Zertifizierungs-infrastruktur für die PKI-1-Verwaltung

Verzeichnisdienstkonzept

Version 1.2

Stand: 7. Mai 2002

Dr. Volker Hammer,
Dr. Dörte Neundorf
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
hammer@secorvo.de
neundorf@secorvo.de

Dr. Albrecht Rosenhauer
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 183
D-53175 Bonn
Albrecht.Rosenhauer@bsi.bund.de

Inhaltsübersicht

Änderungshistorie

Version	Datum	Status, Änderungen	Autoren
		Das Verzeichnisdienstkonzept wurde vom einem Editorial Board diskutiert. Im Editorial Board haben mitgewirkt: Bayrisches Landesamt für Statistik und Datenverarbeitung (CA), BMI, BSI (PCA-1-Verwaltung), DAASI International GmbH (DFN-Directory, TeleTrusT), DIZ Rheinland Pfalz (CA), Innenministerium Thüringen (Projektleiter TESTA D), KBStLandesamt für Landesvermessung und Datenverarbeitung des Landes Sachsen-Anhalt - Abteilung Landesrechenzentrum (Verzeichnisdienst), SchlumbergerSema - CCI GmbH (CA), TC TrustCenter AG (CA), T-Systems (Directory des IVBB) und T-Telesec (IVBB-CA, TESTA-CA, zentraler Verzeichnisdienst auf der TESTA-D-Plattform).	
1.0	03.04 2002	Vorlage für die Sitzung des Editorial Boards am 10.4. 2002	Volker Hammer, Dörte Neundorf
1.1	26.04 2002	Vom Editorial Board am 10.4. 2002 einstimmig verabschiedete Fassung. (Die Ergebnisse der Abschluss-Sitzung vom 10.4. 2002 wurden eingearbeitet.)	Volker Hammer, Dörte Neundorf

Teil I: Zusammenfassung und Einleitung

Zusammenfassung

Verschiedene Institutionen der öffentlichen Verwaltung der Bundesrepublik Deutschland betreiben Public-Key-Infrastrukturen (PKI) oder bauen sie derzeit auf. Dies wird im Rahmen des Beschlusses der Bundesregierung zur Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung vom 16. Januar 2002 [eSig 160102] explizit angestrebt. PKIs einzelner Bereiche der öffentlichen Verwaltung (im folgenden auch Domänen genannt) werden über eine Wurzel-Zertifizierungsinstanz zur **PKI der öffentlichen Verwaltung** ("PKI-1-Verwaltung") zusammengeführt. Diese Wurzel-Zertifizierungsinstanz wird vom BSI betrieben.

Die Zertifizierungsinstanzen der Domänen-PKIs (Certification Authority, CA) stellen als vertrauenswürdige Dritte Zertifikate für Schlüssel aus. Die Teilnehmer der PKIs benötigen die Zertifikate ihrer Kommunikationspartner, um Nachrichten verschlüsseln und Signaturen überprüfen zu können. Gleiches gilt für die Zertifikate der Zertifizierungsinstanzen. Hierbei ist die Bereitstellung sogenannter Sperrlisten (Cetificate Revocation List, CRL, und Authority Revocation List, ARL) besonders wichtig, da in ihnen ungültig gewordene Zertifikate ausgewiesen werden. Die Sperrlisten müssen ständig aktualisiert werden. Ein Vorgang, der kaum im Rahmen anderer Prozesse automatisiert ablaufen kann. Zertifikate und Sperrlisten werden im folgenden unter dem Begriff *PKI-Informationen* zusammengefasst.

Damit die Clients fehlende Zertifikate in einfacher Weise finden und Sperrlisten automatisch aktualisieren können, werden die PKI-Informationen in einem Verzeichnisdienst zur Verfügung gestellt. Verzeichnisdienste steigern den Nutzen einer Public-Key-Infrastruktur für die Anwender erheblich. Sie sind daher – auch unter Kostengesichtspunkten – ein wesentlicher Teil der **Infrastruktur**. Der Verzeichnisdienst kann in der Regel innerhalb der Domäne einer PKI relativ einfach realisiert werden. Allerdings sollen die Teilnehmer auch domänenübergreifend

kommunizieren können, z. B. wenn eine Bundes- mit einer Landes- oder Kommunalbehörde vertrauliche Nachrichten austauscht. Ein domänenübergreifender Zugriff auf lokale Verzeichnisse ist allerdings meist nicht möglich oder mit großen Schwierigkeiten verbunden.

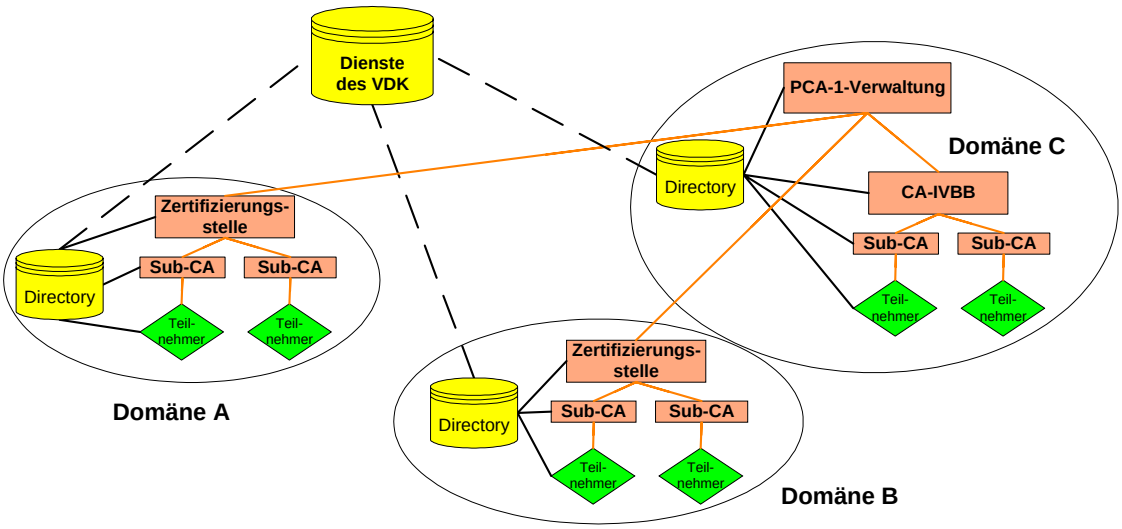

Abbildung 1: Verschiedene PKI-Domänen und die Verbindung zwischen den lokalen Verzeichnisdiensten über die Dienste des Verzeichnisdienstkonzepts.

Eine Möglichkeit, die übergreifende Kommunikation zu unterstützen, besteht darin, die notwendigen und freigegebenen PKI-Informationen zwischen den Verzeichnisdiensten der Domänen auszutauschen. Außerdem könnte ein spezieller Verzeichnisdienst freigegebene PKI-Informationen öffentlich zugänglich machen. Das vorliegende Konzept enthält für beide Ansätze Lösungen, die an den Spezifika der PKI-1-Verwaltung ausgerichtet sind. Dadurch kann eine effektive Verbindung der PKIs der Domänen hergestellt und die angestrebte behördenübergreifende sichere Kommunikation gefördert werden.

Die existierende Netzinfrastruktur für die öffentliche Verwaltung wird dabei in einer logischen Sichtweise grob unterschieden nach:

- den Netzen der Domänen, beispielsweise eines Bundeslandes, innerhalb derer nur die Mitarbeiter der Domäne zugreifen dürfen und die gegenüber anderen Netzen abgeschottet werden.

- dem Intranet der öffentlichen Verwaltung der Bundesrepublik, das alle Mitarbeiter der angeschlossenen Domänen nutzen können. Dieses Intranet ist aber gegenüber dem weltweiten Internet abgeschlossen.
- dem öffentlichen ("restlichen") Internet, das hier zur besseren Unterscheidung als Extranet bezeichnet wird.

Die Verzeichnisdienste der Domänen bleiben durch das Verzeichnisdienstkonzept weitgehend unberührt. Sie müssen lediglich einige Voraussetzungen erfüllen und werden in die Lage versetzt, die PKI-Informationen für die folgende drei neuen *Dienste* bereitzustellen:

- **Der zentrale Verzeichnisdienst der Verwaltung (VDV):** Der zentrale Verzeichnisdienst der Verwaltung erlaubt es allen Mitarbeitern, die an das Intranet der öffentlichen Verwaltung der Bundesrepublik angeschlossen sind, die in diesem Dienst bereitgestellten PKI-Informationen abzufragen.
- **Der Veröffentlichungsdienst (VöD)**: Eine Untermenge der Daten aus dem Verzeichnisdienst der Verwaltung wird im Veröffentlichungsdienst für Teilnehmer aus dem Extranet zur Verfügung gestellt,
- Wenn Domänen den LDAP-Zugriff nach außen (auf Dienste außerhalb ihres Netzes) nicht zulassen, können ihre Mitarbeiter nicht auf den VDV zugreifen. Deshalb wird zusätzlich die Möglichkeit angeboten, die Daten des VDV oder eine Auswahl davon auch in einem lokalen Verzeichnisdienst in der Domäne bereitzustellen. Um die Aktualisierung solcher "Importe" einheitlich zu gestalten, wird der **Austauschdienst (AD)** eingeführt. Er stellt die erforderlichen Verzeichnis-Daten über eine Dateischnittstelle bereit. Von dort können sie in die lokalen Verzeichnisdienste importiert werden. Der Austauschdienst verbessert außerdem die Lastverteilung und Verfügbarkeit im Verzeichnisdienstkonzept.

Die notwendigen Daten werden in diese drei Dienste durch *Aktualisierungsprozesse* eingestellt. Um diese Prozesse möglichst einfach zu gestalten und aufwändige Anpassungen beim Beitritt einer neuen Domäne zu vermeiden, wurde für die drei Dienste eine einheitliche Struktur zum Speichern der Daten

festgelegt, der sogenannte Austausch Directory Information Tree (**Austausch-DIT, A-DIT**). Die Informationen aus den teilnehmenden lokalen Verzeichnissen werden in diesen Austausch-DIT abgebildet. Die lokalen Verzeichnisse können ihre Struktur nahezu unverändert beibehalten. Dies ist ein wesentlicher Erfolgsfaktor für die Realisierung des Verzeichnisdienstkonzepts. Erforderlich sind lediglich eine Harmonisierung der Namensgebung und geringfügige Anpassungen in den Inhalten der lokalen Verzeichnisse. Beides wird mit diesem Konzept angestoßen.

Die Aufgaben und das Zusammenwirken der verschiedenen Beteiligten müssen koordiniert werden. Deshalb ist der Austausch der PKI-Informationen zwischen Verzeichnisdiensten und ihre öffentliche Bereitstellung neben technischen auch an rechtliche und organisatorische Voraussetzungen gebunden. Die Verantwortung für die zugelieferten Daten verbleibt bei den Domänen. Ein "Steuerungsgremium der PKI-1-Verwaltung" und die PCA haben eine koordinierende und kontrollierende Rolle. Um die Verantwortlichkeiten zwischen den Beteiligten abzustimmen, müssen die Vereinbarungen zum Beitritt von Zertifizierungsinstanzen zur PKI-1-Verwaltung um wenige Punkte erweitert werden. Das Verzeichnisdienstkonzept enthält dazu einen Vorschlag für die Anpassung von Vertragsdokumenten. Enthalten sind ebenfalls Vorschläge für die organisatorischen Abläufe und die spezifischen Sicherheitsmaßnahmen.

Das Verzeichnisdienstkonzept beschreibt damit die Maßnahmen, die erforderlich sind, um die drei genannten Dienste und die erforderlichen Austauschprozesse zu implementieren und rechtlich und organisatorisch in die PKI-1-Verwaltung einzubinden.

Die Erstellung dieses Konzepts wurde von einem Editorial Board begleitet. Das Editorial Board hat dieses Verzeichnisdienstkonzept in seiner Sitzung am 10.4. 2002 einstimmig als Grundlage für eine künftige Implementierung empfohlen. In der vorliegenden Form wird es weiteren Gremien zur Abstimmung vorgelegt.

1 Einleitung

1.1 Struktur des Dokuments

Das vorliegende Verzeichnisdienstkonzept ist wie folgt strukturiert:

Teil I besteht aus einer Einführung in den Kontext des Projektes und die Struktur des Dokumentes (Kapitel 1) sowie aus einer zusammenfassenden Übersicht über die technischen Ansätze des Verzeichnisdienstkonzepts (Kapitel 2). Es gibt damit einen Überblick für diejenigen Leser, die lediglich am Konzept, nicht aber an den technischen Details interessiert sind.

Die **Teile II und III** beschreiben die technischen Umsetzungen und Prozesse, die den Kern des Verzeichnisdienstkonzepts bilden. Sie erläutern die Zusammenhänge für Leser, die an den technischen Details interessiert sind, insbesondere für die PKI- und Directory-Spezialisten.

- In Teil II werden unter dem Stichwort "Directory Information Tree" die Anforderungen an die Namensgebung in den Domänen, das Namenskonzept für die Dienste des Verzeichniskonzepts und die Umsetzungsregeln dargestellt (Kapitel 3). Im selben Teil wird in Kapitel 4 das Directory-Schema diskutiert. Auch hier werden die Vorgaben für die teilnehmenden Domänen, das Schema für die zentralen Dienste und die Umsetzung spezifiziert.
- In Teil III werden die verschiedenen Aktualisierungsprozesse beschrieben (Kapitel 5 - 9). Im einzelnen sind dies der Aktualisierungsprozess zum Verzeichnisdienst der Verwaltung, der Aktualisierungsprozess zum Austauschdienst, die Aktualisierung des Veröffentlichungsdienstes und der Aktualisierungsprozess vom Austauschdienst zum lokalen Verzeichnisdienst in der Domäne.

Teil IV beschreibt weitere technische Teilkonzepte, nämlich die Bereitstellung von Zertifikaten und Sperrlisten für den Abruf über HTTP, den Abruf über LDAP und die erforderliche Testunterstützung.

Die Kapitel des **Teils V** stellen Maßnahmen zusammen, die zur Realisierung und für den Betrieb der Dienste des Verzeichnisdienstkonzepts neben der technischen Spezifikation erforderlich sind. Die Kapitel sind als Checklisten zu verstehen, die einerseits das technische Konzept ergänzen, andererseits aber unter dem jeweiligen Blickwinkel Punkte aufgreifen, die in den vorgenannten Teilen bereits angesprochen wurden. Diese Redundanz wird in Kauf genommen, um die zur Realisierung erforderlichen Arbeiten für den jeweiligen Aspekt im Zusammenhang darzustellen. Die Kapitel bereiten den Inhalt des Konzepts daher vor allem für diejenigen Leser auf, die für die Realisierung verantwortlich sind oder die sich über die Aufgaben im Rahmen des Beitritts einer Domäne zu den Diensten des Verzeichnisdienstkonzepts informieren wollen. Kapitel 13 gibt Hinweise zur rechtlichen Verankerung des Konzepts und entwickelt einen Vorschlag für die Vertragsbeziehungen. Kapitel 14 beschreibt die organisatorischen Aspekte und enthält die wesentlichen Ablaufprozesse. Kapitel 15 gibt Hinweise für die erforderlichen Sicherheitskonzepte. Kapitel 16 stellt die wesentlichen Arbeiten für die Realisierung zusammen. Schließlich gibt Kapitel 17 einen Ausblick auf mögliche und sinnvolle Erweiterungen in späteren Ausbaustufen.

Den **Abschluss** bilden das Literaturverzeichnis und ein ausführliches Glossar. In den **Anhängen** finden sich die Spezifikationen für die wesentlichen Aktualisierungsprozesse. Außerdem werden dort die wichtigsten Teile der Umfrage in den Domänen dokumentiert, die im Laufe des Projekts durchgeführt wurde.

1.2 Aufbau von Verzeichnisdiensten

Das Kapitel gibt einen knappen Überblick über die Art, wie Informationen in Verzeichnisdiensten gespeichert werden, und führt dabei in die in diesem Dokument verwendeten Begriffe ein.

Verzeichnisse sind wie eine 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. Die Distinguished Names der Objekte werden hierarchisch organisiert. Beispielsweise werden die Entries der Mitarbeiter einer Organisation "unter" dem Entry der Organisation gespeichert. Die Organisation wiederum wird der Gruppe untergeordnet, in der sie angesiedelt ist, z. B. dem Bundesland oder der Kommune. Das Bundesland wiederum ist unter dem Wurzelknoten für Deutschland "c=DE" eingeordnet. 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).

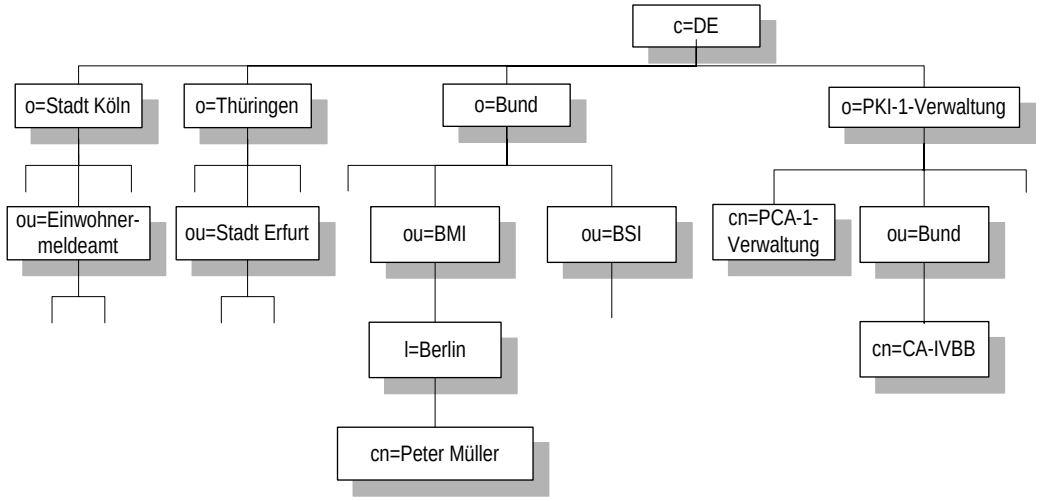

Abbildung 2: Beispiel für einen Directory Information Tree. Ein Teilnehmer-Entry und die CA liegen in den Teilbäumen des IVBB[1].

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.

1 Zur Namensgebung für Kommunen siehe auch die Alternativen in [PKI1V Namensregeln].

In diesem Dokument ist der DIT-DN zu unterscheiden von den Namen im Zertifikat. Sie 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.

Zu jedem DIT-DN wird im Baum ein **Entry** gespeichert, der verschiedene Daten zum Objekt enthalten kann. 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. 3).

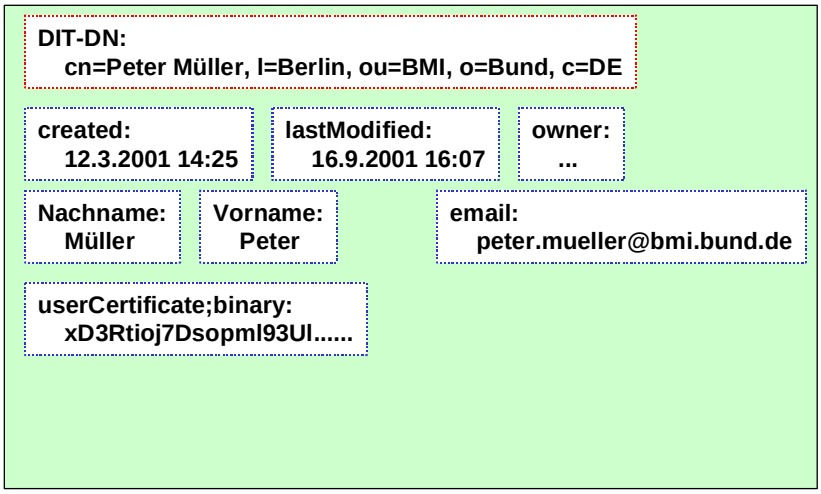

Abbildung 3: Ein Teilnehmer-Entry als Container für unterschiedliche Attribute. Die eindeutige "Adresse" ist der DIT-DN

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 festgelegt, auf welcher Ebene des DIT welche Typen

von Entries zulässig sind. Für jeden Entry ergeben sich somit aus DIT-Struktur und Schema-Definition die Struktur seines eindeutigen Namens und die zulässigen Attribute. Das "unterste" Attribut, das den Namen des Entries von den anderen Entries auf der gleichen Ebene unterscheidet, wird auch als **namensgebendes Attribut** bezeichnet (entspricht dem relativen Namen oder "Relative Distinguished Name" dieser Ebene). In Abbildung 2 wäre dies für den Teilnehmer-Entry das Attribut *cn*.

Hinweis: die Vorgaben zur Bildung von DIT-DNs und Subject-DNs werden in [PKI1V Namensregeln] beschrieben. Sie sind verbindlich für alle Domänen.

1.3 Abgrenzung des Konzepts für den Verzeichnisdienst

Das Verzeichnisdienstkonzept ist begrenzt auf die verzeichnisdienstspezifischen Voraussetzungen für produktive Lösungen zur allgemeinen Bereitstellung von Sperrlisten, CA-Zertifikaten und Teilnehmer-Zertifikaten zur Verschlüsselung von E-Mail.

Das Verzeichnisdienstkonzept nimmt an, dass die Domänen die jeweils richtigen Informationen zum Austausch bereitstellen. Aus dieser Sicht ist der konkrete Aufbau und Inhalt von Zertifikaten und Sperrlisten für das Verzeichnisdienstkonzept irrelevant.

Für die zum Austausch von PKI-Informationen benötigten Aktualisierungsprozesse zwischen den Verzeichnisdiensten wird außerdem angenommen, dass die benötigten Daten einschließlich der PKI-Informationen

- entweder in einem Directory vorliegen, das über das Zugriffsprotokoll LDAP (Lightweight Directory Access Protocol) abgefragt werden kann,
- oder im LDIF-Format (LDAP Data Interchange Format, [LDIF]) zur Verfügung gestellt werden. Diese direkte Bereitstellung von Daten in einem geeigneten Format ermöglicht auch solchen Zertifizierungsstellen die Teilnahme, die ihre PKI-Informationen nicht in ein Directory schreiben.

Ob und wie Zertifizierungsinstanzen oder andere Komponenten diese Voraussetzung schaffen, wird nicht betrachtet.

Die Verzeichnisdienste der Domänen und ihre Anwendungen werden bis auf die Aspekte des Verzeichnisdienstkonzepts als "Black Boxes" betrachtet. Daraus ergeben sich die folgenden Abgrenzungen:

- Es ist die Aufgabe der Domänen, zu prüfen, welche ihrer Teilnehmer-Zertifikate sie unter den gegebenen rechtlichen Rahmenbedingungen und gegebenenfalls weiteren Sicherheitsbedingungen in die Dienste des Verzeichnisdienstkonzepts exportieren dürfen. Vom Betreiber der Dienste des Verzeichnisdienstkonzepts und von den importierenden Domänen werden keine weiteren Prüfungen durchgeführt.
  Das Ergebnis dieser Prüfung müssen die Betreiber der Domänen-PKIs umsetzen, indem sie die auszutauschenden PKI-Informationen explizit im lokalen Directory kennzeichnen. Informationen in den Verzeichnisdiensten der Domänen, die nicht geeignet gekennzeichnet sind, werden nicht übermittelt. Das Verzeichnisdienstkonzept definiert geeignete Steuerungsmechanismen für die Kennzeichnung der Daten. Dabei wird zwischen Datensätzen nur für den VDV und Datensätzen für VDV und Veröffentlichungsdienst unterschieden.
- Die Zugriffe lokaler Anwendungen auf die lokalen Verzeichnisdienste von Domänen werden nicht betrachtet.
- Die Domänen müssen durch ihre internen Sicherheitsmaßnahmen (vgl. Kapitel 15) gewährleisten, dass sie das vom Verzeichnisdienstkonzept geforderte Sicherheitsniveau, die notwendige Qualität der Daten und Anforderungen an die Schnittstellen oder Prozesse des Verzeichnisdienstkonzepts einhalten. Es werden keine weitergehenden organisatorischen Anforderungen oder Sicherheitsanforderungen an Verzeichnisse der Domänen definiert.
- Für den Veröffentlichungsdienst im Extranet wird angenommen, dass er in enger Kooperation mit dem Betreiber des Verzeichnisdienstes der Verwal-

tung (VDV) betrieben wird. Der Aktualisierungsprozess wird deshalb in diesem Verzeichnisdienstkonzept nur bezüglich des Datenumfangs und einiger Service-Parameter, nicht aber hinsichtlich des Austauschformats für Daten oder der Prozess-Schritte spezifiziert.

Für die erste Ausbaustufe des Verzeichnisdienstkonzepts gelten die folgenden weiteren Abgrenzungen:

- Im Rahmen der Dienste des Verzeichnisdienstkonzepts werden keine Teilnehmer-Zertifikate, die spezifisch für SSL eingesetzt werden, bereitgestellt. Dies gilt auch für Zertifikate, die für andere spezifische Authentisierungs- oder Autorisierungszwecke herangezogen werden sollen.
- Das Verzeichnisdienstkonzept erlaubt, die Bedingungen für fortgeschrittene Signaturen im Sinne des Signaturgesetzes (SigG) zu erfüllen. Das Verzeichnisdienstkonzept ist jedoch nicht an den Anforderungen für qualifizierte Signaturen im Sinne des Signaturgesetzes ausgerichtet. Das heißt insbesondere, dass das Konzept bezüglich der Sperrinformationen keinen Verzeichnisdienst zur automatischen Überprüfung von Zertifikaten für qualifizierte Signaturen nach SigG vorsieht.
- PKI-Informationen aus dem SPHINX-Pilotversuch werden in diesem Verzeichnisdienstkonzept nicht berücksichtigt.
- PKI-Informationen aus Domänen privater Einrichtungen (beispielsweise von Unternehmen) sowie von internationalen Institutionen werden bei der Konzeption ebenfalls nicht berücksichtigt.
- OCSP-Dienste sind nicht Gegenstand des Verzeichnisdienstkonzepts.
- Die Integration von CAs, die nicht zur PKI-1-Verwaltung zählen, wird in der Regel nicht ohne weiteres möglich sein. Für die Ausbaustufe 1 ist dies auch nicht Gegenstand des Verzeichnisdienstkonzepts.

1.4 Zielgruppen

Das Verzeichnisdienstkonzept ist primär am Bedarf der teilnehmenden öffentlichen Verwaltungen ausgerichtet. Die Zielgruppe "öffentliche Verwaltung" umfasst die Verwaltungen und die Parlamente von Bund, Ländern und Kommunen. In den geschätzten Zahlen sind alle Nutzer berücksichtigt. Darüber hinaus identifizierte Teilnehmergruppen werden nur insoweit unterstützt, als dies das Konzept für die genannte Gruppe zulässt. Der Zeithorizont für die folgenden Schätzungen ist Ende 2004. Die erwarteten Zahlen aus der Abschätzung der Zielgruppen sind Grundlage des Mengenmodells, das im Endausbau durch die drei Dienste des Verzeichnisdienstkonzepts unterstützt werden muss.

CA-Betreiber: Die Dienste des VDKs unterstützen alle von der PKI-1-Verwaltung zertifizierten Zertifizierungsinstanzen und die diesen nachgeordneten CAs. Potenziell sind darunter Zertifizierungsstellen für alle Institutionen der öffentlichen Verwaltung und Parlamente der Bundesrepublik zu fassen.

Anzahl CAs gesamt	Anzahl zertifizierte Teilnehmer gesamt
ca. 20	ca. 200 000

Tabelle 1: Anzahl der erwarteten CAs und zertifizierten Teilnehmer der PKI-1-Verwaltung

Directory-Betreiber: Die PKI-Domänen der PKI-1-Verwaltung können jeweils einzeln ein Directory betreiben; es ist jedoch davon auszugehen, dass in einigen Fällen mehrere Domänen ein gemeinsames Directory nutzen. So werden die "PCA-1-Verwaltung" und die Zertifizierungsinstanzen der Bundesministerien und der Bundesbehörden ihre Zertifikate in das Directory des IVBB einstellen. Denkbar ist auch, dass einzelne CAs direkt LDIF-Dateien erzeugen und kein eigenes Directory betreiben. Diese werden dann als eigene Domäne ohne Directory gewertet.

Anzahl der Directories	Zusätzliche Domänen ohne Dir.
ca. 10	ca. 5

Tabelle 2: Anzahl der erwarteten Directories und zusätzlichen Domänen

Directory-Nutzer des Veröffentlichungsdienstes: Der Veröffentlichungsdienst soll PKI-Informationen sowohl für Teilnehmer aus dem Bereich der öffentlichen Verwaltung als auch für externe Teilnehmer bereitstellen. Für eine erste Abschätzung der Last werden die erwarteten Zahlen für den Endausbau in der folgenden Tabelle aufgeführt.

	Anzahl der Teilnehmer aus öffentlicher Verwaltung	Anzahl der Teilnehmer extern	Gesamtzahl der Teilnehmer
Abfrage von TN-Zertifikaten	200.000	10.000	210.000
Abfrage von Sperrlisten	40.000	10.000	50.000

Tabelle 3: Angenommene Zahl der Teilnehmer des Veröffentlichungsdienstes

Anmerkung: Diese Zahlen geben noch keine Auskunft über die Zahl der Zugriffe und das entstehende Datenvolumen. Für eine aussagekräftige Abschätzung des Lastaufkommens im Betrieb müssen diese Zahlen validiert und in einem differenzierteren Mengenmodell berücksichtigt werden. Dieses benötigt insbesondere auch sinnvolle Annahmen für die Zahl der Zugriffe auf Zertifikate und Sperrlisten je Teilnehmer, die einzuarbeiten sind.

Im Rahmen des Projektes wurden einige Domänen dazu befragt, welche Zahlen sie bis Ende 2004 erwarten. Die folgende Tabelle gibt die Ergebnisse dieser Befragung wieder. Unter der Annahme, dass sich die Anzahl der Domänen bis 2004 noch etwa verdoppeln wird, passen diese Zahlen recht gut zu den in Tabelle 3 angegebenen Schätzungen.

Domäne	Anzahl produktive CAs bis Ende 2004	Anteil zertifizierte TN bis Ende 2004		Anzahl Directories (aktuell)
		prozentual	absolut	
PCA	1	-	10 –20 CAs	nutzt IVBB-Directory
IVBB	4	50 %	20.000	2
Sachsen-Anhalt	1	k.A.	k.A.	1
Testa	2+x	k.A.	k.A.	2
Bayern	4	10% - 20%	12.000-24.000	2
Rheinland-Pfalz	1	40 %	6.000	ca. 60 (Exchange-Server)
Freie Hansestadt Hamburg	2	100 %	25.000	1
Summe	15		ca. 60.000	

Tabelle 4: Mengenschätzungen der Domänen

1.5 Projektablauf

Das Projekt "Verzeichnisdienstkonzept" umfasste die folgenden Arbeitspakete:

i. die Definition eines *Directory-Schemas*, in dem festgelegt wird, welche Daten ausgetauscht und veröffentlicht werden,

ii. die Festlegung von *Namensregeln* für den Directory Information Tree, in dem die Entries im Rahmen des Verzeichnisdienstkonzepts abgelegt werden,

iii. den Entwurf von *Aktualisierungsprozessen*, die die Aktualisierung des zentralen Datenbestandes ermöglichen, wenn sich die Ausgangsdaten in den Domänen geändert haben,

iv. die Darstellung, wie der *Abruf von Daten* aus dem öffentlich zugänglichen Verzeichnis durch Clients erfolgt, und

v. den Entwurf des *Aktualisierungsprozesses für die Verzeichnisdienste der Domänen,* mit dem die zum Austausch bereitgestellten Daten in die Domänen importiert werden und dort zur Aktualisierung genutzt werden können, soweit dies von der Domäne gewünscht ist.

Die einzelnen Arbeitspakete sind eng miteinander verzahnt und hängen von zahlreichen Rahmenbedingungen ab. Statt sie sequentiell und einzeln zu bearbeiten, wurde deshalb ein zweistufiges Vorgehen gewählt. In einem ersten Schritt wurde eine abstrakte Ausrichtung des Lösungsansatzes für das Gesamtkonzept durch die Abstimmung der Zielsetzung [PKI1V-VDK-Ziel] im Editorial Board (1. Sitzung, 05.12. 2001) erreicht. Im Anschluss wurde eine Umfrage bei den Domänen hinsichtlich der bereits existierenden Rahmenbedingungen durchgeführt (Ergebnisse im Anhang). Basierend auf diesen Grundlagen wurden im zweiten Schritt in weiteren Analysen die technischen Details der Arbeitspakete ausgearbeitet [PKI1V-VDK-Analyse AP], [PKI1V-VDK-Analyse DIT und Schema]. Die Analyseergebnisse und die daraus resultierenden

Entwurfsentscheidungen wurden wiederum mit dem Editorial Board abgestimmt (2. Sitzung, 20.02. 2002).

Im vorliegenden Dokument findet sich nun eine konsolidierte Gesamtfassung des Verzeichnisdienstkonzepts. Die Zielsetzung und die Analysedokumente wurden so integriert, dass alle erforderlichen Informationen und Zusammenhänge aus diesem Dokument ersichtlich sind. In der abschließenden Sitzung des Editorial Boards am 10.4. 2002 wurden letzte technische Details, rechtliche und organisatorische Aspekte und das Sicherheitskonzept diskutiert. Das Editorial Board stellte auf dieser Sitzung in einer einstimmigen Beschlussfassung fest, dass das vorliegende Verzeichnisdienstkonzept eine tragfähige Grundlage für die künftige Implementierung des Verzeichnisdienstes der PKI-1-Verwaltung darstellt.

Dieses Dokument ist damit die Grundlage für die Abstimmung über die Realisierung zentraler Verzeichnisdienste der PKI-1-Verwaltung. Der Abstimmungsprozess beteiligt Bund, Länder und Kommunen sowie Fachgremien auf einer breiteren Basis. Ziel des Abstimmungsprozesses ist eine Beschlussfassung des KoopA über die Realisierung der in diesem Konzept vorgeschlagenen Dienste, gegebenenfalls in modifizierter Form.

2 Übersicht über das Verzeichnisdienstkonzept

Dieses Kapitel fasst das Grundkonzept des Verzeichnisdienstkonzepts (VDK) zusammen. Es beginnt mit einer Zusammenstellung des Leistungsumfangs und detailliert dann die technischen Prozesse und Abläufe.

2.1 Leistungsumfang des Verzeichnisdienstes

Ziel des konzipierten Verzeichnisdienstes der PKI-1-Verwaltung ist es, den Teilnehmern einen effizienten Zugriff auf Sperrlisten, CA-Zertifikate und Zertifikate anderer Teilnehmer zu erlauben. Dies geschieht auf Basis der in der Zusammenfassung genannten drei Dienste: dem Verzeichnisdienst der Verwaltung, dem Veröffentlichungsdienst und dem Austauschdienst.

Der Leistungsumfang des Verzeichnisdienstes nach diesem Konzept ergibt sich

- aus den Diensten, die sie für die Teilnehmer bereitstellen,
- aus dem Umfang der Daten, die auszutauschen sind, und
- den Prozessen, mit denen die Daten gepflegt und abgerufen werden.

2.1.1 Dienste des Verzeichnisdienstkonzepts

Die Dienste, die die Zielstruktur des Verzeichnisdienstkonzepts bestimmen, ergeben sich aus den Zugriffsmöglichkeiten der Zielgruppen, für die die PKI-Informationen zur Verfügung gestellt werden sollen. Es können zwei unterschiedliche Zielgruppen identifiziert werden:

- Die Mitarbeiter der öffentlichen Verwaltungen der Bundesrepublik. Für diese Zielgruppe wird der **Verzeichnisdienst der Verwaltung** im gemeinsamen Intranet der öffentlichen Verwaltung aufgebaut. Auf diesen Dienst haben nur Mitarbeiter Zugriff, die Zugang zum Intranet der öffentlichen Verwaltung haben. Im Rahmen dieser Vorbedingung kann der Zugriff jedoch anonym erfolgen.

- Die Teilnehmer, die außerhalb des Intranets der öffentlichen Verwaltung auf PKI-Informationen aus der PKI-1-Verwaltung zugreifen wollen. Für diese Zielgruppe wird ein **externer Veröffentlichungsdienst** (kurz: Veröffentlichungsdienst) eingerichtet. Dieser ist aus dem Internet ohne Einschränkungen zugreifbar. Der Zugriff kann anonym erfolgen.

Der externe Veröffentlichungsdienst stellt eine Teilmenge der Entries aus dem Verzeichnisdienst der Verwaltung bereit. Entries, die in den externen Veröffentlichungsdienst eingestellt werden sollen, müssen daher im Verwaltungsverzeichnis (Intranet) enthalten sein. Die Domänen entscheiden und steuern, welche Entries in den Verzeichnisdienst der Verwaltung und welche Teilmenge daraus in externen Veröffentlichungsdienst übertragen werden. Das logische Strukturmodell der beteiligten Verzeichnisdienste in Abbildung 4 zeigt, dass die Domänen Daten an den Verzeichnisdienst der Verwaltung im Intranet liefern, aus dem sie wiederum in den Veröffentlichungsdienst im Extranet übertragen werden.

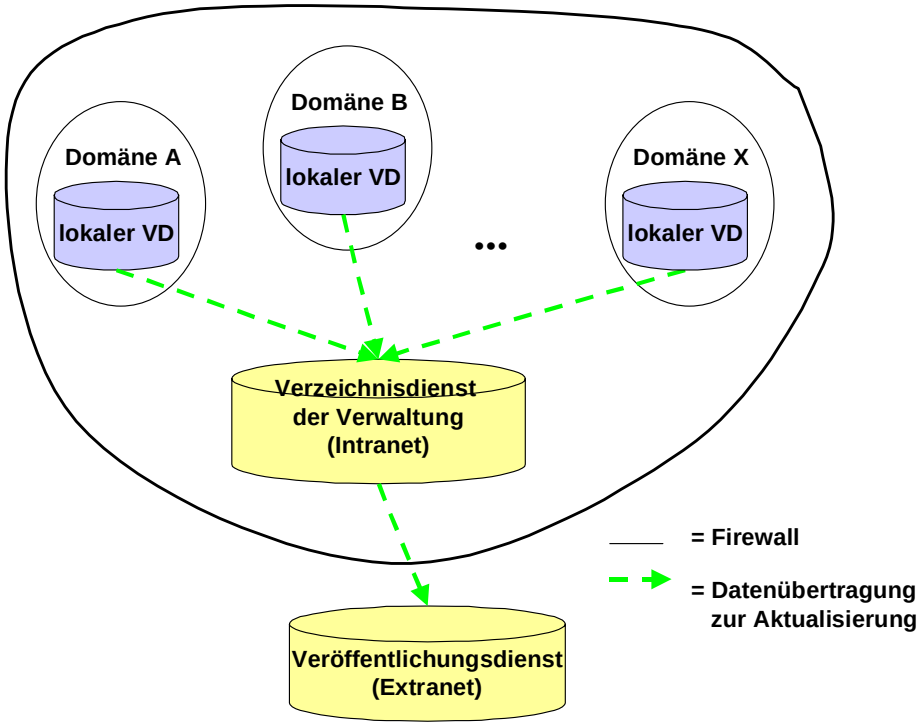

Abbildung 4: Logisches Strukturmodell der Verzeichnisdienste und Grenzen zwischen den "Communities"

Die Teilnehmer einzelner Domänen haben unterschiedlichen Bedarf, auf PKI-Informationen zuzugreifen. Beispielsweise kann es Teilnehmergruppen geben, die nur selten mit Zertifikaten Externer arbeiten, und andere, die regelmäßig Kontakt mit bestimmten Partnerbehörden aus anderen Domänen haben. Außerdem liegen innerhalb der Domänen jeweils spezifische Voraussetzungen für den Zugriff auf öffentliche und lokale PKI-Informationen vor. Sie können sich unterscheiden hinsichtlich

- des Zugangs zu öffentlichen Teilen des Internets, z. B. unter Sicherheitsaspekten,
- der Leistungsfähigkeit des lokalen Netzwerkes und
- des Datenumfangs, den ein lokales Verzeichnis bereitstellen soll, beispielsweise bei begrenzter Leistungsfähigkeit verfügbarer Server oder hinsichtlich der lokalen Aufwände für die Administration.

Es kann deshalb für eine Domäne sinnvoll sein, für ihre Mitarbeiter nicht nur den Zugriff auf ein öffentliches Verzeichnis zuzulassen, sondern auch die PKI-Informationen anderer Domänen zu importieren und im lokalen Verzeichnisdienst zur Verfügung zu stellen. So könnte es z. B. für bestimmte Landesbehörden sinnvoll sein, die PKI-Informationen einiger Bundesministerien und -behörden, mit denen besonders viel kommuniziert wird, zu replizieren und damit die Zugriffe auf externe Verzeichnisse stark zu reduzieren.

- Daher ergibt sich zusätzlich der Bedarf nach einem **Austauschdienst (AD):** Die Domänen, die entsprechenden Bedarf haben, sollen PKI-Informationen anderer Domänen importieren können. Dazu wird im Rahmen des Konzepts auch ein Austauschdienst für PKI-Informationen spezifiziert. Der Austauschdienst ist nur von den beteiligten Domänen, nicht aber von den Teilnehmern im Intranet zugreifbar. Er stellt die erforderlichen Informationen in einem von den Domänen zu verarbeitenden Format zur Verfügung.

