenden kurz *PKI-Informationen*) domänenübergreifend bereitgestellt werden.

Der Beitrag zeigt die praktischen Probleme einer Veröffentlichung von Zertifikaten und Sperrlisten in einem gemeinsamen Directory auf und beschreibt Lösungskonzepte. Diese sind die Grundlage für die Realisierung des übergreifenden Verzeichnisdienstes der PKI für die öffentliche Verwaltung in Deutschland, der PKI-1-Verwaltung [PKI-1V]. Die Konzepte sind weitgehend verallgemeiner- und übertragbar. Die zu Grunde liegenden Fragestellungen können daher auch als Checkliste für übergreifende Verzeichnisdienste in anderen Bereichen genutzt werden.

1 Herausforderungen

Die Domänen der PKI-1-Verwaltung bieten ihre Zertifikate und Sperrlisten in dem Rahmen an, der mit ihrer bestehenden Technikausstattung unterstützt wird. Intern ist dies in der Regel einfach möglich, extern aber oft deutlich schwieriger oder unter Umständen gar nicht zu leisten. Ohne eine geeignete Bereitstellung können aber beispielsweise Zertifikatsketten nicht vollständig oder nur mit großem Aufwand geprüft werden. Zwischen Teilnehmern können zusätzliche Kommunikationsschritte erforderlich sein, um die Voraussetzungen für eine gesicherte Telekommunikation zu schaffen. Selbst wenn PKI-Informationen einer Domäne öffentlich bereitgestellt werden, müssen die PKI-Clients teilweise spezifisch konfiguriert werden, um diese abrufen zu können. Diese Ausgangssituation erhöht den Aufwand für die Teilnehmer so, dass letztlich der Zweck der PKI in Frage stehen kann.

Für die PKI-1-Verwaltung wird deshalb ein übergreifender Verzeichnisdienst realisiert, in dem die Zertifikate und Sperrlisten verschiedener Domänen bereitgestellt werden. Die Einrichtung eines solchen Dienstes stößt in aller Regel aber auf eine sehr heterogene organisatorisch-technische Ausgangssituation, die vielfältige typische Probleme aufweist:

- Die lokalen Verzeichnisdienste haben unterschiedliche Einsatzzwecke. Sie dienen etwa der Berechtigungsverwaltung und Administration einer ganzen technischen Infrastruktur (z. B. Active Directory), dem Informationsaustausch zwi-

[1] Der Beitrag ist eine überarbeitete Fassung von Hammer, V. / Neundorf, D. / Rosenhauer, A. / Schmidt, A. (2003): Das Verzeichnisdienstkonzept der PKI-1-Verwaltung, in: Grimm, R. / Keller, H.B. / Rannenberg, K. (Hrsg.): Informatik 2003 - Innovative Informatikanwendungen (Proceeding) - Mit Sicherheit Informationstechnik, Gesellschaft für Informatik, Bonn, 2003, 363 ff. Die Abbildungen sind [VDK] entnommen.

schen Bundesbehörden (IVBB-Directory) oder als reines PKI-Directory.
- Die unterschiedlichen Zwecke führen zu einem unterschiedlichen Aufbau der Directories und der Datenstrukturen sowohl hinsichtlich der Informationen in Entries[2] als auch der Einordnung der Entries in den Directory Information Tree[3] (DIT). Die Vorgaben der PKI haben auf diese Gestaltung oft nur geringen Einfluss.
- Eine Harmonisierung ist nicht zu erwarten. Vielmehr sind die Domänen rechtlich eigenständig und können ihre Technik und Organisation unabhängig weiterentwickeln.
- „Individuelle“ Entwicklungen in Domänen, z. B. Veränderungen des DITs oder die Migration zu anderen Produkten, dürfen aber das übergreifende Verzeichnis nicht beeinflussen. Andernfalls müsste der praktische Betrieb kontinuierlich die lokalen Änderungen nachvollziehen. Ein stabiler Service wäre dann kaum zu erbringen.
- Technische Probleme verhindern, dass Daten zwischen den beteiligten Directories einfach ausgetauscht werden können.