Die folgende Abbildung stellt die Gesamtstruktur mit den drei benannten Diensten dar. Neben den Diensten sind auch die verschiedenen Prozesse dargestellt:

- der Aktualisierungsprozess von der Domäne zum Verzeichnisdienst der Verwaltung (1)
- der Aktualisierungsprozess von der Domäne zum Austauschdienst (2)
- der Abrufprozess von PKI-Informationen aus dem Verzeichnisdienst der Verwaltung bzw. dem Veröffentlichungsdienst (3)
- der Aktualisierungsprozess vom Austauschdienst zur Domäne (4)
- der Aktualisierungsprozess vom Verzeichnisdienst der Verwaltung zum Veröffentlichungsdienst (5)

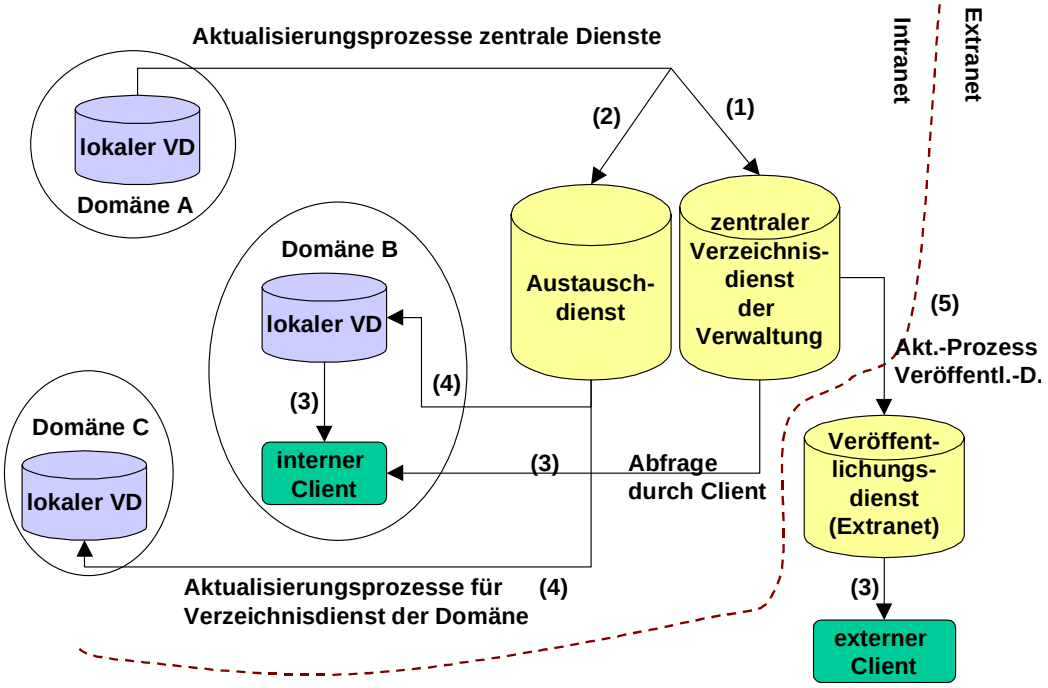

Abbildung 5: Grundstruktur der Prozesse im Verzeichnisdienstkonzept. Zur Vereinfachung steht Domäne A stellvertretend für alle Domänen, die Daten zuliefern, B und C stellvertretend für alle Domänen, die Daten nach intern replizieren. Jede Domäne kann beide "Rollen" innehaben.

Die genannten Dienste werden im weiteren auch als "Dienste des Verzeichnisdienstkonzepts" bezeichnet. Alle drei Dienste werden aus der Sicht des Verzeichnisdienstkonzepts als "Black Boxes" betrachtet, für die nur die Aspekte diskutiert werden, die für den Austausch und die Bereitstellung der PKI-Informationen relevant sind.

2.1.2 Umfang der ausgetauschten Daten

Im Rahmen der Ausbaustufe 1 des Verzeichnisdienstkonzepts wird nur der Austausch von Entries mit PKI-Informationen unterstützt. Dies sind Entries für

- Zertifizierungsstellen (CA),
- CRL Distribution Points (CDP),
- Teilnehmer-Entries mit Zertifikaten.

Für jede Art von Entries wird in der Schema-Definition festgelegt, welche Attribute enthalten sein müssen und welche Attribute enthalten sein dürfen.

Bei den meisten der heutigen E-Mail-Clients treten Probleme auf, wenn mehrere Zertifikate in einem **Teilnehmer-Entry** gespeichert sind und Clients daraus ein passendes auswählen sollen. Daher werden in der ersten Ausbaustufe nur Verschlüsselungszertifikate bereitgestellt. Verschlüsselungszertifikate sind Zertifikate, die zur Verschlüsselung von Mails oder Dateien geeignet sind. Dies schließt nicht aus, dass sie auch zur Prüfung von Signaturen verwendet werden können. Prinzipiell können in einem Directory-Entry mehrere Zertifikate bereitgestellt werden. Das Verzeichnisdienstkonzept wird jedoch so angelegt, dass in der ersten Ausbaustufe nur ein Verschlüsselungszertifikat je Teilnehmer-Entry in den Diensten des Verzeichnisdienstkonzepts bereitgestellt wird. Diese Entscheidung basiert auf dem Faktum, dass Signaturzertifikate gemäß S/MIME-Standard mit der E-Mail mitgeschickt werden. Darüber hinaus wird eine Konsistenz mit [ISIS-MTT Part 4] erreicht.

Für die **Entries von Zertifizierungsinstanzen** wird die Zahl der Zertifikate nicht limitiert. Der jeweils relevante Entry enthält alle CA-Zertifikate, die die Domäne, aus der der Entry stammt, bereitstellt. Im Entry wird nur die aktuellste Sperrliste abgelegt. Die Sperrlisten sind aus der Sicht des Verzeichnisdienstkonzepts nicht auf Verschlüsselungszertifikate beschränkt. Die Sperrlisten können daher auch von Anwendungen genutzt werden, die die zu prüfenden Zertifikate aus beliebigen Quellen erhalten, beispielsweise SSL-Zertifikate im Rahmen des Verbindungsaufbaus von SSL oder Signatur-Zertifikate aus einer E-Mail.

Welche Teilnehmer- und Zertifizierungsinstanz-Entries in den Verzeichnisdienst der Verwaltung oder den Veröffentlichungsdienst eingestellt bzw. über den Austauschdienst bereitgestellt werden, unterliegt grundsätzlich der Verantwortung und Entscheidung der Datenquelle, also der Domäne, die die CA betreibt und die Daten zum Austausch zur Verfügung stellt. Das Konzept stellt eine Möglichkeit bereit, mit der die Domäne steuern kann, welche Entries weitergegeben werden. Beispielsweise könnte ein Bundesministerium entscheiden, die Entries der Poststelle, der Pressestelle und einer Informationsstelle für den Veröffentlichungsdienst der PKI-1-Verwaltung bereitzustellen, die Entries von Mitarbeitern dagegen nur intern zugänglich zu machen.

2.2 Überblick über die technische Konzeption

Im Rahmen des technischen Konzepts muss festgelegt werden,

- wo die zugelieferten Entries mit PKI-Informationen im zentralen Verzeichnisdienst und im Austauschdienst gespeichert werden,
- welche Informationen in den relevanten Entries abzulegen sind,
- wie die Aktualisierungsprozesse von den Domänen zu den Diensten des Verzeichnisdienstkonzepts erfolgen,
- wie Teilnehmer die PKI-Informationen aus dem öffentlichen Verzeichnisdienst abfragen können und
- wie der Aktualisierungsprozess vom Austauschdienst in die lokalen Verzeichnisdienste der Domänen organisiert wird.

2.2.1 Namensregeln: Directory Information Tree

Jeder Entry, der in einem Directory gespeichert wird, hat als eindeutigen Schlüssel einen "Directory Namen", den sogenannten Distinguished Name (DN) (vgl. auch das einleitende Kapitel 1.2 mit detaillierteren Begriffsklärungen). Die Namen der Entries werden dabei hierarchisch organisiert; dadurch ergibt sich der sogenannte Directory Information Tree (DIT). Die Directory-Namen müssen

nicht identisch mit den Namen in den zugehörigen Zertifikate sein. Die im folgenden getroffenen Festlegungen gelten, sofern nicht ausdrücklich anders festgelegt, daher ausschließlich für den Namen im Verzeichnis und nicht für den Namen im Zertifikat. Zur besseren Unterscheidung wird der Directory-Name mit DIT-DN, der Name im Zertifikat mit Subject-DN bezeichnet.

Jede der an der PKI-1-Verwaltung beteiligten Domänen hat beim Aufbau ihres Verzeichnisdienstes die Struktur ihres DIT gemäß ihren eigenen Bedürfnissen festgelegt. Es ist daher davon auszugehen, dass die Domänen unterschiedliche DIT-Strukturen für die Teilnehmer-Entries verwenden.

Prozesse zur Pflege des Directories können auf die spezielle DIT-Struktur abgestimmt werden, beispielsweise die automatische Erzeugung neuer Entries durch ein Personalverwaltungssystem. Außerdem kann die Struktur zur Verwaltung von Zugriffsrechten genutzt werden, wenn z. B. nur Teilnehmer mit Einträgen in bestimmten Teilbäume Zugriff auf bestimmte Ressourcen erhalten. Entsprechend darf die Struktur des DITs der Domänen nicht grundlegend verändert werden.
Hinweis: die Vorgaben zur Bildung von DIT-DNs und Subject-DNs werden in [PKI1V Namensregeln] beschrieben. Sie sind verbindlich für alle Domänen.

Im Rahmen des Verzeichnisdienstkonzepts muss ein Weg gefunden werden, der trotz der unterschiedlichen Struktur der verschiedenen Domänen die Teilnehmereinträge in einer für alle zu verarbeitende Form bereitstellt. Als Lösung bietet sich an, für das Verzeichnisdienstkonzept einen speziellen Directory Information Tree zu definieren, den **Austausch-DIT**. Dieser wird nach sehr einfachen Namensregeln gestaltet sein, die über die Zeit nicht verändert werden müssen. Für die Teilnehmer-Entries jeder Domäne gibt es Regeln, nach denen die komplexeren DIT-Strukturen der Domänen auf den einfacheren Austausch-DIT abgebildet werden. Dabei wird der DIT in den Domänen nicht verändert.

Jede Domäne kann diesen Austausch-DIT als *zusätzlichen Teilbaum* in ihr bestehendes Directory integrieren und damit Daten fremder Domänen intern bereitstellen. Alle Daten, die vom Austauschdienst in den lokalen Verzeichnis-

dienst importieren werden sollen, können dann in diesem speziellen Teilbaum abgelegt werden. Werden neue Domänen integriert, können deren Daten ebenfalls in die bereits vorhandene Struktur des Austausch-DITs übernommen werden, auch wenn die neue Domäne intern eine andere DIT-Struktur verwendet.

Der Austausch-DIT beschreibt die DIT-Struktur für alle drei Dienste des Verzeichnisdienstkonzepts. Er ist hinsichtlich der Teilnehmer-Entries verbindlich für die drei Dienste des Verzeichnisdienstkonzepts. Er gilt auch für die Daten, die die Verzeichnisdienste der Domänen mit den Standardprozessen des Verzeichnisdienstkonzepts rück-importieren wollen.

Damit müssen alle beteiligten Verzeichnisdienste nur einmalig hinsichtlich der Struktur des Austausch-DITs erweitert werden. Die Aufnahme weiterer Domänen mit abweichenden Namensregeln verändert die Struktur des Austausch-DITs bezüglich der Teilnehmer-Entries nicht. Eine erneute Anpassung der Verzeichnisdienste in bereits teilnehmenden Domänen ist daher in Zukunft nicht erforderlich. Dieser Ansatz erlaubt außerdem eine Implementierung des Verzeichnisdienstkonzepts, ohne dass sich zukünftig teilnehmende Domänen bereits im Vorfeld auf abschließende Namensstrukturen festlegen müssen.

Der **Austausch-DIT-DN für Teilnehmer-Entries** wird auf eine einheitliche, flache Struktur reduziert, die nur die namensgebenden Attribute enthält, die in allen Domänen für alle Teilnehmer-Entries erwartet werden können. Die Struktur besteht aus dem Attribut c=de, aus einem o-Attribut, einem ou-Attribut und der E-Mail-Adresse. Der in Abbildung 6 dargestellte Domäneneintrag (linker Teilbaum) "*cn=Peter Müller, l=Berlin, ou=BMI, o=Bund, c=DE*" wird danach z. B. auf "*mail=Peter.Müller@bmi.bund.de, ou=BMI, o=Bund, c=DE*" verkürzt (Austausch-DIT in der Mitte).

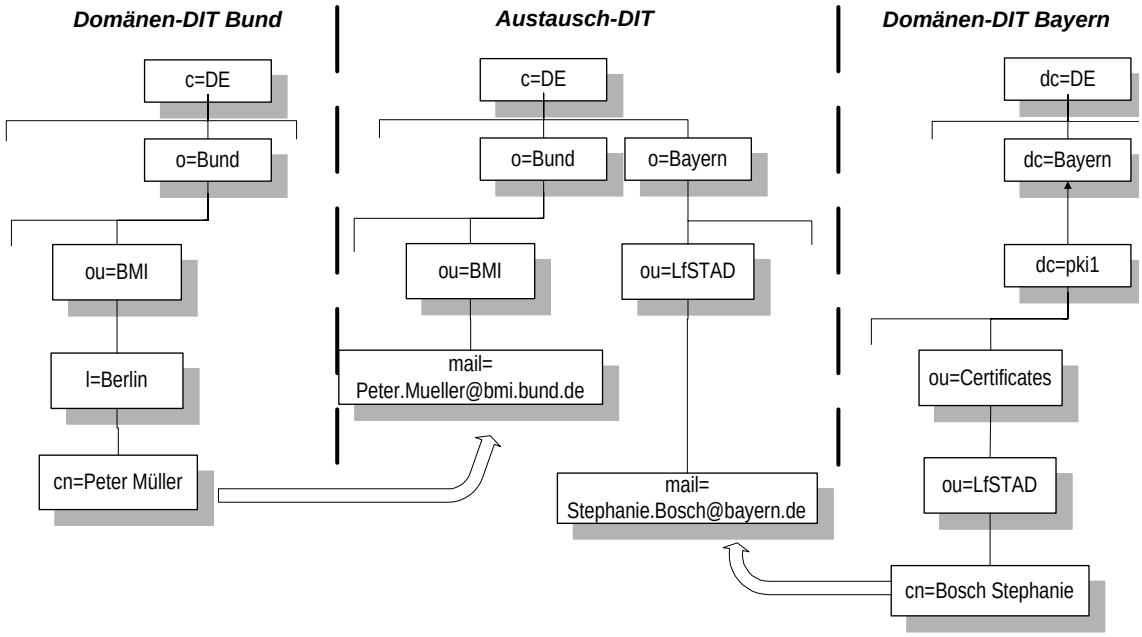

Abbildung 6: Umsetzung von Teilnehmer-Entries aus zwei Domänen (links und rechts) in den Austausch-DIT (Mitte) für Teilnehmer aus dem BMI und aus Bayern.

Trotz der Veränderung des DIT-DNs im Austausch-DIT ist die Suche nach den Teilnehmer-Einträgen weiterhin unverändert möglich. Denn dabei wird nach einzelnen Attributen gesucht, die im Entry enthalten sind, z. B. dem Nachnamen oder der E-Mail-Adresse. Eine Suche nach einem Teilnehmer-Entry mit Hilfe des vollständigen DIT-DN ist nicht zu erwarten. Deshalb kann der Distinguished Name im Austausch-DIT gegenüber dem in der zuliefernden Domäne verändert werden.

Für **Entries von Zertifizierungsinstanzen** ist eine Veränderung der DIT-DNs nicht sinnvoll. Zertifizierungsinstanzen werden in der Regel anhand ihres gesamten DIT-DNs gesucht, so dass Veränderungen des DIT-DNs dazu führen, dass die Zertifikate und Sperrlisten nicht mehr gefunden werden. Also muss auch bei der Umsetzung die Gleichheit von DIT-DN und Subject-DN erhalten bleiben; die Struktur des DIT-DN für CA-Entries muss in allen Verzeichnissen gleich sein.

Um trotzdem eine stabile Struktur für den Teilbaum der PKI-1-Verwaltung zu erhalten, müssen sich alle Domänen an die Namensregeln der PCA halten (siehe hierzu die jeweils aktuelle Version des Namenskonzepts der PKI-1-

Verwaltung). Dadurch wird auch für die Entries von CAs Stabilität der Namensregeln und damit die Vereinfachung der Konfiguration der Verzeichnisdienste erreicht.

Im Falle von abweichenden DIT-DNs im Verzeichnis einer Domäne liegt es in der Verantwortung der Domäne, die entsprechende Anpassung für den Austausch-DIT im Rahmen der Aktualisierungsprozesse vorzunehmen. Nur für Windows 2000-Systeme wird eine automatische Namensumsetzung angeboten.

2.2.2 Directory-Schema

Das Directory-Schema beschreibt mit den Objektklassen und Attribut-Typen, 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.

Das Schema der drei Dienste des Verzeichnisdienstkonzepts wird für PKI-Informationen nur Objektklassen nach [X.509 2001] verwenden. Für das Schema der Domänen ist eine strikte Orientierung an diesem Standard nicht erforderlich, da eine Umsetzung der Objektklassen im Rahmen der Aktualisierungsprozesse erfolgen kann. Domänen dürfen daher beliebige Objektklassen verwenden, sofern die Entries alle für die Umsetzung erforderlichen Attribute enthalten.

Zusätzlich müssen die Domänen Steuerungsattribute in ihr Directory-Schema aufnehmen, die die Auswahl der zu übertragenen Informationen steuern. Diese Attribute kennzeichnen, welche Entries im Rahmen der Aktualisierungsprozesse an die drei Dienste des Verzeichnisdienstkonzepts und andere Domänen weitergegeben werden sollen und welche Einträge in den Veröffentlichungsdienst eingestellt werden sollen.

Die Pflege dieser zusätzlichen Attribute ist Aufgabe der jeweiligen Domäne. Das Verzeichnisdienstkonzept trifft nur Annahmen zur erwarteten Semantik, den Wertebereichen und gegebenenfalls den zulässigen Formaten.

2.2.3 Aktualisierungsprozesse für die Dienste des VDKs

Wenn sich in einer Domäne PKI-relevante Daten ändern (z. B. ein neues Zertifikat ausgestellt wird oder eine neue Sperrliste erzeugt wird), muss dies in den Diensten des Verzeichnisdienstkonzepts nachgeführt werden. Die Aktualisierungsprozesse für den Verzeichnisdienst der Verwaltung und den Austauschdienst können relativ ähnlich implementiert werden. Sie werden deshalb hier zusammenfassend beschrieben.

Die Aktualisierungsprozesse für die drei Dienste des Verzeichnisdienstkonzepts müssen die Veränderungen in den lokalen Verzeichnisdiensten der Domänen in den drei Diensten nachführen können.

Es kann nicht vorausgesetzt werden, dass alle teilnehmenden Domänen einheitliche automatische Replikationsmechanismen unterstützen. Da jedoch vorausgesetzt werden kann, dass alle Verzeichnisdienste der Domänen LDAP unterstützen, verwenden die hier spezifizierten Aktualisierungsprozesse zwischen den Domänen und den Diensten des Verzeichnisdienstkonzepts eine standardisierte Dateischnittstelle im LDIF-Dateiformat [LDIF].

Die LDIF-Dateien mit den auszutauschenden Daten werden in den Domänen in regelmäßigen Abständen erzeugt. Sie enthalten alle veränderten Datensätze. Bei der Erzeugung werden bereits die notwendigen Umsetzungen auf den Austausch-DIT durchgeführt. Die LDIF-Datei wird dann zu den beiden Diensten im Intranet übertragen. Dort wird eine Überprüfung auf Korrektheit und Plausibilität durchgeführt. Schließlich werden die Daten in die beiden Dienste im Intranet eingestellt. Abbildung 7 zeigt die Struktur am Beispiel des Veröffentlichungsdienstes.

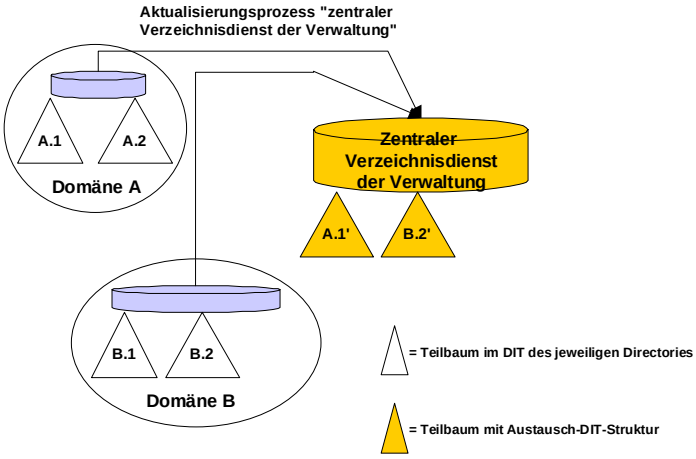

Abbildung 7: Im zentralen Verzeichnisdienst der Verwaltung werden ausgewählte Teilbäume der lokalen Directories bereitgestellt.

Aus **Performanzgründen** werden im Normalfall lediglich die Differenzen zur bereits ausgetauschten Datenbasis übertragen. Ein Mechanismus zum Vollabgleich erlaubt zusätzlich einen regelmäßigen Abgleich des Gesamtbestandes zur Löschung "toter" Entries und ein Wiederaufsetzen nach Störungen.

Um die **Skalierbarkeit** und **Flexibilität** zu verbessern, werden die Maßnahmen zur Umsetzung von Daten soweit wie möglich in der lokalen Domäne durchgeführt. Dadurch können Domänen, die von den Vorgaben abweichen, mit individuellen Anpassungen ebenfalls an den Aktualisierungsprozessen teilnehmen.

Die Aktualisierungsprozesse werden – in vereinfachter Darstellung – etwa wie folgt ablaufen:

- Zu einem durch den Aktualisierungsrhythmus bestimmten Zeitpunkt werden in der Domäne aus dem lokalen Verzeichnisdienst alle Entries per LDAP ausgelesen, die über die Kennzeichnung "relevant für Aktualisierungsprozess" verfügen und seit dem letzten Lauf verändert wurden.
- Die ausgelesenen Daten werden lokal für den Aktualisierungsprozess aufbereitet: Sofern erforderlich, werden Umsetzungen von Attribut-Typen vorgenommen oder von mehreren Zertifikaten die überflüssigen gelöscht. Die aufbereiteten Daten werden in einer LDIF-Datei abgelegt.
- In diesem Prozess-Schritt könnten auch die Löschbefehle für Entries ergänzt werden, sofern diese Informationen lokal verfügbar sind. Es muss in der

weiteren Analyse geklärt werden, mit welchen Mitteln die zu löschenden oder lokal bereits gelöschten Entries festgestellt werden können.

- Die LDIF-Datei wird über eine gesicherte Kommunikationsverbindung an den Betreiber des Verzeichnisdienstes der Verwaltung und des Austauschdienstes übermittelt. Die Übertragung wird immer von der Domäne initiiert ("Push-Konzept"), so dass die Domäne die volle Kontrolle über ihre Daten behält.
- Auf den beiden Diensten des Verzeichnisdienstkonzepts im Intranet der Verwaltung laufen kontinuierliche Prozesse, die den Eingang von LDIF-Dateien feststellen. Für den **Verzeichnisdienst der Verwaltung** wird die Datei auf Konsistenz geprüft und gegebenenfalls nachbereitet. Anschließend werden die enthaltenen Anweisungen abgearbeitet und die Entries im Verzeichnis des Veröffentlichungsdienstes eingetragen, aktualisiert oder gelöscht. Die geprüften Dateien werden außerdem im **Austauschdienst** bereitgestellt.

2.2.4 Abruf von Daten aus den Verzeichnisdiensten

Clients müssen Anfragen an den zentralen Verzeichnisdienst der Verwaltung und an den Veröffentlichungsdienst stellen, um Zertifikate und Sperrlisten zu erhalten. Es soll möglichst kein Änderungsbedarf an der Konfiguration der Clients für Zugriffe auf den Veröffentlichungsdienst entstehen, auch wenn im Laufe der Zeit aus technischen Gründen andere Server oder Maßnahmen zur Lastverteilung erforderlich werden. Dazu werden beide Dienste je einen eigenen dauerhaften DNS-Namen erhalten.

Auch die initiale Einrichtung soll möglichst wenig Zusatzkonfiguration auf Seiten der Clients erfordern. Daher erfordert der Zugriff nur solche Funktionalitäten, wie gängige Clients sie zur Verfügung stellen.

Deshalb werden der Verzeichnisdienst der Verwaltung und der Veröffentlichungsdienst per LDAP ansprechbar sein. Zusätzlich wird eine Abrufmöglichkeit über HTTP angeboten; dort werden allerdings nur CA-Zertifikate und Sperrlisten zur Verfügung gestellt, aber keine Teilnehmerzertifikate.

2.2.5 Aktualisierungsprozess für die Domänen

Die Verzeichnisdienste der Domänen sollen die Möglichkeit haben, PKI-Informationen aus anderen Domänen lokal bereitzustellen. Das heißt, dass im Verzeichnisdienst, den die Domäne lokal für ihre Teilnehmer benutzt, auch Einträge aus dem Austausch-DIT geladen werden. Damit eine Domäne dies mit Standardprozessen des Verzeichnisdienstkonzepts tun kann, muss sie in ihrem Verzeichnisdienst die Struktur des Austausch-DITs ergänzen. Sie kann dann die Ausschnitte des Austausch-DITs, die sie nach intern replizieren will, wählen. Die Änderungen in diesen Ausschnitten des Austausch-DITs werden dann regelmäßig im lokalen Verzeichnisdienst nachgeführt.

Die Differenzierung erfolgt nach Domäne und außerdem nach CA-Informationen und Teilnehmer-Informationen.

Die folgende Abbildung stellt grundsätzlich dar, welche Teilbäume ausgetauscht werden.

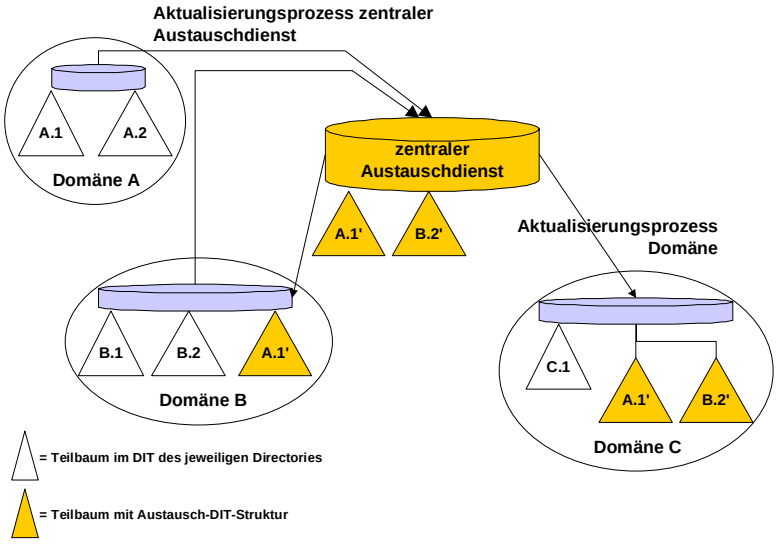

Abbildung 8: Grundsätzliche Funktionsweise der Aktualisierung der Domänen. A, B und C stehen stellvertretend für Domänen mit unterschiedlichen Profilen. Domäne C verwendet einen speziellen Zweig für den Import des Austausch-DIT.

Auch der Austausch von Daten zwischen dem Austauschdienst und den Verzeichnisdiensten der Domänen muss in einer generischen Lösung realisiert werden. Es gelten dieselben Überlegungen, die für die Aktualisierungsprozesse für die Dienste des Verzeichnisdienstkonzepts angestellt wurden. Deshalb wird

auch für diesen Aktualisierungsprozess LDIF als Übergabeformat für Daten gewählt. Eine Lösung des Aktualisierungsprozesses für Verzeichnisdienste von Domänen, der ebenfalls auf LDAP / LDIF basiert, weist zudem den Vorteil auf, dass innerhalb des Verzeichnisdienstkonzepts nur eine "Sprache" verwendet wird (vgl. auch [ISIS-MTT Part 4]).

Im Aktualisierungsprozess für die Domänen wird aus **Performanzgründen** ebenfalls nur die Differenzen zur bisherigen Datenbasis ausgetauscht. Ein zusätzlicher Vollabgleich ist optional möglich.

Die Namenswurzel einzelner Domänen ist unter Umständen inkompatibel zum Austausch-DIT. Zum Beispiel verwendet Bayern als Namenswurzel "dc=de", während der Austausch-DIT mit "c=de" beginnt. Um die **Flexibilität** der Standardprozesse zu erhöhen, könnte der in eine Domäne replizierte Ausschnitt des Austausch-DITs für Teilnehmer-Entries in einen besonderen Teilbaum des Domänen-Verzeichnisses verlegt werden (z. B. in Bayern nach "dc=Austausch-DIT, dc=de"). Die Maßnahmen zur Umsetzung werden in der Domäne lokal durchgeführt.

Aus den bisherigen Anforderungen und Festlegungen ergibt sich die folgende grobe Beschreibung der Aktualisierungsprozesse für die Verzeichnisdienste der Domänen nach dem Pull-Ansatz:

- Zu einem durch den Aktualisierungsrhythmus bestimmten Zeitpunkt versucht die Domäne, eine gesicherte Kommunikationsverbindung zum Austauschdienst aufzubauen. Gelingt dies, ruft sie den aktuellen Satz an Änderungsdaten im LDIF-Format ab, der lokal repliziert werden soll. Dieser Satz ist gegebenenfalls bereits geeignet nach dem Ausschnitt selektiert. Der Abruf erfolgt ausschließlich auf Initiative der Domäne ("Pull-Konzept").
- Die in den abgerufenen Dateien enthaltenen Anweisungen werden lokal abgearbeitet und die Entries im konfigurierten Ausschnitt des Austausch-DITs eingetragen, aktualisiert oder gelöscht. In diesem Prozess-Schritt könnten aus den übertragenen Daten Entries gezielt selektiert werden. Das Verzeichnisdienstkonzept wird nur einfache Basis-Regeln für diese Filterung anbieten.

Die Domänen können diese jedoch in eigener Verantwortung ergänzen. **Hinweis:** Die Entries der eigenen Teilnehmer und CAs, für die die Domäne die Pflegeverantwortung hat, werden durch diesen Aktualisierungsprozess nicht verändert.

- Der Aktualisierungsprozess muss sowohl die Frage der Löschung von Entries als auch das Problem von Verzeichnisdiensten mit abweichender Namenswurzel korrekt behandeln können.

2.2.6 Aktualisierungsprozess für den Veröffentlichungsdienst

Im Verzeichnisdienst der Verwaltung sind Entries mit einem Steuerattribut als "für den Veröffentlichungsdienst relevant" gekennzeichnet. Der Aktualisierungsprozess für den Veröffentlichungsdienst überträgt für diese Entries alle Veränderungen in den Veröffentlichungsdienst. Das zu verwendende Verfahren bestimmen die Betreiber der beiden betroffenen Dienste. Es muss dabei eine zeitnahe Replikation gewährleisten.

Teil II: DIT und Schema

3 Directory Information Tree

Dieses Kapitel stellt die Anforderungen an die Namensregeln in den Domänen, die Namensregeln im Austausch-DIT und den Umsetzungsprozess zwischen beiden dar. Die resultierenden Prozessspezifikationen finden sich zusammen mit der Umsetzung des Schemas im Anhang.

3.1 Anforderungen an Namensregeln in den Domänen

Die Namen **von CAs und CDPs im Domänen-Directory** müssen exakt den Namensregeln aus [PKI1V Namensregeln] folgen. Dies gilt auch für Windows 2000-PKIs, für die die zulässigen Ausnahmen ebenfalls in [PKI1V Namensregeln] festgelegt sind.

Wenn eine Domäne die Sonderregelung für Windows 2000-Systeme verwendet, so muss dies für CAs und CDPs der Fall sein. In diesem Fall muss der Aktualisierungsprozess zum VDV in der Domäne so konfiguriert werden, dass die entsprechende Umsetzung der Namenswurzel aktiviert wird, die der Aktualisierungsprozess zur Verfügung stellt.

Für die **Namen von Teilnehmern im Domänen-Directory** gelten ebenfalls die Vorgaben aus [PKI1V Namensregeln]. Durch die Konfigurationsmöglichkeiten des Aktualisierungsprozesses von der Domäne zum VDV wird allerdings eine hohe Flexibilität gewährleistet. Für die DIT-Umsetzung ist es außerdem erforderlich, dass eine E-Mail-Adresse im DIT-DN oder (bevorzugt) als Attribut im Entry vorhanden ist (zur Ablage der E-Mail-Adresse vgl. 4.1.2.4).

3.2 Der Austausch-DIT

Alle Dienste des VDKs verwenden die im Austausch-DIT festgelegten Namensregeln, die wie folgt definiert sind:

Für die **Namen von Entries von Zertifizierungsinstanzen im Austausch-DIT** wird festgelegt: Der DIT-DN aller CAs entspricht exakt dem Distinguished Name im "subject" des Zertifikats. Dies entspricht dem Standard X.509 und erlaubt Clients, nach Auswertung eines Zertifikats den Ausstellernamen aus dem Zertifikat (Issuer Distinguished Name) direkt für die Abfrage der Sperrliste aus dem Verzeichnis zu verwenden.

Damit gelten die Vorgaben zum Subject-DN in den Namensregeln der PCA auch für die DIT-DNs der CAs im Austausch-DIT.

Die **Entries für CRL Distribution Points im Austausch-DIT** werden unter der ausstellenden CA angeordnet. Für Windows 2000-Systeme wird eine entsprechende Umsetzung vorgenommen, die außerdem einen cn konstruiert, der aus dem Kürzel "CDP" und dem CA-Namen besteht.

Für die **Namen von Entries von Teilnehmern** wird festgelegt: Die Entries von Teilnehmern werden im Austausch-DIT direkt unterhalb der Institution eingeordnet, zu der sie gemäß ihrem regulären DIT-DN gehören. Als kennzeichnende Attribute werden c=de, ein o und ein ou verwendet. Als namensgebendes Attribut wird die E-Mail-Adresse verwendet, abgelegt im Attribut "mail". Damit ergibt sich folgende Struktur für den Teilnehmernamen:

- "mail=[E-Mail-Adresse], ou=[Institution], o=[Teilnehmer-Namensraum der Vertrags-CA], c=DE".

3.3 DIT-Umsetzung

Die folgenden Abschnitte beschreiben die konkreten Umsetzungsvorschriften vom Domänen-DIT in den Austausch-DIT für die verschiedenen Entry-Typen. Ausgangspunkt ist eine im Sinne der Namensregeln korrekte Namensvergabe in den Domänen.

3.3.1 DIT-DN-Umsetzung CA

Die hier beschriebene Umsetzung wird durchgeführt für alle Entries, die die Objektklasse des Prozess-Parameters *OC-CA* enthalten.

Wenn der Prozess-Parameter *Dir_Constraints* den Wert "none" enthält, es sich also um ein System in Standardkonfiguration handelt, wird ein im Sinne des Namenskonzepts gültiger DIT-DN der CA vorausgesetzt. Dieser wird unverändert in den A-DIT übernommen. (Fehler werden beim Hinzufügen des Entries zum VDV bemerkt, da dort eine Verletzung der A-DIT-Regeln auftritt. Daher erfolgt hier keine weitere Prüfung.)

Enthält der Parameter *Dir_Constraints* den Wert "Win2k", handelt es sich also um ein Windows 2000-System, erfolgt eine Umsetzung des CA-DIT-DNs. Es können nur solche CA-Entries umgesetzt werden, deren Namen den Namensregeln entsprechen. Die Umsetzung wird auf Basis des Parameters *CA_Subject_DN_root* durchgeführt, der die Wurzel des Subject-DN der CA angibt, und des CN der CAs:

- Die *CA_Subject_DN_root* bildet den obersten Teil des A-DIT-DNs der CA;
- er wird ergänzt um den untersten CN des CA-Entries im D-DIT.

Hinweis: In der Standardkonfiguration von Windows 2000 sind u.U. die CA-Entries mehrfach enthalten. Sofern dies der Fall ist, muss die Domäne mittels der Steuerattribute sicherstellen, dass nur *ein* Entry repliziert wird und dass dies der Entry mit den aktuellen Informationen ist. Werden mehrere Entries für eine CA mit demselben Subject-DN repliziert, so kann nicht beeinflusst werden, welcher dieser Entries letztlich in die Dienste des VDKs übertragen wird.

3.3.2 DIT-DN Umsetzung CDP

Die hier beschriebene Umsetzung wird durchgeführt für alle Entries, deren Objektklasse der im Parameter *OC_CDP* festgelegten Objektklasse entspricht.

Wenn der Prozess-Parameter *Dir_Constraints* den Wert "none" enthält, es sich also um ein System in Standardkonfiguration handelt, wird ein im Sinne der

Namensregeln gültiger DIT-DN des CDP vorausgesetzt. Daher erfolgt keine Umsetzung, sondern eine Übernahme des vorhandenen DIT-DN-Attributes. (Fehler werden beim Hinzufügen des Entries zum VDV bemerkt, da dort eine Verletzung der A-DIT-Regeln auftritt. Daher erfolgt hier keine weitere Prüfung.)

Enthält der Prozess-Parameter *Dir_Constraints* den Wert "Win2k", handelt es sich also um ein Windows 2000-System, erfolgt eine Umsetzung des CDP-DIT-DN. Es können nur solche CDP-Entries umgesetzt werden, die den Namensregeln entsprechen. Dann erfolgt die Umsetzung in die Struktur des A-DIT auf Basis des Parameters *CA_Subject_DN_root*, der die Wurzel des Subject-DN der CA angibt, und des CN des CDPs:

CA_Subject_DN_root bildet den obersten Teil des A-DIT-DN der CA; er wird ergänzt um den CN des CA-Entries im D-DIT (der identisch mit dem CN des CDP ist). Das unterste namensgebende Attribut bildet schließlich der CN des CDP, ergänzt durch ein vorangestelltes "CDP " (mit Leerzeichen).

3.3.3 DIT-DN-Umsetzung Teilnehmer

Für den DIT-DN der Teilnehmer in den Domänen gibt es keine direkten Vorgaben in den Namensregeln. Er muss lediglich die Attribute c=de, o, ou und cn enthalten. (Sind o, ou und cn nicht im DIT-DN enthalten, so können sie ersatzweise auch als einwertiges Attribut im Entry enthalten sein.)

Die Zielstruktur im A-DIT ist (vgl. 3.2):

- *c*=de
- *o*=[Organisation] (z. B. "Bund" oder "Thüringen" oder "Stadt Köln"[2])
- *ou*=[Organisationseinheit] (z. B. "BSI" oder "BMI" oder "Einwohnermeldeamt Stadt München")
- *mail* als namensgebendes Attribut.

2 Zur Namensgebung für Kommunen siehe die Alternativen in [PKI1V Namensregeln].

Die Konstruktion der Zielstruktur erfolgt in fünf Schritten: einer optionalen Vorbearbeitung zur Anpassung der Domänen-Struktur an die Vorgaben, der Konstruktion des c=de, der Konstruktion von o und ou und der Umsetzung der E-Mail-Adresse.

3.3.3.1 Vorbearbeitung

Bevor die Entries individuell umgesetzt werden, wird eine Umsetzung der Namens-Wurzel durchgeführt. Dabei wird für alle Entries vom Typ der im Parameter *OC_Person* festgelegten Objektklasse die im Prozess-Parameter *EE_D-DIT-Naming-ROOT* festgelegte Namenswurzel durch *EE_A-DIT_Naming_ROOT* ersetzt.

Dies ermöglicht eine komfortable Umsetzung von nicht der Norm entsprechenden Namenswurzeln (z. B. ein "dc=de" Knoten wie bei Windows 2000). Die Umsetzung kann von der Domäne konfiguriert werden, ist aber insofern verpflichtend, als dass nach der Umsetzung die Teilnehmer-Entries die zu Beginn genannten Rahmenbedingungen in jedem Fall erfüllen müssen. Hier erfolgt keine separate Behandlung von Windows 2000-Systeme.

3.3.3.2 C im TN-A-DIT-DN

Die Konstruktion wird in folgenden Schritten durchgeführt:

- Ein c=de wird in den A-DIT übernommen.
- Wenn im DN kein c enthalten ist oder es anders als mit de belegt ist, wird die Verarbeitung dieses Entries mit einem Fehler abgebrochen.

3.3.3.3 O im TN-A-DIT-DN

Die Konstruktion wird in folgenden Schritten durchgeführt:

- Aus dem D-DIT-DN wird das höchste o übertragen, da anzunehmen ist, dass es die charakterisierende Einheit darstellt.
- Wenn im DN kein o enthalten ist, aber ein singlevalued o-Attribut Bestandteil des Entry ist, wird statt dessen dieses umgesetzt.

- Ist dies nicht der Fall, so wird die Verarbeitung dieses Entries mit einem Fehler abgebrochen.

3.3.3.4 OU im TN-A-DIT-DN

Die Konstruktion wird in folgenden Schritten durchgeführt:

- Aus dem D-DIT-DN wird das ou mit der im Parameter *rank_D-DIT-ou_for_A-DIT* bezeichneten Nummer übertragen. Damit ist es möglich, in den Domänen verwendete administrative ou's auszulassen und das charakterisierende ou (im allgemeinen ein Behördenkürzel) zu verwenden.
- Wenn der D-DIT-DN kein ou enthält, aber ein singlevalued ou-Attribut im Entry enthalten ist, wird der Wert des Attributs verwendet.
- Trifft keiner dieser Fälle zu, wird die Verarbeitung dieses Entries mit einem Fehler abgebrochen.

3.3.3.5 mail im TN-A-DIT-DN

Für die Konstruktion des mail-Attributes kann vorausgesetzt werden, dass mindestens eines der möglichen Quell-Attribute einwertig ist (vgl. Anforderungen an die Domänen zum Directory-Schema im Kapitel 4.1.2.4).

Die Konstruktion des mail-Attributes im A-DIT-DN wird in folgenden Schritten durchgeführt:

- Der Wert für mail wird aus dem im Parameter *AT_userEMail* konfigurierbaren Attribut des D-DIT-Teilnehmer-Entries entnommen. Dieses Attribut muss im D-DIT einwertig sein.
- Ist der Parameter konfiguriert, das Attribut aber leer, mehrwertig oder nicht vorhanden, wird ein Fehler erzeugt.
- Ist der Parameter leer, so werden zuerst die D-DIT-Entry-Attribute "mail", "email", "rfc822", "emailaddress" und dann die D-DIT-DN-Attribute "mail", "email", "rfc822", "emailaddress" in dieser Reihenfolge ausgewertet und der Wert des ersten nichtleeren, einwertigen Attributes übernommen.

- Kann so keine E-Mail-Adresse identifiziert werden, wird ein Fehler ausgegeben.

4 Directory-Schema

In diesem Kapitel werden die Schema-Anforderungen für die Domäne, das Schema des Austausch-DITs und die Umsetzung von Attributen im Rahmen des Aktualisierungsprozesses zum VDV beschrieben.

4.1 Schema-Anforderungen an die Domänen

4.1.1 Objektklassen

Hinsichtlich der in den Domänen für CAs, CDPs und Teilnehmer verwendeten Objektklassen bestehen keine Einschränkungen. Es wird allerdings empfohlen, für alle Entries eines Typs dieselbe Objektklasse zu verwenden. Dadurch kann der Konfigurationsaufwand gering gehalten werden.

Die verwendeten Objektklassen können im Prozess konfiguriert werden (in den Parametern *OC_CA*, *OC_CDP* und *OC_Person*). Sie werden auf die entsprechenden Objektklassen des A-DIT umgesetzt.

In der ersten Ausbaustufe erfolgt im Verzeichnisdienstkonzept keine Unterscheidung verschiedener Teilnehmertypen (z. B. Gruppen und Dienste). Verwendet eine Domäne mehrere Objektklassen, kann sie entweder in einem eigenen, lokal spezifischen Preprocessing-Schritt eine Anpassung vornehmen oder die Aktualisierungsprozesse mit verschiedenen Konfigurationen mehrfach starten.

4.1.2 Erforderliche Attributtypen

Die Identifikation der zu übertragenden Daten erfolgt anhand der Namen der Attribute. Dabei sind einige der Namen durch Prozessparameter konfigurierbar, um möglichst einfache Anpassungen an die Gegebenheiten in den Domänen zu ermöglichen. Bei anderen werden die gängigen Standards vorausgesetzt.

Ob die in den folgenden Abschnitten genannten Attribute eingerichtet werden müssen oder ob die Verwendung bereits existierender Attribute möglich ist,

muss im Einzelfall überprüft werden. Ziel des Designs war es jedoch, die erforderlichen Anpassungen so klein wie möglich zu halten.

4.1.2.1 Steuerattribute

Im D-DIT müssen in jedem auszutauschenden Entry drei Steuerattribute zur Steuerung des Aktualisierungsprozesses vorhanden sein (Name und Wertebereich sind konfigurierbar):

- Ein Attribut, das angibt, ob ein Entry im VDV und im Austauschdienst veröffentlicht werden soll. Der Name des Attributes wird im Parameter *AT_VDV_visible* angegeben, der Wert, der die auszutauschenden Entries kennzeichnet, im Parameter *Val_VDV_visible.* Dieses Attribut wird zur Auswahl der Entries ausgewertet, aber nicht in den A-DIT übertragen.
- Ein Attribut, das angibt, ob ein Entry im Veröffentlichungsdienst veröffentlicht werden soll. Der Name des Attributes wird im Parameter *AT_VoeD_visible* angegeben, der Wert (bzw. eine Wertliste), der den Austausch kennzeichnet, im Parameter *Val_VoeD_visible.* Dieses Attribut wird auf das A-DIT-Attribut publicVisible umgesetzt. (**Hinweis:** Durch die Konfigurationsmöglichkeiten kann das gleiche Attribut wie für den Austausch zum VDV mit anderem Wert verwendet werden.)
- Ein Attribut, das das Datum der letzen Veränderung enthält. Der Name des Attributes wird im Parameter *AT_LastModified* konfiguriert; das Attribut wird in den A-DIT umgesetzt. Die Festlegung des genauen Zeitformates erfolgt in der Implementierungsphase.
- Ein Attribut, das angibt, wer bei Problemen und Störfällen informiert werden muss. Der Name des Attributes wird im Parameter *AT_internalNotification* festgelegt. Als Werte sind die in Kapitel 4.2.1.1 für das Attribut vDKInternalNotification festgelegten zulässig.

4.1.2.2 Attributtypen CA-Entry

Unabhängig von ihrer Objektklasse muss jeder CA-Entry im D-DIT über die folgenden Attribute verfügen und diese auch zur Ablage der entsprechenden Informationen nutzen (eine Umsetzung von Attributen mit anderen Namen erfolgt nicht):

- commonName,
- alle Attribute der Objektklasse pkiCA,
- die Steuerattribute wie in 4.1.2.1 definiert.

4.1.2.3 Attributtypen CDP-Entry

Unabhängig von ihrer Objektklasse muss jeder CDP-Entry über die folgenden Attribute verfügen und diese auch zur Ablage der entsprechenden Informationen nutzen (eine Umsetzung von Attributen mit anderen Namen erfolgt nicht):

- alle Attribute der Objektklasse cRLDistributionPoint,
- Steuerattribute wie in 4.1.2.1 definiert.

4.1.2.4 Zwingende Attributtypen im TN-Entry

Unabhängig von ihrer Objektklasse muss jeder Teilnehmer-Entry im D-DIT über die folgenden Attribute verfügen und diese auch zur Ablage der entsprechenden Informationen nutzen:

- cn
- Falls der Parameter *AT_userEMail* nicht leer ist, muss das definierte Attribut vorhanden sein und genau einen Wert enthalten.
  Ist der Parameter leer, muss mindestens eines der Attribute email, mail, rfc822 oder emailaddress vorhanden und einwertig sein. Wenn diese Attribute alle leer oder mehrwertig sind, werden statt dessen die Attribute email, mail, rfc822 oder emailaddress aus dem D-DIT-DN verwendet; insofern muss dann mindestens eines davon vorhanden sein.

- Steuerattribute wie in 4.1.2.1 definiert.

Sollten in einer Domäne mehrere Teilnehmer mit derselben E-Mail-Adresse geführt werden, muss die Domäne sicherstellen, dass jeweils nur einer dieser Entries in die Dienste des VDKs übertragen wird.

4.1.2.5 Optionale Attributtypen im TN-Entry

Neben den in Kapitel 4.1.2.4 genannten verpflichtenden Attributen werden auch die folgenden Attribute aus dem D-DIT übertragen, sofern sie vorhanden sind:

o, ou, cn, gn, sn, l (locality), c, serialNumber[3], ein Attribut zur Ablage des Benutzerzertifikates wie im Parameter *AT_userCertificate* konfiguriert.

Alle Attribute außer *AT_userCertificate* dürfen mehrwertig sein.

Eine Überprüfung der Einwertigkeit von *AT_userCertificate* erfolgt nicht. Es ist jedoch damit zu rechnen, dass ein störungsfreier Abruf der Zertifikate nicht möglich ist, wenn mehrere Zertifikate für einen Teilnehmer-Entry in die Dienste des VDKs übertragen werden.

4.1.3 Weitere Anforderungen

- Die Verzeichnisdienste müssen UTF8/Unicode unterstützen.
- Alle PKI-Informationen müssen im binary-Format codiert werden.

4.2 Schema des Austausch-DITs

Im Schema des A-DIT gibt es drei Typen von Entries: die CA-Entries, die CDP-Entries und die Teilnehmer-Entries.

Implementierungshinweis:
Das Schema aus dem A-DIT kann identisch für alle Dienste des VDKs verwendet werden. Die Steuerungsattribute des Verzeichnisdienstkonzepts dürfen bei anonymen Anfragen an den VDV und den Veröffentlichungsdienst nicht sichtbar

[3] wie in ISIS-MTT, eine Umsetzung von anderen Attributen erfolgt nicht.

sein. Details der Zugriffsregeln sind im Rahmen der Implementierung festzulegen.

4.2.1 Zu definierende Objektklassen

Um eine strukturierte Schema-Definition der unterschiedlichen Typen von Entries zu unterstützen, werden zwei VDV-spezifische Objektklassen definiert.

4.2.1.1 Objektklasse für Steuerattribute

Die Hilfsklasse vDKControl dient zur Ablage der Steuerinformationen. Sie ist Bestandteil aller Entries im A-DIT. Sie enthält vier optionale Steuerattribute:

- vDKVoeDPublicVisible steuert, ob der Entry auch im Veröffentlichungsdienst oder nur im VDV und im Austauschdienst geführt wird. (Wert ist TRUE, wenn der Entry im Veröffentlichungsdienst veröffentlicht werden soll, sonst FALSE.)
- vDKLastModifiedSource gibt das Datum der letzten Änderung der Quelldomäne an. (Das endgültige Zeitformat muss im Rahmen der Implementierung festgelegt werden.)
- vDKActiveIndicator gibt das Datum des letzten Vollabgleichs an, in dem der Entry enthalten war. (Das endgültige Zeitformat muss im Rahmen der Implementierung festgelegt werden.) Es wird vom Aktualisierungsprozess gesetzt.
- vDKInternalNotification kennzeichnet die Einträge, an deren E-Mail-Adresse Status- und Informationsmeldungen hinsichtlich des Betriebs des VDKs gesendet werden sollen. Das Attribut kann mehrwertig sein. Dabei bilden die verschiedenen Werte ab, welche Funktion der Inhaber des Entries bei der Administration und Störungsbehebung innerhalb des VDKs hat. Folgende Werte sind möglich (neben "Leer" und "False"):
  - "Administrator": An diese E-Mail-Adressen werden Statusmeldungen gesendet, die keine Antwort erfordern, z. B. Informationen über Wartungsintervalle bei beteiligten Diensten.

- "Support": An diese Adressen werden Hinweise zum Betrieb des VDKs gesendet, die eine Reaktion erfordern, aber nicht dringend sind.
- "Problem": An diese Adressen werden Nachrichten gesendet, die eine baldige Reaktion erfordern.
- "Emergency": An diese Adressen werden Nachrichten gesendet, die eine sofortige Reaktion erfordern.

4.2.1.2 Objektklasse für Teilnehmer-Entries

Für die Teilnehmer-Entries im A-DIT wird eine strukturelle Klasse vDKPerson eingerichtet.

Sie enthält zwingend die Attribute cn und mail.

Optional sind die Attribute o, ou, gn, sn, l (locality), c, serialNumber. Alle optionalen Attribute sind mehrwertig.

4.2.2 Schemata

4.2.2.1 Schema für CA-Entries

Für die CA-Entries wird im A-DIT folgendes Schema verwendet:

- Strukturelle Objektklasse:
  - organizationalRole
- Hilfsobjektklassen:
  - pKICA (für Zertifikate und Sperrlisten)
  - vDKControl (für Steuerattribute)

4.2.2.2 Schema für CDP- Entries

Für die CDP-Entries wird im A-DIT folgendes Schema verwendet:

- Strukturelle Objektklasse:
  - cRLDistributionPoint

- Hilfsobjektklasse:
  - vDKControl (für Steuerattribute)

4.2.2.3 Schema für Teilnehmer-Entries

Für die Teilnehmer-Entries wird im A-DIT folgendes Schema verwendet:

- Strukturelle Objektklasse:
  - vDKPerson
- Hilfsobjektklassen
  - pKIUser (für Zertifikate)
  - vDKControl (für Steuerattribute)

4.3 Umsetzung der Objektklassen und Attributnamen

4.3.1 Umsetzung Steuerattribute

Das Attribut *vDK-VoeD-publicVisible* im A-DIT erhält den Wert TRUE genau dann, wenn in dem durch *AT_VoeD_visible* bezeichneten Attribut ein Wert der in *Val_VoeD_visible* gespeicherten Liste enthalten ist. Andernfalls wird es auf FALSE gesetzt.

Der Inhalt des durch *AT_LastModified* bezeichneten Attributs wird in das Attribut vDKLastModifiedSource übertragen. (Ob eine Konvertierung des Formates erforderlich ist, muss im Rahmen der Implementierung geklärt werden.)

Der Inhalt des durch *AT_internalNotification* bezeichneten Attributs im D-DIT wird in das Attribut vDKLastModifiedSource im A-DIT übertragen.

4.3.2 Umsetzung CA-Entries

Die CA-Entries werden auf die Objektklasse organizationalRole umgesetzt. Dabei werden ihr commonName und die zu pkiCA gehörenden Attribute übertragen.

Zusätzlich erfolgt die Umsetzung der Steuerattribute.

4.3.3 Umsetzung CDP-Entries

Die CDP-Entries werden auf die Objektklasse cRLDistributionPoint umgesetzt. Dabei werden ihr commonName und die zur Klasse gehörenden Attribute übertragen.

Zusätzlich erfolgt eine Umsetzung der Steuerattribute.

Hinweis: Im Falle von absoluten CDP-Adressen mit Angabe des Servers kann der "richtige" Ziel-Entry im Veröffentlichungsdienst liegen. Zur Vereinfachung der Prozesse werden auch solche Entries immer zuerst in den VDV repliziert, auch wenn sie von dort nicht ausgelesen werden.

4.3.4 Umsetzung Teilnehmer-Entries

Die Teilnehmer-Entries werden auf die Objektklasse VDV-Person umgesetzt. Dabei werden alle vorhandenen Attribute übernommen, sofern sie im Schema des A-DIT vorhanden sind.

Zusätzlich erfolgt eine Umsetzung der Steuerattribute.

4.4 Umsetzung Attributwerte

In einem letzten Schritt werden schließlich die Werte der Attribute kontrolliert, geändert und ergänzt.

4.4.1 CAs und CDPs

Hier müssen für Standardsysteme keine Änderungen durchgeführt werden. Für Windows 2000-Systeme wird der DIT-DN umgesetzt.

Es wird außerdem überprüft, ob

- in CA-Entries eine Sperrliste und ein Zertifikat enthalten sind und
- in CDP-Entries eine Sperrliste enthalten ist.

Ist dies nicht der Fall, wird eine Warnung ausgegeben.

4.4.2 Teilnehmer

Bei den Teilnehmer-Entries sind folgende Schritte zur Wertumsetzung erforderlich:

- DIT-Umsetzung: Das DN-Attribut im A-DIT-Entry wird gemäß den definierten Regeln aus Kapitel 4 konstruiert und in den A-DIT-Entry eingefügt.
- Bis auf die E-Mail-Adresse werden alle Attribute aus dem Entry, die im Schema des A-DIT-Teilnehmer-Entry vorhanden sind, in den A-DIT-Entry übertragen. Dabei können alle Attribute außer dem cn und dem das Zertifikat enthaltene Attribut mehrwertig sein. (Kontrolle erfolgt nur für den cn.)
- Das für den A-DIT-DN konstruierte mail-Attribut wird in den neuen Entry übertragen.
- Ergänzung weiterer Attributwerte aus A-DIT-DN und D-DIT-DN:
  - Alle Attribute, die eine E-Mail-Adresse enthalten (*mail, email, rfc822, emailaddress, AT_userEMail*), werden ignoriert.
  - Alle Attribute, die nicht im Schema des A-DIT enthalten sind, werden nicht berücksichtigt.
  - Der cn aus dem D-DIT-DN wird in das passende Attribut des A-DIT-Entries übertragen. Dabei wird ein ggf. schon durch die Attributumsetzung erzeugter Eintrag überschrieben (der Wert aus dem D-DIT-DN hat also Vorrang). Konnte weder bei der Attributumsetzung noch aus dem D-DIT-DN ein cn ermittelt werden, erfolgt ein Abbruch mit Fehlermeldung (Verletzung der Namensregeln).
  - Alle weiteren Attribute, die im A-DIT-DN oder im D-DIT-DN enthaltenen sind, werden in den Entry geschrieben. Dabei werden Attribute bei Bedarf mehrwertig gesetzt. Es wird außerdem überprüft, dass nicht mehrere gleiche Attribute mit demselben Inhalt im Entry entstehen.

Teil III: Aktualisierungsprozesse

Dieser Teil des Dokumentes stellt die fünf Prozesse des Verzeichnisdienstkonzepts (die Nummern verweisen auf Abbildung 9) dar:

- den Aktualisierungsprozess von der Domäne zum Verzeichnisdienst der Verwaltung (1)
- den Aktualisierungsprozess von der Domäne zum Austauschdienst (2)
- den Abrufprozess von PKI-Informationen aus dem Verzeichnisdienst der Verwaltung bzw. dem Veröffentlichungsdienst (3)
- den Aktualisierungsprozess vom Austauschdienst zur Domäne (4)
- den Aktualisierungsprozess vom Verzeichnisdienst der Verwaltung zum Veröffentlichungsdienst (5)

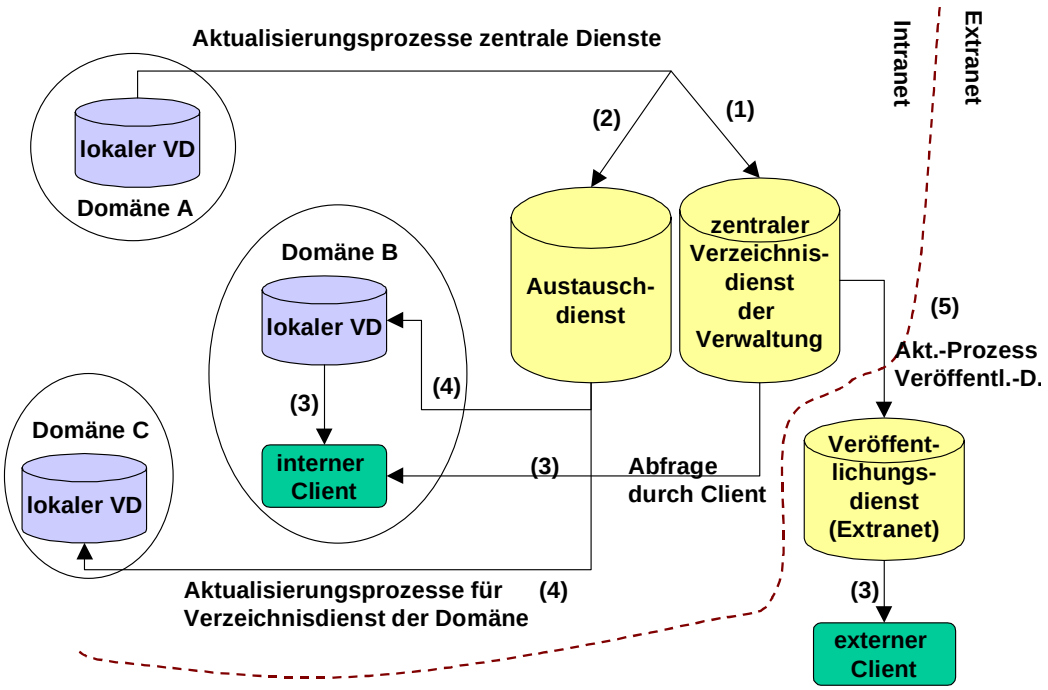

Abbildung 9: Grundstruktur der Prozesse im Verzeichnisdienstkonzept. Zur Vereinfachung steht Domäne A stellvertretend für alle Domänen, die Daten zuliefern, und die Domänen C und D stellvertretend für alle Domänen, die Daten nach intern replizieren. Jede Domäne kann beide "Rollen" innehaben.

Abbildung 9 stellt die Aktualisierungs- und Abrufprozesse in einer logischen Sicht dar. Die physische Realisierung kann davon abweichen, beispielsweise

weil zwischen dem Intranet des IVBB und dem Intranet von TESTA D eine gewisse Überlappung besteht.

Das Verzeichnisdienstkonzept wird für die Aktualisierungsprozesse von der Metapher der "Produkt-Idee" geleitet: Jede Domäne kann eine bereitgestellte Sammlung von fertig implementierten Prozessen installieren (das "Produkt"). Wenn Mindest-Voraussetzungen im lokalen Verzeichnisdienst erfüllt sind, müssen die Prozesse nur noch korrekt konfiguriert werden, um an den Diensten des Verzeichnisdienstkonzepts der PKI-1-Verwaltung teilnehmen zu können.

5 Allgemeine Rahmenbedingungen der Prozesse

5.1 Service-Qualität

Die Service-Qualität der Dienste des Verzeichnisdienstkonzepts kann anhand der Faktoren Verfügbarkeit und Datenqualität definiert werden:

Verfügbarkeit: Es wird erwartet, dass der Verzeichnisdienst der Verwaltung, der Austauschdienst und der Veröffentlichungsdienst eine sehr hohe Verfügbarkeit erreichen. Die Dienste des Verzeichnisdienstkonzepts sollen eine Verfügbarkeit von 99,7 % erreichen (etwa 26,5 Stunden Gesamtausfallzeit/Jahr). Einzelne Störfälle dieser Dienste müssen innerhalb von 4 Stunden beherrscht werden. Der / die Betreiber der Dienste haben entsprechende technische und organisatorische Vorsorge zu treffen, z. B. Redundanz von Komponenten, Bereitstellung von Eskalationswegen und Verfügbarkeit von Personal. Im Rahmen der Implementierung sind die Details der Verfügbarkeitsanforderungen zu klären, beispielsweise, auf welche Weise Wartungszeiträume zu werten sind.

Datenqualität: Die Datenqualität bestimmt sich aus der Übereinstimmung der Daten in den Diensten des Verzeichnisdienstkonzepts mit denen aus den Verzeichnisdiensten der zuliefernden Domänen. Die Verantwortung für die Bereitstellung der Aktualisierungsdaten und den Betrieb der Anteile der Aktualisierungsprozesse innerhalb der Domänen liegt vollständig bei den Domänen.

Die Datenqualität wird beeinflusst von den zeitlichen Verzögerungen und von möglichen Störungen in den Aktualisierungsprozessen. Für die Ausbaustufe 1 sollen die Ziele der folgenden Tabelle bezüglich der Datenqualität erreicht werden. Sie berücksichtigen die Bedeutung der jeweiligen Entries. Außerdem wird angenommen, dass die Maßnahmen des Verzeichnisdienstkonzepts zur Erreichung einer hohen Datenqualität nicht wesentlich über den Maßnahmen liegen sollen, die im allgemeinen von den Domänen erwartet werden können. (**Hinweis:** Die in der Tabelle geforderte Datenqualität impliziert organisatorische Maßnahmen beim Betreiber der Dienste des Verzeichnisdienstkonzepts und bei

den Domänen, um die Überwachung der Prozesse und die notwendigen Reaktionszeiten zu erreichen)

Typ der Aktualisierung	Verzögerung im Verzeichnisdienst der Verwaltung und Austauschdienst gegenüber Verzeichnisdienst der Domäne	Verzögerung im Veröffentlichungsdienst gegenüber Verzeichnisdienst der Domäne
CA- und CDP-Entries anlegen oder aktualisieren	**im Normalbetrieb:** max. 60 Minuten Verzögerung (30 Minuten für die Übertragung von der Domäne zum VDV, 30 Minuten zum Einstellen) **bei leichten Störfällen** (z. B. Ausfall einer Komponente): werktags max. 12 Stunden Verzögerung **bei schweren Störfällen** (z. B. Ausfall mehrerer Komponenten)**:** keine Zusicherung. Das Verzeichnisdienstkonzept bietet aber Rückfallmöglichkeiten zur bilateralen Überbrückung.	**im Normalbetrieb:** max. 90 Minuten Verzögerung (30 Minuten für die Übertragung von der Domäne zum VDV, 30 Minuten vom VDV zum Veröffentlichungsdienst, 30 Minuten zum Einstellen) **bei leichten Störfällen:** (z. B. Ausfall einer Komponente): werktags max. 12 Stunden Verzögerung **bei schweren Störfällen:** keine Zusicherung.
Teilnehmer-Entries anlegen oder aktualisieren	**im Normalbetrieb:** max. 25 Stunden Verzögerung (Replikation einmal täglich, 30 Minuten für die Übertragung von der Domäne zum VDV, 30 Minuten zum Einstellen) **bei leichten Störfällen** (z. B. Ausfall einer Komponente): werktags max. 48 Stunden Verzögerung **bei schweren Störfällen** (z. B. Ausfall mehrerer Komponenten)**:** keine Zusicherung. Das Verzeichnisdienstkonzept bietet aber Rückfallmöglichkeiten zur bilateralen Überbrückung.	**im Normalbetrieb:** max. 26 Stunden Verzögerung (Replikation einmal täglich, 30 Minuten für die Übertragung von der Domäne zum VDV, 30 Minuten zum Einstellen) **bei leichten Störfällen** (z. B. Ausfall einer Komponente): werktags max. 48 Stunden Verzögerung **bei schweren Störfällen** (z. B. Ausfall mehrerer Komponenten)**:** keine Zusicherung. Das Verzeichnisdienstkonzept bietet aber Rückfallmöglichkeiten zur bilateralen Überbrückung.
Löschen von Teilnehmer-Entries	**im Normalbetrieb:** max. 32 Tage Verzögerung (Replikation mindestens einmal je Monat über Vollabgleich)	Wie VDV wegen 1:1-Replikation
Löschen von CA- und CDP-Entries	keine Zusicherung, da manueller Prozess	keine Zusicherung, da manueller Prozess

Tabelle 5: Zielsetzung für die Datenqualität in der Ausbaustufe 1 des Verzeichnisdienstkonzepts

Die in der Tabelle vorgeschlagenen Werte sind im Rahmen der Realisierung mit den Betreibern der Dienste des VDKs abzustimmen und zu vereinbaren. Soweit sie die Prozesse der Domänen betreffen, sind sie als Richtlinien zu verstehen. Die Domänen sind aber uneingeschränkt für die Bereitstellung der Daten verantwortlich.

5.2 Implementierungsplattformen

Die Aktualisierungsprozesse werden so implementiert, dass sie plattformübergreifend unter Unix, Windows NT und Windows 2000 lauffähig sind ("Produkt-Idee").

6 Aktualisierung Verzeichnisdienst der Verwaltung

Der Verzeichnisdienst der Verwaltung ist der Dienst, mit dem die PKI-1-Verwaltung PKI-Informationen für alle Teilnehmer zur Verfügung stellt, die auf das Intranet der Behörden zugreifen können. Der Aktualisierungsprozess von der Domäne zum Verzeichnisdienst der Verwaltung dient dazu, Änderungen in Entries der teilnehmenden Domänen in den VDV zu übertragen.

6.1 Übersicht

Wenn sich in einer Domäne PKI-relevante Daten ändern (z. B. ein neues Zertifikat ausgestellt wird oder eine neue Sperrliste erzeugt wird), muss dies in den Diensten des Verzeichnisdienstkonzepts nachgeführt werden. Der Aktualisierungsprozess für den Verzeichnisdienst der Verwaltung unterstützt dabei die in der folgenden Tabelle aufgeführten Veränderungen. Angegeben sind jeweils die Veränderungen von Daten in einer Domäne und der daraus resultierende Vorgang im Verzeichnisdienst der Verwaltung.

Veränderung in der Domäne (Ursache)	Aufgabe des Aktualisierungsprozesses (Aktualisierung im VDV)
Neuer Entry für einen PKI-Teilnehmer oder eine CA im Verzeichnisdienst einer Domäne, der veröffentlicht bzw. ausgetauscht werden soll	Anlegen des Entries in den Diensten des Verzeichnisdienstkonzepts.
Wechsel von Verschlüsselungszertifikaten, CA-Zertifikaten, Sperrlisten oder anderen Attributwerten im Entry des Verzeichnisdienstes für die Domäne	Änderung des Zertifikats, der Sperrlisten oder anderer Attributwerte in den Diensten des Verzeichnisdienstkonzepts.
Löschen eines Zertifikats im Verzeichnisdienst der Domäne	Löschen des Zertifikats in den Diensten des Verzeichnisdienstkonzepts.
Löschen eines Entries in einer Domäne, der in die Diensten des Verzeichnisdienstkonzepts repliziert wurde	Löschen des entsprechenden Entries in den Diensten des Verzeichnisdienstkonzepts.

Tabelle 6: Aufgaben der Aktualisierungsprozesse für die Dienste des Verzeichnisdienstkonzepts

Die Domänen verwenden eigene Verzeichnisdienste, die aus unterschiedlichen Gründen verschieden aufgebaut sind. Da innerhalb der Dienste des Verzeichnisdienstkonzepts trotzdem eine einheitliche Struktur – der Austausch-DIT - verwendet wird, müssen die Daten der Domänen daher so aufbereitet werden,

dass sie der Namensstruktur und dem Schema des Austausch-DITs entsprechen.

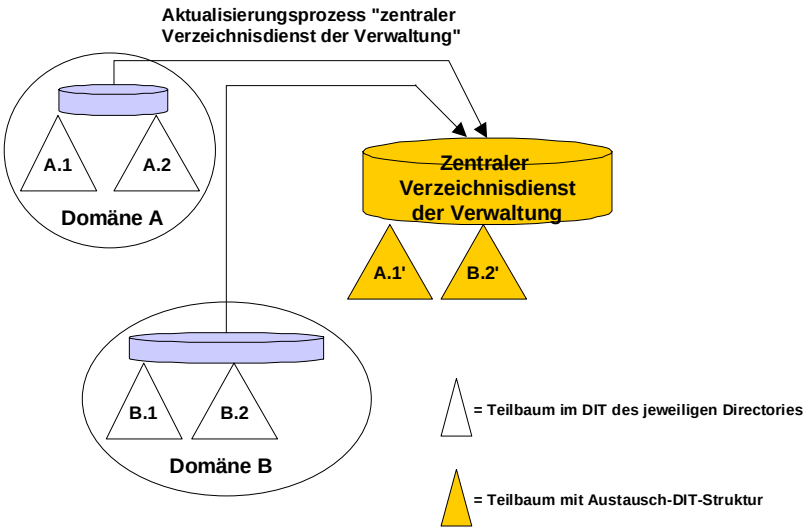

Abbildung 10: Im Veröffentlichungsdienst der Verwaltung werden ausgewählte Teilbäume der lokalen Directories bereitgestellt.

Der Aktualisierungsprozess von den Domänen zum Verzeichnisdienst der Verwaltung verwendet zum Datenaustausch die standardisierte Dateischnittstelle im LDIF-Dateiformat [LDIF]. Es ergibt sich die folgende Struktur des Aktualisierungsprozesses für den Verzeichnisdienst der Verwaltung:

- Zu einem durch den Aktualisierungsrhythmus bestimmten Zeitpunkt werden in der Domäne aus dem lokalen Verzeichnisdienst alle Entries ausgelesen, die über die Kennzeichnung "relevant für Aktualisierungsprozess" verfügen und seit dem letzten Lauf verändert wurden.
- Die ausgelesenen Daten werden lokal für den Aktualisierungsprozess aufbereitet: Sofern erforderlich, werden Umsetzungen von Objektklassen, Attribut-Typen und Attribut-Werten vorgenommen. Die aufbereiteten Daten werden in einer LDIF-Datei abgelegt.
- Die LDIF-Datei wird über eine gesicherte Kommunikationsverbindung an den Betreiber des Verzeichnisdienstes der Verwaltung übermittelt.

Im Rahmen der Prozess-Schritte in der Domäne werden auch die Löschbefehle für Entries ergänzt, soweit entsprechende Informationen vorliegen.

- Auf dem Verzeichnisdienst der Verwaltung läuft ein kontinuierlicher Prozess, der den Eingang von LDIF-Dateien feststellt. Die Datei wird auf Konsistenz geprüft und gegebenenfalls nachbereitet. Anschließend werden die enthaltenen Anweisungen abgearbeitet und die Entries im Verzeichnis des Veröffentlichungsdienstes eingetragen, aktualisiert oder gelöscht.

Aus **Performanzgründen** werden regelmäßig lediglich die Differenzen zur bereits ausgetauschten Datenbasis übermittelt. In größeren Abständen werden jedoch die Daten für einen Vollabgleich bereitgestellt. Dieser erlaubt es, beim Eintritt neuer Domänen und nach Störungen eine vollständige und konsistente Datenbasis zu erhalten.

Um die **Skalierbarkeit** und **Flexibilität** zu verbessern, werden die Maßnahmen zur Umsetzung von Daten soweit wie möglich in der lokalen Domäne durchgeführt. Dadurch können Domänen, die von den Vorgaben abweichen, mit individuellen Anpassungen ebenfalls an den Aktualisierungsprozessen teilnehmen.

Die Domänen haben die Verantwortung für die Bereitstellung und Qualität ihrer Daten. Anlässe für die Veränderungen von Entries in den Domänen (also z. B. die Neuausstellung von Zertifikaten) und die Kennzeichnung bestimmter Entries zum Abgleich mit den Diensten des Verzeichnisdienstkonzepts sind unter alleiniger Verantwortung der jeweiligen Domäne zu überwachen und zu bearbeiten.

Prozess-Struktur

Für den Aktualisierungsprozess für den Verzeichnisdienst der Verwaltung wird folgendes logisches Strukturmodell definiert (vgl. Abb. 11):

- Der Aktualisierungsprozess für den Verzeichnisdienst der Verwaltung untergliedert sich in zwei Teilprozesse: den **Teilprozess der Domäne**, der die Aktualisierungsdaten bereitstellt, und den **Teilprozess des VDV**, der die Aktualisierungsdaten in den Verzeichnisdienst der Verwaltung einstellt.
- Ein kontinuierlich ablaufender **Rahmenprozess der Domäne** stößt periodisch einen oder mehrere unterschiedlich konfigurierte Teilprozesse der Domäne an.

- Ein **Rahmenprozess des VDV** überprüft kontinuierlich, ob neue Daten einzustellen sind, und stößt bei Bedarf den Teilprozess des VDV an.

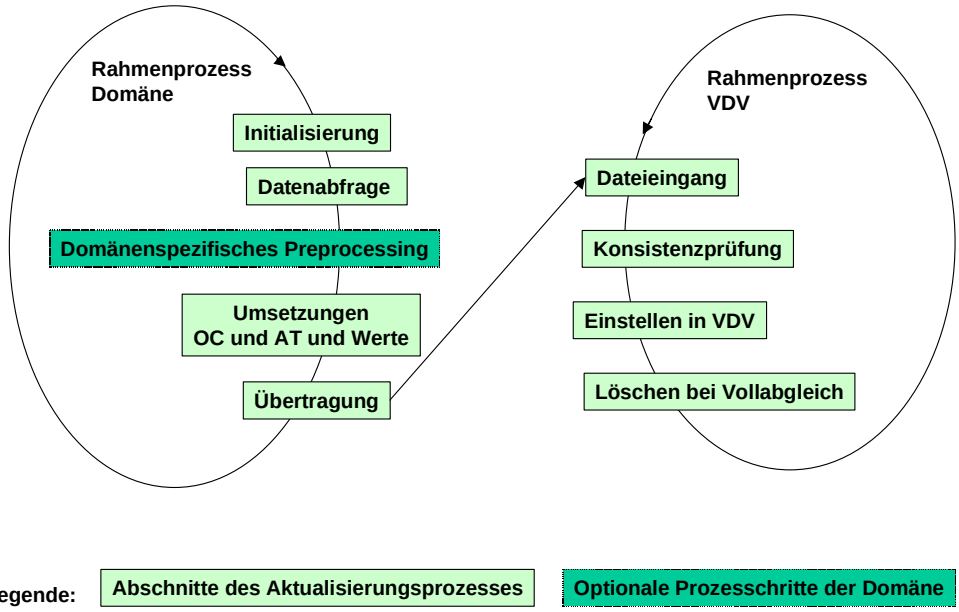

Abbildung 11: Grundstruktur des Aktualisierungsprozesses für den Verzeichnisdienst der Verwaltung (VDV)

Jeder der Teilprozesse wird in mehrere Teilprozessabschnitte zerlegt. Die Modularisierung soll die Anpassung an lokale Erfordernisse der Domänen und die Weiterentwicklung des Verzeichnisdienstkonzepts erleichtern.

Der **Teilprozess der Domäne** besteht aus folgenden Abschnitten:

(1) Initialisierung

(2) Datenabfrage

(3) domänenspezifisches Preprocessing

(4) Umsetzungen der Objektklassen, Attributtypen und Attributwerte

(5) Übertragung der LDIF-Datei

Das Preprocessing der Domäne ist optional. Die Domäne kann in diesem Schritt spezifische Anpassungen vornehmen oder auch Löschbefehle aus anderen Quellen ergänzen. Sofern die Domäne die Bedingungen an den Input für den Prozessabschnitt (4) erfüllt, kann sie auch die Datenabfrage in einem selbst

implementierten Prozessabschnitt durchführen und die Ergebnisdatei an Prozessabschnitt (4) übergeben.

Der **Teilprozess des Verzeichnisdienstes der Verwaltung** besteht aus folgenden Abschnitten:

(6) Dateieingang

(7) Konsistenzprüfungen

(8) Einstellen in den Verzeichnisdienst der Verwaltung

(9) Löschen im Falle eines Vollabgleichs

Sofern Löschbefehle bereits in der empfangenen LDIF-Datei enthalten sind, werden sie in Prozessabschnitt (7) ausgeführt. Abschnitt (9) ist vorgesehen, um im Falle eines Vollabgleichs zusätzliche Löschungen vornehmen zu können. Diese können sich beispielsweise auf Entries beziehen, die nicht aktualisiert wurden (vgl. dazu auch die Details zum Löschen).

6.2 Details des Aktualisierungsprozess VDV

6.2.1 Datenumfangs von LDIF-Dateien für den VDV

Die Aufteilung des Datenumfangs von LDIF-Dateien muss folgenden Kriterien Rechnung tragen:

- Um eine gute Skalierbarkeit für die Aktualisierungsprozesse zu ereichen, muss zwischen Dateien für den Vollabgleich und der Übertragung der Differenz seit dem letzten Aktualisierungsprozess unterschieden werden.
- Die Entries von CAs und CDPs einerseits und Teilnehmern andererseits können unter Sicherheits- und Policy-Gesichtspunkten unterschiedliche Replikationsrhythmen erfordern.
- Die Unterscheidung zwischen Entries von CAs und CDPs einerseits und Teilnehmern andererseits erleichtert außerdem die Implementierung des Aktualisierungsprozesses, weil beispielsweise unterschiedliche Namensregeln für die Wurzel des Directory Information Trees gelten können.

Daraus ergibt sich folgendes Vorgehen: Die LDIF-Dateien des Verzeichnisdienstkonzepts werden mit jeweils spezifischem Datenumfang erzeugt. Die Dateinamen der LDIF-Dateien unterscheiden sich je nach ihrem Inhalt (die Kürzel werden später bei der Namensgebung für Dateien weiterverwendet):

- Erstes Unterscheidungskriterium sind die Domänen. Jede Domäne erzeugt eigene Dateien der folgenden Kategorien.
- Umfang "CA", Typ "diff" enthält nur Entries von CAs und CDPs (eines Teilbaums aus der Domäne), die seit der letzten Aktualisierung geändert wurden. Löschbefehle für CAs und CDPs werden nicht unterstützt.
- Umfang "CA", Typ "voll" enthält alle Entries von CAs und CDPs (eines Teilbaums aus der Domäne). Löschbefehle für CAs und CDPs werden nicht unterstützt.
- Umfang "EE", Typ "diff" enthält nur Entries von Teilnehmern (eines Teilbaums aus der Domäne), die seit der letzten Aktualisierung geändert wurden. Löschbefehle für Entries können enthalten sein.
- Umfang "EE", Typ "voll" enthält alle Entries von Teilnehmern (eines Teilbaums aus der Domäne). Löschbefehle für Entries können enthalten sein.

6.2.2 Neue OU-Teilbäume im Austausch-DIT

Die Entries für Organisational Units im Austausch-DIT werden nicht übertragen. Sie werden automatisch eingerichtet, wenn ein Teilnehmer-Entry für eine Organisational Unit übertragen wird und diese im Austausch-DIT noch nicht existiert.

6.2.3 Auswahl von Entries für den VDV und den Veröffentlichungsdienst

Es werden insgesamt vier Konfigurationsparameter eingeführt: zur Festlegung des Attribut-Typs und des geforderten Wertes für "Bereitstellen im VDV" und zur Festlegung des Attribut-Typs und des geforderten Wertes für "Bereitstellen im Veröffentlichungsdienst". Dabei werden Wertlisten je Parameter unterstützt.

Im Verzeichnisdienst der Verwaltung muss nur noch die Information verfügbar sein, ob ein Entry auch in den Veröffentlichungsdienst repliziert werden soll. Die verschiedenen Varianten aus den Domänen werden dazu im Rahmen der Umsetzung von Attribut-Typen und Werten im Schema des Austausch-DITs auf einen Attribut-Typ und einen Wert abgebildet (siehe dazu Kapitel 5).