Unter den grundsätzlich möglichen technischen Lösungsalternativen mussten auf Grund der Gegebenheiten die Varianten „Referral-Server“[4] und „LDAP-Proxy“[5] verworfen werden. Realisiert wird ein Verzeichnis mit Replikation.

Die zentralen technischen Konzepte werden im weiteren vorgestellt. Die wichtigsten Sicherheitsmaßnahmen sowie rechtliche und organisatorische Regelungen können nur kurz skizziert werden. Eine detaillierte Darstellung des Verzeichnisdienstkonzepts findet sich in [VDK].

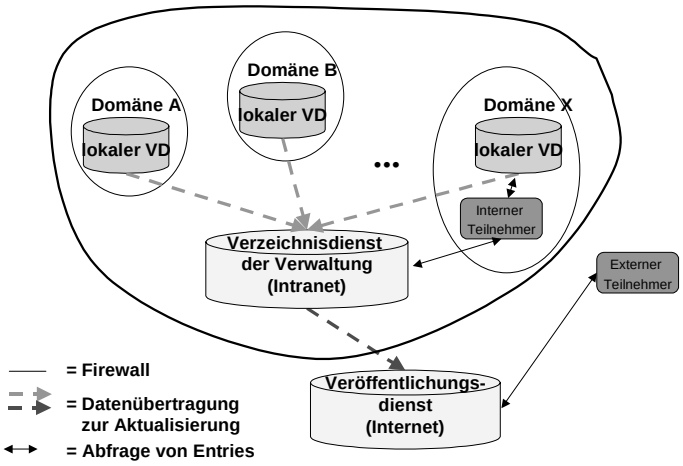

Abb. 1: Logische Architektur der Verzeichnisdienste im Konzept

2 Zentrale Elemente

2.1 Teilnehmergruppen und Architektur

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.
- Zum Anderen sollen Bürger und Unternehmen die PKI-Informationen der Verwaltung abrufen können. Der Umfang der sichtbaren Informationen für diese Zielgruppe soll jedoch gegenüber der internen Sicht für Verwaltungsmitarbeiter reduziert werden können.

Aus den bestehenden Netzwerk-Strukturen im Bereich der öffentlichen Verwaltung wurde die in Abb. 1 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).

Beide Dienste werden im Weiteren zusammenfassend als *Dienste des Verzeichnisdienstkonzepts* bezeichnet.

Zugeliefert werden die PKI-Informationen von der PCA sowie den direkt nachgeordneten CAs. Jede dieser CAs bildet im Verständnis des Verzeichnisdienstkonzepts eine PKI-Domäne. Den nachgeordneten CAs steht es frei, weitere CAs innerhalb ihrer Domäne einzurichten.

Der Client-Zugriff aller internen und externen Teilnehmer erfolgt prinzipiell über LDAP (Lightweight Directory Access Protocol, [LDAP]). Ein Datei-download per HTTP kann aber für CA-Zertifikate und Sperrlisten über einen zusätzlichen Server unterstützt werden.

2.2 Inhalte der Verzeichnisdienste

Für die Auswahl der Inhalte, die in den Verzeichnisdiensten des Verzeichnisdienstkonzepts bereitgestellt werden sollen, sind zwei Aspekte zu unterscheiden: die Auswahl der Entries und die Inhalte in den Entries. Für beide Aspekte sind Datenschutz

[2] Siehe Gateway in diesem Heft.
[3] Siehe Gateway in diesem Heft.
[4] Ein Referral-Server fungiert als „Verweis-Quelle“ auf die Stelle, die die eigentlichen Informationen bereithält. Der Client fragt beim Referral-Server an. Als Antwort erhält er einen Verweis (den „Referral“) auf den Verzeichnisdienst, in dem die Informationen zum gesuchten Eintrag geführt werden müssten, so sie denn vorhanden sind. Für diese Lösung muss der Referral-Server eine Informationsbasis haben, anhand derer er die Zuständigkeiten der „eigentlichen“ Verzeichnisdienste kennt. Außerdem muss der Client den Referral auswerten können.
[5] Ein LDAP-Proxy leitet Anfragen von Clients, die er nicht selbst beantworten kann, an den zuständigen Verzeichnisdienst weiter. Die Antwort, die er von diesem erhält, gibt er dann an den Client zurück. Er verwendet dazu wie der Referral-Server eine Informationsbasis über die Zuständigkeiten. Allerdings merkt der Client nicht, dass ein anderer Verzeichnisdienst die Informationen liefert.

und andere Vertraulichkeitsaspekte zu berücksichtigen.