6.2.4 Identifikation veränderter Entries

Die Identifikation veränderter Entries wird über ein "lastModified"-Attribut durchgeführt, das in jedem Entry der Domäne enthalten sein muss. Der Zeitpunkt der letzten Änderung muss auf Sekundengenauigkeit eingetragen sein. Das Attribut muss mindestens dann gesetzt werden, wenn sich eines der Attribute ändert, die zum Verzeichnisdienst der Verwaltung übertragen werden. Domänen, die ein solches Attribut nicht führen, müssen es in ihr Schema aufnehmen und geeignet pflegen.

Hinweis: Es wird grundsätzlich angenommen, dass die Veränderungen von Entries in den Verzeichnisdiensten der Domänen in Form von elementaren Operationen oder als Transaktionen durchgeführt werden. D.h. es kann nicht auftreten, dass der Aktualisierungsprozess einen CA-Entry liest und dort gerade eine CRL gelöscht wurde, die neue aber noch nicht wieder eingestellt ist. Außerdem müssen *keine Situationen* behandelt werden, in denen ein Zugriff auf einen Entry wegen anderer Prozesse nicht möglich ist ("locked").

6.2.4.1 Prozess-Überschneidungen beim Datenzugriff

Sofern gleichzeitig mit dem Abruf von Entries durch den Aktualisierungsprozess ein anderer Prozess Daten auf dem lokalen Verzeichnisdienst ändert, kann es zu Prozess-Überschneidungen beim Datenzugriff kommen. In diesem Fall kann es vorkommen, dass der Aktualisierungsprozess Änderungen übersieht. Ursache ist, dass das LastModified Attribut nur mit Sekundengenauigkeit geführt wird. Folgendes Szenario muss in der Implementierung berücksichtigt werden:

- Der Aktualisierungsprozess sucht zu einem bestimmten Zeitpunkt t_n alle seit t_{n-1} geänderten Entries.

- Nachdem ein Entry im Rahmen dieser Anfrage als "nicht relevant" gefiltert wurde, wird er aber in der gleichen Sekunde (t_n) geändert. Dieser Entry würde nicht mehr berücksichtigt, wenn der nächste Lauf des Aktualisierungsprozesses alle Änderungen mit" lastModified > t_n "abfragt.

Der Suchfilter für die Abfrage verwendet deshalb die Bedingung "lastModified >= t_n" (vgl. Abb. 12). Dadurch werden Entries, die exakt im Zeitpunkt t_n geändert wurden, möglicherweise in beiden Läufen, mindestens aber im zweiten Lauf berücksichtigt. Das Problem sollte nur sehr selten auftreten. Deshalb ist der Umfang der möglichen Doppel-Übertragungen akzeptabel.

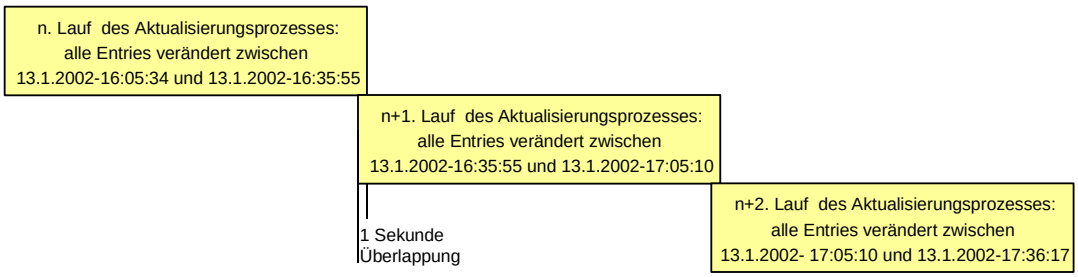

Abbildung 12: Im Aktualisierungsprozess überlappen sich die Änderungszeiträume, für die Entries übertragen werden.

Auf der Seite des empfangenden Verzeichnisdienstes der Verwaltung entsteht dadurch allerdings das Problem, dass für einen Entry, der in zwei Dateien mit dem gleichen lastModified vorkommt, nicht unmittelbar zu entscheiden ist, welcher Entry der neuere ist. Dieses Problem kann gelöst werden, indem der Erzeugungszeitpunkt der Datei geprüft wird.

6.2.4.2 Zeit-Synchronisation für Aktualisierungsprozess

Im allgemeinen Fall muss angenommen werden, dass der Teilprozess in der Domäne auf einem anderen Server betrieben wird als der Verzeichnisdienst der Domäne. Wenn die Uhren der beiden Server, z. B. nach Störfällen, mit einer Abweichung eingestellt werden, können Aktualisierungen bis zum nächsten Vollabgleich verloren gehen. Daher wird die folgende Prozess-Synchronisation vorgenommen:

Der Aktualisierungsprozess verwendet einen zu diesem Zweck reservierten Hilfs-Entry im Verzeichnisdienst der Domäne, um die dortige Systemzeit festzu-

stellen. Beim Start des Prozesses schreibt er in diesen Hilfseintrag und liest den Wert "lastModified" wieder aus. Damit verfügt er über die Serverzeit des Verzeichnisdienstes.

6.2.5 Löschen von Entries

Entries sollen in den Diensten des Verzeichnisdienstkonzepts gelöscht werden, wenn sie nicht mehr benötigt werden. Die Löschungen sollen zwar zeitnah erfolgen, sind aber nicht wirklich sicherheitskritisch (durch die Policies der Domänen sollte sichergestellt sein, dass die Zertifikate der zu löschenden Entries abgelaufen oder gesperrt sind).

Um die Löschung durchzuführen, sollten LDIF-Dateien mit Löschbefehlen bereitgestellt werden. Auch wenn dies nicht möglich ist, sollten die Datenbestände der Dienste des VDKs regelmäßig "aufgeräumt" werden.

6.2.5.1 Zeitliche Rahmenbedingungen für Löschungen von Entries

Es ist ausreichend, die Löschung von Teilnehmer-Entries in den Diensten des Verzeichnisdienstkonzepts einmal im Monat durchzuführen. Kürzere Zeiträume für Löschungen sind möglich.

CA-Entries und CDP-Entries haben einen zentralen Stellenwert für die Verfügbarkeit von PKI-Anwendungen. Sie werden deshalb in der Ausbaustufe 1 nur manuell gelöscht. Dazu ist ein entsprechendes Verfahren zu definieren.

Um "tote" CA- und CDP-Entries zu identifizieren, wird im Rahmen des Vollabgleichs eine Prüfung auf das letzte Aktualisierungsdatum durchgeführt. Werden CA- oder CDP-Entries länger als einen Monat nicht geändert, erfolgt eine Warnung.

6.2.5.2 Bereitstellung der Löschinformationen

Die Löschung von Teilnehmer-Entries im Verzeichnisdienst der Verwaltung kann auf verschiedene Weise durchgeführt werden.

Das Konzept des Aktualisierungsprozesses erlaubt es, bereits in der Ausbaustufe 1 etwa vorhandene LDIF-Löschbefehle zu verwenden. Löschbefehle werden nur von den Domänen in die LDIF-Datei eingetragen. Die Domänen, die Informationen aus dem Austauschdienst reimportieren, führen die Löschung von "toten" Entries nur im Rahmen eines Vollabgleichs mit dem gleichen Verfahren wie der Verzeichnisdienst der Verwaltung durch.

Während der Ausbaustufe 1 wird zusätzlich die Löschung von Entries durch das Setzen eines Aktiv-Indikators beim Vollabgleich durchgeführt. Dazu werden im Rahmen eines Voll-Abgleichs alle Entries gekennzeichnet, die angeliefert wurden (im Attribut vDKActiveIndicator). Anschließend werden alle Entries, die nicht gekennzeichnet wurden, gesucht und dann gelöscht.

Der Löschprozess erlaubt ein zweistufiges Vorgehen:

- **Löschungen im Teilbaum:** Zunächst werden die Entries aus dem gerade über den Vollabgleich aktualisierten Teilbaum gelöscht, die ein bestimmtes Alter aufweisen.
- **Löschungen im gesamten Austausch-DIT:** Danach werden die Entries aus dem gesamten Austausch-DIT identifiziert, die ein bestimmtes Alter aufweisen, und anschließend gelöscht.

Beide Stufen des Löschens können unterschiedlich konfiguriert werden bezüglich des Alters der Entries. Dadurch ist es beispielsweise möglich, im aktuellen Teilbaum alle Entries zu löschen, die älter als 31 Tage sind, und im Austausch-DIT die Entries zu löschen, die länger als 62 Tage nicht mehr aktualisiert wurden. Die Löschung wird nur durchgeführt, wenn die Zahl der zu löschenden Entries im aktuellen Teilbaum unter einer bestimmten Prozentzahl der aktiven Entries bleibt. Im Austausch-DIT wird eine Maximal-Zahl angegeben, ab der die Löschung nicht mehr automatisch durchgeführt wird.

Es wird empfohlen, die Tragfähigkeit dieser Lösung nach 6 bis maximal 12 Monaten zu überprüfen.

6.2.5.3 Sonderfälle

Löschbefehle für Organisational Units im Austausch-DIT werden nicht übertragen. Sie werden im Rahmen eines Vollabgleichs im Verzeichnisdienst der Verwaltung automatisch gelöscht, wenn keine Teilnehmer-Entries mehr im entsprechenden Teilbaum enthalten sind.

Wenn beim Löschen von Entries in der Quell-Information nur der DIT-DN aus der Domäne enthalten ist, können Informationen für die Umsetzung auf den Austausch-DIT fehlen. In diesem Fall ergeben sich folgende Konsequenzen (insbesondere zeitliche Verzögerungen beim Löschen), die aber für die Ausbaustufe 1 in Kauf genommen werden:

- Im Teilprozess der Domäne kann der DN nicht richtig umgesetzt werden. Es werden andere Regeln angewandt, die einen "falschen" A-DIT-DN erzeugen. Dieser kann aber nicht existieren, da die E-Mail-Adresse ein global eindeutiges Attribut ist.
- Im Verzeichnisdienst der Verwaltung wird versucht, einen nicht existierenden Entry zu löschen. Diese Operation wird ignoriert.
- Nach einem Vollabgleich wird im Standardablauf festgestellt, dass der "richtige" Entry nicht mehr aktiv ist. Der Entry wird darauf hin gelöscht.

6.2.6 Gültigkeit von Sperrlisten und Replikationsrhythmus

Die Policies der Domänen geben nach jetzigem Stand eine tägliche Erzeugung und Bereitstellung von Sperrlisten vor. Allerdings werden in einigen Domänen Sperrlisten häufiger ausgestellt. Die PCA stellt Sperrlisten nur alle 7 Tage aus. Wann ein Client feststellt, dass eine Sperrliste abgelaufen ist, hängt von der konkreten Nutzung im Einzelfall ab. Im IVBB wird von den Clients die Abfrage von Sperrlisten unabhängig vom Ablauf ihrer Gültigkeitsdauer durchgeführt. Clients aller Domänen können daher prinzipiell zu beliebigen Zeitpunkten Sperrlisten abrufen. Deshalb sollen Sperrlisten in allen Diensten des Verzeichnisdienstkonzepts möglichst aktuell sein.

Unter Berücksichtigung der Ziele aus Kapitel 5.1 werden folgende Festlegungen getroffen, um eine rechtzeitige Replikation von Sperrlisten zu gewährleisten:

- Grundsätzlich sind die Domänen selbst dafür verantwortlich, dass Sperrlisten mit geeignetem Gültigkeitszeitraum rechtzeitig erzeugt werden. Sie müssen den Teilprozess zur Replikation in der Domäne so anstoßen, dass die neuen Sperrlisten rechtzeitig an den Verzeichnisdienst der Verwaltung übermittelt werden. Den Domänen wird aber empfohlen, den folgenden Vorschlägen zu folgen.
- Es wird dringend empfohlen, den Aktualisierungsprozess vom Typ "CA" mit dem Datenumfang "diff" (Differenzaktualisierung für CA- und CDP-Entries) alle 30 Minuten anzustoßen.
- Für den Vollabgleich von CA- und CDP-Entries wird in Ausbaustufe 1 ein Rhythmus von einmal pro Monat gefordert.
- Die größte zeitliche Verschiebung in der Bereitstellung entsteht für den Veröffentlichungsdienst. Es muss sichergestellt werden, dass auch dort immer eine gültige Sperrliste abgerufen werden kann. Da gemäß der Vorgaben aus Kapitel 5.1 mit einer zeitlichen Verzögerung der Bereitstellung durch die Replikationsmechanismen zu rechnen ist, wird den Domänen **dringend empfohlen**, die Gültigkeitszeiträume von zwei aufeinander folgenden Sperrlisten zu überlappen (Abb. 13). Die empfohlene Mindest-Überlappungszeit entspricht der Summe der Worst-Cases der Einzelverzögerungen von der Erzeugung bis zur Veröffentlichung im Veröffentlichungsdienst. Gemäß Kapitel 5.1 soll die Verzögerung im Normalbetrieb unter 90 Minuten bleiben. Dies wäre die empfohlene Mindestüberlappung. Wird die Überlappung vergrößert, können auch noch kurze Störungen überbrückt werden. Allerdings tritt bei zu großer Überlappung ein Konflikt zu dem Ziel auf, dass nach dem Erscheinen einer neuen Sperrliste die alte nicht mehr weiterverwendet werden soll.

  Wenn die Rück-Replikation in Domänen unterstützt werden soll, wird eine

Verlängerung der Überlappung auf 2 Stunden empfohlen (vgl. Kapitel 9.2.6).

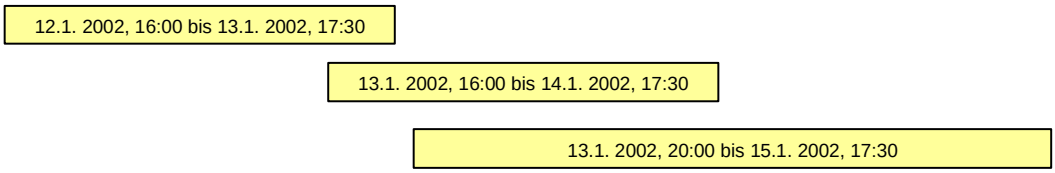

Abbildung 13: Überlappende Gültigkeitsdauern von Sperrlisten

- Den Replikationsrhythmus für Differenzaktualisierungen für Teilnehmer-Entries können die Domänen selbst festlegen. Es wird jedoch empfohlen, diese Aktualisierung mindestens einmal täglich durchzuführen.
- Für den Vollabgleich von Teilnehmer-Entries wird in Ausbaustufe 1 ein Rhythmus von einmal pro Monat gefordert.

6.2.7 Push-Konzept von der Domäne zum VDV

Der Aktualisierungsprozess von der Domäne zum Verzeichnisdienst der Verwaltung wird in der Ausbaustufe 1 des Verzeichnisdienstkonzepts mit einem Push-Mechanismus von der Domäne zum VDV realisiert. Da die Domäne die Übertragung auslöst, können ohne weitere Mechanismen zu beliebigen Zeitpunkten LDIF-Dateien an den Verzeichnisdienst der Verwaltung übertragen werden. Ein zusätzliches Trigger-Konzept, durch das Aktualisierungen zwischen der Domäne und dem VDV koordiniert werden könnten, ist nicht erforderlich.

6.2.8 Wiederaufsetzen im Falle von Störungen

Die Datenqualität kann beeinträchtigt werden, wenn eine Domäne LDIF-Dateien erzeugt, diese aber nicht beim Verzeichnisdienst der Verwaltung zur Aktualisierung verwendet werden.

In der Ausbaustufe 1 soll eine möglichst einfache Implementierung erreicht werden. Eine Sequenz-Prüfung der erzeugten, übertragenen und im Verzeichnisdienst der Verwaltung eingestellten LDIF-Dateien erhöht den Implemen-

tierungsaufwand jedoch erheblich. Es wird deshalb vorgeschlagen, die folgende Policy für die Behandlung von Störfällen zu definieren:

- Wird ein **schwerer Störfall** erkannt, durch den möglicherweise größere Datenbestände verloren oder verändert wurden, wird ein Vollabgleich für die betreffenden Teilbäume durchgeführt. Der Vollabgleich wird in der Domäne manuell durch die Systemadministration angestoßen. Ein Vollabgleich wird auch durchgeführt, wenn Manipulationen erkannt wurden oder befürchtet werden müssen.
- **CA- und CDP-Entries:** Die Domäne muss unverzüglich sicherstellen, dass in den Diensten des Verzeichnisdienstkonzepts eine gültige Sperrliste zur Verfügung steht. Für CA- und CDP-Entries kann in Störfällen eine mehrstündige Verzögerung der Übertragung akzeptiert werden, wenn die in den Diensten des Verzeichnisdienstkonzepts veröffentlichte Liste noch gültig ist und keine großen Schäden für die Anwender der PKI zu erwarten sind. Abhängig von der Erzeugungsfrequenz der Sperrliste in der Domäne, ihrer Gültigkeitsdauer und dem Replikationsrhythmus des Aktualisierungsprozesses (Annahme: max. jede Stunde) kann in dringenden Fällen mit vier Alternativen reagiert werden:
  - Rücksetzen des Konfigurationsparameters zur Kennzeichnung des Zeitpunktes der letzten erfolgreichen Übertragung ("startTimeOfLastSuccessfulRetrieval") für den Aktualisierungsprozess auf einen Zeitpunkt vor dem Erzeugen der fraglichen PKI-Informationen. Dadurch werden im nächsten Lauf des Aktualisierungsprozesses alle Entries berücksichtigt, die nach diesem Zeitpunkt geändert wurden.
  - Erneutes Speichern (oder Erzeugen) von Sperrlisten für die fraglichen Entries und Einstellen in den Verzeichnisdienst der Domäne: dadurch wird "lastModified" geändert.
  - Manuelles Auslösen eines Vollabgleichs.
  - Keine Aktion, weil die Sperrliste z. B. stündlich erzeugt wird und das Problem mit dem nächsten Update automatisch behoben wird.

- Für **Teilnehmer-Entries** entscheidet die Domäne, ob eine Korrektur vor dem nächsten Vollabgleich notwendig ist oder ob dieser abgewartet werden kann. Prinzipiell stehen die gleichen Maßnahmen zur Verfügung wie für CA-Entries beschrieben. Die Erstellung neuer Zertifikate für alle betroffenen Teilnehmer dürfte im Allgemeinen jedoch ausscheiden.

Mit dieser Policy ist eine sehr einfache Implementierung auf der Basis von Änderungszeitpunkten für Attribute möglich. Die Policy sollte allerdings anhand der Betriebserfahrung bewertet und gegebenenfalls in der nächsten Ausbaustufe überarbeitet werden.

6.2.9 Sicherheitsmaßnahmen

In den vorangegangenen Festlegungen sind eine Reihe impliziter Sicherheitsmaßnahmen enthalten, die dazu beitragen, dass ein gemeinsames Sicherheitsniveau erreicht werden kann, beispielsweise im Rahmen der Service-Qualität, der Fehlerbehandlung, der Überwachung der Prozesse, des Push-Ansatzes zur Datenübertragung von der Domäne zum VDV oder des Wiederaufsetzens im Falle von Störungen.

In diesem Abschnitt werden einige ergänzende Maßnahmen zusammengestellt, die zur Sicherheit des Aktualisierungsprozesses für den VDV beitragen. Eine Übersicht über alle im Rahmen der Implementierung zu berücksichtigenden Maßnahmen gibt das Sicherheitskonzept in Kapitel 15 dieses Dokumentes.

6.2.9.1 Konsistenzprüfungen und Separierung des Dateneingangs beim VDV

Interne Angreifer aus einer Domäne könnten versuchen, den Verzeichnisdienst der Verwaltung dadurch zu stören, dass sie fehlerhafte oder manipulierte LDIF-Dateien übertragen. Je nach Angriffsszenario könnten sie dies auch für die Teilbäume versuchen, die nicht ihrer Domäne zugeordnet sind, um beispielsweise eine falsche CRL in den Entry der PCA einzuspielen.

Um Angriffe zu verhindern, die die Grenze einer Domäne überschreiten, müssen auf der Seite des Verzeichnisdienstes der Verwaltung Konsistenzprüfungen durchgeführt werden.

Eine Realisierung des Aktualisierungsprozesses mit Konsistenzprüfungen beim Empfänger unterstützt in jedem Fall auch Tests für neu aufgenommene Domänen oder nach Änderungen. Die Integration der Konsistenzprüfungen in den Standard-Prozess erlaubt es daher, die gleiche Implementierung in der Test- und der Produktiv-Umgebung einzusetzen. Folgende Konsistenzprüfungen werden durchgeführt:

- Auf der Seite des Verzeichnisdienstes der Verwaltung werden alle Entries daraufhin geprüft, ob die Quelle der Daten (liefernde Domäne) mit den Namenswurzeln der Entries korreliert.
- Es wird sichergestellt, dass jede Domäne ihre LDIF-Dateien nur in einen für sie zugewiesenen Bereich einstellen kann. Dazu wird eine geeignete Authentisierung durchgeführt, wenn auf diesen Bereich zugegriffen wird.

6.2.9.2 Kommunikationsverbindung

Die Firewalls der Domänen und der Betreiber der Dienste des Verzeichnisdienstkonzepts müssen den jeweiligen Bereich vor Angriffen aus dem Internet schützen. Die notwendige Öffnung der Firewalls für die Prozesse des Verzeichnisdienstkonzepts wird deshalb minimal ausgelegt. Es wird lediglich eine fest konfigurierte 1:1 Verbindung auf einem definierten Port zugelassen. Die Zugriffsrechte für die Prozesse werden auf die unbedingt notwendigen Rechte eingeschränkt.

Die LDIF-Dateien werden in Ausbaustufe 1 grundsätzlich über eine kryptographisch gesicherte Verbindung von der Domäne an den Verzeichnisdienst der Verwaltung übertragen. Die Übertragung soll im Intranet der Verwaltung erfolgen. Beim Verbindungsaufbau wird eine gegenseitige Authentisierung mit voreingestellten Zertifikaten oder Schlüsseln durchgeführt. Zur Realisierung könnte z. B. Secure Copy / Secure Shell eingesetzt werden.

Die notwendigen Schlüsselinformationen können in Software-PSEs abgelegt werden. Alle Beteiligten müssen durch geeignete organisatorische Maßnahmen sicherstellen, dass der Zugriff auf die Software-PSEs und Passworte nur Berechtigten möglich ist.

Das "Produkt" soll die notwendigen Komponenten für die sichere Verbindung für alle geforderten Plattformen oder zumindest Hinweise auf kompatible Komponenten und Bezugsquellen enthalten.

6.2.9.3 Dateimanagement: Wiederaufsetzen und Audit

Um in Störfällen ein Wiederaufsetzen zu ermöglichen und die notwendigen Informationen für ein Audit der Prozesse sicherzustellen, werden folgende Regeln für das Dateimanagement festgelegt:

- Dateien, die in den Domänen zur Erstellung von zu übertragenden LDIF-Dateien dienen, können gelöscht werden, sobald sie nicht mehr benötigt werden.
- Zu übertragende bzw. eingegangene LDIF-Dateien und Log-Dateien sind auf der Seite der Domäne und beim VDV für mindestens zwei Monate aufzubewahren. Als Log-Dateien zählen auch solche Dateien, in denen Aufzeichnungen über die Zugriffskontrolle zur Durchsetzung von Rollentrennung geführt werden.

7 Aktualisierung Austauschdienst

7.1 Übersicht

Der Austauschdienst stellt eine Sammlung von LDIF-Dateien bereit, die dem aktuellen Stand des Austausch-DITs im Verzeichnisdienst der Verwaltung entsprechen. Diese LDIF-Dateien können dann im Rahmen des Aktualisierungsprozesses für den Verzeichnisdienst der Domäne abgerufen werden. Der Aktualisierungsprozess zum Austauschdienst muss daher sicherstellen, dass die LDIF-Dateien mit Aktualisierungsinformationen zum Abruf auf dem Server des Austauschdienstes rechtzeitig zur Verfügung stehen.

7.2 Details

Neben den im einleitenden Kapitel dieses Teils genannten allgemeinen Prozessparametern gelten zusätzlich auch für die folgenden Punkte dieselben Festlegungen wie für den Aktualisierungsprozess für den VDV:

- Namensregeln für Dateien,
- Löschen von Entries,
- Aufbau der LDIF-Dateien,
- Gültigkeit von Sperrlisten und Replikationsrhythmus und
- Auswahl von Entries für den Verzeichnisdienst der Verwaltung und den Veröffentlichungsdienst

7.2.1 Datenumfang von LDIF-Dateien für den Austauschdienst

In der Ausbaustufe 1 des Verzeichnisdienstkonzepts sollen die Daten zum Austauschdienst möglichst so angeliefert werden, wie sie später von den Domänen abgerufen werden. Eine Umsetzung von Entries oder eine Änderung des Umfangs der LDIF-Dateien soll vermieden werden. Deshalb ist es sinnvoll,

den Prozess der Aktualisierung des Austauschdienstes mit den Anforderungen beim Abruf der Daten durch die Domänen abzustimmen.

Bisher liegen keine konkreten Anforderungen zur Separierung von Daten vor, die sich von der Unterteilung der LDIF-Dateien für den Verzeichnisdienst der Verwaltung unterscheiden. Es wird deshalb angenommen, dass die Unterscheidung von LDIF-Dateien nach Entries von CAs und CDPs einerseits und Teilnehmern andererseits ausreichend ist. Diese Unterscheidung entspricht der Separierung für den Aktualisierungsprozess von der Domäne zum Verzeichnisdienst der Verwaltung.

Die obigen Kriterien für den Datenumfang und die Strukturierung der LDIF-Dateien für den Verzeichnisdienst der Verwaltung erlauben es damit, auch hinreichend flexible "Abonnements" für die Aktualisierung des Austausch-DITs in den Domänen zu unterstützen.

In der Ausbausstufe 1 werden im Austauschdienst nur die Daten zur Verfügung gestellt, die auch für den Verzeichnisdienst der Verwaltung angeliefert werden. Der Umfang der LDIF-Dateien wird für den Austauschdienst nicht verändert.

Hinweis: Trotz dieser Einschränkung bestehen verschiedene Möglichkeiten, den Datenumfang im Austausch-DIT einer Domäne zu steuern:

- Domänen können in bilateraler Absprache vereinbaren, dass die Quell-Domäne bestimmte Teilbäume in separaten LDIF-Dateien an den Verzeichnisdienst der Verwaltung übergibt. Dazu sind bereits Konfigurationsmöglichkeiten im Aktualisierungsprozess von der Domäne zum VDV vorgesehen.
- Die Domäne, die Daten in ihren lokalen Austausch-DIT repliziert, kann die vom Austauschdienst abgerufenen LDIF-Dateien durch ein Preprocessing filtern, bevor sie die Daten in den lokalen Verzeichnisdienst einstellt.

7.2.2 Übernahme der LDIF-Dateien vom VDV

Weil die LDIF-Dateien des Austauschdienstes identisch mit denen für die Aktualisierung des VDV sind, kann der Aktualisierungsprozess für den Austauschdienst vereinfacht werden: Die LDIF-Dateien, die beim Verzeichnisdienst der

Verwaltung eingehen, werden nach einer Konsistenzprüfung beim VDV direkt (als Datei) zum Austauschdienst übertragen. Die Durchführung dieses Kopierens darf nicht länger dauern als das Einstellen der Entries im VDV. Alternativ könnte der Teilprozess der Domäne die LDIF-Dateien jeweils an beide Dienste übertragen. Für die Ausbaustufe 1 erscheint die erste Lösung jedoch hinreichend. Sie muss aber in den weiteren Ausbaustufen überprüft werden, um bei einem höherem Nutzungsgrad eine Unabhängigkeit der beiden Dienste sicherzustellen.

Damit ergibt sich die Prozessstruktur in Abbildung 14.

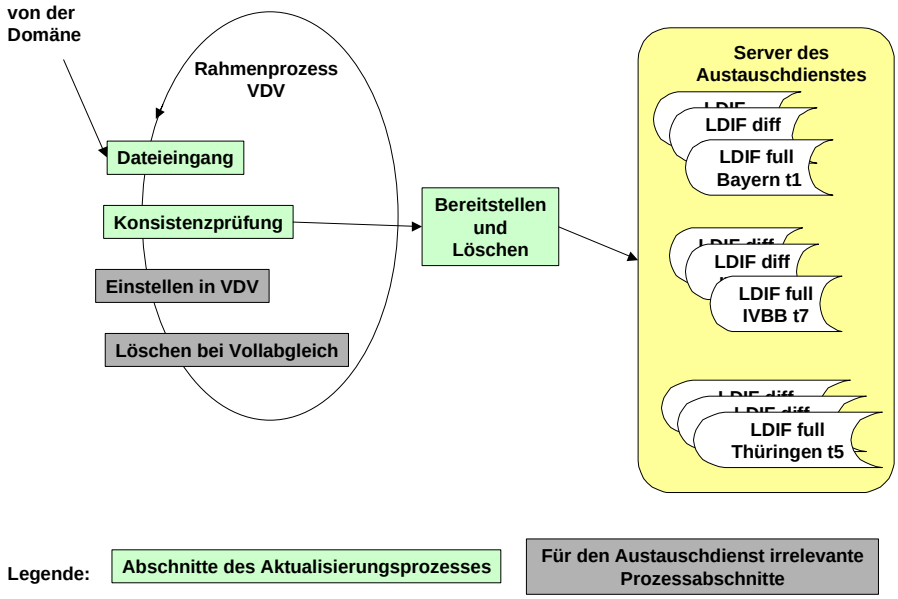

Abbildung 14: Grundstruktur des Aktualisierungsprozesses für den Austauschdienst. Jede Gruppe von LDIF-Dateien stellt eine aktuelle Generation dar (Vollabgleich und mehrere Differenzen)

7.2.3 Kommunikationsverbindung

Für die Übertragung der Dateien zwischen den beiden Diensten ist mindestes das Sicherheitsniveau zu realisieren, das auch für die Übertragung von den Domänen an den VDV gefordert ist. Die Implementierung kann deshalb von der Verteilung der Dienste auf verschiedene Systeme abhängen.

7.2.4 Implementierungsplattformen

Wenn das Konzept für den Austauschdienst die Daten aus dem Verzeichnisdienst der Verwaltung übernimmt, kann die Implementierung auf die beiden Plattformen abgestellt werden, die von dem oder den Betreibern des Verzeichnisdienstes der Verwaltung und des Austauschdienstes eingesetzt werden. Der Abruf muss von allen Plattformen nach Kapitel 5.2 unterstützt werden.

7.2.5 Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen für den Aktualisierungsprozess zum Austauschdienst sind äquivalent zu denen für den Prozess zum Verzeichnisdienst der Verwaltung. Dies betrifft z. B. Rollentrennung und Aufzeichnungspflichten beim Betreiber des Austauschdienstes.

Hinsichtlich des Dateimanagements für Wiederaufsetzen und Audit auf der Seite der Domäne wird die Entscheidung für den Aktualisierungsprozess zum VDV übernommen:

Der Austauschdienst stellt für jeden Teilbaum, für den aus einer Domäne LDIF-Dateien übertragen wurden, jeweils einen Vollabgleich und alle Differenzen seit dem Vollabgleich zur Verfügung. Bei Eintreffen eines neuen Vollabgleichs wird der alte Satz Dateien archiviert (alte Generation). Die letzte Generation von LDIF-Dateien für einen Teilbaum kann Sperrlisten für abgeschaltete CAs enthalten, die noch für lange Zeiträume bereitgestellt werden müssen. Generationen von Dateien, die nicht mehr aktualisiert werden, müssen deshalb von Hand gelöscht werden. Log-Dateien sind auf der Seite der Domäne und beim VDV für mindestens zwei Monate aufzubewahren. Als Log-Dateien zählen auch solche Dateien, in denen Aufzeichnungen über die Zugriffskontrolle zur Durchsetzung von Rollentrennung geführt werden.

8 Aktualisierung Veröffentlichungsdienst

Die Replikation vom Verzeichnisdienst der Verwaltung in den Veröffentlichungsdienst im Extranet ist von dem oder den Betreibern des VDV und des VöD direkt zu realisieren. Der Aktualisierungsprozess muss lediglich eine gegebenenfalls festgelegte Reduktion des Datenumfangs durchführen.

Der Replikationsprozess darf nur Entries in den Veröffentlichungsdienst übertragen, die mit den dafür vorgesehenen Steuerattribute gekennzeichnet sind (zur Kennzeichnung siehe Kapitel 4.1).

Der Umfang der je Entry in den Veröffentlichungsdienst übertragenen Daten muss so reduziert werden, wie es das Schema für den Veröffentlichungsdienst nach Kapitel 5 vorgibt.

Die Replikationsrhythmen müssen sicherstellen, dass die Anforderungen an die Service-Qualität (siehe Kapitel 5.1) erfüllt werden.

Nach einer Aktualisierung von Entries von CAs oder CDPs im Veröffentlichungsdienst ist die entsprechende HTTP-Seite automatisch zu aktualisieren (vgl. unten Kapitel 11).

Eine detailliertere Spezifikation dieses Prozesses erfolgt im Rahmen des Verzeichnisdienstkonzepts nicht, da die Implementierung einer 1:1-Replikation bereits auf der Basis der eingesetzten Produkte unterstützt werden könnte. Falls LDAP / LDIF eingesetzt werden soll, können die Spezifikationen für den Aktualisierungsprozess "Verzeichnisdienst der Verwaltung" mit geringem Aufwand angepasst werden.

9 Aktualisierung Domäne

Der Aktualisierungsprozess zur Domäne dient dazu, einen Ausschnitt des Austausch-DITs innerhalb der Domäne bereitzustellen. Dabei soll die Domäne den Teil des Austausch-DITs, den sie selbst zuliefert, nicht rückimportieren. Die "eigenen" Entries der Domäne werden also nicht an zwei Stellen im lokalen Verzeichnisdienst gehalten, sondern nur im originären DIT.

9.1 Übersicht

Der Aktualisierungsprozess vom Austauschdienst zur Domäne dient dazu, dass die Domänen Teilbäume des Austausch-DITs in ihren lokalen Verzeichnisdienst replizieren und intern (innerhalb ihrer Firewall) bereitstellen können. Der Aktualisierungsprozess verwendet zum Datenaustausch die standardisierte Dateischnittstelle im LDIF-Dateiformat. In den LDIF-Dateien, die der Austauschdienst zum Abruf bereitstellt, liegen die Entries bereits im Format des Austausch-DITs für das Schema des Verzeichnisdienstes der Verwaltung vor.

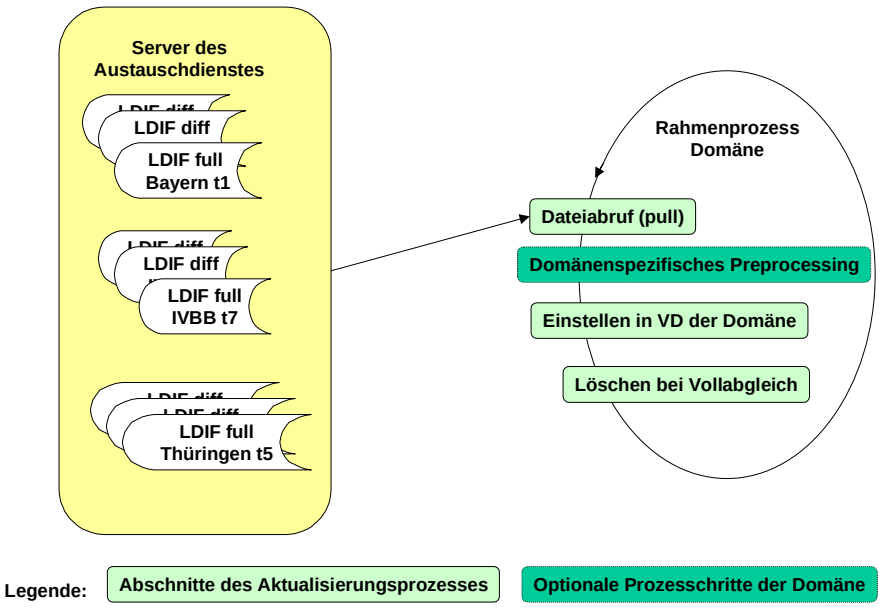

Abbildung 15: Grundstruktur des Aktualisierungsprozesses für den Verzeichnisdienst der Domäne. Der Pfeil zeigt den Datenfluss. Die Verbindung wird von der Domäne aufgebaut.

Es ergibt sich die folgende Struktur für den Aktualisierungsprozess zur Domäne:

- Die Domäne konfiguriert vorab lokal die Teilbäume des Austausch-DITs, die sie nach intern replizieren will.
- Zu einem durch den Aktualisierungsrhythmus bestimmten Zeitpunkt ruft die Domäne alle LDIF-Dateien für die ausgewählten Teilbäume des Austausch-DITs ab, die noch nicht lokal verfügbar sind. Der Abruf wird von der Domäne initiiert und über eine gesicherte Kommunikationsverbindung mit dem Austauschdienst abgewickelt.
- Im Rahmen eines lokalen Preprocessing können die Daten an spezifische Anforderungen der Domäne angepasst werden. Dieser Prozessabschnitt ist jedoch nicht Gegenstand des Verzeichnisdienstkonzepts.
- Die Entries aus den abgerufenen Dateien werden in den lokalen Verzeichnisdienst eingestellt.

Im Rahmen der Prozess-Schritte wird bei einem Vollabgleich festgestellt, welche Entries zu löschen sind.

Diese Prozessstruktur weist sehr große Ähnlichkeit mit dem Teilprozess auf, der im Aktualisierungsprozess zum Verzeichnisdienst der Verwaltung auf der Seite des VDV ausgeführt wird. Dementsprechend können viele Detailfestlegungen und Spezifikationen an den entsprechenden Prozessabschnitten orientiert werden.

9.2 Details

9.2.1 Service-Qualität

In Ausbaustufe 1 werden den Domänen auf dem Austauschdienst LDIF-Dateien zur Replikation angeboten. Die Domänen verwenden einen periodischen Prozess, um diese Daten abzurufen. Die Verantwortung für die Bereitstellung der Daten liegt beim Austauschdienst bzw. vorgelagert bei den Quell-Domänen. Für die Ausbaustufe 1 werden für CA- und CDP-Entries im Austausch-DIT im

Verzeichnisdienst der Domäne die folgenden Randbedingungen bezüglich der Datenqualität in der Domäne gefordert:

- Die Bereitstellung von LDIF-Dateien im Austauschdienst soll entsprechend der Bereitstellung im Verzeichnisdienst der Verwaltung erfolgen, also mit maximal 60 Minuten Verzögerung.
- Für den Abruf der LDIF-Dateien durch die Domäne vom Austauschdienst werden ein Replikationsrhythmus von 30 Minuten und damit weitere 30 Minuten Verzögerung angenommen.
- Für das Einstellen der LDIF-Dateien in den Verzeichnisdienst der Domäne werden wiederum 30 Minuten angenommen.
- Damit ergibt sich im Normalbetrieb eine maximale Verzögerung von 2 Stunden.
- Die weiteren Vorgaben aus Tabelle 5 sind entsprechend zu übertragen.

Die hier vorgegebenen Werte sind als Richtlinien für die Domänen zu verstehen. Die Verantwortung für den Abruf liegt bei den Domänen.

9.2.2 Datenumfang von LDIF-Dateien für den Abruf durch Domänen

Der Datenumfang und die Gruppierung der im Austauschdienst angebotenen Dateien ergeben sich analog zu den Festlegungen in 6.2.1.

Die Unterscheidung nach Umfang "CA" (CA- und CDP-Entries) und "EE" (Teilnehmer-Entries) wird je Domäne unterstützt (vgl. Kapitel 6.2). Jede Domäne kann frei entscheiden, welche Teilbäume des Austausch-DITs sie "abonniert". Durch die Strukturierung der Dateien ist sichergestellt, dass die Domäne die Auswahl so treffen kann, dass sie die Entries ihrer eigenen Teilnehmer nicht rückrepliziert. (Der interne Austausch-DIT enthält also die eigenen Entries nicht nochmals.)

9.2.3 Auswahl und Umsetzung von Entries für den Verzeichnisdienst der Domäne

Die Auswahl von Entries, die in den Verzeichnisdienst der Domäne eingestellt werden, ergibt sich implizit aus den abgerufenen LDIF-Dateien. In der Ausbaustufe 1 des Verzeichnisdienstkonzepts wird kein zusätzlicher Mechanismus zur Auswahl unterstützt. Es bleibt der Domäne unbenommen, durch ein lokales Preprocessing spezielle Entries auszuwählen, indem z. B. alle Entries außer denen von Gruppen gelöscht werden. Dazu können allerdings nur Informationen genutzt werden, die in den LDIF-Dateien enthalten sind.

Der Prozessabschnitt "Einstellen in den Verzeichnisdienst der Domäne" bietet eine Möglichkeit, um den Austausch-DIT für Teilnehmer-Entries von der allgemeinen Wurzel "c=de" auf eine lokal andere Wurzel umzusetzen, z. B. ou=A-DIT, dc=Bayern, dc=de. Dadurch können diese Entries innerhalb der DIT-Struktur des Verzeichnisdienstes der Domäne von den eigenen Entries separiert werden. Es ist damit auch möglich, den Namensvorgaben von Active Directory Rechnung zu tragen.

Für CA- und CDP-Entries wird diese Konfigurationsmöglichkeit in Ausbaustufe 1 nicht unterstützt.

9.2.4 Identifikation veränderter Entries

Die Identifikation veränderter Entries ist nur im ersten Teilprozess des Aktualisierungsprozesses von der Domäne zum VDV relevant. Der Aktualisierungsprozess vom Austauschdienst zur Domäne erhält in den LDIF-Dateien nur die Entries, die aktualisiert werden müssen. Hier sind daher keine weiteren Schritte erforderlich.

9.2.5 Löschen von Entries

Die Domänen setzen in der Ausbaustufe 1 das gleiche Verfahren zum Löschen von "toten" Entries ein, das auch im Aktualisierungsprozess für den Verzeichnisdienst der Verwaltung verwendet wird (Kapitel 6.2).

9.2.6 Gültigkeit von Sperrlisten und Replikationsrhythmus

Die Rhythmen zum Abruf von LDIF-Dateien ergeben sich implizit aus den Festlegungen in Kapitel 6.2. Für die Gültigkeitsdauer von Sperrlisten ist jedoch eine Erweiterung notwendig:

Gegenüber dem Veröffentlichungsdienst ergibt sich durch den Aktualisierungsprozess vom Austauschdienst in die Domäne eine weitere Verzögerung von maximal 30 Minuten für die Bereitstellung von Sperrlisten (vgl. Kapitel 9.2.1 und Kapitel 5.1). Es muss aber sichergestellt werden, dass auch in der Domäne immer gültige Sperrlisten aus anderen Domänen abgerufen werden können. Den Domänen wird deshalb **dringend empfohlen**, die Gültigkeitszeiträume von zwei aufeinander folgenden Sperrlisten um mindestens **2 Stunden zu überlappen**. Die empfohlene Mindest-Überlappungszeit entspricht der Summe der maximalen Einzelverzögerungen von der Erzeugung in der Quell-Domäne bis zur Veröffentlichung im Verzeichnisdienst einer anderen Domäne.

9.2.7 Abfrage durch die Domäne vom Austauschdienst (Pull-Konzeptentscheidung)

Auch im Aktualisierungsprozess für die Domäne soll die Domäne die Kommunikationsverbindung aufbauen und die LDIF-Dateien aktiv abfragen.

Da die Domäne initiativ wird, können auf diese Weise ohne weitere Mechanismen zu beliebigen Zeitpunkten LDIF-Dateien aus dem Austauschdienst abgerufen werden. Ein Trigger-Konzept für besondere Aktualisierung wird in der Ausbaustufe 1 nicht unterstützt. Das Pull-Konzept ist mit einem geeigneten Replikationsrhythmus für LDIF-Dateien mit CA- und CDP-Entries (30 min) ausreichend, um die vorgeschlagene Service-Qualität nach Kapitel 9.2.1 zu erreichen.

9.2.8 Wiederaufsetzen im Falle von Störungen

Das Wiederaufsetzen nach Störungen erfolgt automatisch oder ist im Rahmen der Konfiguration des Prozesses möglich:

- Wenn der Prozess nur zeitweise unterbrochen war, stellt er bei der nächsten erfolgreichen Verbindung zum Austauschdienst fest, welche Dateien lokal noch nicht verfügbar sind. Damit synchronisiert er sich automatisch auf den neuesten Stand.
- Wenn der lokale Verzeichnisdienst gestört ist und der Austausch-DIT komplett rekonstruiert werden muss, ist es ausreichend, die lokale Konfiguration so anzupassen, dass alle Dateien vom Austauschdienst abgerufen und anschließend in den Verzeichnisdienst der Domäne geladen werden.

9.2.9 Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen für den Aktualisierungsprozess vom Austauschdienst zur Domäne sind analog zu den in Kapitel 6.2 genannten zu gestalten. Dabei können die Vorgaben jedoch insoweit reduziert werden, als die Domäne die Ergebnisse des Aktualisierungsprozesses intern bereitstellt und insofern auch die Folgen aus Störungen selbst trägt.

In diesem Abschnitt werden deshalb nur solche Punkte zusammengestellt, die der Abstimmung zwischen den Parteien oder zur Beurteilung spezieller Risiken für das Sicherheitsniveau der Domäne dienen.

9.2.9.1 Keine Konsistenzprüfung abgerufener LDIF-Dateien

Im Rahmen der Ausbaustufe 1 wird auf Seite der Domänen auf eine Konsistenzprüfung für LDIF-Dateien, die vom Austauschdienst abgerufen wurden, verzichtet. Die Domänen verlassen sich auf die Maßnahmen beim Eingang in den Verzeichnisdienst der Verwaltung. Das Risiko von Manipulationen im Bereich der Betreiber der Dienste des Verzeichnisdienstkonzepts wird akzeptiert. **Begründung:** Im Rahmen der Prozesse im VDV oder dem Austauschdienst sind sowohl die LDIF-Dateien als auch die Informationen über den Datenursprung unter der Kontrolle der Betreiber der Dienste des Verzeichnisdienstkonzepts. Um einen gesicherten Kanal für diese Informationen zu schaffen, müssten die LDIF-Dateien von der Quell-Domäne signiert werden. In der Ziel-Domäne wiederum wäre eine Schlüsselverwaltung notwenig, in der die Relation

zwischen Schlüsseln der Quelldomänen und den entsprechenden Teilbäumen des Austausch-DITs zu konfigurieren wäre. Für die Ausbaustufe 1 werden diese Maßnahmen als zu aufwändig angesehen. Mit steigenden Nutzerzahlen und im Rahmen der Weiterentwicklung des Verzeichnisdienstkonzepts sollte diese Entscheidung aber überprüft werden.

9.2.9.2 Kommunikationsverbindung

Wie im Aktualisierungsprozess von der Domäne zum VDV wird auch bei der Aktualisierung der Domänen die Verbindung von der Domäne aufgebaut. Es sind die gleichen kryptographischen Mechanismen einzusetzen. Die Firewalls und die Zugriffsrechte sind dementsprechend restriktiv zu konfigurieren.

9.2.9.3 Dateimanagement: Wiederaufsetzen und Audit

Die Dateien zum Wiederaufsetzen des Austausch-DITs in der Domäne stehen gemäß der Vorgaben für den Austauschdienst im Austauschdienst zur Verfügung. Zu Revisionszwecken in Streitfällen kann auf die LDIF-Dateien sowohl von der Quell-Domäne als auch vom Archiv des Austauschdienstes zurückgegriffen werden. Eine lokale Archivierung der LDIF-Dateien ist deshalb nicht erforderlich. Damit ergibt sich die folgende Entwurfsentscheidung: Der Aktualisierungsprozess zur Domäne löscht standardmäßig bei jedem Vollabgleich für einen Teilbaums des Austausch-DITs die in der Domäne vorhandenen LDIF-Dateien des Teilbaums. Log-Dateien werden behandelt wie im Aktualisierungsprozess zum VDV (vgl. Kapitel 6.2).

Teil IV: Weitere technische Teilkonzepte

10 Abfrage von PKI-Informationen per LDAP

Zwei der drei Dienste des Verzeichnisdienstkonzepts – der Verzeichnisdienst der Verwaltung und der Veröffentlichungsdienst – können direkt von Clients abgefragt werden. Dabei können Anfragen nach Teilnehmer-Zertifikaten, CA-Zertifikaten und Sperrlisten gestellt werden. Dieses Kapitel beschreibt die Spezifika dieser Abrufe.

Der zentrale Verzeichnisdienst der Verwaltung und der Veröffentlichungsdienst erhalten je einen eigenen DNS-Namen. Der Abruf erfolgt per LDAP über den Standard-Port 389. Clients müssen LDAPv3 unterstützen.[4]

Der Zugriff ist anonym und ohne Passwort möglich. Die Begrenzung des berechtigten Teilnehmerkreises für den zentralen Verzeichnisdienst der Verwaltung erfolgt über die Abgrenzungsmechanismen des Intranets und ist nicht Gegenstand des Verzeichnisdienstkonzepts.

Es wird empfohlen, dass Clients das Suchattribut "mail" verwenden, um nach Teilnehmerzertifikaten zu suchen. Für CA-Zertifikate und Sperrlisten soll der ganze DN aus dem Zertifikat verwendet werden. Eine Suche nach bestimmten Attributen oder Objektklassen wird nicht empfohlen, da dadurch spezifische Anpassungen für die unterschiedlichen Dienste notwendig werden könnten.

Der VDV wird die Anzahl der pro Abruf zurückgelieferten Entries auf 50 beschränken, der Veröffentlichungsdienst auf 10, um Denial-of-Service-Attacken durch fehlerhafte Anfragen oder Angriffe zu verhindern. Aus

4 Die Unterstützung von LDAPv2 wäre ausreichend, sofern der Client zusätzlich UTF8/UNICODE unterstützt. Da LDAPv2 als Standard ausläuft und um Interoperabilitätsprobleme in den übertragenen Zeichensätzen zu vermeiden, wird an dieser Stelle jedoch LDAPv3 gefordert.

demselben Grund wird eine Suche nach Teilstrings von E-Mail-Adressen nicht unterstützt.

Einige PKI-Informationen werden auch per HTTP bereitgestellt (vgl. Kapitel 11). Diese Daten können anonym über Port 80 abgerufen werden.

Die Entscheidung darüber, ob der Zugriff auf den LDAP-Server erlaubt oder beispielsweise durch vorhandene Firewalls oder andere Sicherheitsmaßnahmen verhindert wird, liegt in der Verantwortung der Domänen. Dieses Thema wird im VDK nicht untersucht.

Werden die in Zertifikaten gespeicherten Informationen bezüglich CDPs, AIAs oder anderer URIs zum Abruf von Zertifikaten und Sperrlisten verwendet, so liegt es in der Verantwortung der ausstellenden Domäne, für die Kompatibilität der Zertifikatseinträge mit der Namensgebung im VDV zu sorgen. Das Verzeichnisdienstkonzept und [PKI1V Namensregeln] enthalten Hinweise auf sinnvolle Vorgehensweisen. Die Einhaltung der Regeln und der Test der Funktionstüchtigkeit sind Aufgaben der Domänen und nicht Gegenstand des Verzeichnisdienstkonzepts.

11 Bereitstellung von PKI-Informationen per HTTP

Dieses Kapitel beschreibt das Vorgehen zur Bereitstellung und Aktualisierung der PKI-Informationen per HTTP.

Im Rahmen der Implementierung des Verzeichnisdienstkonzepts werden zwei HTTP-Server mit jeweils einem eigenem DNS-Namen eingerichtet. Sie sind jeweils dem Verzeichnisdienst der Verwaltung bzw. dem Veröffentlichungsdienst zugeordnet und entsprechend im Intranet bzw. im Extranet zugreifbar. Die Webserver und die Aktualisierungsprozesse für die HTTP-Seiten sind identisch aufgebaut. Die enthaltenen Daten unterscheiden sich danach, ob sie nur im VDV oder auch im Veröffentlichungsdienst bereitgestellt werden.

Die Seitenstruktur für die Bereitstellung der PKI-Informationen ergibt sich wie folgt:

- Auf einer Einstiegsseite werden alle Domänen aufgelistet, die am Verzeichnisdienstkonzept teilnehmen.
- Jede Domäne erhält im Laufe des Beitrittsverfahrens zu den Diensten des VDKs eine Unter-Seite. Die Unter-Seite hat den Namen des ou-Attributs, den die Zertifizierungsinstanzen im Austausch-DIT erhalten (entspricht der Gruppierung der CAs der Domäne im Austausch-DIT, Achtung: Umlaute und Sonderzeichen müssen aufgelöst werden!).
- Die Unter-Seite der Domäne enthält für jede CA Links auf Dateien, die das CA-Zertifikat und die Sperrliste enthalten.
- Die Dateien, auf die die Links der Dateien verweisen, erhalten als Namen jeweils den CN der CA. Die Endung ".crl" bzw ".crt" gibt an, ob es sich um ein Zertifikat oder eine Sperrliste handelt.
  Beispiel für einen vollständigen Link wäre dann
  http://PKI-1-V.PCA.de/PKI-Informationen/Thueringen/TESTA CA1.crl
- Die Zertifikate und Sperrlisten werden im DER-Format zur Verfügung gestellt (und ggf. vorher konvertiert).

- Die Konfiguration der Clients zum Abruf der Seiten und die Erzeugung entsprechender (CDP- oder AIA-) Einträge in den Zertifikaten liegt in der Verantwortung der Domänen.

Im Rahmen der Ausbaustufe 1 werden Teilnehmer-Zertifikate nicht per HTTP bereitgestellt.

Die HTTP-Seiten für CA-Informationen werden von Skripten mit Daten aus dem Verzeichnisdienst der Verwaltung bzw. dem Veröffentlichungsdienst generiert. Die Aktualisierung wird je Domäne angestoßen, nachdem die Daten einer LDIF-Datei vom Umfang "CA" in den entsprechenden Verzeichnisdienst eingestellt wurden.

Diese Vorgaben für die Skripte dieser Aktualisierung sind für eine Implementierung hinreichend und werden im Verzeichnisdienstkonzept nicht weiter spezifiziert.

12 Testunterstützung

Testbedarf im Rahmen des Verzeichnisdienstkonzepts besteht für drei verschiedene Szenarien:

- Prozesse des Verzeichnisdienstkonzepts werden verändert. Diese Veränderungen sollen getestet werden.
- Eine Domäne führt Tests mit Test-Zertifikaten aus, die noch nicht die Inhalte des Produktiv-Betriebs haben.
- Eine Domäne will testen, ob Angaben in produktiven Zertifikaten funktionstüchtig sind. (Dazu muss die Testumgebung aber unter den originalen DNS-Namen erreichbar sein, siehe unten.)

Es wird deshalb dringend empfohlen, im Rahmen des Verzeichnisdienstkonzepts einen separaten Server für Testzwecke zu betreiben. Für diesen Server sollten die folgenden Vorschläge im Rahmen der Realisierung geprüft und bei positiver Entscheidung als Vorgaben festgelegt werden:

- Der Server bietet einen Test-VDV und einen Test-Austauschdienst. Parallel zum Test-VDV sollte auch ein Test-HTTP-Server zur Verfügung stehen. Die beiden Dienste sind soweit wie möglich identisch mit den Parametern der produktiven Systemen konfiguriert. (Auf den Veröffentlichungsdienst kann vermutlich verzichtet werden.)
- Die beiden Test-Dienste müssen für die gegenseitige Authentisierung bei der Datenübertragung eigenes Schlüsselmaterial einsetzen. Im Rahmen der Implementierung muss entschieden werden, ob die Domänen für die Sicherung der Kommunikationsverbindung zu den Test-Diensten ebenfalls separates Schlüsselmaterial einsetzen müssen oder ob sie das gleiche Schlüsselmaterial verwenden dürfen, das auch für die produktiven Aktualisierungsprozesse eingesetzt wird.

- Die Zugangs- und Zugriffskontrolle stellt sicher, dass nur Berechtigte auf die Test-Dienste zugreifen können. Das bedeutet, dass beispielsweise kein anonymer Zugang möglich ist.

Im Rahmen der Implementierung sollte geprüft werden, ob für Zwecke des dritten Testszenarios z. B. mit Hilfe von Network Address Translation der Test-VDV unter dem DNS-Namen des produktiven VDV angesprochen werden kann (aber mit anderem Port).

Der Test-Server könnte in Notfallplänen als Plattform für den Notbetrieb des Austauschdienstes vorgesehen werden.

Teil V: Weitere Aspekte der Implementierung des VDKs

Die Kapitel dieses Teils stellen Maßnahmen zusammen, die zur Realisierung des Verzeichnisdienstkonzepts neben der technischen Spezifikation erforderlich sind. Diese Maßnahmen müssen konsistent zum technischen Konzept sein. Die Kapitel sind als Checklisten zu verstehen, die einerseits das technische Konzept ergänzen, andererseits aber unter dem jeweiligen Blickwinkel Punkte aufgreifen, die in den bisherigen Teilen bereits angesprochen wurden. Diese Redundanz wird in Kauf genommen, um die zur Realisierung erforderlichen Arbeiten für die Aspekte Recht, Organisation und Sicherheit jeweils im Zusammenhang darzustellen. Das Kapitel "Recht" nimmt dabei eine besondere Rolle ein, weil es die weiteren Maßnahmen verankert. Es enthält auch einen Strukturvorschlag für die Organisation der Rechtsbeziehungen und die Aufteilung der Verantwortlichkeiten.

13 Rechtliche Ausgestaltung

Dieses Kapitel gibt Hinweise zur rechtlichen Ausgestaltung des Betriebs des Verzeichnisdienstkonzepts. Sie sind als Vorschlag für die weitere Abstimmung zu verstehen und sollen den erwarteten Regelungsbedarf deutlich machen. Es werden nur solche Aspekte betrachtet, die für das Verzeichnisdienstkonzept relevant sind. Das Kapitel ist auch als zusammenfassende Checkliste für die rechtliche Ausgestaltung der Realisierung zu verstehen, weshalb Überschneidungen mit Inhalten anderer Kapitel unvermeidlich sind.

Zunächst werden die beteiligten Organisationen identifiziert und ein Vorschlag für den Aufbau der rechtlichen Beziehungen entwickelt. Im nächsten Schritt werden die wesentlichen Verantwortlichkeiten und Zuständigkeiten beschrieben. Der dritte Abschnitt des Kapitels schlägt vor, wie die rechtlichen Beziehungen und Pflichten in existierenden und neuen Dokumenten verankert werden können. Im letzten Abschnitt werden Aspekte einer Kostenregelung angesprochen.

Die Zuständigkeiten für die Aufgaben, die sich aus dem Verzeichnisdienstkonzept ergeben, sind noch nicht endgültig festgelegt. Sie bedürfen der Diskussion und Verabschiedung im weiteren Abstimmungsprozess des Verzeichnisdienstkonzepts. Daher kann hier nur ein erster Vorschlag für die rechtliche Ausgestaltung entwickelt werden. Sollten sich im Rahmen der Abstimmungsprozesse und der Implementierung Veränderungen ergeben, sind die folgenden Überlegungen entsprechend anzupassen. Auch die Referenzen auf Gremien und Organisationen sind als vorläufiger Vorschlag zu verstehen. Wer später der eigentliche rechtliche Vertragspartner ist (für bestimmte Aspekte z. B. ein oder zwei getrennte Steuerungsgremien, das Bundesministerium des Inneren oder die PCA) ist noch zu klären. In den folgenden Ausführungen müssen die verschiedenen Institutionen als mögliche Aufgabenträger verstanden werden.

Eventuell erforderliche Erweiterungen für die dem VDV und dem Veröffentlichungsdienst zugeordneten HTTP-Dienste sind entsprechend zu behandeln.

13.1 Beteiligte Organisationen und deren Beziehungen

Die folgenden fünf Organisationen sind (in einer idealtypischen Darstellung) an der Verankerung, Steuerung und dem Betrieb des Verzeichnisdienstkonzepts beteiligt:

- **Steuerungsgremium**: Das Steuerungsgremium für die Dienste des VDKs beschließt und beauftragt den Betrieb der Dienste des Verzeichnisdienstkonzepts und fällt die wesentlichen Entscheidungen für die Weiterentwicklung der Konzeption von PCA und VDK. Wer die Rolle des Steuerungsgremiums übernimmt, wird in den Beratungen des KoopA festgelegt. Gegenwärtig wird geklärt, wie die an der PKI-1-Verwaltung beteiligten Domänen und CAs gemeinsam die Weiterentwicklung der PKI-1-Verwaltung steuern (Steuerungsgremium der PKI). Es erscheint sinnvoll, zu prüfen, ob die beiden Gremien zusammengefasst werden. Im weiteren wird stellvertretend nur von einem Steuerungsgremium gesprochen.
- **Vertrags-CAs (VCA)**: Vertrags-CAs sind die CAs, die mit der PCA einen Vertrag haben [PKI1V Aufnahmevertrag] und von ihr zertifiziert sind. Sie betreiben oder beauftragen jeweils einen *lokalen Verzeichnisdienst* und nehmen damit an der PKI-1-Verwaltung und an den Diensten des Verzeichnisdienstkonzepts teil. Sie können in ihrem Verantwortungsbereich nachgeordnete Zertifizierungsinstanzen bestätigen. (**Hinweis:** Im Unterschied zum *rechtlichen Zuständigkeitsbereich* einer Vertrags-CA ist der im VDK verwendete Begriff der *Domäne* nur eine organisatorische Abgrenzung im technischen Modell des Verzeichnisdienstkonzepts. Eine Domäne kann z. B. mehrere Vertrags-CAs enthalten.) Die vertragliche Beziehung zwischen Vertrags-CA und PCA regelt die Umstände der Teilnahme an der PKI-1-Verwaltung. Er schließt die Abgabe einer Selbstverpflichtung der Vertrags-CA ein. Die Vertrags-CA muss auch die Sicherheitsleitlinie der PCA akzeptieren. PCA und Vertrags-CA sind damit verantwortlich, die in den genannten Dokumenten festgelegten Dienste zu erbringen und die entsprechenden Vertragsbedingungen einzuhalten.

Im Rahmen des Beitritts sollten auch die Verpflichtungen bezüglich der Dienste des VDKs geregelt werden.

- **PCA-1-Verwaltung:** Als Wurzel-Zertifizierungsinstanz gibt die PCA in ihrer Sicherheitsleitlinie den Zweck und Betrieb der Dienste des Verzeichnisdienstkonzepts bekannt. Sie wickelt außerdem den Beitritt von Vertrags-CAs zur PKI-1-Verwaltung ab. Dieses Beitrittsverfahren sollte um die Aspekte der Dienste des VDKs ergänzt werden. Die existierenden Dokumente [PKI1V Si-Leitlinie], [PKI1V Aufnahmevertrag], [PKI1V Selbsterklärung] wären hinsichtlich der Erfordernisse des VDKs anzupassen (vgl. unten).
- **Betreiber der Domänen-Directories**: Sie betreiben jeweils im Auftrag einer Vertrags-CA den lokalen Verzeichnisdienst.
- **Betreiber der Dienste des Verzeichnisdienstkonzepts:** Als Betreiber der Dienste des VDKs werden die Organisationen angesehen, die mit dem Betrieb der drei im Verzeichnisdienstkonzept spezifizierten Dienste beauftragt werden. Der Betrieb der Dienste kann je Dienst auf eine Organisation übertragen werden, er kann aber auch in einer Organisation zusammengefasst werden. Hinsichtlich der rechtlichen Ausgestaltung müssen die vertraglichen Pflichten jeweils geeignet aufgeteilt oder gebündelt werden. Hier wird zur Vereinfachung der Darstellung im weiteren jeweils nur von einem Betreiber ausgegangen.

Durch die verschiedenen Beteiligten und die der PKI-1-Verwaltung zugrunde liegende föderale Struktur ergeben sich die in Abbildung 16 dargestellten differenzierten Rechtsbeziehungen.

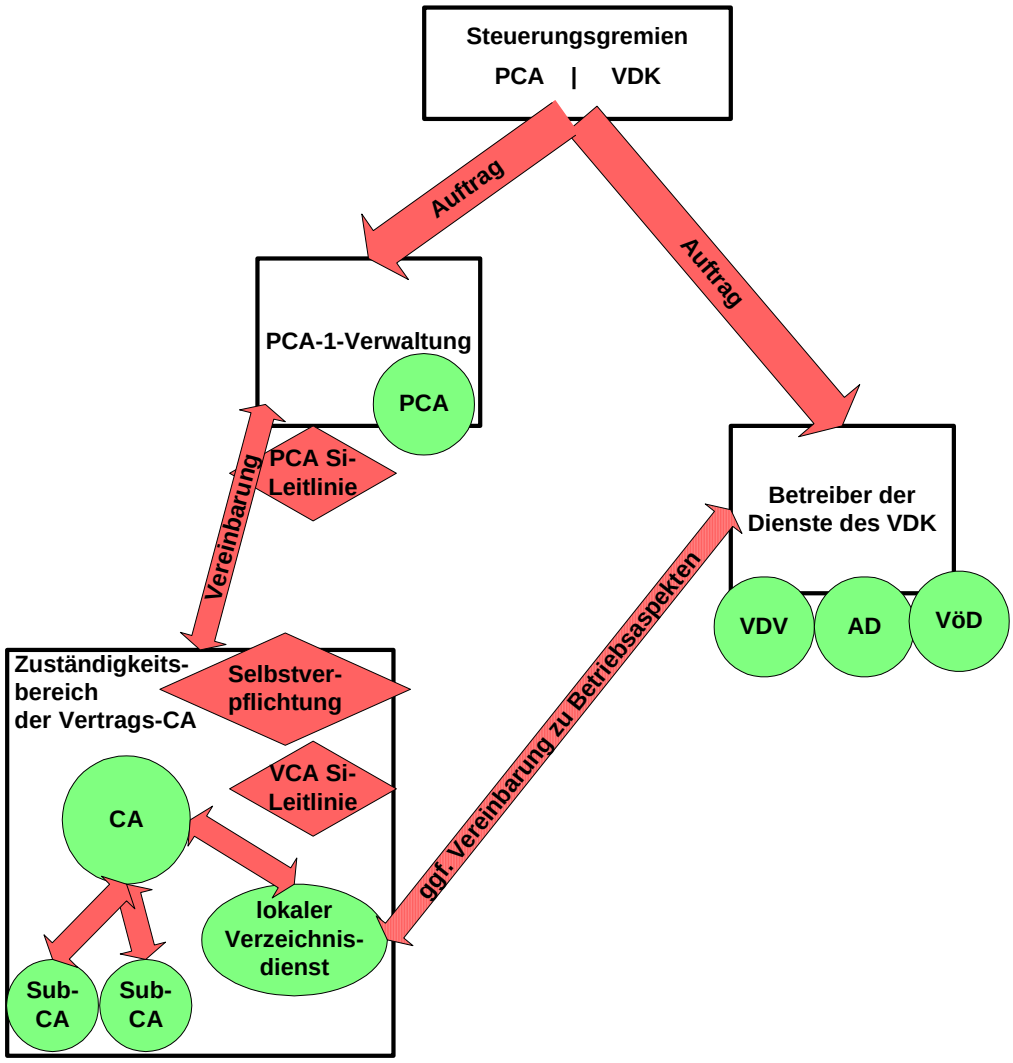

Abbildung 16: Grundlegende Rechtsbeziehungen bei der Umsetzung des Verzeichnisdienstkonzepts

Abbildung 16 zeigt die verschiedenen beteiligten Parteien (in Rechtecken) mit den von ihnen betriebenen technischen Systemen (in grün). Die roten Elemente stellen die wesentlichen rechtlichen Beziehungen und relevanten Dokumente dar. Der in der Abbildung skizzierte Vorschlag der Rechtsbeziehungen zum Betrieb des Verzeichnisdienstkonzepts wurde nach folgendem Modell strukturiert:

- Das Steuerungsgremium beauftragt als koordinierende Stelle den Betrieb der Dienste des Verzeichnisdienstkonzepts (oder delegiert diese Aufgabe geeignet).

- Das Steuerungsgremium beauftragt als koordinierende Stelle die PCA mit der Aufgabe, das Beitrittsverfahren zu überwachen und den Status der Dienste des VDKs zu beobachten.
- Für die Einbindung der Vertrags-CAs werden die bereits heute existierenden und für den Beitritt zur PKI-1-Verwaltung relevanten Dokumente geeignet erweitert. Die Weitergabe von Verpflichtungen innerhalb ihres Zuständigkeitsbereichs ist Sache der Vertrags-CAs.
- Falls dies erforderlich ist, kann für operative Zwecke noch eine Vereinbarung zwischen dem lokalen Verzeichnisdienst und dem Betreiber der Dienste des Verzeichnisdienstkonzepts geschlossen werden.

13.2 Verantwortlichkeiten

Im folgenden wird ein Vorschlag für die Verteilung der Aufgaben und Verantwortlichkeiten zwischen den einzelnen Organisationen dieser Aufteilung dargestellt.

13.2.1 Steuerungsgremium

Das Steuerungsgremium hat die Aufgaben eines Beschlussorgans. Es entscheidet und beauftragt den Betrieb von PCA und VDK. Es hat daher die konzeptionellen Entscheidungen hinsichtlich der Verantwortlichkeiten zu fällen und die Aufträge an die technischen und organisatorischen Betreiber der verschiedenen Dienste zu erteilen. Es muss sicherstellen, dass die Verträge eingehalten werden und der ordnungsgemäße Betrieb überwacht wird.

In den weiteren Beratungen des Verzeichnisdienstkonzepts wird der KoopA festlegen, wer die Rolle des Steuerungsgremiums übernimmt. Die Verankerung des Steuerungsgremiums sollte in einer geeigneten rechtlichen Form erfolgen. Dabei oder im Rahmen der Konstitution des Steuerungsgremiums müssen die einzelnen Aufgaben im Detail beschrieben und festgelegt werden. Aus der Sicht des Verzeichnisdienstkonzepts sollte das Steuerungsgremium mindestens für die folgenden Aufgaben zuständig sein:

Die Aufgaben zur **Initialisierung des Verzeichnisdienstkonzepts** umfassen u.a.:

- Die Verabschiedung der ablauforganisatorischen Verfahren, z. B. zum Beitritt von Vertrags-CAs und zu deren Ausscheiden (vgl. unten Kapitel 14). Vorschläge für solche Verfahren finden sich im Kapitel über "Organisation".
- Den Beschluss über Sanktionsmöglichkeiten für den Fall, dass sich Vertrags-CAs nicht an die im Vertrag, in der PCA-Sicherheitsleitlinie oder in der Selbstverpflichtung niedergelegten Auflagen halten.
- Die Beschlussfassung über Verfahren und Fristen, unter denen die Dienste des Verzeichnisdienstkonzepts eingestellt werden können.
- Die Beauftragung der PCA-1-Verwaltung und der Dienstebetreiber mit dem Betrieb der Dienste einschließlich gegebenenfalls erforderlicher Service-Level-Agreements.
- Die Festlegung der Abläufe für alle weiteren Aufgaben des Steuerungsgremiums.
- Den Beschluss über die Kostenregelungen für die Teilnahme an den Diensten des Verzeichnisdienstkonzepts.

Die **Kontrolle des laufenden Betriebs** der Dienste des VDKs beinhaltet:

- Diskussion des regelmäßigen Statusberichtes der PCA über die Dienste des Verzeichnisdienstkonzepts.

Die **Pflege und Weiterentwicklung** des Verzeichnisdienstkonzepts umfassen insbesondere:

- Entscheidungen über Weiterentwicklung und Gewährleistung eines Change-Managements, ggf. Festlegung von Vorlauf- und Übergangszeiten bei Veränderungen.
- Sicherstellen der Nachführung und Fortschreibung der Dokumentationen, soweit dies durch Veränderungen geboten ist.

Das Steuerungsgremium kann seine Aufgaben delegieren.

13.2.2 Betreiber der Dienste des Verzeichnisdienstkonzepts

Mit dem Betrieb der Dienste des VDKs können ein oder mehrere Betreiber beauftragt werden. Beauftragte Organisationen könnten auch Unterauftragnehmer hinzuziehen, um Teile der Dienste zu erbringen. Jeder vom Steuerungsgremium beauftragte Betreiber ist verpflichtet, alle ggf. beteiligten Unterauftragnehmer auf dieselben Bedingungen zu verpflichten, die für ihn selbst gelten. Die folgenden Verantwortlichkeiten gelten daher für alle am Betrieb der Dienste des VDKs beteiligten Organisationen, unabhängig von der konkreten Aufteilung der Aufgaben.

Im Falle der Vergabe von Teil-Aufträgen durch das Steuerungsgremium sind zusätzlich zu den im folgenden beschriebenen Bedingungen die Verträge und Service-Level-Agreements so festzulegen, dass die Abgrenzung der Verantwortlichkeit zwischen den Diensten klar geregelt ist und bei Störungen Zuständigkeiten einfach und schnell geklärt werden können. Im folgenden wird jeweils von einem Betreiber gesprochen; gegebenenfalls gelten die Ausführungen für mehrere Betreiber sinngemäß.

Die Aufgaben zur **Initialisierung des Verzeichnisdienstkonzepts** beinhalten u.a.:

- Der Betreiber der Dienste des VDKs muss ein lokales Sicherheitskonzept erstellen und umsetzen.
- Der Betreiber der Dienste des VDKs ist zuständig für das Sicherheitskonzept ab der Zuständigkeitsgrenze der Vertrags-CA. Er muss Aufgaben des übergreifenden Sicherheitskonzepts und die Umsetzung in konkrete Handlungsanweisungen übernehmen.
- Er muss Eskalationswege für Störungen einrichten.

Die Aufgaben des **laufenden Betriebs** umfassen für den Betreiber der Dienste des VDKs:

- Er betreibt einzelne oder alle drei Dienste und die zugehörigen Teile der Aktualisierungsprozesse des Verzeichnisdienstkonzepts und stellt einen ordnungsgemäßen Betrieb im Rahmen der geforderten Service-Qualität sicher.
- Der Betreiber der Dienste wirkt am Beitrittsverfahren von Vertrags-CAs mit.
- Er wirkt an der Aufklärung und der Beseitigung von Störfällen mit und koordiniert Maßnahmen zwischen den Beteiligten und Betroffenen, soweit dies erforderlich ist.
- Der Betreiber der Dienste wirkt an der Vorbereitung und Durchführung von Notfallübungen mit.
- Er muss zum jährlichen Statusbericht des VDKs beitragen.

13.2.3 PCA-1-Verwaltung

Die Aufgaben zur **Initialisierung des Verzeichnisdienstkonzepts** beinhalten u.a.:

- Die PCA dokumentiert in ihrer Sicherheitsleitlinie, dass der VDV und der Veröffentlichungsdienst angeboten werden.
- Die PCA stellt sicher, dass die weiteren Dokumente gemäß der endgültigen Erfordernisse angepasst werden (Vorschläge siehe unten).
- Sie prüft im Rahmen des Beitrittsverfahrens für Vertrags-CAs, ob die geforderten Voraussetzungen erfüllt sind, um am VDK teilzunehmen. Sie hat auch den Auftrag, Verstöße zu sanktionieren oder an das Steuerungsgremium weiterzugeben (Regelungen sind im Rahmen der Implementierung festzulegen).

Die **Mitwirkung im laufenden Betrieb** der Dienste des VDKs umfasst:

- Die PCA-1-Verwaltung wickelt die vom Steuerungsgremium festgelegten Abläufe zum Beitritt und zum Ausscheiden von Vertrags-CAs ab.

- Im Falle von Sanktionen durch das Steuerungsgremium kann die PCA die ausführende Stelle sein (z. B. bei erforderlichen Zertifikatssperrungen). Zusätzlich koordiniert sie das Change-Management.
- Die PCA ist zur Mitwirkung bei der Aufklärung von Störfällen und der Beseitigung von Störungen verpflichtet. Sie sollte berechtigt werden, in begründeten Fällen die notwenigen Audit-Maßnahmen bei den Beteiligten durchzuführen.
- Die PCA kann eine koordinierende Rolle in Störfällen einnehmen, wenn dies erforderlich ist.

Die Mitwirkung an der **Pflege und Weiterentwicklung** des Verzeichnisdienstkonzepts umfasst insbesondere:

- Die PCA liefert jährlich einen Bericht zum Status des Verzeichnisdienstkonzepts (vgl. Kapitel 14 zur Organisation) an das Steuerungsgremium ab.
- Die PCA ist Ansprechpartner bei Problemen, die mit dem Betrieb der Dienste des Verzeichnisdienstkonzepts auftreten. Sie leitet diese Probleme gegebenenfalls an das Steuerungsgremium (oder den Auftraggeber für die Dienste) weiter.
- Die PCA ist Ansprechpartner für Änderungsanträge, die das VDK betreffen. Sie leitet diese Änderungsanträge im Rahmen des Change-Management-Prozesses an das Steuerungsgremium weiter.
- Die PCA überprüft einmal jährlich die Aktualität und Funktionstüchtigkeit der Eskalationswege.
- Die PCA veranlasst einmal jährlich eine Notfallübung für den Bereich des Verzeichnisdienstkonzepts.

Bezüglich der Replikation der PKI-Informationen der PCA hat die PCA-1-Verwaltung die gleiche Rolle wie eine Vertrags-CA.

13.2.4 Vertrags-CAs

Die Teilnahme von Vertrags-CAs und nachgeordneten CAs an den Diensten des Verzeichnisdienstkonzepts ist optional. Grundsätzlich gilt jedoch, dass Ver-

trags-CAs die Namensregeln nach [PKI1V Namensregeln] einhalten und in ihrem Zuständigkeitsbereich durchsetzen müssen, um unter anderem die Option zur Teilnahme offen zu halten. Der Beitritt zur PKI-1-Verwaltung und zu den Diensten des Verzeichnisdienstkonzepts kann deshalb zeitlich auseinander fallen. Es wird den Vertrags-CAs jedoch dringend empfohlen, zumindest alle CA-Entries in die Dienste zu replizieren. Die Bereitstellung von Teilnehmerzertifikaten ist grundsätzlich optional.

Die Vertrags-CA muss beim **Beitritt zur PKI-1-Verwaltung** folgende VDK-spezifischen Auflagen erfüllen:

- Die Vertrags-CA muss sicherzustellen, dass sie und nachgeordnete CAs [PKI1V Namensregeln] einhalten.
- Die Vertrags-CA muss in ihrer Sicherheitsleitlinie darstellen, dass PKI-Informationen aus ihrem Zuständigkeitsbereich nicht in die Dienste des Verzeichnisdienstkonzepts repliziert werden, wenn sie nicht gleichzeitig den Diensten des VDKs beitritt.

Die Vertrags-CA muss beim **Beitritt zu den Diensten des Verzeichnisdienstkonzepts** folgende Aufgaben erfüllen:

- Die Vertrags-CA muss sicherzustellen, dass sie die aus dem Beitritt zu den Diensten des VDK erwachsenden Verfplichtungen erfüllt. Gegebenenfalls hat sie diese Verpflichtungen an die beauftragten Dritten weiterzugeben, insbesondere an den Betreiber des lokalen Verzeichnisdienstes.
- Die Erstellung und Umsetzung eines lokalen Sicherheitskonzepts bezüglich der lokalen Komponenten und Prozesse des VDKs.
- Die an der lokalen Bereitstellung von PKI-Informationen Beteiligten müssen das Beitrittsverfahren zu den Diensten des VDKs durchlaufen (vgl. Kapitel 14), die dort geforderten Voraussetzungen schaffen und entsprechende Erklärungen abgeben.
- Grundsätzlich erfolgt die Veröffentlichung der PKI-Informationen aus dem Bereich einer Vertrags-CA im Rahmen der im Betriebskonzept zugesicherten

Service-Qualität. Die Vertrags-CAs müssen selbst dafür Sorge tragen, dass die Übertragung von PKI-Informationen aus ihrem Zuständigkeitsbereich an den Verzeichnisdienst der Verwaltung rechtzeitig erfolgt. Gegebenenfalls sind interne Abläufe oder die Sicherheitsleitlinie der PCA entsprechend anzupassen.

Die **Mitwirkung im laufenden Betrieb** der Dienste des VDKs beinhaltet:

- Die Vertrags-CA hat die volle Verantwortung für die Richtigkeit und Aktualität der aus ihrem Zuständigkeitsbereich an die Dienste des VDKs übertragenen Informationen.
- Im Produktivbetrieb hat die Vertrags-CA die Verantwortung dafür, die Teile der Aktualisierungsprozesse in ihrem Zuständigkeitsbereich ordnungsgemäß durchzuführen. Sie muss sicherstellen, dass die von ihr geforderte Service-Qualität erreicht wird.
- Die Vertrags-CA muss an der Aufklärung von Störfällen und der Beseitigung von Störungen sowie an Notfallübungen mitwirken.
- Die Vertrags-CA muss zum jährlichen Statusbericht des VDKs beitragen.
- Die Vertrags-CA muss sicherstellen, dass Veränderungen an Komponenten oder Prozessen des VDKs in ihrem Zuständigkeitsbereich nur in Übereinstimmung mit dem Verzeichnisdienstkonzept erfolgen und ein ordnungsgemäßer Betrieb aufrechterhalten wird.

13.3 Verankerung rechtlicher Pflichten

Dieses Kapitel gibt Hinweise zur Ausgestaltung von vertragsrelevanten Dokumenten zwischen den verschiedenen Beteiligten des Verzeichnisdienstkonzepts. Sie sind als Vorschlag und Checkliste für die weitere Abstimmung zu verstehen und müssen im Rahmen der Implementierung an die endgültige Ausgestaltung, auch der Rechtsbeziehungen, angepasst werden. Es werden nur solche Aspekte betrachtet, die für das Verzeichnisdienstkonzept relevant sind.

Die rechtliche Verankerung der genannten Pflichten geschieht im wesentlichen an den in Abbildung 16 rot gekennzeichneten Stellen. Dazu sind zwei bis vier neue Dokumente erforderlich:

- Auch nach der Implementierung des Verzeichnisdienstkonzepts wird die Notwendigkeit bestehen, die Service-Qualität, eine Reihe von technischen Festlegungen, organisatorischen Abläufen und übergreifenden Sicherheitsmaßnahmen für alle Beteiligten verbindlich zu regeln. Hier wird angenommen, dass dazu das vorliegende Dokument zu einem "Betriebskonzept für die Dienste des VDKs " weiterentwickelt wird. Sofern sich dies anbietet, können die entsprechenden Inhalte aber auch in ein anderes Dokument integriert werden.
- Erforderlich ist der Auftrag für den Betreiber der Dienste des VDKs.
- Denkbar wäre eine oben bereits angesprochene Vereinbarung zwischen dem Betreiber des lokalen Verzeichnisdienstes und dem Betreiber der Dienste des VDKs. Das Erfordernis und die Inhalte solcher operativer Absprachen können aber erst festgelegt werden, wenn die Details der Implementierung feststehen. Eine solche Vereinbarung wird deshalb hier nicht weiter diskutiert.
- Die Beauftragung des lokalen Verzeichnisdienstes und Vereinbarungen mit nachgeordneten CAs sind Sache der Vertrags-CAs. Sie werden hier deshalb nicht betrachtet.