Auswahl von Entries
Für einen PKI-Verzeichnisdienst sind nur solche Typen von Entries relevant, die PKI-Informationen enthalten: CA-, CRL-Distribution-Point- und Teilnehmer-Entries. Die Entscheidung über die Veröffentlichung eines Entries aus diesen drei Typen kann grundsätzlich nur innerhalb der jeweiligen Domäne geregelt und getroffen werden. Dafür sind mehrere Kriterien zu berücksichtigen.

Die Veröffentlichung von Entries für CAs und CRL Distribution Points (CDP) wird in der Regel keine Probleme aufwerfen, sondern vielmehr erwünscht sein. Für die Veröffentlichung der Entries von Teilnehmern können beispielsweise Betriebsvereinbarungen, individuelle Einwilligungen oder die Policy der Organisation eine Rolle spielen. So könnten z. B. Funktionszertifikate generell veröffentlich werden, Mitarbeiter-Zertifikate aber nur bei bestimmten Aufgaben und bei Zustimmung des Mitarbeiters.

Die Domänen verfügen häufig bereits über individuelle Kennzeichen für die Freigabe von Entries zur Veröffentlichung. Diese werden in Form konfigurierbarer Parameter auch für die Replikationsprozesse des Verzeichnisdienstkonzepts genutzt.

Datenumfang von Entries
Der Datenumfang von Entries im VDK ergibt sich aus notwendigen und optionalen Attributen. CA-Entries müssen die CA-Zertifikate und Sperrlisten enthalten. Entsprechend werden in CDP-Entries nur die Sperrlisten eingestellt. In den Teilnehmer-Entries sind die Teilnehmer-Zertifikate zur Verfügung zu stellen. Da bei vielen gängigen Clients zur Zeit allerdings Probleme auftreten, wenn in einem Teilnehmer-Entry mehrere Zertifikate enthalten sind,[6] darf bis auf weiteres nur ein Zertifikat in den Teilnehmer-Entry eingestellt werden. Dieses muss zur Verschlüsselung zugelassen sein.[7]

In jedem Entry müssen außerdem die Informationen vorhanden sein, anhand derer der Entry gesucht und gefunden werden kann. CA-Entries werden nach [X.509] im Directory unter ihrem Subject DN erwartet (siehe auch unten DIT).[8]

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. Weitere optionale Attribute sind beispielsweise zusätzliche „organizationalUnits“, die „locality“ oder die „serialNumber“ des Zertifikats.

Schließlich sind in allen Entries die Steuerinformationen für die Prozesse des Verzeichnisdienstkonzepts erforderlich. Über den definierten Umfang hinaus werden keine weiteren Attribute in die Dienste des Verzeichnisdienstkonzepts übertragen. Dadurch wird beispielsweise vermieden, dass Passworte oder Zugangsrechte, die in der Domäne zur Administration im lokalen Directory abgelegt werden, öffentlich zugänglich sind.

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 einen stabilen Directory Information Tree (DIT) und ein einheitliches Directory-Schema abbilden lassen. Die Notwendigkeit eines stabilen DIT erzwingt deshalb Namensregeln für die DIT-Distinguished Names in den Diensten des Verzeichnisdienstkonzepts. Der aus diesen Regeln entstehende DIT wird im Weiteren auch als *Austausch-DIT* bezeichnet. Die harmonisierten, verbindlichen Namensregeln für die PKI-1-Verwaltung sind in [NR] dokumentiert. Die Namensregeln des Austausch-DIT haben unterschiedliche Konsequenzen in den Domänen für die CA- und CDP-Entries einerseits und die Teilnehmer-Entries andererseits, die im Folgenden erläutert werden.

CA- und CDP-Entries im DIT
Für CA- und CDP-Entries gelten besondere Anforderungen: Sie müssen im DIT an den Stellen platziert werden, auf die bestimmte Angaben in Zertifikaten verweisen.[9] Da die Namensstruktur im Austausch-DIT festgelegt ist, müssen sich die Domänen bei der Wahl der Subject DNs für CAs und den Angaben für CDPs an diese Struktur halten. Andernfalls ist eine Abbildung in die Dienste des Verzeichnisdienstkonzepts nicht möglich.

Windows 2000 PKIs verwenden allerdings spezifische Namen im DIT für die Bereitstellung von CAs und CDPs. CA-Zertifikate können jedoch mit dem Subject DN aus dem Austausch-DIT ausgestellt und geeignet im Active Directory abgelegt werden. In Zertifikaten können mehrere unterschiedliche CDPs angegeben werden. Sie verweisen dann auf verschiedene Abrufstellen im lokalen Verzeichnisdienst und dem Austausch-DIT des VDK. Die DIT-Namen lokaler CDPs werden im Zuge der Replikation auf die Namen im Austausch-DIT „umgesetzt“ (ähnlich wie die Entries für Teilnehmer, siehe unten).

Im Zuge der Einführung des Verzeichnisdienstkonzepts müssen wenige bestehende CAs zu den neuen Regeln migrieren. Dies erfolgt im Zuge der regelmäßigen Re-Zertifizierung der CAs.

Teilnehmer-Entries im DIT
Für die Behandlung von Teilnehmer-Entries bestehen größere Spielräume. Sie müssen nicht an einem bestimmten Platz im DIT abgelegt, sondern nur gefunden werden. Dazu werden automatische oder manuelle Suchprozesse verwendet, die sich auf die E-Mail-Adresse oder Kenntnisse über Namen und Organisation des Teilnehmers stützen.

Die DIT-Namen von Teilnehmer-Entries können deshalb im Aktualisierungsprozess auf ein einheitliches Format abgebildet werden, wenn die Suchinformationen verfügbar sind. Die Namensgebung im Zertifikat (Subject DN) ist davon nicht betroffen. Auch für den Entry im lokalen Verzeichnis

[6] Sie wählen aus den abgerufenen Zertifikaten unter Umständen eines mit falschem keyUsage oder ausgelaufenem Gültigkeitszeitraum aus.

[7] Auf Teilnehmer-Zertifikate zur Prüfung eines Signaturschlüssels kann im Verzeichnis verzichtet werden, weil sie von allen gängigen E-Mail-Sicherheitsprodukten mit der signierten Nachricht mitgeschickt werden. Entsprechendes gilt für Zertifikate zum Zwecke von SSL-Authentisierungen, die im Protokoll mitgeschickt werden. Es spricht aber aus der Sicht des Verzeichnisdienstkonzepts nichts dagegen, ein „Multi-Purpose Zertifikat“ für mehrere Zwecke einzustellen.

[8] Der Subject Distinguished Name (Subject DN) ist der Name des Zertifikatinhabers, wie er im Zertifikat eingetragen ist.

[9] Nach [X.500 ff] muss der Eintrag einer CAs im Directory unter ihrem Subject DN abgelegt werden. Durch die Forderung ergibt sich implizit eine Übereinstimmung von Subject DN und DIT-DN. Neuere Clients können allerdings über das Zertifikat-Attribut „authorityInfoAccess“ nach [RFC 3280] gezielt auf den Eintrag einer CA an einer abweichenden Stelle im Directory verwiesen werden. Entsprechend müssen CDPs im Directory an der Stelle eingeordnet sein, auf die mit dem Zertifikat-Attribut „cRLDistribution Points“ verwiesen wird.