Wesentliche Verpflichtungen können aber durch die Ergänzung bereits vorhandener rechtlich bindender Dokumente erreicht werden. Die Sicherheitsleitlinie der PCA, die Beitrittsvereinbarung zwischen PCA und Vertrags-CA und die Selbstverpflichtung der Vertrags-CAs existieren bereits heute und können erweitert werden. Auch die heute schon im Rahmen des Beitrittsverfahrens vorgesehene Sicherheitsleitlinie der Vertrags-CA kann genutzt werden. Manche Pflichten werden auch im Rahmen des Beitrittsverfahrens geregelt (siehe Kapitel 14). An die PCA können die notwendigen Aufgaben entweder durch Erweiterung des bestehenden Erlasses zum Betrieb der PCA oder durch eine un-

abhängige Beauftragung übertragen werden. Die Lösung hängt unter anderem von künftigen Zuständigkeiten für die Aufsicht über die PCA ab.

Die folgenden Abschnitte stellen zusammen, welche neuen Vereinbarungen benötigt werden bzw. um welche Punkte existierende Dokumente ergänzt werden müssen.

Soweit Vertrags-CAs bereits vor der Änderung der Vertragsdokumente beigetreten sind, müssen deren Pflichten entsprechend erweitert werden.

13.3.1 Betriebskonzept der Dienste des Verzeichnisdienstkonzepts

Das "Betriebskonzept der Dienste des VDKs" dient als Referenz für den Betrieb der Dienste. Es kann im wesentlichen aus dem vorliegenden Dokument [PKI1V-VDK-Erg] weiterentwickelt werden und sollte die folgenden Teile mit übergreifender Relevanz für alle Beteiligten enhalten:

- Festlegungen und Details zur Gewährleistung der Service-Qualität (vgl. Kapitel 5.1),
- technische Festlegungen, z. B. Schema-Anforderungen, Namensregeln des Austausch-DITs (soweit nicht in [PKI1V Namensregeln] geregelt) und Umsetzungsregeln,
- Prozess-Spezifikationen,
- Organisationskonzept und organisatorischen Abläufe (Kapitel 14 in der noch anzufertigen Detaillierung) sowie
- lokale Sicherheitsmaßnahmen, die das übergreifende Sicherheitskonzept unterstützen, und Vorschläge zu Notfallmaßnahmen.

Das Betriebskonzept sollte geeignet mit den jeweils relevanten Teilen zum Vertragsbestandteil bei allen genannten Vertragsbeziehungen werden.

13.3.2 Auftrag für den Betreiber der Dienste des VDKs

Der Betreiber der Dienste des VDKs wird vom Steuerungsgremium mit dem Betrieb der Dienste des VDKs beauftragt. Bestandteil des Auftrags müssen sein:

- die oben genannten Aufgaben des Betreibers der Dienste des VDKs ,
- ein Service-Level-Agreement, mit dem die Einhaltung der im Betriebskonzept festgelegten Service-Qualität garantiert wird,
- die relevanten Anteile des Betriebskonzepts der Dienste des VDKs ,
- eine Regelung zum Change-Management, nach der Änderungen in den Diensten und Abläufen nur nach vorheriger Absprache mit dem Steuerungsgremium oder der PCA durchgeführt werden dürfen (einschließlich des Rahmens für Veränderungen und Mindestfristen für Anpassungen),
- das Recht des Steuerungsgremiums, Revisionen durchzuführen (beispielsweise in Anlehnung an die Klausel des Vertrags zwischen der PCA und Vertrags-CAs). Das Steuerungsgremium sollte eine Prüfgruppe mit der Durchführung beauftragen dürfen.

Es sind außerdem die Pflichten für das Vorgehen bei Störungen und die Eskalationswege festzulegen.

Zur Beauftragung könnte z. B. eine Erweiterung des TESTA-D Rahmenvertrags durchgeführt werden.

13.3.3 Erweiterungen der PCA-Sicherheitsleitlinie

Die aktuell geltende Sicherheitsleitlinie findet sich in [PKI1V Si-Leitlinie]. Sie sollte um VDK-relevante Punkte ergänzt werden.

Einzufügen wäre eine Erklärung zum Verzeichnisdienst der PKI-1-Verwaltung, die beinhalten könnte,

- dass der Verzeichnisdienst der Verwaltung und der Veröffentlichungsdienst im Rahmen der PKI-1-Verwaltung betrieben werden,

- dass die Entscheidung über die Bereitstellung von PKI-Informationen in der Hoheit der Vertrags-CAs liegt und insofern auf deren Sicherheitsleitlinien verwiesen wird,
- welche Service-Qualität erwartet werden kann,
- wer in welcher Weise die PKI-Informationen aus den Diensten abrufen kann und
- an wen sich Teilnehmer im Falle von Störungen des Verzeichnisdienstes wenden sollen.

Um den Teilnehmern die Konfiguration ihrer Komponenten zu erleichtern, sollte auch ein Hinweis auf die konsolidierten Namenregeln [PKI1V Namensregeln] aufgenommen werden.

Die Formulierung des § 3.2 Abs. 5 sollte auf die Aspekte des Verzeichnisdienstkonzepts ausgeweitet werden. (**Hinweis:** Es besteht in diesem Punkt Redundanz mit dem Vertrag zwischen der PCA und der Vertrags-CA)

13.3.4 Erweiterungen des Auftrags für den Betreiber der PCA

Der Auftrag zum Betrieb der PCA muss vom Steuerungsgremium um die oben genannten Verantwortlichkeiten erweitert werden. Soweit weitere Aufgaben vom Steuerungsgremium an die PCA übertragen werden sollen, sind diese zu ergänzen.

13.3.5 Erweiterung des Vertrages zwischen PCA und Vertrags-CA

Der bereits existierende Vertrag (vgl. [PKI1V Aufnahmevertrag]) sollte um die folgenden Punkte ergänzt werden:

- Der Vertrags-CA sollte die Möglichkeit zur Teilnahme an den Diensten des Verzeichnisdienstkonzepts eingeräumt werden, soweit sie die geforderten Voraussetzungen erfüllt (z. B. in § 5).
- Die bestehenden Modalitäten der Kündigung der Teilnahme und der Beendigung des Betriebes sollten um die Aspekte des VDKs ergänzt werden. Eine

separate Kündigung der Teilnahme an den Diensten des VDKs sollte zugelassen werden (die Vertrags-CA bleibt in diesem Fall weiter in der PKI-1-Verwaltung, repliziert aber nicht mehr in die Dienste).

- Die Möglichkeiten zur Überprüfung des Betriebs und zur außerordentlichen Kündigung (§ 3 Abs. 3) sollten auf die Aspekte des Verzeichnisdienstkonzepts ausgeweitet werden. Die Kündigung sollte dabei auch nur für die Dienste des VDKs möglich sein.
- Es sollte eine Verpflichtung zur Anpassung an Änderungen des VDKs im Rahmen des Change-Managements bestehen. Soweit die Vertrags-CA nicht am Verzeichnisdienstkonzept teilnimmt, betrifft dies nur die Namensregeln.
- Die Haftungsregelungen für Schäden, die aus Störungen im Bereich der Dienste des VDKs entstehen können, ist entsprechend der bereits für andere Aufgaben existierenden Regelung einzuschränken.

13.3.6 Erweiterungen der Selbstverpflichtung der Vertrags-CA

Die existierende Selbsterklärung [PKI1V Selbsterklärung] sollte wie folgt modifiziert bzw. ergänzt werden. Die kursiven Texte stellen den gegenwärtigen Stand dar.

- **Punkt 1:**
  "den ordnungsgemäßen Betrieb der Zertifizierungsstelle nach dem aktuellen Stand der Technik sicherzustellen,"
  Vorschlag: nach "Zertifizierungsstelle" ergänzen um "... und der Verzeichnisdienstleistungen, soweit sie nach der Sicherheitsleitlinie der Vertrags-CA bereitgestellt werden, ...". Außerdem ergänzen um: "Soweit Replikationen in den Verzeichnisdienst der Verwaltung und den Veröffentlichungsdienst erfolgen, werden die Vorgaben des Betriebskonzepts für die Dienste des Verzeichnisdienstkonzepts erfüllt."
- **Punkt 9:**
  "die für den operativen Betrieb erforderlichen Standardsicherheitsmaßnahmen nach IT-Grundschutzhandbuch umzusetzen und in einem Sicherheits-

konzept zu dokumentieren,"

Vorschlag: ergänzen um "Soweit Verzeichnisdienstleistungen nach der Sicherheitsleitlinie der Vertrags-CA bereitgestellt werden, werden für sie ebenfalls Sicherheitsmaßnahmen des IT-Grundschutzes und die nach dem Betriebskonzept der Dienste des VDKs geforderten Maßnahmen umgesetzt und dokumentiert."

- **Punkte**

  5.: *"den mit der Wurzelzertifizierungsstelle vereinbarten Namensraum einzuhalten,"*

  13: "*sicherzustellen, dass Zertifikate nur auf den Namen des Antragstellers bzw. auf ein von diesem gewähltes Pseudonym ausgestellt werden,*"

  und 15: *"auf ein Pseudonym ausgestellte Zertifikate als solche kenntlich zu machen,"*

  Vorschlag: "Die Vertrags-CA verpflichtet sich, den vereinbarten Namensraum einzuhalten und die konsolidierten Namensregeln [PKI1V Namensregeln] anzuwenden und in ihrem Zuständigkeitsbereich durchzusetzen." Es wäre sinnvoll, die in der aktuellen Fassung der Selbsterklärung enthaltenen Details zur Namensgebung in die konsolidierten Namensregeln [PKI1V Namensregeln] zu verlagern und nur noch auf die Einhaltung dieses Dokuments zu verpflichten. Die Punkte könnten in der Selbsterklärung entfallen, wenn sie über die Namensregeln oder anderweitig abgedeckt sind.

- **Punkt 8:**

  "die eigenen Sicherheitsleitlinien nach anerkannten Standards (z. B. RFC 2527) der Allgemeinheit in verständlicher Form zugänglich zu machen,"
  Vorschlag zur Änderung oder neuer Punkt: Die Vertrags-CA gibt in ihrer Sicherheitsleitlinie bekannt, ob und welche Informationen in den VDV und Veröffentlichungsdienst mit welcher Service-Qualität repliziert werden. Sie verpflichtet sich zur rechtzeitigen Aktualisierung der Zertifikate und Sperrinformationen, so dass jederzeit (im Rahmen der Service-Qualität des VDKs) gültige Informationen in den Diensten zur Verfügung stehen.

- **Neu:** Die Vertrags-CA verpflichtet sich, nach dem Beitritt zu den Diensten des Verzeichnisdienstkonzepts an der Beseitigung und Aufklärung von Störungen mitzuwirken und einen jährlichen Bericht über den Status des Verzeichnisdienstes im Zuständigkeitsbereich der Vertrags-CA abzugeben.

13.3.7 Anforderungen an die Sicherheitsleitlinie der Vertrags-CA

Die Vertrags-CA muss gemäß [PKI1V Selbsterklärung, Nr. 8] eine eigene Sicherheitsleitlinie veröffentlichen. Diese Sicherheitsleitlinie muss den Sachstand bezüglich der Unterstützung der Dienste des VDKs darstellen.

Solange die Vertrags-CA dem Verzeichnisdienstkonzept *noch nicht beigetreten* ist, muss enthalten sein:

- die Aussage, dass PKI-Informationen aus ihrem Zuständigkeitsbereich nicht in den VDV und Veröffentlichungsdienst repliziert werden.

Sobald die Vertrags-CA den Diensten des Verzeichnisdienstkonzepts *beigetreten ist*, muss enthalten sein:

- eine Aussage, welche Informationen in den VDV und Veröffentlichungsdienst mit welcher Service-Qualität repliziert werden,
- (solange diese Entscheidung für das VDK gilt:) dass je Teilnehmer-Entry nur ein Zertifikat in die Dienste des VDKs repliziert wird,
- die Informationen zur Ausstellung und Gültigkeitsdauer von Sperrlisten in einer Form, aus der der Teilnehmer erkennen kann, ob er durch die Überlappung im Normalbetrieb der Dienste des VDKs immer eine gültige Sperrliste vorfindet oder ob es zu "Lücken" kommen kann,
- eine Information zur Kontaktaufnahme bei Störungen im Bereich des Verzeichnisdienstes.

13.4 Kostenregelung

Eine konkrete Festlegung einer möglichen Struktur der Gebühren für die Teilnahme an den Diensten des Verzeichnisdienstkonzepts der PKI-1-Verwaltung

kann erst im Rahmen der Implementierung erfolgen. Sie hängt unter anderem von der endgültigen Verteilung von Aufgaben, von den entstehenden administrativen Abläufen und den Verträgen mit den Betreibern der Dienste des Verzeichnisdienstkonzepts und den anderen Beteiligten ab. Zu berücksichtigende Elemente einer Gebührenregelung können sein:

- Eine Gebühr für den Beitritt einer Vertrags-CA, die den Aufwand z. B. hinsichtlich der Tests, der Einrichtung der Wurzelknoten für die Namensbereiche im Austausch-DIT (neue "o="-Knoten für Teilnehmer, "ou="-Knoten für die CAs), Support für die Installation der Prozesse etc. abdeckt.
- Eine regelmäßige Gebühr für die Teilnahme an den Diensten des VDKs. Die regelmäßige Gebühr könnte unter anderem umfassen:
  - anteilig die laufenden Kosten für die Betreuung des Verzeichnisdienstkonzepts bei der PCA,
  - die anteiligen Lizenzgebühren für die Entries in den Diensten des Verzeichnisdienstkonzepts aus dem Bereich einer Vertrags-CA im Austausch-DIT,
  - anteilige Betriebskosten der Dienste des Verzeichnisdienstkonzepts und
  - eine Umlage von Kosten für die Pflege und Weiterentwicklung der Prozesse.

14 Organisatorische Aspekte

Im Kapitel "Recht" wird eine Aufteilung der Verantwortlichkeiten und der rechtlichen Pflichten zwischen den verschiedenen beteiligten Organisationen vorgeschlagen. In diesem Kapitel wird davon ausgegangen, dass diese Aufgabenteilung verabschiedet wurde. Die folgenden Abschnitte beschreiben darauf aufbauend die organisatorischen Anforderungen, die sich aus dem Verzeichnisdienstkonzept für die Abläufe und die Aufbauorganisation der an der PKI-1-Verwaltung beteiligten Organisationen ergeben. Das Kapitel enthält Vorschläge für den weiteren Abstimmungsprozess und soll den erwarteten Regelungsbedarf deutlich machen. Es ist auch als zusammenfassende Checkliste für die organisatorischen Aspekte der Realisierung zu verstehen, weshalb Überschneidungen mit Inhalten anderer Kapitel unvermeidlich sind.

Für die hier beschriebenen Anforderungen ist folgendes zu beachten:

- Es sind nur Anforderungen aufgeführt, die sich aus dem Verzeichnisdienstkonzept ergeben.
- Die Darstellung entspricht der *Konzeptsicht*. Für einige Aspekte besteht noch Klärungsbedarf. Beispielsweise können Änderungen in der weiteren Abstimmung des Verzeichnisdienstkonzepts oder in der Implementierungsphase Auswirkungen auf organisatorische Abläufe haben. Weitere Anpassungen können sich aus Abhängigkeiten in der Aufteilung von Aufgaben zwischen dem Steuerungsgremium der PKI-1-Verwaltung und der PCA ergeben. Die organisatorischen Anforderungen sind deshalb im Rahmen der Implementierung zu ergänzen und zu detaillieren.
- Die organisatorischen Maßnahmen, die zur Erfüllung des Sicherheitskonzepts erforderlich sind, sind im Rahmen des Sicherheitskonzepts aufgeführt. Sie werden über den organisatorischen Ablauf beim Beitritt einer Vertrags-CA durch die Forderung eines Sicherheitskonzepts eingebunden.

- Die verbindliche Verankerung der organisatorischen Anforderungen erfolgt über die Verantwortungsaufteilung und Vorschläge zu den rechtlichen Regelungen (Kapitel 13).

14.1 Anforderungen an die Aufbauorganisation

14.1.1 Organisatorische Anforderungen an die PCA

Die PCA-1-Verwaltung (im weiteren kurz PCA) ist für die Durchsetzung der Policy für die PKI-1-Verwaltung verantwortlich. Aus den durch das Verzeichnisdienstkonzept erweiterten Aufgaben ergeben sich Anforderungen an die Aufbauorganisation.

Die PCA muss intern die Zuständigkeiten im Rahmen des Verzeichnisdienstkonzepts regeln für:

- die Stelle, die Ansprechpartner der CAs und für Änderungsanträge zur PKI-1-Verwaltung ist,
- die Durchführung der unten unter "Ablauforganisation" definierten Prozesse, soweit die PCA hieran beteiligt ist,
- die jährliche Erstellung eines Berichts zum Verzeichnisdienstkonzept,
- die Eskalation von Störfällen und
- die Zuständigkeiten zur Beherrschung von Notfällen.

Hinweis: Da die PCA die Wurzel-Zertifizierungsinstanz betreibt, muss sie auch die entsprechenden "organisatorischen Anforderungen an CAs" erfüllen.

14.1.2 Organisatorische Anforderungen an CAs

Jede CA, die den Diensten des VDKs beitritt, muss Regelungen der Zuständigkeiten treffen für:

- eine Stelle, die Ansprechpartner der PCA ist,
- das Einstellen von PKI-Informationen in das lokale Verzeichnis,

- die Administration der lokalen Teilprozesse des Verzeichnisdienstkonzepts,
- die Überwachung der lokalen Teilprozesse des Verzeichnisdienstkonzepts,
- das Audit der lokalen Teilprozesse des Verzeichnisdienstkonzepts,
- die Eskalation von Störfällen und
- die Reaktionen in Störfällen.

Die für diese Aufgaben notwendigen Stellen sind in Übereinstimmung mit den Anforderungen des Rollenkonzepts (Kapitel 15.3) im erforderlichen Umfang mit zuverlässigem, qualifiziertem Personal auszustatten. Es ist dafür Sorge zu tragen, dass die Stellen in alle für sie relevanten Abläufe eingebunden sind.

Sofern die Vertrags-CA innerhalb ihres Zuständigkeitsbereichs weitere CAs zertifiziert, muss sie sicherstellen, dass es eine Stelle gibt, die die Anbindung *aller nachgeordneten CAs* an die Dienste des VDKs koordiniert. Die Stelle ist als Ansprechpartner für die PCA zu benennen. Sie ist dafür verantwortlich, dass der ordnungsgemäße Betrieb für ihren Zuständigkeitsbereich sichergestellt wird. Die Anforderungen für den Beitritt einer CA (vgl. unten) sind daher für nachgeordnete CAs entsprechend anzuwenden.

Die Vertrags-CA muss sicherstellen, dass alle Anforderungen des Verzeichnisdienstkonzepts im Verlaufe des Beitrittsverfahrens und darüber hinaus eingehalten werden.

14.1.3 Organisatorische Anforderungen an Betreiber der Dienste des Verzeichnisdienstkonzepts

Im Rahmen der Implementierung des Verzeichnisdienstkonzepts müssen ein oder mehrere Betreiber beauftragt werden, den Verzeichnisdienst der Verwaltung, den Austauschdienst und den Veröffentlichungsdienst bereitzustellen. Jeder Betreiber eines der Dienste des Verzeichnisdienstkonzepts muss Regelung der Zuständigkeiten treffen für:

- eine Stelle, die Ansprechpartner der PCA ist,

- die Durchführung der unter Ablauforganisation definierten Prozesse, soweit der Dienst hieran beteiligt ist,
- die Administration der Teilprozesse des jeweils betriebenen Dienstes,
- die Überwachung der Teilprozesse des jeweils betriebenen Dienstes,
- das Audit der Teilprozesse des jeweils betriebenen Dienstes,
- die Definition, Umsetzung und Kontrolle des lokalen und übergreifenden Sicherheitskonzepts,
- die Eskalation von Störfällen und
- die Reaktionen in Störfällen.

Die für diese Aufgaben notwendigen Stellen sind in Übereinstimmung mit den Anforderungen des Rollenkonzepts (Kapitel 15.2.2) im erforderlichen Umfang mit zuverlässigem, qualifiziertem Personal auszustatten. Jeder Betreiber muss sicherstellen, dass alle Anforderungen des Verzeichnisdienstkonzepts in geeignete interne Abläufe umgesetzt werden. Es ist dafür Sorge zu tragen, dass die Stellen in alle für sie relevanten Abläufe eingebunden sind.

Es wird empfohlen, im Rahmen des Implementierungsprozesses und der Beauftragung die Aufgaben für die Betreiber der Dienste des Verzeichnisdienstkonzepts genauer festzulegen. Insbesondere sollten festgelegt werden:

- die Dokumentationspflichten einschließlich des internen Sicherheitskonzepts,
- ihre Rolle im Rahmen der unten beschriebenen Abläufe,
- ein definierter Änderungs- und Freigabeprozess für Änderungen an den Diensten des Verzeichnisdienstkonzepts oder den Aktualisierungsprozessen.

14.2 Ablauforganisation

In diesem Abschnitt werden Abläufe mit ihren Beteiligten beschrieben, die zum ordnungsgemäßen Betrieb des Verzeichnisdienstkonzepts erforderlich sind. Dies sind:

- der Beitritt und das Ausscheiden von Vertrags-CAs,
- das Löschen von CA-Entries und CDP-Entries im A-DIT,
- die Regelung von Ausnahmen,
- das übergreifende Change-Management für das Verzeichnisdienstkonzept,
- die jährliche Überprüfung des Verzeichnisdienstkonzepts und
- die Auflösung der Dienste des Verzeichnisdienstkonzepts.

14.2.1 Beitritt von CAs

Die folgende Beschreibung des Beitrittsverfahrens zu den Diensten des Verzeichnisdienstkonzepts stellt sicher, dass ein ordnungsgemäßer Betrieb der Dienste des VDKs erwartet werden kann. Der Beitritt zum den Diensten des VDKs kann zeitlich später als der Beitritt zur PKI-1-Verwaltung erfolgen. Der Ablauf ist daher so zu implementieren, dass er unabhängig vom Beitritt zur PKI erfolgen kann.

Die folgende Ablaufbeschreibung soll einen vollständigen Überblick über die Voraussetzungen geben. In einigen Punkten treten deshalb Dopplungen mit dem Beitritt der Vertrags-CA zur PKI auf. In diesem Fall werden die Ergebnisse des Beitritts zur PKI übernommen. Dies betrifft beispielsweise die Abstimmung des Namensraums oder die Abgabe der Selbsterklärung.

Das Beitrittsverfahren wird mittels des Vertrags zwischen PCA und Vertrags-CA geregelt. Der Beitritt von Vertrags-CAs zu den Diensten des VDKs erfolgt im Regelfall in vier Schritten. Im Falle der Ausweitung von CA-Aufgaben kann ein vereinfachtes Verfahren definiert werden (siehe unten). Für CAs die mit Windows 2000 arbeiten, gelten die Anforderungen mit den entsprechenden Ausnahmeregeln aus [PKI1V Namensregeln].

Schritt 1: Voraussetzungen für den Beitritt

Im ersten Schritt wird gefordert, dass die CA die lokalen Voraussetzungen für den ordnungsgemäßen Betrieb des Verzeichnisdienstkonzepts schafft. Dazu

muss die CA zum Zeitpunkt der Antragstellung sicherstellen, dass die in der folgenden Liste aufgeführten Konzepte und Vorgaben erstellt und umgesetzt wurden. An dieser Stelle wird angenommen, dass die Inhalte der Vertragsdokumente entsprechend Kapitel 13 angepasst wurden. Sollte dies nicht der Fall sein, sind geeignete Anpassungen der folgenden Checkliste vorzunehmen. Soweit Dokumente als Voraussetzung für den Beitritt *vorzulegen* sind, wird in der Liste darauf gesondert hingewiesen.

- Die Vertrags-CA schlägt folgende Namensbestandteile vor für den (Vorschlag vorzulegen, wird mit der PCA abgestimmt):
  - Wurzelknoten für die DIT-DNs der Teilnehmer-Entries ("o="),
  - Wurzelknoten für die DIT-DNs der CAs und CDPs (ou=) sowie
  - Namen der untergeordneten HTTP-Seite, auf der die Vertrags-CA und die nachgeordneten CAs ihre Zertifikate und CRLs veröffentlichen sollen.
- Die Vertrags-CA definiert die Zuständigkeiten für den lokalen Betrieb der Prozesse des Verzeichnisdienstkonzepts in Übereinstimmung mit den Anforderungen des Sicherheitskonzepts und der Aufbau-Organisation der CA. Dies schließt die Überwachung von nachgeordneten CAs bei der Einrichtung und Modifikation von VDK-relevanten Prozessen ein.
- Die Vertrags-CA trifft Regelungen, welche Entries in den VDV und den Veröffentlichungsdienst repliziert werden und wer für die Belegung der Steuerungsattribute verantwortlich ist.
- Die Vertrags-CA passt den lokalen Directory Information Tree und das lokale Directory-Schema an die Vorgaben der Namensregeln [PKI1V Namensregeln] und des Verzeichnisdienstkonzepts an.
- Die Vertrags-CA definiert die Konfigurationsparameter und Maßnahmen für den Betrieb der lokalen Teilprozesse gemäß der Vorgaben des Verzeichnisdienstkonzepts, u.a. Festlegung der Periode für Differenzabgleiche zum VDV auf der Basis der geforderten Service-Qualität und Festlegung der Periode für den Vollabgleich.

- Die Vertrags-CA definiert die Konfigurationsparameter und Maßnahmen für die Erzeugung von Sperrlisten in ihrem Zuständigkeitsbereich mit geeignetem Überlappungszeitraum in Abhängigkeit von der Policy der CA und den Replikationsrhythmen für Aktualisierungsprozesse.
- Die Vertrags-CA definiert lokale Verfahren für die Ablauforganisation des Verzeichnisdienstkonzepts, z. B. für das Löschen von CA- und CDP-Entries der eigenen Domäne oder anderer Domänen.
- Die Vertrags-CA erstellt ein lokales Sicherheitskonzept gemäß Kapitel 15.3 für den Verzeichnisdienst der Domäne und die Aktualisierungsprozesse des Verzeichnisdienstkonzepts.
- Die Vertrags-CA definiert die Zuständigkeiten für die Eskalation im Falle von Störungen der Dienste des Verzeichnisdienstkonzepts und von Personal für die Reaktion auf Störungen.
- Die Vertrags-CA muss in ihrer Sicherheitsleitlinie darstellen, welche PKI-Informationen aus ihrem Zuständigkeitsbereich mit welcher Service-Qualität in die Dienste des Verzeichnisdienstkonzepts repliziert werden. Die Vertrags-CA erstellt und veröffentlicht dort auch die notwendigen Kontaktinformationen für die Eskalation und Behebung von Störungen (vorzulegen).
- Die Vertrags-CA erarbeitet und integriert VDK-spezifische Notfall-Maßnahmen in ihre Notfall-Pläne und in die Notfallpläne des Betreibers des Verzeichnisdienstes der Domäne. Sie stellt sicher, dass entsprechende Erweiterungen von Notfallmaßnahmen für nachgeordnete CAs ihres Zuständigkeitsbereichs vorgenommen werden.
- Die Vertrags-CA definiert einen Change-Management-Prozess, durch den sichergestellt wird, dass bei Änderungen an den lokalen Teilprozessen des

Verzeichnisdienstkonzepts oder anderen VDK-relevanten Veränderungen im Zuständigkeitsbereich der CA[5] folgende Schritte eingehalten werden:

- Aufsetzen eines Change-Management-Prozesses mit klaren Verantwortlichkeiten,
- Erstellung eines Change-Management-Plans,
- gegebenenfalls Information anderer Beteiligter am VDK einschließlich der PCA, um z. B. beim Auflösen von CAs oder bei Änderungen in der Aufteilung von Teilbäumen mit Entries von Teilnehmern Störungen zu vermeiden,
- gegebenenfalls Tests der Veränderungen und
- Umsetzung der Veränderungen in den produktiven Abläufe.

Die Vertrags-CA erklärt, dass die Vorgaben des Verzeichnisdienstkonzepts einschließlich dieser Liste erfüllt werden und innerhalb der Zuständigkeit der CA für alle nachgeordneten CAs durchgesetzt werden (Erklärung vorzulegen).

Schritt 2: Vorbereitung von Tests

Sind die Voraussetzungen aus Schritt 1 gegeben, werden im zweiten Schritt die Voraussetzungen geschaffen, um Tests durchzuführen.

Die CA muss die erforderlichen Komponenten zur Sicherung der Kommunikationsverbindung zum VDV und Austauschdienst beschaffen.

Die CA erhält Zugriff auf die Testsysteme des VDKs. Die Testsysteme des VDKs werden gemäß der Vorgaben des Sicherheitskonzepts konfiguriert, z. B. durch Einrichten des Eingangsbereichs und der Schlüsselverwaltung für die Authentisierung des Teilprozesses der Domäne. Die Testsysteme werden au-

5 Beispiele können sein: das Einrichten oder Auflösen von nachgeordneten CAs, Replikation neuer Teilbäume mit Entries von Teilnehmern, Änderung des Steuerattributs für die Veröffentlichung von Teilnehmer-Entries oder das Ändern der Gültigkeitsdauer von Sperrlisten.

ßerdem gemäß der vereinbarten Namens-Bestandteile erweitert (z. B. Einrichten des Wurzel-Knotens für Teilnehmer des neuen Namensraumes, des ou-Knotens im Teilbaum "o=PKI-1-Verwaltung" und der entsprechenden HTTP-Seite).

Die PCA stellt sicher, dass die Integration der beitretenden CA in die bestehenden Eskalations- und Notfallpläne erfolgt, damit die Kommunikationswege im nächsten Schritt überprüft werden können.

Schritt 3: Durchführung von Tests

Als dritter Schritt müssen Tests durchgeführt werden. An den Test sind die beitretende Domäne, der Betreiber der Testsysteme des VDKs und mindestens eine Domäne beteiligt, die bereits am Verzeichnisdienstkonzept teilnimmt ("Partner-Domäne"). Auf den Testsystemen des Verzeichnisdienstkonzepts müssen folgende Tests erfolgreich durchgeführt und dokumentiert sein:

- das Einstellen und automatische Aktualisieren eines CA-Entries in den Test-VDV,
- das Einstellen von Teilnehmer-Entries in den Test-VDV,
- der Abruf von CA-Zertifikaten und CRLs vom Test-HTTP-Server, der dem Test-VDV zugeordnet ist,
- die Übernahme von CA-Entries aus dem Test-Austauschdienst in eine der bereits produktiven Domänen (die importierende Domäne kann ihrerseits ebenfalls ein Testsystem einsetzen),
- Verfügbarkeit und Funktionstüchtigkeit der Eskalationswege im Falle von Störungen der Dienste des Verzeichnisdienstkonzepts.

Der Schritt wird abgeschlossen, indem der PCA ein Testplan mit den Testergebnissen und einer Zusammenfassung vorgelegt wird. Das Dokument muss von den für die Tests verantwortlichen Mitarbeitern der beitretenden Domäne, des Betreibers der Testsysteme des VDKs und der Partner-Domäne unterzeichnet sein.

Schritt 4: Freischalten des Produktiv-Betriebs

Sind die Voraussetzungen aus Schritt 4 gegeben, erhält die CA Zugriff auf die produktiven Systeme des VDKs**.** Die Produktiv-Systeme werden gemäß der Vorgaben des Sicherheitskonzepts konfiguriert und um die vereinbarten Namens-Bestandteile erweitert (z. B. Einrichten des Wurzel-Knotens für Teilnehmer des neuen Namensraumes, des ou-Knotens im Teilbaum "o=PKI-1-Verwaltung" und der entsprechenden HTTP-Seite). Der Produktiv-Betrieb wird aufgenommen.

Vereinfachtes Verfahren für die Erweiterung von Domänen

Sofern eine bereits beauftragte CA ihren Einsatzbereich ausweitet, kann ein vereinfachtes Verfahren zur Anwendung kommen. Dies könnte beispielsweise bei der TESTA-CA der Fall sein, wenn sie von einem neuen Bundesland beauftragt wird.

In einem solchen Fall können alle Anforderungen als erfüllt angesehen werden, für die

- sich keine Abweichungen gegenüber den Anforderungen eines früheren Beitritts ergeben,
- die Annahme berechtigt erscheint, dass die bisher definierten und praktizierten Abläufe auch geeignet sind, um den erweiterten Zuständigkeitsbereich der CA ordnungsgemäß zu unterstützen.

Hinweis: Da sich beim Beitritt eines neuen Bundeslandes oder einer Kommune die oberen Namensteile im DIT zumindest für die Teilnehmer ändern, sind dann auch die entsprechenden Abstimmungen der Namensregeln mit der PCA notwendig. Die Einrichtung der Entries im Austausch-DIT ("o=" für Teilnehmer und ggf. "ou=" für CAs) ist ebenfalls erforderlich. Die vorlaufenden Tests werden für diesen Fall dringend empfohlen.

14.2.2 Ausscheiden von Vertrags-CAs

Vertrags-CAs können ihre Teilnahme an der PKI-1-Verwaltung gemäß [PKI1V Aufnahmevertrag] regulär mit einer Frist von 3 Monaten kündigen. Die PCA kann einer Vertrags-CA regulär mit einer Frist von 12 Monaten kündigen. Die Möglichkeit zur Kündigung sollte so erweitert werden, dass die Vertrags-CA die Teilnahme an den Diensten des VDKs separat kündigen kann.

Beim Ausscheiden einer Vertrags-CAs müssen aus der Sicht des Verzeichnisdienstkonzepts die folgenden Schritte eingehalten werden. Sofern nachgeordnete CAs betroffen sind, gilt entsprechendes.

Unmittelbar nach der Kündigung erstellt die PCA mit der Domäne einen **Austrittsplan**. In diesem Austrittsplan ist mit den entsprechenden Details zu regeln:

- Wer ist verantwortlich für die Durchführung und Überwachung des Plans?
- Übernimmt eine andere CA die Sperrung der bisher ausgestellten Zertifikate?[6]
- Falls nicht: werden nur die CA-Zertifikate gesperrt oder werden auch alle Teilnehmer-Zertifikate zurückgezogen? Für welchen Zeitraum sollen diese Sperrinformationen noch über das Verzeichnisdienstkonzept zugänglich gemacht werden?
- Wann werden der CA-Entry und gegebenenfalls betroffene CDP-Entries in den Diensten des Verzeichnisdienstkonzepts gelöscht? (Dabei sind die Abläufe für das Löschen von CA- und CDP-Entries zu beachten).
- Wer ist vom Ausscheiden der CA zu informieren?
- Welche Aktualisierungen in rechtlich relevanten Dokumenten sind erforderlich, z. B. in der Sicherheitsleitlinie der Vertrags-CA?

6 Zumindest für die gegenwärtig bekannten Produkte muss angenommen werden, dass dies technisch nicht oder nur mit großen Problemen möglich ist. Die Frage ist insofern aus der Sicht des Verzeichnisdienstkonzept relevant, weil sie mit darüber entscheidet, ob ein CA-Entry aufrecht erhalten werden muss.

- Wer ist Ansprechpartner bei Problemen?
- Wann werden die Teilnehmer-Entries der Domäne gelöscht und welche Maßnahmen müssen dazu ergriffen werden?
- Wann und in welcher Weise sind die Eskalationspläne und Notfallpläne des Verzeichnisdienstkonzepts zu überarbeiten?

14.2.3 Löschung von CA-Entries und CDP-Entries im A-DIT

Insbesondere nachgeordnete CAs können in Verzeichnisdiensten "auslaufen", beispielsweise wenn sie gesperrt wurden oder umbenannt werden und die "alte" CA ihren Betrieb ordnungsgemäß einstellt. In diesem Fall kann nach dem Gültigkeitsende des letzten Teilnehmer-Zertifikats der CA-Entry in den Diensten des Verzeichnisdienstkonzepts gelöscht werden. Es sind auch Situationen denkbar, in denen eine nachgeordnete CA nicht mehr in die Dienste des VDKs repliziert werden sollen.

Verantwortlich auf der Seite der ausscheidenden CA ist aus der Sicht des Verzeichnisdienstkonzepts die Vertrags-CA. Zum Löschen einer CA müssen aus der Sicht des Verzeichnisdienstkonzepts die folgenden Schritte eingehalten werden:

- Die Vertrags-CA meldet der PCA möglichst einen Monat vor Betriebsende, dass die ausscheidende CA ihren Betrieb einstellen wird. Dieser Meldung ist eine Erklärung mit dem Termin der Betriebseinstellung und dem Gültigkeitsende der Sperrliste beizufügen. Die Vertrags-CA muss außerdem erklären, dass mit der letzten replizierten Sperrliste alle verbliebenen Teilnehmer-Zertifikate gesperrt wurden und nach dem Gültigkeitsende der letzten Sperrliste keine gültigen Teilnehmerzertifikate mehr existieren.
- Die Vertrags-CA stellt sicher, dass bis einschließlich dieser letzten Sperrliste eine ordnungsgemäße Replikation erfolgt, sofern diese erforderlich ist.

- Die PCA setzt den Termin für den Anstoß zur Löschung des CA-Entries auf einen Zeitpunkt nach dem Gültigkeitsende der letzten Sperrliste fest. Der zeitliche Abstand soll mindestens eine Woche betragen.
- Die PCA informiert mindestens eine Woche vor dem Anstoß zur Löschung alle Domänen und die Stellen, die die Eskalation von Störungen und die Reaktionen auf Notfälle zentral koordinieren.
- Die PCA informiert zum festgelegten Zeitpunkt (nach dem Gültigkeitsende der Sperrliste) alle Betreiber der Dienste des Verzeichnisdienstkonzepts und alle beigetretenen Domänen darüber, dass der Entry in den Verzeichnisdiensten gelöscht werden kann.
- Die Betreiber der Dienste des Verzeichnisdienstkonzepts melden die Löschung an die PCA zurück. Die Domänen organisieren die Löschung in den lokalen Verzeichnisdiensten intern ohne Rückmeldung an die PCA.

Für ausgelaufene CDPs ist der Ablauf entsprechend anzuwenden.

14.2.4 Ausnahmeregelungen

In begründeten Fällen und in Notsituationen sind Ausnahmen von den vorgegebenen Abläufen oder Sicherheitsmaßnahmen unter folgenden Voraussetzungen zulässig:

- Sofern die Ausnahme nicht zur Behebung einer schweren Störung des produktiven Betriebs notwendig ist, muss die Ausnahme bei der PCA beantragt werden. Der Antrag muss begründet werden. Die PCA kann die Ausnahme in begründeten Fällen zulassen. Die Ausnahme ist zu befristen. Die CA und die PCA überwachen, dass die Befristung eingehalten wird. Sofern die Abweichungen die Sicherheit des Verzeichnisdienstkonzepts beeinträchtigen, sind die Beteiligten des VDKs von der PCA zu informieren.
- Sofern in einem schweren Störfall zur Behebung Ausnahmen von Vorgaben gemacht werden, sollen sich diese an den Notfallplänen des Verzeichnisdienstkonzepts orientieren. Die Abweichungen sind zu dokumentieren und

schnellstmöglich der PCA mitzuteilen. Die PCA muss unter Beteiligung der CAs einen Plan entwickeln, wie zum ordnungsgemäßen Betrieb zurückzukehren ist. Die Schritte sind mit Terminen zu versehen. Sofern die Abweichungen die Sicherheit des Verzeichnisdienstkonzepts beeinträchtigen, sind die Beteiligten des VDKs von der PCA zu informieren.

14.2.5 Change-Management für das VDK

Es ist zu erwarten, dass das Verzeichnisdienstkonzept anhand gewonnener Erfahrungen und mit dem Ausbau der PKI-1-Verwaltung ergänzt oder modifiziert werden muss. Außerdem können neue Versionen der in den Domänen und bei den Betreiber der Dienste des VDKs eingesetzten Systeme Anpassungen erforderlich machen. Um den Abhängigkeiten zwischen den verschiedenen Beteiligten Rechnung zu tragen, ist im Rahmen der Implementierung ein Change-Management-Prozess zu definieren.

Alle Beteiligten sind allerdings selbst dafür verantwortlich, frühzeitig Änderungsanträge zu stellen. Adressat von Änderungsanträgen ist die PCA, die den Change-Management-Prozess anstößt und überwacht. Die Entscheidung über die Umsetzung eines Änderungsantrags trifft das Steuerungsgremium der PKI-1-Verwaltung.

Der Change-Management-Prozess sollte mindestens folgende Schritte enthalten:

- die Festlegung der verantwortlichen Stelle für die inhaltliche Betreuung,
- Erstellung eines Änderungsplans. Der Änderungsplan muss enthalten:
  - alle Veränderungen des Verzeichnisdienstkonzepts, die sich aus dem Änderungsantrag ergeben, einschließlich der organisatorischen Abläufe und des Sicherheitskonzepts,
  - einen Zeitplan für die Abwicklung einschließlich der Einführungsphase und
  - einen Vorschlag für die Kostenübernahme.