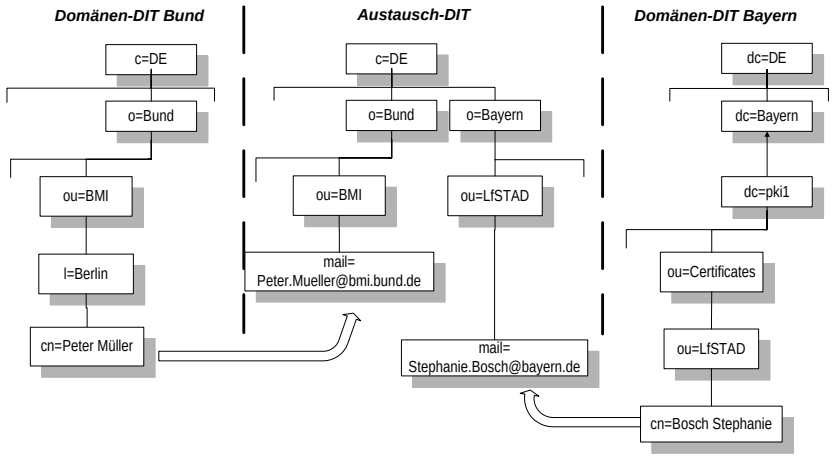

Abb. 2: Umsetzung von Teilnehmer-Entries aus zwei Domänen (links und rechts) in den Austausch-DIT (Mitte) für Teilnehmer aus dem BMI und aus Bayern.

gelten lediglich wenige Minimalanforderungen, die die Voraussetzung für die Umsetzung des Entries sicherstellen.

Abb. 2 zeigt beispielhaft, wie unterschiedliche Namensformate in den Austausch-DIT 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. Dadurch ist eine sehr einfache Realisierung möglich. Zusätzliche Maßnahmen in den Domänen werden vermieden.

Directory Schema

Das Directory-Schema beschreibt formal, welche Informationen die Entries der einzelnen Objekttypen enthalten. Für CAs ergeben sie sich aus dem Distinguished Name und der ObjectClass „pkiCA“ nach [X.509 2001]. CDP-Entries werden mit der ObjectClass „cRLDistributionPoint“ aufgebaut.

Teilnehmer-Entries enthalten in den Diensten des VKD

- die Attribute, die den DIT Distinguished Name[10] im Austausch-DIT bilden. Dies sind die E-Mail-Adresse (‚mail=’), die Bezeichnung der Organisation (‚ou=’), die Bezeichnung der Domäne (‚o=’) und ‚c=DE’;[11]
- weitere Attribute, die der Suche des Entries dienen (vgl. oben);
- das userCertificate in der Objektklasse pKIUser nach [X.509 2001] und
- Steuerungsattribute, u. a. das Datum der letzten Aktualisierung und das Kennzeichen, das über die Replikation in den VöD entscheidet.

Diese Attribute müssen lokal vorhanden sein. Das zugehörige – und in der Regel bereits existierende – lokale Schema kann jedoch sehr flexibel definiert sein. Weichen lokale Attribut-Namen und Objekt-Klassen von denen des VDK ab, dann werden sie im Rahmen des Aktualisierungsprozesses noch innerhalb der Domäne auf das Schema des Austausch-DITs abgebildet.

2.4 Aktualisierungsprozess

Die Aktualisierungsdaten werden von den Domänen periodisch an den VDV geliefert. Da die Domänen die Verantwortung für die Veröffentlichung haben und über die notwendigen Kontrollinformationen verfügen, kontrollieren sie auch den Umfang der zu replizierenden Daten. Dazu werden im Rahmen des Aktualisierungsprozesses unter der vollständigen Kontrolle der Domäne die gekennzeichneten Entries aus dem lokalen Verzeichnis abgerufen und auf den vorgesehenen Datenumfang reduziert. Das Kennzeichen für Entries, die zur späteren Bereitstellung im VöD freigegeben sind, wird im Rahmen dieses Umsetzungsprozesses vereinheitlicht. Erst die lokal aufbereiteten Daten werden an die Dienste des Verzeichnisdienstkonzepts übertragen. Die Prozess-Struktur ist in Abb. 3 dargestellt.

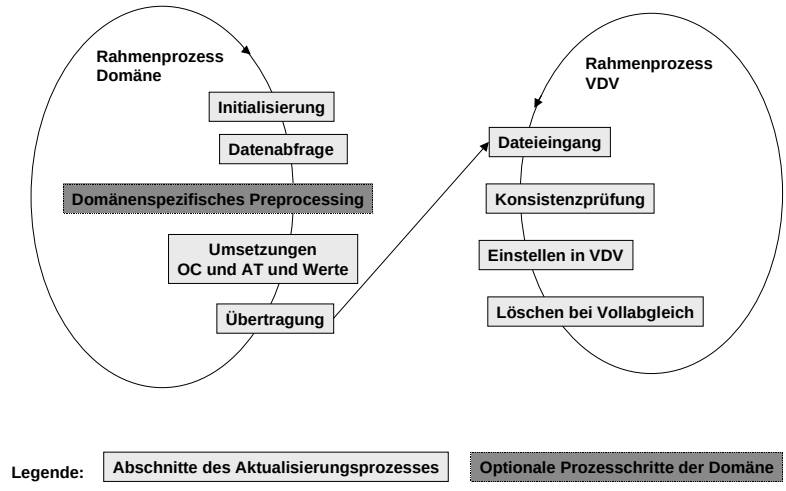

Abb. 3: Grundstruktur des Aktualisierungsprozesses für den VDV (OC= Objektklasse, AT=Attribut-Typ)

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]). Da alle gängigen Verzeichnisdienst-Produkte LDAP-Abfragen unterstützen, kann eine LDIF-Datei mit verfügbaren Tools einfach erstellt werden. Soweit CA-Produkte direkt LDIF-Dateien erzeugen können, kann sogar auf einen lokalen Verzeichnisdienst verzichtet werden.

[10] Die vorgegebene Namensform ist: „cn=[Name der CA], ou=[Name der CA-Gruppe], o=PKI-1-Verwaltung, c=DE“

[11] o und ou mussten wegen bestehender Vorgaben in dieser Weise eingesetzt werden.

Um die Skalierbarkeit zu verbessern, 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 im Falle von Recovery-Maßnahmen werden alle freigegebenen Entries übertragen.

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 innerhalb des VDK genutzt.

Für die Auswahl der Entries wird auf Steuerinformation zurückgegriffen, die oft in den Domänen-Verzeichnissen schon vorhanden ist. Welche Bedingungen für die Auswahl auszuwerten sind, kann konfiguriert werden. Das Verzeichnisdienstkonzept greift daher in die Pflegeprozesse für die Steuerinformation nicht ein.

Die Dienste des Verzeichnisdienstkonzepts sollen „aufgeräumt“ sein, d. h., dass in den Domänen gelöschte Entries auch im VDV und VöD gelöscht werden sollen. Allerdings wirft das **Löschen von Entries** ein spezielles Problem auf: Neue Entries oder Änderungen bestehender Entries können in den lokalen Verzeichnisdiensten anhand des letzten Änderungsdatums leicht identifiziert werden. Eine entsprechende 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.

Die **Aktualisierung des Veröffentlichungsdienstes** wird über einen bilateralen Prozess direkt aus dem VDV vorgenommen. Welche Entries übertragen werden dürfen wird anhand der von den Domänen gelieferten Steuerinformation entschieden.

2.5 Das „Installationspaket“

Die Replikation in den VDV wird trotz aller lokalen Unterschiede in den verschiedenen Domänen sehr ähnliche Probleme aufwerfen. Ein wesentlicher Bestandteil des Verzeichnisdienstkonzepts ist es deshalb, den Replikationsprozess nicht individuell zu implementieren. Vielmehr sollen Skripte bereitgestellt werden, mit denen die Replikation durchgeführt werden kann. Bestandteil des Verzeichnisdienstkonzepts ist ein Installationspaket, durch das der Aufwand für die Domänen sehr gering gehalten wird. In der Prozess-Spezifikation wurden über geeignete Verallgemeinerungen und Konfigurationsparameter die notwendigen Anpassungsmöglichkeiten vorgesehen.