- die Information aller Vertrags-CAs und weiterer Betroffener über die geplante Veränderung mit Möglichkeit zur Stellungnahme,
- Entscheidung über die Durchführung des Änderungsplans,
- Implementierung der Änderungen,
- Tests aller Änderungen,
- die Information aller Vertrags-CAs und weiterer Betroffener über den Abschluss der Implementierung und der Tests mit einem Zeitplan für die Einführung und
- die Einführung.

Je nach Anpassungsaufwand ist den Vertrags-CAs ausreichend Zeit einzuräumen, um in ihrem Zuständigkeitsbereich über die Veränderungen zu informieren und Tests und die Einführung vorzubereiten.

14.2.6 Jährliche Überprüfung des Verzeichnisdienstkonzepts

Die jährliche Überprüfung des Verzeichnisdienstkonzepts dient dazu, Probleme im Betrieb zu erkennen und abstellen zu können. Außerdem bietet sie die Möglichkeit, frühzeitig auf neue Entwicklungen zu reagieren und Anpassungen des Verzeichnisdienstkonzepts anzustoßen.

Die jährliche Überprüfung des Verzeichnisdienstkonzepts wird von der PCA durch die folgende Abläufe realisiert:

- **Jährliche Überprüfung der Eskalationswege:**
  Die PCA stößt mindesten einmal im Jahr per E-Mail gemäß Verteiler eine Überprüfung der Eskalationswege an. Sie überprüft, ob sie mindestens einen Rücklauf je Vertrags-CA und je Betreiber der Dienste des Verzeichnisdienstkonzepts erhält. Auf der Basis der Rückläufe werden die Unterlagen zur Information über Eskalationswege aktualisiert. Die Unterlagen werden anschließend an die Beteiligten verteilt.
- **Jährliche Notfall-Übung:**
  Die PCA definiert mindestens einmal jährlich ein Notfall-Szenario. Sie legt

nach Möglichkeit wechselnde Parteien fest, die sich an der Übung beteiligen müssen. Die Notfall-Übung wird unter möglichst realistischen Bedingungen durchgeführt, wobei die Störung des produktiven Betriebs gering gehalten werden soll. Die Ergebnisse der Übung werden dokumentiert. Anhand der Auswertung werden die Notfallpläne des Verzeichnisdienstkonzepts überarbeitet. Alle am Verzeichnisdienstkonzept Beteiligten sind auf die Veränderungen hinzuweisen.

- **Jährlicher VDK-Status-Bericht:**
  Die PCA erstellt einen jährlichen Bericht zum Status des Verzeichnisdienstkonzepts. Der Bericht soll qualitative Aussagen machen über den erreichten Ausbau, den Umfang der Nutzung durch die Teilnehmer, das Schadenspotential der Anwendungen bei Störungen, den Grad der Abhängigkeit von einzelnen Komponenten des VDKs und die Angemessenheit des erreichten Sicherheitsniveaus. Er soll mögliche Performanzprobleme aufzeigen und Hinweise zu einer notwendigen Weiterentwicklung enthalten. Die PCA fragt vor Erstellung des Berichts bei den Domänen die erforderlichen Informationen ab, die mit vertretbarem Aufwand gewonnen werden können, beispielsweise aus den zusammenfassenden Log-Dateien oder Störfall-Berichten. Der Bericht soll außerdem die Ergebnisse der Überprüfung der Eskalationswege und der Notfall-Übung zusammenfassen. Er soll auch den Stand der laufenden Anpassungsprozesse des Verzeichnisdienstkonzepts dokumentieren. Der Bericht wird dem Steuerungsgremium der PKI-1-Verwaltung zur Beratung vorgelegt.

14.2.7 Auflösung der Dienste des Verzeichnisdienstkonzepts

Ein Ablaufplan, der bei der Einstellung des Betriebs der Dienste des Verzeichnisdienstkonzepts einzuhalten ist, ist während der Implementierungsphase zu entwickeln. Er soll berücksichtigen, ob auch der Betrieb der PCA eingestellt wird oder ob dieser aufrecht erhalten wird.

15 Sicherheitskonzepte des VDKs

Dieses Kapitel dient zur Überprüfung und Ergänzung der im technischen Konzept enthaltenen Sicherheitsmaßnahmen. Es schlägt Maßnahmen für die weitere Abstimmung vor, mit denen ein adäquates Sicherheitsniveau erreicht werden sollte. Das Kapitel hat damit auch Checklisten-Charakter für die weitere Ausarbeitung und Realisierung eines Sicherheitskonzepts für den Betrieb der Dienste des VDKs. Überschneidungen mit Inhalten anderer Kapitel sind deshalb unvermeidlich. Die abschließende Ausgestaltung muss im Rahmen der Realisierung erfolgen. Die festgelegten Vorgaben können dann beispielsweise in Service-Level-Agreements, das Betriebskonzept für die Dienste des VDKs oder andere rechtlich relevante Dokumente einfließen.

Das Verzeichnisdienstkonzept muss als Bestandteil einer *Infrastruktur* gesehen werden. Die Leistungen der Infrastruktur werden durch das Zusammenwirken verschiedener Beteiligter erbracht.

Dementsprechend enthält auch das Sicherheitskonzept übergreifende Aspekte. Die beteiligten Organisationen müssen die Vorgaben dieser übergreifenden Sicherheitsmaßnahmen erfüllen soweit sie in ihre Verantwortung fallen und in ihre lokalen Sicherheitskonzepte integrieren.

Für Sicherheitsmaßnahmen verantwortlich sind der Betreiber der Dienste des VDKs und die Vertrags-CAs. Die Verantwortung des Betreibers der Dienste des VDKs beginnt danach an der Grenze der Zuständigkeit der Domäne, schließt also die wesentlichen Teile der übergreifenden Maßnahmen ein (vgl. dazu auch die Verantwortungsaufteilung in Kapitel 13). Zum Erreichen des Sicherheitsniveaus müssen deshalb zwei Sicherheitskonzepte zusammenwirken: das des Betreibers der Dienste des VDKs und das der jeweiligen Vertrags-CA.

Im folgenden werden dargestellt:

- das erforderliche Sicherheitsniveau,

- die Maßnahmen zur Erreichung dieses Sicherheitsniveaus, die sich auf die Sicherheitskonzepte des Betreibers der Dienste des VDKs und der Vertrags-CA beziehen, in jeweils eigenen Abschnitten,
- sowie die im Rahmen der ersten Ausbaustufe des Konzepts akzeptierten Schwachstellen.

Hinweis: In diesem Dokument werden nur Anforderungen aus dem Bereich des Verzeichnisdienstkonzepts an das Sicherheitskonzept betrachtet. Vorgelagerte Prozesse, beispielsweise die Zertifizierung und das Einstellen von PKI-Informationen in den lokalen Verzeichnisdienst der Domäne, werden hier nicht untersucht.

15.1 Sicherheitsniveau

Der Verzeichnisdienstkonzept ist Bestandteil der Infrastruktur, die als PKI-1-Verwaltung aufgebaut wird. Für diese PKI werden Sicherheitsmaßnahmen gefordert, die den IT-Grundschutz sicherstellen. Entsprechend sind auch **für das Verzeichnisdienstkonzept Sicherheitsmaßnahmen des IT-Grundschutzes** zu ergreifen. Anwendungen, für die dieses Sicherheitsniveau nicht ausreichend ist, müssen eigene Maßnahmen ergreifen, um ihre Sicherheitsziele zu erreichen. Wegen der besonderen Bedeutung der Verfügbarkeit von Sperrlisten für die Anwendungen werden im Bereich der Verfügbarkeit allerdings bereits mit dem jetzigen Konzept erste Maßnahmen ergriffen, die über den IT-Grundschutz hinausgehen (vgl. dazu die Vorgaben in Kapitel 5.1).

Begründung

Die folgenden kurze Schutzbedarfsanalyse zeigt, dass das geforderte Sicherheitsniveau für die mit dieser Ausbaustufe zu erwartenden Schadenspotential hinreichend ist.

Hinsichtlich der Anwendungen können folgende Annahmen getroffen werden:

- Im Verlaufe des Zeithorizonts bis Ende 2004 muss bereits mit hohen Teilnehmerzahlen gerechnet werden. Eine Störung der Dienste des Verzeichnis-

dienstkonzepts könnte deshalb die Arbeit vieler Teilnehmer beeinträchtigen. Störungen in den Diensten des Verzeichnisdienstkonzepts könnten dazu führen, dass Teilnehmer auf den Einsatz von Verschlüsselung verzichten, Probleme bei Signaturprüfung auftreten oder ganz allgemein Arbeitsabläufe beeinträchtigt werden.

- Die PKI-1-Verwaltung ist für den Schutz von sensitiven Daten ausgelegt. Die Zulassung zur Verwendung für Dokumente mit der Klassifizierung "Verschlusssache - nur für den Dienstgebrauch" wird zur Zeit geprüft.
- Die PKI-1-Verwaltung ist nicht für qualifizierte Signaturen im Sinne des Signaturgesetzes ausgelegt. Es kann deshalb angenommen werden, dass keine rechtsverbindlichen Anwendungen auf der PKI-1-Verwaltung aufsetzen, die beispielsweise ein hohes monetäres Schadenspotential aufweisen.

Abhängig von den Teilnehmerzahlen und den Anwendungen, die sich auf den Austauschdienst und den Veröffentlichungsdienst abstützen, kann eine Störung im Verzeichnisdienst der PKI-1-Verwaltung viele Teilnehmer und Anwendungen betreffen. Ist deshalb für den Zeithorizont bis 2004 ein mittleres Schadenspotential anzunehmen. Deshalb werden die folgenden Sicherheitsziele definiert:

- **Vertraulichkeit:** PKI-Informationen, die zur Veröffentlichung in den Diensten des Verzeichnisdienstkonzepts bereitgestellt werden, müssen per Definition nicht geschützt werden. Sofern Informationen exklusiv nur für den Verzeichnisdienst der Verwaltung oder den Austauschdienst (also nicht zur allgemeinen Veröffentlichung im Extranet) übermittelt werden, sind Maßnahmen des Grundschutzes gegen externe Angreifer ausreichend.
- **Integrität:** Die PKI-Informationen sind mit starker Kryptographie gegen Verfälschung geschützt; die jeweilige Integritätsprüfung der PKI-Information muss von den Anwendungen durchgeführt werden. Allerdings kann diese nur erfolgreich sein, wenn jeweils die richtigen Informationen im Verzeichnisdienst bereitgestellt werden. So könnte eine falsch eingestellte Sperrliste für die Wurzel-Zertifizierungsinstanz zu einem Denial-of-Service aller PKI-

Anwendungen führen, die diese Sperrliste abrufen. Externe Angreifer dürfen deshalb nicht in der Lage sein, PKI-Informationen im Rahmen der Aktualisierungs-Prozesse des Verzeichnisdienstkonzepts zu verfälschen. Die Maßnahmen zur Sicherung der Integrität dieser Prozesse sollen einen Integritätsschutz durchsetzen, mit dem erwartet werden kann, dass externe Angreifer zuverlässig abgewehrt werden. Der Kreis möglicher interner Angreifer muss soweit wie möglich eingegrenzt werden.

- **Verfügbarkeit:** Die Nichtverfügbarkeit von PKI-Informationen einschließlich fehlender Aktualisierung kann zum Denial-of-Service der abhängigen Anwendungen führen. Die möglichen kumulierten Schäden aus einer solche Störung in Form von Verzicht auf Verschlüsselung, Problemen bei Signaturprüfungen, Beeinträchtigungen von Arbeitsabläufen, Unmut über die Störung, Arbeitszeitverlusten und möglichen Rufschäden sind aus der Sicht der Nutzer der PKI-1-Verwaltung als mittel einzuschätzen, soweit sie zeitlich begrenzt werden können. Zum gegenwärtigen Stand des Aufbaus der PKI-1-Verwaltung wird allerdings nicht angenommen, dass sehr zeitkritische Prozesse von den Leistungen der PKI-1-Verwaltung abhängen. Insgesamt erscheinen daher die Vorgaben zur Verfügbarkeit und Daten-Qualität, wie sie im Kapitel 5.1 getroffen wurden, als ausreichend. Um diese Anforderungen zu erreichen, werden im Rahmen des Verzeichnisdienstkonzepts deshalb parallel drei Ziele verfolgt:

  - Leichte Störfälle in den Prozessen oder Diensten des Verzeichnisdienstkonzepts sollen möglichst ohne Folge für die Anwendung überbrückt werden oder in ihren Auswirkungen auf einen kleinen Anteil der Teilnehmer begrenzt werden. Die Maßnahmen können sich dabei auf die Verfügbarkeit von CA- und CDP-Entries konzentrieren. Geringfügige Beeinträchtigungen der Aktualität dieser Daten können in solchen Situationen in Kauf genommen werden.

  - Die Dienste des Verzeichnisdienstkonzepts der PKI-1-Verwaltung müssen eine hohe Verfügbarkeit und definierte Reaktionszeiten auf leichte Störfälle sicherstellen.

- Das Verzeichnisdienstkonzept unterstützt verschiedene Rückfalloptionen zum Wiederaufsetzen von Prozessen oder Recovery der PKI-Informationen. Ein Ausfall zentraler Komponenten kann notfalls über bilateralen Datenaustausch überbrückt werden.

Unter dieser Bewertung ist für alle beteiligten Komponenten und Prozesse des Verzeichnisdienstkonzepts ein Sicherheitsniveau zu fordern, das mindestens dem IT-Grundschutz entspricht. Es wird empfohlen, dieses Sicherheitsniveau bereits zu Beginn der Ausbaustufe 1 zu realisieren, auch wenn zu diesem Zeitpunkt noch relativ wenige Teilnehmer zu erwarten sind. Das zu fordernde Sicherheitsniveau ist vom Steuerungsgremium der PKI-1-Verwaltung in jährlichen Abständen zu überprüfen.

Für schwere Störfälle wird im Rahmen der Service-Qualität keine Zusicherung gegeben. Für die Ausbaustufe 1 sollte es aber möglich sein, selbst bei einem Totalausfall der Dienste des Verzeichnisdienstkonzepts mit bilateraler Kommunikation erste Überbrückungsmaßnahmen einzuleiten.

Gewährleistung des ordnungsgemäßen Betriebs

Um einen ordnungsgemäßen Betrieb der Dienste des Verzeichnisdienstkonzepts sicherzustellen und Störungen möglichst zu vermeiden, werden Verfahren für den Beitritt und das Ausscheiden von Domänen vorgeschrieben. Im Rahmen dieser Verfahren sind bei den Beteiligten die Voraussetzung für den ordnungsgemäßen Betrieb zu schaffen und zu testen. Außerdem müssen übergreifende und dazu passende lokale Change-Management-Prozesse definiert werden. Im Falle von Abweichungen von Vorgaben des Verzeichnisdienstkonzepts kann das Steuerungsgremium mit Sanktionsmöglichkeiten reagieren. Außerdem soll parallel zu den Diensten des Verzeichnisdienstkonzepts im Wirkbetrieb ein Server zu Testzwecken zur Verfügung stehen. Störungen des Wirkbetriebs durch Tests sollten dadurch nahezu völlig vermieden werden. Die genannten Maßnahmen sind in den Kapiteln 12, 13 und 14 dargestellt.

Sicherheitsmaßnahmen

Die im folgenden geforderten Sicherheitsmaßnahmen dienen dazu, die Service-Qualität der Dienste des Verzeichnisdienstkonzepts sicherzustellen und das erforderliche Sicherheitsniveau zu erreichen. Die Maßnahmen sind in den rechtlichen Regelungen mit den Beteiligten verankert (vgl. Kapitel 13 und 14). Im Rahmen der Implementierung des Verzeichnisdienstkonzepts ist zu prüfen, inwieweit das Sicherheitskonzept zu detaillieren und in bereits existierende Dokumente der PKI-1-Verwaltung einzuarbeiten ist.

Der nächste Abschnitt beschreibt die Sicherheitsmaßnahmen, die beim Betreiber der Dienste des Verzeichnisdienstkonzepts zu ergreifen sind. Er sollte auch für die Betreuung der übergreifenden Sicherheitsmaßnahmen zuständig sein. Anschließend werden die Sicherheitsmaßnahmen in den Domänen aufgeführt. Diese müssen die relevanten Teile der übergreifenden Sicherheitsmaßnahmen in ihren lokalen Sicherheitskonzepten aufgreifen.

15.2 Konzept-Teile beim Betreiber der Dienste des VDKs

Unabhängig davon, ob der Betrieb der Dienst des Verzeichnisdienstkonzepts auf einen oder auf mehrere Dienstleister verteilt ist, wird im folgenden nur von einem Betreiber gesprochen. Bei einer Aufteilung der Zuständigkeiten gelten die Anforderungen für alle Dienstleister entsprechend. Es muss außerdem sichergestellt werden, dass an den Schnittstellen zwischen den Betreibern keine Sicherheitslücken entstehen. Für zentrale Aufgaben ist jeweils ein Verantwortlicher zu beauftragen.

Die Sicherheitsmaßnahmen des Verzeichnisdienstkonzepts betreffen zunächst lokale Vorgaben. Allerdings ist es für einige Sicherheitsziele erforderlich, dass mehrere Beteiligte zusammenwirken. Dieses Zusammenwirken muss in einem übergreifenden Konzept abgestimmt werden und mündet dann in ergänzende Maßnahmen auf der lokalen Ebene. Es wird vorgeschlagen, dass der Betreiber der Dienste des VDKs für die Koordination und für alle Maßnahmen des über-

greifenden Sicherheitskonzepts verantwortlich ist, die außerhalb der Grenzen der Vertrags-CA liegen (vgl. Kapitel 13.2.2).

Im folgenden werden zuerst die Sicherheitsmaßnahmen des übergreifenden Sicherheitskonzepts und dann die lokalen Maßnahmen beim Betreiber der Dienste des VDKs vorgestellt.

15.2.1 Übergreifende Aspekte des Sicherheitskonzepts

Das Verzeichnisdienstkonzept enthält bereits eine Reihe von übergreifenden Sicherheitsmaßnahmen. Sie sind Im Rahmen der Implementierung zu präzisieren und in lokale Maßnahmen umzusetzen. Die Ausarbeitung der Details kann je nach Vorgehensweise während der Implementierung durch den Betreiber der Dienste des VDKs erfolgen oder durch Dritte unterstützt werden. Das übergreifende Sicherheitskonzept sollte vom Steuerungsgremium der PKI-1-Verwaltung oder zumindest von der PCA verabschiedet werden.

Damit umfassen die Aufgaben des Betreiber der Dienste des VDKs:

- Abstimmung der Einzelmaßnahmen zwischen seinem Sicherheitskonzept und den Maßnahmen der Vertrags-CAs,
- Einrichten von Eskalationswegen für Störungen,
- Entwicklung von Notfallplänen, die zur Beherrschung übergreifender Störfälle geeignet sind,
- Koordination der Reaktionen im Falle von übergreifenden Störungen und Information von Betroffenen, soweit dies erforderlich ist,
- die Kontrolle von Veränderungen des Verzeichnisdienstkonzepts hinsichtlich ihrer Auswirkungen auf das übergreifende Sicherheitskonzept,
- das Management des übergreifenden Sicherheitskonzepts und seine Weiterentwicklung (vgl. Kapitel 13 und 14). Er nutzt dazu bei Bedarf den Change-Management-Prozess des Verzeichnisdienstkonzepts und die Abstimmung im Steuerungsgremium.

Die bisher im Verzeichnisdienstkonzept vorgesehenen Bestandteile des übergreifenden Sicherheitskonzepts einschließlich der Reaktionsmöglichkeiten auf Störfälle werden im folgenden skizziert. Sie sind der Anknüpfungspunkt für die Ausgestaltung der Sicherheitsmaßnahmen während der Implementierung. Die Maßnahmen sind in das übergreifende Notfallkonzept einzubeziehen.

Übergreifende Maßnahmen zur Gewährleistung der Verfügbarkeit

Um die Verfügbarkeit der Dienste des Verzeichnisdienstkonzepts zu erreichen, werden Maßnahmen im Rahmen der Beauftragung der Betreiber der Dienste des VDKs, zur Verringerung der Ausbreitung, zur frühzeitigen Erkennung und zur Reaktion auf Störungen ergriffen:

Die **Beauftragung der Betreiber der Dienste des VDKs** muss Vorgaben zur Verfügbarkeit der Dienste (vgl. Kapitel 5.1), zu Eskalations-Wegen und Einbindung bei der Störfall-Beherrschung enthalten. Es ist weiter zu fordern, dass die TK-Anbindung der Dienste des VDKs redundant ausgelegt ist.

Um eine **geringere Abhängigkeit** von einzelnen Komponenten und Prozess-Schritten und eine **langsamere Ausbreitung von Störungen** zu erreichen, werden folgende Maßnahmen ergriffen:

- Durch Überlappung von Sperrlisten sollten zeitliche Spielräume entstehen, durch die auf kleinere Störungen reagiert werden kann, ohne dass dies relevante Auswirkungen auf die Anwendungen hat.
- Durch den Import von Teilen des Austausch-DITs in die Domänen entsteht eine redundante Datenhaltung. Störungen der zentralen Dienste sollten deshalb zunächst nur einige Teilnehmer aus den Domänen und die externen Teilnehmer betreffen.
- Die Zulieferung von Quell-Domänen an den Verzeichnisdienst der Verwaltung wird je Domäne auf Konsistenz geprüft (vgl. unten Maßnahmen zur Gewährleistung der Integrität). Dadurch kann ein Angriff in einer Domäne die Daten einer anderen Domäne im Austausch-DIT nicht beeinflussen.

Um **Störungen kurzfristig zu erkennen** und koordiniert reagieren zu können, werden folgende Maßnahmen ergriffen:

- Die Spezifikation der Aktualisierungsprozesse sieht bei Störfällen innerhalb der Teilprozesse vor, dass das zuständige Überwachungspersonal informiert wird.
- Bei den Vertrags-CAs und den Betreibern der Dienste des Verzeichnisdienstkonzepts sind Eskalationswege einzurichten und bekannt zu geben. Die Funktionstüchtigkeit der Eskalationswege wird von der PCA regelmäßig überprüft. Die PCA übernimmt außerdem eine Koordinationsfunktion in Störfällen.
- Das Schema des Verzeichnisdienstes der Verwaltung bietet die Möglichkeit, Entries von Teilnehmern besonders zu kennzeichnen, wenn sie in die Störfallbehandlung einbezogen werden sollen. Damit besteht eine einfache Möglichkeit, um die Eskalationswege zu überprüfen (Festlegung erfolgt im Attribut vDKInternalNotification, Details dazu finden sich in 4.2.1.1). Die Details der Kennzeichnung und die Regelungen für die Zugriffsbeschränkungen sind im Rahmen der Implementierung festzulegen.

Die folgenden Maßnahmen eröffnen **Reaktionsmöglichkeiten im Falle von Verfügbarkeitsstörungen**:

- Jeder Teilprozess kann manuell angestoßen werden. Sollen Daten in den Diensten des Verzeichnisdienstkonzepts aktualisiert werden und sind die dortigen Teilprozesse aktiv, genügt das Auslösen in der Quell-Domäne. Dies kann z. B. zum Wiederaufsetzen von Diensten genutzt werden.
- Falls die implementierte Kommunikationsverbindung oder die Sicherheitsmaßnahmen für die Übertragung gestört sind, können ersatzweise beliebige andere Kommunikationswege genutzt werden, die zur Übertragung von Dateien geeignet sind. In einer solchen Situation könnte bei Bedarf auf die Maßnahmen der Integritätssicherung verzichtet werden, um den Störfall zu überbrücken.

- Die LDIF-Dateien können sowohl in den Diensten des Verzeichnisdienstkonzepts als auch in den importierenden Domänen notfalls auch mit Standard-Werkzeugen in den Austausch-DIT eingespielt werden. Im Rahmen des Notfallkonzepts sollten die dazu erforderlichen Schritte und Komponenten beschrieben werden.
- Die LDIF-Dateien eines Teilbaums des Austausch-DITs werden gemäß der Prozess-Spezifikation an verschiedenen Stellen redundant aufbewahrt: in der Quell-Domäne, beim Verzeichnisdienst der Verwaltung, im Austauschdienst und gegebenenfalls bei den importierenden Domänen. Dadurch bestehen in Störfällen hinreichende Möglichkeiten, die Datenbestände des Austausch-DITs zu rekonstruieren.
- In Störfällen kann zeitweise auf die Replikation von Teilnehmer-Entries verzichtet werden, da dies nur geringe Einbußen für die Anwendungen zur Folge hat. Die Replikation von CA-Entries kann über die LDIF-Dateischnittstelle zumindest für alle nicht-Windows-2000-Domänen vollständig per Hand vorgenommen werden.
- Bei Störungen des Verzeichnisdienstes der Verwaltung können die LDIF-Dateien mit geringem manuellen Aufwand direkt zum Austauschdienst übertragen werden (unter Verzicht auf die Integritätssicherung und Konsistenzprüfung beim Eingang). Der automatisierte Import in die Domänen funktioniert dann weiter. Die Teilnehmer, die die PKI-Informationen aus ihren Domänen-Verzeichnisdiensten abrufen, sind dann weiter arbeitsfähig.
- Wenn die zentralen Dienste völlig ausgefallen sind, können die LDIF-Dateien auch direkt zwischen den beteiligten Domänen ausgetauscht werden. Die lokalen Teilprozesse müssen dann manuell gestartet werden.
- Der Test-Server ist als Notfall-Server für den Austauschdienst vorgesehen.

Die genannten Maßnahmen sind in Notfallübungen zu erproben.

Übergreifende Maßnahmen zur Gewährleistung der Integrität

Um an den Daten während der Replikation **Manipulationen durch Unberechtigte zu verhindern**, werden folgende Maßnahmen ergriffen:

- Zur Integritätssicherung werden die Daten zwischen den Beteiligten mittels einer kryptographisch gesicherten Verbindung übertragen.
- Um zulässige Datenquellen sicher zu identifizieren, wird starke gegenseitige Authentisierung eingesetzt.
- Im Rahmen der Implementierung ist mindestens IT-Grundschutz für die kryptographische Sicherung zu realisieren. Dazu sind zulässige Komponenten und Anforderungen an die Handhabung des Schlüsselmaterials festzulegen. Außerdem muss festgelegt werden, wie die notwendigen Daten für die Authentifikation zwischen den Beteiligen auszutauschen und in welchem Rhythmus Schlüsselwechsel vorgeschrieben sind.
- Alle Beteiligten müssen eine restriktive Zugangs- und Zugriffskontrolle für alle Prozesse und Komponenten durchsetzen.

Um in den Diensten des Verzeichnisdienstkonzepts die **Daten einzelner Domänen gegeneinander abzugrenzen**, werden folgende Maßnahmen ergriffen:

- Der Dateneingang beim Verzeichnisdienst der Verwaltung ist separiert je Domäne. Der Zugriff auf jeden Eingangsbereich wird durch die starke Authentisierung kontrolliert.
- Für eingegangene Daten wird sichergestellt, dass sie nur Entries der der Datenquelle zugeordneten Teilbäume des Austausch-DITs enthalten.

Die folgenden Maßnahmen eröffnen **Reaktionsmöglichkeiten im Falle von Integritätsstörungen**:

- Sofern manipulierte Daten durch Angriffe von innen in die Dienste des Verzeichnisdienstkonzepts eingespielt wurden, kann dies mit den regulären Prozessen korrigiert werden. Wenn der Angriff in der Domäne erfolgte, muss zuerst sichergestellt werden, dass die Daten im Quellverzeichnis korrekt sind.

Die Korrektur in den Diensten des Verzeichnisdienstkonzepts erfolgt dann durch die regulären Prozesse, durch manuelles Auslösen eines Vollabgleichs oder durch die Eingriffsmöglichkeiten bei Verfügbarkeitsproblemen.

- Sofern die Authentifikation einer Datenquelle unterlaufen werden kann, ist der entsprechende Zugang auf der Seite des VDV zu sperren. Die Daten können dann von der Quell-Domäne auf anderem Wege an den VDV übermittelt und dort manuell in den Teilprozess beim VDV eingestellt werden. Das betroffene Schlüsselmaterial ist zu wechseln.

Übergreifende Maßnahmen zur Gewährleistung der Vertraulichkeit

Im Rahmen des Verzeichnisdienstkonzepts sind zwei Bereiche mit Vertraulichkeitsanforderungen zu unterscheiden: zum einen die Daten, die in die Dienste des Verzeichnisdienstkonzepts repliziert werden, und zum anderen solche Daten, die im Rahmen des Betriebs des VDKs benötigt werden oder entstehen.

Um **Entries des Verzeichnisdienstkonzepts** gegen unberechtigte Kenntnisnahme zu schützen, werden folgende Maßnahmen ergriffen:

- Es müssen nur Entries gegen unbefugte Kenntnisnahme geschützt werden, die zwar in den VDV, nicht aber in den Veröffentlichungsdienst repliziert werden sollen. Die Daten für den VDV können außerdem von den Domänen importiert werden. Die Domänen betreiben eigene Intranets, der VDV wird im Intranet der Verwaltung betrieben. Die Sicherheitsmaßnahmen dieser Intranets gegen Zugriffe von außen sind ausreichend für das geforderte Sicherheitsniveau.
- Das Verzeichnisdienstkonzept bietet Steuerungsmöglichkeiten für die Bereitstellung von Daten im Verzeichnisdienst der Verwaltung und im Veröffentlichungsdienst. Diese Steuerungsattribute sind gemäß der Vorgaben für den Aktualisierungsprozess zum Veröffentlichungsdienst von den Betreibern der Dienste des VDKs einzusetzen.

- Die Kontrolle über die Steuerungsattribute und damit über die Auswahl der zu replizierenden Entries sowie über die Teilprozesse, die die Daten zur Replikation bereitstellen, liegt ausschließlich bei den Vertrags-CAs.
- Die Vertrags-CAs werden im Rahmen des Beitrittsverfahrens verpflichtet, interne Regelungen für die Veröffentlichung von Entries zu definieren und die korrekte Belegung der Steuerungsattribute sicherzustellen.
- Um das "Sammeln" von Daten aus den Verzeichnisdiensten zu erschweren, wird der Umfang der Antworten auf Anfragen zahlenmäßig begrenzt.
- Die LDIF-Dateien werden zwischen den Beteiligten des Verzeichnisdienstkonzepts über kryptographisch gesicherten Verbindungen übertragen und sind dadurch gegen Ausforschung geschützt.
- Die Zugriffsberechtigungen auf die Dienste des Verzeichnisdienstkonzepts sind restriktiv einzurichten. Es wird außerdem angenommen, dass die Absicherung des Intranets der Verwaltung gegen Externe ausreichend ist, um Entries, die nur im VDV bereitgestellt werden sollen, vor der Kenntnisnahme aus dem Internet zu schützen. Eine entsprechende Absicherung wird von den Intranets der Domänen erwartet, soweit sie Daten des Verzeichnisdienstkonzepts importieren.

Im Rahmen des Verzeichnisdienstkonzepts wird **Schlüsselmaterial** zur Authentisierung von Datenquellen und zur Sicherung der Integrität übertragener Daten verwendet. Während der Implementierung sind die Anforderungen für die Handhabung der PSEs und der Passworte für ihre Freigabe festzulegen.

Die **Log-, Audit- und Archiv-Daten** sind von den Betreibern geeignet zu sichern, soweit sie personenbezogene Daten enthalten. Sie sind außerdem gegen Verfälschung zu sichern.

Übergreifende Maßnahmen für Audit- und Nachweismöglichkeiten

Im Rahmen des Verzeichnisdienstkonzepts kann auf verteilte Daten zum Zwecke von Audits und für Nachweise zurückgegriffen werden. Es wird aller-

dings angenommen, dass aufgrund der Haftungsregelungen und des grundsätzlichen Interesses an einer konstruktiven Zusammenarbeit primär Analysemöglichkeiten für Unregelmäßigkeiten benötigt werden. Nachweismöglichkeiten mit hoher Beweissicherheit sind im Verzeichnisdienstkonzept bislang nicht vorgesehen.

Um die notwendigen Audit- und Nachweismöglichkeiten im Verzeichnisdienstkonzept zu erreichen, werden folgenden Maßnahmen ergriffen:

- Die beteiligten Betreiber müssen intern eine Rollentrennung und Zugangs- und Zugriffskontrolle durchsetzen, die lokale Möglichkeiten zum Audit sicherstellt.
- Die beteiligten Betreiber haben Aufbewahrungspflichten für LDIF-Dateien und Log-Dateien zur Dokumentation, die von den implementierten Aktualisierungsprozessen unterstützt werden.
- Jede ausgetauschte LDIF-Datei ist während eines Zeitraums von etwa zwei Monaten mehrfach redundant vorhanden: bei der Daten-Quelle, auf den Servern des VDV und des Austauschdienstes und bei den Domänen, die die Daten reimportieren. Zwischen diesen Exemplaren können Konsistenzprüfungen durchgeführt werden, wenn Klärungsbedarf hinsichtlich ihres Inhaltes besteht. Entsprechend werden auch die korrespondierenden Aktionen der verschiedenen Aktualisierungsprozesse in jeweils eigenen Log-Dateien festgehalten.

Im allgemeinen Fall sollte das Vorhalten der Daten bei unterschiedlichen Stellen für Überprüfungen ausreichend sein. Im Rahmen der Implementierung ist allerdings zu überprüfen, ob Aufgaben zusammenfallen, z. B. TESTA als Datenquelle und TESTA als Betreiber des VDV. In diesem Fall ist zu entscheiden, ob das Sicherheitsniveau für Nachweise ausreichend ist oder ob zusätzliche Maßnahmen ergriffen werden müssen.

15.2.2 Sicherheitskonzept des Betreibers der Dienste des VDKs

Der Betreiber der Diensten des Verzeichnisdienstkonzepts muss ein Sicherheitskonzept für seinen Zuständigkeitsbereich realisieren, dass die Verfügbarkeit der Prozesse, die Integrität der Daten und die Vertraulichkeit des Schlüsselmaterials zur Sicherung der Verbindungen zu den Diensten des VDKs **mindestens mit IT-Grundschutz-Maßnahmen** absichert. Die notwendigen Maßnahmen sind in die jeweiligen lokalen Betriebs- und Sicherheitskonzepte einzuarbeiten und umzusetzen. Soweit keine passenden Bausteine verfügbar sind, sind Maßnahmen mit einem dem Grundschutz entsprechenden Sicherheitsniveau zu definieren. Das lokale Sicherheitskonzept muss die Maßnahmen einschließen, die sich aus dem **übergreifenden Sicherheitskonzept** für den Betreiber der Dienste des VDKs ergeben.

Neben den Maßnahmen für die einzelnen technischen Komponenten sind insbesondere Maßnahmen für die im folgenden aufgeführten Bereiche zu realisieren.

15.2.2.1 IT-Sicherheitsmanagement

Der Betreiber muss über ein IT-Sicherheitsmanagement verfügen. Die Sicherheitsmaßnahmen des Verzeichnisdienstkonzepts müssen in einem Sicherheitskonzept dokumentiert werden. Änderungen am Sicherheitskonzept müssen einem definierten Change-Management-Prozess unterliegen. Veränderungen des Verzeichnisdienstkonzepts müssen durch die lokale Prozessorganisation daraufhin überprüft werden, ob sie zu Änderungen am Sicherheitskonzept führen. Das Sicherheitsmanagement muss sicherstellen, dass die Sicherheitsmaßnahmen für das Verzeichnisdienstkonzept in regelmäßigen Abständen überprüft werden.

15.2.2.2 Infrastruktur

Das lokale Sicherheitskonzept muss gewährleisten, dass die Komponenten des Verzeichnisdienstkonzepts in die Sicherheitsmaßnahmen für Gebäude, Verkabelung und Serverräume einbezogen sind.

Die infrastrukturellen Maßnahmen bezüglich der Lage von Räumen, dem Zutritt, der Stromversorgung und Klimatechnik, dem Brandschutz, der Datenarchivierung und der Datenvernichtung müssen auf die Komponenten des Verzeichnisdienstkonzepts ausgeweitet werden.

15.2.2.3 Telekommunikationsanbindung

Der Betreiber der Dienste des VDKs muss eine redundante Telekommunikationsanbindung mit 2-Wege-Führung sicherstellen.

15.2.2.4 Organisation

Es sind klare Regelungen für die Zuständigkeiten und Abläufe zu dokumentieren und durchzusetzen (vgl. [IT-Grundschutzhandbuch]). Dies schließt ein Rollenkonzept ein (vgl. nächster Abschnitt).

15.2.2.5 Personelle Sicherheitsmaßnahmen

Der Betreiber der Dienste des VDKs muss ein **Rollenkonzept** definieren und umsetzen, in dem mindestens die folgenden Rollen getrennt werden:

- **Administrative Rollen** sorgen dafür, dass die lokalen Anteile der Aktualisierungsprozesse des Verzeichnisdienstkonzepts korrekt konfiguriert, getestet und in den produktiven Betrieb überführt werden. Sie wirken außerdem bei der Behebung von Störfällen mit.
- **Operative Rollen** überwachen den Betrieb der lokalen Teilprozesse des Verzeichnisdienstkonzepts (Monitoring), können sie gegebenenfalls manuell aufrufen oder sie neu starten. Sie eskalieren und behandeln Störfälle im Rahmen der Eskalationswege.
- **Beaufsichtigende Rollen** geben die Konfigurationsvorschriften für die Aktualisierungsprozesse des Verzeichnisdienstkonzepts frei, beteiligen sich an der Aufklärung von Störfällen und führen bei Bedarf Audits durch (z. B. *Revisor*).

Die Rollenbeschreibungen sind gegebenenfalls in Abhängigkeit von den Regeln zur Handhabung von Schlüsselmaterial zu ergänzen.

Im Rahmen der Implementierung ist zu prüfen, ob bei der Zuweisung von Rollen zu Personen Funktionstrennung durchgesetzt werden muss. Die Zuweisung von Rollen zu Personen ist zu dokumentieren. Die Rolleninhaber müssen über die notwendigen Qualifikationen verfügen. Die Zugangs- und Zugriffsmöglichkeiten müssen in Übereinstimmung mit der Rollenzuweisung begrenzt werden.

Zusätzlich müssen die Rollen für die Eskalationswege und die Störfallbehandlung festgelegt werden.

Die Zuweisung von Rollen zu Personen muss Vertretungsregelungen vorsehen, um den Verfügbarkeitsanforderungen und Reaktionen auf Störungen Rechnung zu tragen.

Die Zuordnung von Rollen und den damit verbundenen Zugriffsrechten ist unmittelbar mit Veränderungen in den Aufgaben der Personen anzupassen, beispielsweise beim Wechsel von Mitarbeitern zwischen Abteilungen oder beim Ausscheiden.

15.2.2.6 Datensicherungs-Konzept

Jeder Betreiber muss alle Komponenten, die zu den lokalen Teilprozessen des Verzeichnisdienstkonzepts, ihrer Überwachung und ihrem Audit beitragen, in seinem Backup-Konzept und Datenträgerarchiv berücksichtigen. Es ist sicherzustellen, dass ein Wiederaufsetzen von Prozessen so möglich ist, dass die Zusicherungen für die Service-Qualität der Dienste des Verzeichnisdienstkonzepts eingehalten werden können.

15.2.2.7 Zugangs- und Zugriffsschutz-Maßnahmen

Firewalls und die Zugangs- und Zugriffskontrolle für Systeme, Prozesse und Daten sind grundsätzlich restriktiv zu konfigurieren, d.h. es dürfen nur die kleinst möglichen Rechte vergeben werden, die für den Betrieb der lokalen Teilprozesse des Verzeichnisdienstkonzepts erforderlich sind. Die Konfigura-

tionsvorgaben sind schriftlich zu dokumentieren. Sie müssen insbesondere sicherstellen, dass:

- nur Berechtigte die Konfiguration der Teilprozesse des Verzeichnisdienstkonzepts ändern können,
- nur die notwendigen Teilprozesse Schreibrechte auf die LDIF-Dateien bzw. die Teilbäume des Verzeichnisdienstkonzepts haben,
- die lokalen Attribute zur Kennzeichnung von Entries im Rahmen des Verzeichnisdienstkonzepts nur von Berechtigten verändert werden können (z. B. zur Steuerung der Replikation oder zur Kennzeichnung von Entries für die Störfall-Kommunikation),
- je nach Verzeichnisdienst nur berechtigte Teilnehmer des Intranets der Verwaltung oder des Extranet lesend auf die Datenbestände zugreifen können,
- nur berechtigte Administratoren auf das Schlüsselmaterial zur Authentisierung von Datenquellen und die zur Nutzung erforderlichen Passworte zugreifen können,
- der Zugriff auf Log-, Audit- und Archiv-Daten so gesichert ist, dass sie nicht unberechtigt gelöscht oder verfälscht werden können.

Für die Dienste des Verzeichnisdienstkonzepts ergeben sich nach dem gegenwärtigen Stand die in der folgenden Tabelle aufgeführten Zuordnungen von Rollen und Zugriffsrechten. Der Zugriff ist mit personengebundener UserID und Passwort zu schützen, wenn dies nicht anders vermerkt ist.