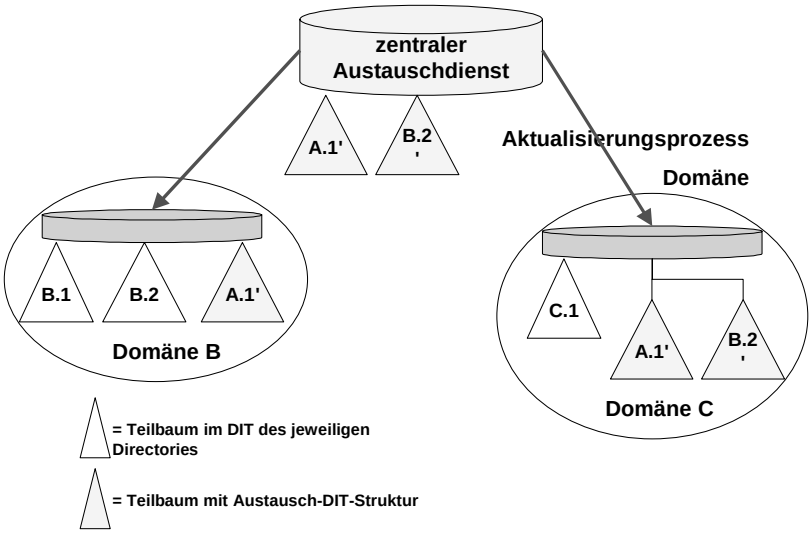

Abb. 4: Rück-Replikation vom Austausch-DIT in eine Domäne.

3 Sicherheitsaspekte

Die PKI-1-Verwaltung und damit auch der übergreifende Verzeichnisdienst sollen ein dem IT-Grundschutz vergleichbares Sicherheitsniveau erreichen.[12] Für den Verzeichnisdienst stehen zwei Schutzziele im Mittelpunkt der Überlegungen: der Schutz der Daten vor unbefugter Verfälschung und die Verfügbarkeit der PKI-Informationen. Letzteres bekommt um so höheres Gewicht, je mehr Anwender künftig innerhalb und außerhalb der Verwaltung die Zertifikate der PKI-1-Verwaltung verwenden. Zwei zentrale Maßnahmen werden im folgenden kurz skizziert.

Es muss für den **Integritätsschutz** sichergestellt werden, dass jede Domänen ihre Entries nur selbst pflegen kann. Andere Domänen oder gar Dritte dürfen sie nicht verändern oder löschen. Dies wird erreicht, indem sich die Domäne gegenüber dem VDV mit kryptographischen Verfahren authentisiert, wenn sie Daten zuliefern will. Auch die Übertragung der Daten erfolgt mit einer kryptographisch gesicherten Verbindung. Vor dem Einstellen von Daten wird schließlich geprüft, ob die zugelieferten Entries im Namensraum der Domäne liegen.

Eine **Reaktionsmöglichkeit in Störungssituationen** ergibt sich daraus, dass die Domänen die Daten aus dem Austausch-DIT auch rückimportieren können (vgl. Abb. 4). Sie erweitern dazu ihren DIT und ggf. ihr Schema geeignet und rufen von einem speziellen Server die LDIF-Dateien der anderen Domänen ab, die sie lokal bereitstellen wollen. Durch diese Maßnahme ergeben sich mehrere Vorteile. Zunächst wird die Skalierbarkeit des Gesamtkonzepts verbessert. Außerdem verringert sich die Abhängigkeit von den zentralen Diensten. Bei schweren Störungen der Dienste des Verzeichnisdienstkonzepts können die LDIF-Dateien sogar bilateral zwischen den Domänen ausgetauscht werden. Die Daten würden dann zwar nicht mehr für externe Teilnehmer, aber immer noch innerhalb der Domänen zur Verfügung stehen.

[12] Zu domänenübergreifenden Directories ist noch kein Grundschutz-Baustein verfügbar. Allerdings können Maßnahmen so ausgewählt werden, dass der Schutz gegen externe Angriffe, die mit begrenzten Mitteln ausgeführt werden, erreicht wird. Für die Schutzziele Vertraulichkeit und Integrität sind relativ einfache Strategien ausreichend. Für die Verfügbarkeit sollte ein etwas über dem Grundschutz liegendes Niveau erreicht werden. Zur Begründung siehe [VDK].

Außerdem müssen auch die **Sicherheitsbedürfnisse der Domänen** beachtet werden. Die Maßnahmen hierzu wurden schon in den vorangegangenen Abschnitten beschrieben. So berücksichtigt der domänenkontrollierte Teil der Aktualisierungsprozesse, dass Dritte nicht „in die Domäne“ eingreifen müssen. Außerdem erfordert das Prozessdesign nur eine minimale Öffnung der Firewall für die Übertragung der Aktualisierungsdaten. Schließlich kann auf die Öffnung des LDAP-Zugriffs nach außen für die Mitarbeiter verzichtet werden, wenn die Domäne den Mechanismus der Rückreplikation nutzt.

4 Rechtliche und organisatorische Aspekte

Für einen produktiven Betrieb des Verzeichnisdienstkonzepts müssen die Pflichten für die verschiedenen beteiligten Organisationen festgelegt werden, damit eine Mindest-Service-Qualität erreicht wird.

Die **rechtlichen Regelungen** konnten weitgehend in die bestehenden Strukturen der PKI-1-Verwaltung eingebettet werden, ohne dass diese modifiziert werden mussten. Die Verantwortung für die ordnungsgemäße Zulieferung von Informationen liegt bei den Domänen. Dementsprechend werden die CAs, die der PKI-1-Verwaltung beitreten, darauf verpflichtet. Außerdem müssen sie dafür sorgen, dass die Namensregeln eingehalten werden.

Die CAs der Domänen müssen ihrerseits sicherstellen, dass ihr Betreiber für das lokale Directory die Anforderungen einhält. Für den Betrieb der zentralen Dienste des Verzeichnisdienstkonzepts wurde ein Betreiber im Rahmen von TESTA-D beauftragt. Die eventuell erforderliche Weiterentwicklung des Verzeichnisdienstkonzepts wird über ein Leitungsgremium in einem definierten Verfahren erfolgen.

Organisatorische Regeln zielen darauf, einen reibungslosen Betrieb zu erreichen und eine Mindestqualität der Daten sicherzustellen. Sie betreffen u. a. den Beitritt von Domänen, ihr Ausscheiden und die Auflösung von CAs. Außerdem wurde ein Prozess für das Change-Management des Verzeichnisdienstkonzepts festgelegt.

5 Status und Ausblick

Die beiden Dienste des Verzeichnisdienstkonzepts sind seit Ende 2002 mit dem definierten Schema im Rahmen des TESTA D Netzes umgesetzt und 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. Die Implementierung der Replikationsskripte erfolgt, sobald sich mindestens zwei Domänen mit unterschiedlicher Directory-Technik beteiligen.

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. Um Migrations-Probleme und Hürden für Inter-Domänen-Verzeichnisse für PKIs von vornherein zu vermeiden, sollten diese so früh wie möglich festgelegt werden.

Literatur

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

[LDAP] 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

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

[RFC 3280] Housley, R. / Polk, W. / Ford, W. / Solo, D. (2002): RFC 3280 – *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF, 2002, z. B. ftp://ietf.org/.

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

[X.500 ff] ITU-T – International Telecommunication Union – Telecommunication Sector: ITU-T Recommendation X.500 ff – Information Technology – Open Systems Interconnection – The Directory.

Aktuelle Informationen zum Verzeichnisdienstkonzept der PKI-1-Verwaltung und die Dokumente selbst sind zu finden unter: http://www.bsi.bund.de/aufgaben/projekte/sphinx/verwpki/struktur.htm