Rolle	Zugriffsrechte
Administrative Rollen	schreibend: Konfigurationsdateien Aktualisierungsprozesse des VDKs löschend: LDIF-Dateien
Operative Rollen	ausführend: Prozesse, Konfigurationsdateien Aktualisierungsprozesse des VDKs
Beaufsichtigende Rollen	lesend, löschend: Log-Dateien lesend: LDIF-Dateien
Aktualisierungsprozesse der Domänen	nur mit starker Authentifikation: • nur schreibendes Zugriffsrecht auf den jeweiligen Eingangsbereich beim Verzeichnisdienst der Verwaltung • nur lesenden Zugriff auf das Ausgangsverzeichnis des Austauschdienstes

Rolle	Zugriffsrechte
Aktualisierungs-prozesse beim Betreiber	schreibende, löschende Zugriffsrechte auf die notwendigen Konfigurations-, LDIF- und Log-Dateien und das Schlüsselmaterial für die starke Authentifizierung. schreibenden und löschenden Zugriff auf den jeweils zu aktualisierenden Verzeichnis-dienst
VDK-Notification-Teilnehmer	mit globaler UserID und globalem Passwort (Wechsel z. B. einmal jährlich): lesender Zugriff auf das Attribut vDKInternalNotification und alle anderen Attribute der Entries im VDV.
Teilnehmer aus dem Bereich des Intranets der Verwaltung	anonymer Zugriff ohne Passwort, lesend auf die Entries des VDV. Nicht sichtbar sind die Steuerattribute einschließlich vDKInternalNotification. • Wildcards in E-Mail-Adressen werden nicht unterstützt • maximal 50 Entries pro Anfrage • nicht sichtbar sind die Steuerattribute einschließlich vDKInternalNotification.
Teilnehmer außer-halb des Bereichs des Intranets der Verwaltung	anonymer Zugriff ohne Passwort, lesend auf die Entries des Veröffentlichungsdienstes mit folgenden Einschränkungen: • Wildcards in E-Mail-Adressen werden nicht unterstützt • maximal 10 Entries pro Anfrage • nicht sichtbar sind die Steuerattribute einschließlich vDKInternalNotification.

Tabelle 7: Zugriffsrechte für Rollen beim Betreiber der Dienste des Verzeichnisdienstkonzepts

15.2.2.8 Policy für Schlüsselmaterial

Für das Schlüsselmaterial, das zur Authentisierung von Datenquellen und Integritätssicherung während der Datenübertragung verwendet wird, sind lokale Maßnahmen in Übereinstimmung mit dem übergreifenden Sicherheitskonzept festzulegen und durchzusetzen. Die folgende Liste ist nach der Entscheidung über die technische Realisierung der kryptographischen Sicherung im Rahmen der Implementierung anzupassen und von den Vertrags-CAs bzw. den Betreibern zu detaillieren:

- Berechtigung und Abläufe zur Erzeugung und bei der Installation von Schlüsseln einschließlich des Schlüsselwechsels,
- Berechtigte und Verfahren für die Nutzung des Schlüsselmaterials,
- Sicherheitsmaßnahmen zum Schutz des Schlüsselmaterials und erforderlicher Passworte,
- Handhabung und Verteilung der zur Nutzung erforderlichen Passworte, auch unter Verfügbarkeitsgesichtpunkten,

- Reaktionen und Eskalationen bei Störfällen einschließlich des Verdachts auf Kompromittierung,
- Backups für Schlüsselmaterial und Passworte, um die Verfügbarkeit und das Wiederaufsetzen nach Störungen zu ermöglichen, ggf. auch für berechtigte Stellvertreter der verantwortlichen Administratoren,
- Vorgaben, wann das Schlüsselmaterial und Passworte zu wechseln sind, beispielsweise nach dem Ausscheiden von Mitarbeitern, die auf das Schlüsselmaterial zugreifen konnten.

15.2.2.9 Notfallvorsorge und Eskalationswege

Das lokale Sicherheitskonzept und die Rollenverteilung müssen sicherstellen, dass auf Störfälle schnell und nachhaltig reagiert wird. Dazu sind die folgenden Maßnahmen unter Berücksichtigung des übergreifenden Sicherheitskonzepts zu ergreifen:

- klare Festlegung von Kontaktstellen für die Meldung bzw. Aufnahme von Störfällen,
- Definition von Regeln und Zuständigkeiten für die Behandlung von Störfällen einschließlich der internen und externen Eskalationswege,
- Gewährleistung, dass jede Störfallbehandlung definiert abgeschlossen wird,
- Sicherstellen der Verfügbarkeit des Personals,
- Bereitstellen und Pflege der notwendigen Kontaktinformationen für alle Beteiligten einschließlich der Teilnehmer, u.a. durch geeignete Kennzeichnung im Verzeichnisdienst der Verwaltung (vgl. oben),
- Dokumentationsrichtlinien für die Störfälle und ihre Behandlung,
- jährliche Auswertung der Störfall-Dokumentation, um häufige Probleme und schwere Störfälle für konzeptionelle Änderungen identifizieren zu können.

15.3 Sicherheitskonzept der Vertrags-CAs

Hinweis: Dieser Abschnitt ist in vielen Punkten textgleich mit Kapitel 15.2.2. Allerdings ergeben sich für die Vertrags-CAs an manchen Punkten Unterschiede, beispielsweise im Rollenkonzept oder für die Zugriffsrechte. Diese Abweichungen sind hier berücksichtigt. Möglicherweise werden auch im Rahmen der weiteren Abstimmung zusätzliche Unterschiede zugelassen, so dass sich eine getrennte Darstellung empfiehlt.

Jede Vertrags-CA muss für ihren Zuständigkeitsbereich, d. h. auch die nachgeordneten CAs und die beauftragten Betreiber der lokalen Verzeichnisdienste, ein Sicherheitskonzept realisieren, dass die Verfügbarkeit der Prozesse (vgl. die Vorgaben in Kapitel 5.1), die Integrität der Daten und die Vertraulichkeit des Schlüsselmaterials Sicherung der Verbindungen zu den Diensten des VDKs **mindestens mit IT-Grundschutz-Maßnahmen** absichert. Die notwendigen Maßnahmen sind in die jeweiligen lokalen Betriebs- und Sicherheitskonzepte einzuarbeiten und umzusetzen. Soweit keine passenden Bausteine verfügbar sind, sind Maßnahmen mit einem dem Grundschutz entsprechenden Sicherheitsniveau zu definieren. Das lokale Sicherheitskonzept muss die Maßnahmen einschließen, die sich aus dem **übergreifenden Sicherheitskonzept** für die Vertrags-CAs ergeben.

Neben den Maßnahmen für die einzelnen technischen Komponenten sind insbesondere Maßnahmen für die im folgenden aufgeführten Bereiche zu realisieren.

15.3.1 IT-Sicherheitsmanagement

Die Vertrags-CA muss über ein IT-Sicherheitsmanagement verfügen. Die Sicherheitsmaßnahmen des Verzeichnisdienstkonzepts müssen in einem Sicherheitskonzepts dokumentiert werden. Änderungen am Sicherheitskonzept müssen einem definierten Change-Management-Prozess unterliegen. Veränderungen des Verzeichnisdienstkonzepts müssen durch die lokale Prozessorganisation daraufhin überprüft werden, ob sie zu Änderungen am Sicherheitskon-

zept führen. Das Sicherheitsmanagement muss sicherstellen, dass die Sicherheitsmaßnahmen für das Verzeichnisdienstkonzept in regelmäßigen Abständen überprüft werden.

15.3.2 Infrastruktur

Das lokale Sicherheitskonzept muss gewährleisten, dass die Komponenten des Verzeichnisdienstkonzepts in die Sicherheitsmaßnahmen für Gebäude, Verkabelung und Serverräume einbezogen sind.

Die infrastrukturellen Maßnahmen bezüglich der Lage von Räumen, dem Zutritt, der Stromversorgung und Klimatechnik, dem Brandschutz, der Datenarchivierung und der Datenvernichtung müssen auf die lokalen Komponenten des Verzeichnisdienstkonzepts ausgeweitet werden.

15.3.3 Telekommunikationsanbindung

Es wird empfohlen, dass die CAs über redundante Telekommunikationsverbindungen zum lokalen Verzeichnisdienst und der lokale Verzeichnisdienst über redundante Telekommunikationsverbindungen zum VDV verfügt.

15.3.4 Organisation

Es sind klare Regelungen für die Zuständigkeiten und Abläufe zu dokumentieren und durchzusetzen (vgl. [IT-Grundschutzhandbuch]). Dies schließt ein Rollenkonzept ein (vgl. nächster Abschnitt).

15.3.5 Personelle Sicherheitsmaßnahmen

Jede Vertrags-CA muss ein **Rollenkonzept** definieren und umsetzen, in dem mindestens die folgenden Rollen festgelegt werden:

- **Administrative Rollen** sorgen dafür, dass die lokalen Anteile der Aktualisierungsprozesse des Verzeichnisdienstkonzepts korrekt konfiguriert, getestet und in den produktiven Betrieb überführt werden. Sie wirken bei der Behebung von Störfällen mit.

- **Operative Rollen** überwachen den Betrieb der lokalen Teilprozesse des Verzeichnisdienstkonzepts (Monitoring), können sie gegebenenfalls manuell aufrufen oder sie neu starten. Sie eskalieren und behandeln Störfälle im Rahmen der Eskalationswege.
- **Verantwortliche für die Datenpflege** stellen sicher, dass die Steuerattribute für die Aktualisierungsprozesse des VDKs korrekt gesetzt werden.
- **Beaufsichtigende Rollen** geben die Regeln für die Verwendung der Steuerattribute und die Konfigurationsvorschriften für die lokalen Anteile der Aktualisierungsprozesse des Verzeichnisdienstkonzepts frei, beteiligen sich an der Aufklärung von Störfällen und führen bei Bedarf Audits durch (z. B. *Revisor*).

Die Rollenbeschreibungen sind gegebenenfalls in Abhängigkeit von den Regeln zur Handhabung von Schlüsselmaterial zu ergänzen.

Im Rahmen der Implementierung ist zu prüfen, ob von den Vertrags-CAs bei der Zuweisung von Rollen zu Personen Funktionstrennung durchgesetzt werden soll. Die Zuweisung von Rollen zu Personen ist zu dokumentieren. Die Rolleninhaber müssen über die notwendigen Qualifikationen verfügen. Die Zugangs- und Zugriffsmöglichkeiten müssen in Übereinstimmung mit der Rollenzuweisung begrenzt werden.

Zusätzlich müssen die Rollen für die Eskalationswege und die Störfallbehandlung festgelegt werden.

Die Zuweisung von Rollen zu Personen muss Vertretungsregelungen beinhalten, um den Verfügbarkeitsanforderungen und Reaktionen auf Störungen Rechnung zu tragen.

Die Zuordnung von Rollen und den damit verbundenen Zugriffsrechten ist unmittelbar mit Veränderungen in den Aufgaben der Personen anzupassen, beispielsweise beim Wechsel von Mitarbeitern zwischen Abteilungen oder beim Ausscheiden.

15.3.6 Datensicherungs-Konzept

Jede Vertrags-CA muss alle Komponenten, die zu den lokalen Teilprozessen des Verzeichnisdienstkonzepts, ihrer Überwachung und ihrem Audit beitragen, in ihrem Backup-Konzept und Datenträgerarchiv berücksichtigen. Es ist sicherzustellen, dass ein Wiederaufsetzen von Prozessen so möglich ist, dass die Zusicherungen für die Service-Qualität der Dienste des Verzeichnisdienstkonzepts eingehalten werden können.

15.3.7 Zugangs- und Zugriffsschutz-Maßnahmen

Um die Eingriffe in die existierenden Sicherheitskonzepte der Domänen möglichst klein zu halten, werden alle Kommunikationsverbindungen aktiv von der Domäne aufgebaut und kontrolliert.

Firewalls und die Zugangs- und Zugriffskontrolle für Systeme, Prozesse und Daten sind grundsätzlich restriktiv zu konfigurieren, d.h. es dürfen nur die kleinst möglichen Rechte vergeben werden, die für den Betrieb der lokalen Teilprozesse des Verzeichnisdienstkonzepts erforderlich sind. Die Konfigurationsvorgaben sind schriftlich zu dokumentieren. Sie müssen insbesondere sicherstellen, dass:

- nur Berechtigte die Konfiguration lokaler Teilprozesse des Verzeichnisdienstkonzepts ändern können,
- nur die notwendigen Teilprozesse Schreibrechte auf den LDIF-Dateien bzw. den Teilbäumen des Verzeichnisdienstkonzepts haben,
- die lokalen Attribute zur Kennzeichnung von Entries im Rahmen des Verzeichnisdienstkonzepts nur von Berechtigten verändert werden können (z. B. zur Steuerung der Replikation oder zur Kennzeichnung von Entries für die Störfall-Kommunikation),
- je nach Verzeichnisdienst nur berechtigte Teilnehmer der jeweiligen Domäne lesend auf die Datenbestände zugreifen können,

- nur berechtigte Administratoren auf das Schlüsselmaterial zur Authentisierung von Datenquellen und die zur Nutzung erforderlichen Passworte zugreifen können.
- der Zugriff auf Log-, Audit- und Archiv-Daten so gesichert ist, dass sie nicht unberechtigt gelöscht oder verfälscht werden können.

Sofern eine Domäne Daten vom Austauschdienst rück-importiert, muss das Intranet der Domäne gegen Zugriffe aus dem Extranet abgeschottet sein. Dazu muss das lokale Sicherheitskonzept nachweisen, dass Externe nicht auf die Daten des Austausch-DITs zugreifen können.

Für die Dienste des Verzeichnisdienstkonzepts ergeben sich nach dem gegenwärtigen Stand die in der folgenden Tabelle aufgeführten Zuordnungen von Rollen und Zugriffsrechten. Der Zugriff ist mit personengebundener UserID und Passwort zu schützen, wenn dies nicht anders vermerkt ist.

Rolle	Zugriffsrechte
Administrative Rollen	schreibend: lokale Konfigurationsdateien Aktualisierungsprozesse des VDKs löschend: LDIF-Dateien
Operative Rollen	ausführend: Prozesse, Konfigurationsdateien Aktualisierungsprozesse des VDKs
Beaufsichtigende Rollen	lesend, löschend: Log-Dateien lesend: LDIF-Dateien
Verantwortliche für die Datenpflege	UserID und Passwort: lesenden und schreibenden Zugriff auf die Steuerattribute für die Aktualisierungsprozesse des VDKs in den lokalen Entries
Aktualisierungsprozesse der Domänen zum VDV	schreibende, löschende Zugriffsrechte auf die notwendigen Konfigurations-, LDIF- und Log-Dateien und das Schlüsselmaterial für die Starke Authentifizierung. Schreibenden Zugriff (UserID und Passwort) auf den Hilfs-Entry des lokalen Verzeichnisdienstes lesenden Zugriff auf den lokalen Verzeichnisdienst, soweit dies für die Replikation erforderlich ist (sicherheitsrelevante Attribute in Entries, die nicht erforderlich sind, sollten nicht zugreifbar sein.)
Aktualisierungsprozesse der Domänen vom VDV zur Domäne	schreibende, löschende Zugriffsrechte auf die notwendigen Konfigurations-, LDIF-Dateien und das Schlüsselmaterial für die starke Authentifizierung. schreibenden und löschenden Zugriff auf den lokalen Austausch-DIT
optional: VDK-Notification-Teilnehmer aus der Domäne	mit gemeinsamer UserID und gemeinsamem Passwort (Wechsel z. B. einmal jährlich): lesender Zugriff auf das Attribut vDKInternalNotification im Verzeichnisdienst der Domäne und alle anderen VDK-relevanten Attribute der Entries
Teilnehmer aus dem Intranet der Domäne	anonymer Zugriff ohne Passwort, lesend auf die Entries des Austausch-DITs. Nicht sichtbar sind die Steuerattribute einschließlich vDKInternalNotification. • maximal 50 Entries pro Anfrage

Rolle	Zugriffsrechte
Teilnehmer außerhalb des Intranets der Domäne	**kein Zugriff**

Tabelle 8: Zugriffsrechte für Rollen bei der Vertrags-CA

15.3.8 Policy für Schlüsselmaterial

Für das Schlüsselmaterial, das zur Authentisierung von Datenquellen und Integritätssicherung während der Datenübertragung verwendet wird, sind lokale Maßnahmen in Übereinstimmung mit dem übergreifenden Sicherheitskonzept festzulegen und durchzusetzen. Die folgende Liste ist nach der Entscheidung über die technische Realisierung der kryptographischen Sicherung im Rahmen der Implementierung anzupassen und von den Vertrags-CAs bzw. den Betreibern zu detaillieren

- Berechtigung und Abläufe zur Erzeugung und bei der Installation von Schlüsseln einschließlich des Schlüsselwechsels,
- Berechtigte und Verfahren für die Nutzung des Schlüsselmaterials,
- Sicherheitsmaßnahmen zum Schutz des Schlüsselmaterials und erforderlicher Passworte,
- Handhabung und Verteilung der zur Nutzung erforderlichen Passworte, auch unter Verfügbarkeitsgesichtpunkten,
- Reaktionen und Eskalationen bei Störfällen einschließlich des Verdachts auf Kompromittierung,
- Backups für Schlüsselmaterial und Passworte, um die Verfügbarkeit und das Wiederaufsetzen nach Störungen zu ermöglichen, ggf. auch für berechtigte Stellvertreter der verantwortlichen Administratoren,
- Vorgaben, wann das Schlüsselmaterial und die Passworte zu wechseln ist, beispielsweise nach dem Ausscheiden von Mitarbeitern, die auf das Schlüsselmaterial zugreifen konnten.

15.3.9 Notfallvorsorge und Eskalationswege

Das lokale Sicherheitskonzept und die Rollenverteilung müssen sicherstellen, dass auf Störfälle schnell und nachhaltig reagiert wird. Dazu sind die folgenden Maßnahmen unter Berücksichtigung des übergreifenden Sicherheitskonzepts zu ergreifen:

- klare Kontaktstellen für die Meldung bzw. Aufnahme von Störfällen,
- Regeln und Zuständigkeiten für die Behandlung von Störfällen einschließlich der internen und externen Eskalationswege,
- Gewährleistung, dass jede Störfallbehandlung definiert abgeschlossen wird,
- Sicherstellen der Verfügbarkeit des Personals,
- Bereitstellen und Pflege der notwendigen Kontaktinformationen für alle Beteiligten einschließlich der Teilnehmer, u.a. durch geeignete Kennzeichnung im Verzeichnisdienst der Verwaltung (vgl. oben),
- Dokumentationsrichtlinien für die Störfälle und ihre Behandlung,
- jährliche Auswertung der Störfall-Dokumentation, um häufige Probleme und schwere Störfälle für konzeptionelle Änderungen identifizieren zu können.

15.4 Akzeptierte Schwachstellen

Die im folgenden aufgeführten Schwachstellen sind konzeptbedingt nach den Planungen für die Ausbaustufe 1. Sie wurden in den Sitzungen des Editorial Boards am 20.2. 2002 und am 10.4. 2002 diskutiert und für die Ausbaustufe 1 akzeptiert.

- **Wiedereinspielen alter Sperrlisten:** Durch die Replikationsmechanismen ergeben sich Verzögerungen zwischen der Erzeugung neuer Sperrlisten und ihrer Bereitstellung im Veröffentlichungsdienst bzw. einer importierenden Domäne. Um trotzdem zu jedem Zeitpunkt eine gültige Sperrliste anbieten zu können, müssen sich die Gültigkeitszeiträume der Sperrlisten überlappen. Während des Überlappungszeitraums könnte ein Angreifer versuchen, die

ältere Sperrliste als die aktuellste vorzuspiegeln. Der nach dem VDK geforderte Mindest-Überlappungszeitraum wird deshalb kurz gehalten (2 Stunden, längere Überlappungszeiträume werden allerdings nicht ausgeschlossen).

- **VDV ist "Single Point of Failure":** Aus Gründen der Vereinfachung wurde für die Ausbaustufe 1 entschieden, dass die LDIF-Dateien für den Austauschdienst vom VDV übernommen werden. Engpässe in der Leistungsfähigkeit oder eine Störung des Aktualisierungsprozess für den VDV betreffen deshalb mit gewisser Wahrscheinlichkeit auch den Austauschdienst (zu Reaktionsmöglichkeiten siehe "Verfügbarkeit" im übergreifenden Sicherheitskonzept).
- **Keine Überprüfung von Datenquellen beim Import in die Domänen**: Die Zulässigkeit von Entries in einer LDIF-Datei wird über eine Konsistenzprüfung bezüglich der Datenquelle beim Eingang zum VDV sichergestellt. Für Dateien, die vom Austauschdienst in die Domänen rück-importiert werden, kann dies in der Ausbaustufe 1 nicht realisiert werden. Dazu wäre eine Ende-zu-Ende-Integritätssicherung der LDIF-Dateien erforderlich. Manipulationsmöglichkeiten sind jedoch auf das Personal von VDV und AD beschränkt.
- **Angriffe in der PCA:** Systemimmanent führt eine ungültige Sperrliste der Wurzel-Zertifizierungsinstanz in einer PKI zu einem Denial-of-Service-Störfall aller Anwendungen dieser PKI. Während Manipulationen von Sperrlisten nachgeordneter CAs nur zu einem eingeschränkten Störfall führen, würde eine verfälschte Sperrliste der PCA auch in den Diensten des Verzeichnisdienstkonzepts repliziert und einen Denial-of-Service für die gesamte PKI-1-Verwaltung auslösen. Gegenüber dem bisherigen Stand können Angriffe auch im Rahmen des Aktualisierungsprozesse für die Sperrliste der PCA auftreten. (Zu Reaktionsmöglichkeiten siehe "Verfügbarkeit" im übergreifenden Sicherheitskonzept).

16 Realisierung des Verzeichnisdienstkonzepts

Dieses Kapitel stellt die notwendigen Arbeiten für die Realisierung des Verzeichnisdienstkonzepts zusammen, die sich aus den vorherigen Kapiteln ergeben.

Für die Realisierung des Verzeichnisdienstkonzepts kann unterschieden werden nach:

- grundsätzlicher Vorgehensweise,
- technischer Implementierung,
- Arbeiten an Dokumenten,
- Beauftragung des Betriebs von Diensten des VDKs und der
- Betriebsaufnahme.

Im Rahmen der Realisierung werden auch die noch offenen Details festgelegt. Diese sind zwischen den genannten Bereichen abzustimmen.

16.1 Grundsätzliche Vorgehensweise zur Realisierung der Dienste des VDK

Es wird empfohlen, die Realisierung der Dienste des Verzeichnisdienstkonzepts in enger Abstimmung mit zwei "Pilot-Domänen" durchzuführen, um ggf. auftretende Probleme und Interoperabilitätsprobleme so früh wie möglich zu erkennen und zu beheben. Dabei sollte eine der Domänen ein Directory mit Standard-Struktur betreiben, die andere ein Windows 2000-System.

Mit diesen beiden Domänen kann dann auch das Aufnahmeverfahren erstmals explizit durchgeführt und danach ggf. angepasst werden. Auch die Testphase sollte so durchgeführt werden, wie sie für den Beitritt einer Vertrags-CA vorgesehen ist.

Um eine Nutzung von CDPs zum Abruf aus dem VDV oder Veröffentlichungsdienst zu ermöglichen, müssen in den Zertifikaten die entsprechenden Einträge angepasst werden. Die Pfadangabe im CDP-Eintrag sollte dann so aussehen:

- ldap://[DNS-Name des gewünschten Verzeichnisdienstes, falls erforderlich]/<Subject-DN der CA>.

16.2 Technische Implementierung

Für die technische Implementierung sind im wesentlichen folgende Arbeiten durchzuführen:

- einige spezifische Details sind für die Implementierung auszuarbeiten bzw. festzulegen, z. B. zu verwendende Zeitformate für Steuerattribute, Festlegung der technischen Sicherungsmaßnahmen für die Kommunikationsverbindung zwischen Veröffentlichungsdienst und Austauschdienst, zu verwendendes Schlüsselmaterial für Tests, formale DIT- und Schema-Konfiguration, Umfang der Testunterstützung,
- die spezifizierten Prozesse einschließlich der HTTP-Plattform sind zu realisieren,
- die systemweiten Parameter sind festzulegen, z. B. DNS-Namen und Ports, und
- die Details der Testunterstützung sind auszuarbeiten.

Die technische Implementierung kann durch einen unabhängigen Dritten erfolgen, sofern dieser über die notwendigen Kenntnisse verfügt.

Es wird empfohlen, die DNS-Namen der Dienste des Verzeichnisdienstkonzepts möglichst bald festzulegen. Dadurch können diese dann schon bei einem Zertifikatswechsel für CAs und bei neuen Teilnehmerzertifikaten berücksichtigt werden, um CDPs einzutragen.

Das Schema aus dem A-DIT kann identisch für alle Dienste des VDKs verwendet werden. Die Steuerungsattribute des Verzeichnisdienstkonzepts dürfen bei

anonymen Anfragen an den VDV und den Veröffentlichungsdienst nicht sichtbar sein.

16.3 Rahmenbedingungen und Dokumente

Dieses Dokument beschreibt das Verzeichnisdienstkonzept auf der Konzeptebene. Im Rahmen der Implementierungsphase sind einige Konzeptbestandteile zu verfeinern oder in existierende Dokumente einzuarbeiten. Es wird deshalb empfohlen, vor der Aufnahme des Betriebs des Verzeichnisdienstes der PKI-1-Verwaltung folgende Arbeiten an Dokumenten vorzusehen:

- Verabschiedung und Einarbeitung der rechtlichen Regelungen in die Vereinbarung zwischen PCA und Vertrags-CA, die Sicherheitsleitlinie, und die Selbsterklärung der Vertrags-CA. Dabei ist zu beachten, dass auch die konsolidierten Namensregeln aus [PKI1V Namensregeln] durchgesetzt werden müssen, um die Voraussetzungen für eine breite Unterstützung des Verzeichnisdienstkonzepts zu erreichen.
- Ausarbeitung der organisatorischen Abläufe und Ergänzung z. B. um Sanktionsmaßnahmen und Abläufe des Change-Managements, einschließlich geeigneter Muster-Dokumente, z. B. für Testpläne.
- Entscheidung über Gebühren für Teilnehmer.
- Überarbeitung dieses Dokuments zu einem "Betriebskonzept des Verzeichnisdienstes der PKI-1-Verwaltung". Die Prozess-Spezifikationen sind in Abstimmung mit der Implementierung fortzuschreiben.
- Detaillierung des Sicherheitskonzepts, insbesondere des übergreifenden Sicherheitskonzepts einschließlich der Eskalations- und Notfallpläne. Für die Vertrags-CAs könnte ein Muster-Sicherheitskonzept erstellt werden, das die wesentlichen Punkte ausführt, soweit sie nicht sowieso erwartet werden können (z. B. zu Handhabung von Schlüsselmaterial, Eskalationswege und Notfallpläne).
- Ergänzung der Namensregeln um DNS- und HTTP-Namen.

- Anpassung der Spezifikationen im Anhang an die Implementierung, soweit sich aus der technischen Realisierung Veränderungen ergeben.
- Erarbeitung eines Ablaufplans für eine Auflösung/Betriebseinstellung des VDKs.

16.4 Beauftragung des Betriebs von Diensten des VDKs

Der Betrieb der Dienste des Verzeichnisdienstkonzepts muss beauftragt werden. Dazu ist eine entsprechende Leistungsbeschreibung mit Service-Level-Agreement auf Basis der vorliegenden Konzeption zu erstellen. Gegebenenfalls ist der Auftrag auszuschreiben.

Dabei ist vorab zu beurteilen, ob eine getrennte Beauftragung von VDV, Veröffentlichungsdienst und AD erfolgen soll.

17 Ausbaumöglichkeiten

Abschließend werden in diesem Kapitel die Ausbaumöglichkeiten zusammengestellt, die während der Erarbeitung der ersten Ausbaustufe des Konzepts zurückgestellt wurden. Weitere Hinweise zu Ausbaumöglichkeiten können sich aus den Abgrenzungen des Verzeichnisdienstkonzepts (Kapitel 1.3) ergeben.

17.1 Erweiterung des Umfangs der Dienste

Im Hinblick auf die folgenden Punkte könnte der Umfang der bereitgestellten Daten erweitert werden:

- Flexibilisierung des Datenumfangs in Teilnehmer-Entries,
- Aufnahme von CAs, die nicht zu PKI-1-Verwaltung gehören,
- Unterscheidung der Teilnehmer in Personen, Gruppen, Dienste, Pseudonyme etc. (mit oder ohne eigene Objektklassen),
- Bereitstellung von Teilnehmerzertifikaten per HTTP,
- Teilnehmer-Zertifikate für andere Zwecke als Verschlüsselung bzw. generell mehrere Teilnehmer-Zertifikate je Entry (dies setzt voraus, dass gängige Clients die passenden Zertifikate korrekt auswählen können).

17.2 Bedarfsabhängige Erweiterungen

Die folgenden Erweiterungen könnten das Sicherheitsniveau der Datenübertragung und die Gestaltungsmöglichkeiten der Domänen erhöhen, falls sich entsprechender Bedarf herausstellt:

- Einführung zusätzlicher Auswahlmechanismen für Entries für den Reimport in die Domänen. Beispielsweise könnte eine Aufteilung von LDIF-Dateien nach zu definierenden Kriterien im Austauschdienst erfolgen, um die angebotenen Dateien an den spezifischen Bedarf der Domänen anzupassen.

- Spezifische Ablagebereiche im Austauschdienst, die unter Umgehung des VDV gefüllt werden und nur begrenzten Nutzergruppen zugänglich sind. Beispielsweise könnten die Polizeien des Bundes und der Länder den Austauschdienst nutzen, um Entries ihrer Mitarbeiter untereinander bereitzustellen, nicht aber in den VDV oder Veröffentlichungsdienst einzustellen.
- Unterstützung verschlüsselter LDIF-Dateien im Austauschdienst. Dies wäre eine vereinfachte Unterstützung geschlossener Gruppen ohne die "spezifischen Ablagebereiche". Die verschlüsselten Dateien wären zwar für alle Berechtigten sichtbar, könnten aber nur von Schlüsselinhabern sinnvoll verwendet werden. Die Gruppe könnte das Schlüssel-Management selbst organisieren.
- Konsistenzprüfung der eingehenden Dateien in den Domänen, beispielsweise mit Hilfe einer PKI-basierten Ende-zu-Ende-Sicherung. Dies würde die zentrale Stellung des VDV reduzieren.
- Anpassung des Sicherheitsniveaus, falls erforderlich, mit geeigneter Ergänzung und Ausbau der Maßnahmen. Beispielsweise könnte der Austauschdienst unabhängig von VDV betrieben werden.

17.3 Optimierung der Dienste

Durch wachsende Teilnehmerzahlen können Veränderungen oder Erweiterungen erforderlich werden. Außerdem könnten Erfahrungen zeigen, dass die erreichte Performanz nicht zufriedenstellend ist und die Skalierbarkeit der Ausbaustufe 1 nicht ausreicht. In diesen Fällen könnte eine Optimierung der Dienste sinnvoll sein:

- Nutzung von X.500-Replikationsmechanismen (statt Datei-Austausch), soweit verfügbar.
- Überprüfung der Service-Qualität der Ausbaustufe 1. Gegebenenfalls sind Strategien zu einer Verbesserung zu entwickeln.

- Überprüfung und ggf. Veränderungen des Prozesses und der technischen Abläufe beim Wiederaufsetzen nach Störungen.
- Erhöhung der Datenqualität und der Replikationsrhythmen, falls erforderlich.
- Veränderung der Rhythmen für Vollabgleiche.
- Unabhängige Zulieferung von der Domäne zu Verzeichnisdienst der Verwaltung und Austauschdienst über zwei getrennte Verbindungen, um die Verfügbarkeitsanforderungen an den VDV zu vermindern (VDV ist keine zentrale Komponente mehr).
- Zusätzliche Implementierung von Push- oder Trigger-Lösungen, falls erforderlich.
- Automatisierte Löschung von CA- und CDP-Entries (erfordert geeignete Sicherungsmaßnahmen).
- Vollständige Umstellung des Löschprozesses auf LDIF-Löschbefehle aus den Domänen, die dies unterstützen. Ggf. auch Implementierung weiterer Löschverfahren, wenn erforderlich.
- Komplexere Umsetzungsmechanismen für CA- und TN-Namen.

17.4 Ausbau des Sicherheitskonzepts

Hinsichtlich des Ausbaus des Sicherheitskonzepts sind folgende Schritte denkbar:

- Prüfung, ob die Aktualisierungsprozesse für den Verzeichnisdienst der Verwaltung und den Austauschdienst vollständig entkoppelt werden sollen.
- "Akzeptierte Schwachstellen" auf der Basis der Nutzung des Verzeichnisdienstkonzepts und der im Betrieb gewonnenen Erfahrungen überprüfen.
- Vollständigkeit von übertragenen LDIF-Dateien anhand von Sequenznummern überprüfen.
- Überprüfen der Abhängigkeit nach Nutzerzahlen und Anwendungen.

- Ende-zu-Ende-Integritäts-Sicherung.
- Anpassung von Authentifikations-Mechanismen im Falle einer Bereitstellung der Daten über eine Pull-Lösung.
- Konzepterweiterung für schwere Störfälle, um angepasst eskalieren und reagieren zu können.

Literaturverzeichnis

Dokumente des Projekts "Verzeichnisdienstkonzept"

[PKI1V-VDK-Analyse AP]	BSI (Hrsg.): Zertifizierungsinfrastruktur für die PKI-1-Verwaltung: Analyse für das Verzeichnisdienstkonzept: Aktualisierungs- und Abrufprozess, 2002
[PKI1V-VDK-Analyse DIT und Schema]	BSI (Hrsg.): Zertifizierungsinfrastruktur für die PKI-1-Verwaltung: Analyse für das Verzeichnisdienstkonzept: Directory Information Tree und Directory Schema, 2002
[PKI1V-VDK-Erg]	BSI (Hrsg.): Zertifizierungsinfrastruktur für die PKI-1-Verwaltung: Verzeichnis-dienstkonzept, 2001 – 2002 (dieses Dokument, Abschlussdokument des Projektes)
[PKI1V-VDK-GuL]	BSI (Hrsg.): Zertifizierungsinfrastruktur für die PKI-1-Verwaltung: Glossar und Literaturverzeichnis des Verzeichnisdienstkonzepts, 2001 – 2002 (Vorgänger des Literaturverzeichnisses und Glossars in diesem Dokument)
[PKI1V-VDK-Ziel]	BSI (Hrsg.): Zertifizierungsinfrastruktur für die PKI-1-Verwaltung: Zielsetzung des Verzeichnisdienstkonzepts, 2001 – 2002

Materialien des Projekts "Verzeichnisdienstkonzept"

Die im folgenden aufgeführten Materialien wurden im Rahmen der Analysen für das Verzeichnisdienstkonzept bewertet und sind in Abhängigkeit von der Bewertung in der Konzeption berücksichtigt.

[BayBN Policy]	Bayrisches Behördennetz: Sicherheitsrichtlinien (Policy) der Zertifizierungsinstanz (CA) für das Bayerische Behördennetz, Stand vom 17.07. 2001.
[CCI Policy]	Schlumberger/Sema-Competence Center Informatik (CCI) GmbH: Sicherheitsleitlinien des CCI TrustCenters als Zertifizierungsstelle der PKI-1-Verwaltung, Version 1.0.
[DIZ Policy]	T-Systems debis Systemhaus Information Security Services GmbH (Hrsg.): Certificate Policy für die Public-Key-Infrastruktur des Daten- und Informationszentrums Rheinland-Pfalz – Pilotphase, Version 0.7.0, 18.07. 2001.
[eSig 160102]	Beschluss der Bundesregierung zur Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung vom 16. Januar 2002, http://www.bmwi.de/Homepage/download/infogesellschaft/eSig-Kabinettbeschluss.pdf.
[ISIS-MTT Part 4]	ISIS-MTT - T7 & TeleTrusT (2001): ISIS-MTT – Common ISIS-MTT Specification For PKI Applications, PART 4, OPERATIONAL PROTOCOLS (LDAP, OCSP, TSP) Version 1.0, September 2001, www.teletrust.de oder www.t7-isis.de.
[IT-Grundschutz-handbuch]	BSI: IT-Grundschutzhandbuch, jeweils aktuelle Fassung, z. B. unter http://www.bsi.bund.de.
[IVBB-DIR-Schema]	J. Keutel, J. Lüers: Directory-Schema des zentralen IVBB-Directory-Servers (IVBB-X.500), Version 2.0, 9. April 2001.
[IVBB-Teiln 2001]	IVBB (Hrsg.): Beschreibung der Möglichkeiten zur Teilnahme am zentralen X.500-Service des IVBB, Version 01.01 vom 09.04. 2001.
[IVBB-Telesec-CA]	IVBB / DeTeSystems: Secure E-Mail – Anbindung der TeleSec-CA an das zentrale Directory im IVBB, Version 00.01 vom 13.3. 2001.

[LDAPv3]	RFC 2251 - Wahl, M. / Howes, T. / Kille, S.: Lightweight Directory Access Protocol (v3), IETF, December 1997 mit den weiteren Teilen: • Attribute Syntax Definitions (RFC 2252). • UTF-8 String Representation of Distinguished Names (RFC 2253). • The String Representation of LDAP Search Filters (RFC 2254). • The LDAP URL Format (RFC 2255). • A Summary of the X.500(96) User Schema for use with LDAPv3 (RFC 2256).
[LDIF]	The LDAP Data Interchange Format (LDIF) – Technical Specification, RFC 2849, IETF, June 2000.
[PKI1V Anforderungs-katalog]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Anforderungskatalog für Zertifizierungsdienstleister in der Public-Key-Infrastruktur der Verwaltung - PKI-1-VERWALTUNG, Version 1.5 vom 18. Juli 2001, Bonn, 2001.
[PKI1V Aufnahmevertrag]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2001): Vereinbarung zwischen PCA und nachgeordneten Zertifizierungsstellen, Bonn, 2001.
[PKI1V Ausschreibung]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Ausschreibung eines Zertifizierungsdienstleisters für die Public-Key-Infrastruktur der öffentlichen Verwaltung - PKI-1-Verwaltung, Version 1.0, Bonn, 23. März 2001.
[PKI1V Formate und Protokolle]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Zertifizierungsinfrastruktur für die PKI-1-Verwaltung – Technische Grundlagen der Wurzelzertifizierungsstelle - Formate und Protokolle nach MTTv2, Version 1.01, Bonn, Stand: 8. März 2001.
[PKI1V Grobkonzept]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Aufgaben von Zertifizierungsdienstleistern für die Public-Key-Infrastruktur der Verwaltung - PKI-1-Verwaltung, Version 1.05, Bonn, 23. März 2001.
[PKI1V Namensformat MTT]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Zertifizierungsinfrastruktur für die PKI-1-Verwaltung – Technische Grundlagen der Wurzelzertifizierungsstelle - Namensformat nach MTTv2, Version 1.01, Bonn, Stand: 13. März 2001.
[PKI1V Namensregeln]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Zertifizierungsinfrastruktur für die PKI-1-Verwaltung – Namensregeln und -formate, 2002. (Enthält konsolidierte, verbindliche Namensregeln, wird zur Zeit erstellt)
[PKI1V Selbsterklärung]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Selbsterklärung der Zertifizierungsstelle - Anlage 1 zum Vertrag über die Teilnahme an der PKI-1-Verwaltung - Version 1.01, Bonn, 2001.
[PKI1V Si-Leitlinie]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung, Version 1.21, Bonn, 17.04.2001.
[PKI1V Vertragstext]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Vertragstext über die Teilnahme an der PKI-1-Verwaltung, Stand: 15.10.2001, Bonn, 2001.
[PKIX LDAP Schema]	Chadwick, D. W. / Legg, S.: Internet X.509 Public Key Infrastructure LDAP Schema and Syntaxes for PKIs and PMIs; (draft-ietf-pkix-ldap-schema-02.txt) 2001.
[PKIX OpProt LDAPv3]	Chadwick, D.W. (2002): Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv3, Internet-Draft, IETF, draft-ietf-pkix-ldap-v3-05.txt.
[RFC 2247]	RFC 2247 - Kille, S. / Wahl, M. / Grimstad, A. / Huber, R. / Sataluri, S. (1998): Using Domains in LDAP/X.500 Distinguished Names, IETF, 1998.
[RFC 2279]	RFC 2279 - Yergeau, F. (1998): UTF-8, a transformation format of ISO 10646, IETF.
[RFC 2559]	RFC 2559 - Boeyen, S. / Howes, T. / Richard, P. (1999): Internet X.509 Public Key Infrastructure, Operational Protocols - LDAPv2, IETF, 1999.

[RFC 2587]	RFC 2587 - Boeyen, S. / Howes, T. / Richard, P. (1999): Internet X.509 Public Key Infrastructure LDAPv2 Schema, IETF, 1999.
[SNBS Betriebskonzept]	Siemens Nixdorf Business Services: Betriebskonzept X.500 Directory im IVBB, Version 1.1, 2.7. 1998.
[SNBS Feinkonzept]	Siemens Nixdorf Business Services: Feinkonzept X.500 Directory im IVBB, Version 1.01, 9.4. 1998.
[SNBS Realisierungs-konzept]	Siemens Nixdorf Business Services: Realisierungskonzept X.500 Directory im IVBB, Version 1.1, 19.6. 1998.
[Sphinx Dir]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Sphinx - Verzeichnisdienst-Konzept für PKIs, Version 2.2, Bonn, 17. Januar 2001.
[Sphinx Namen]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Sphinx - Sichere E-Mail - Spezifikation und Verwendung von Namen in einer PKI (Namenskonzept), Version 1.1, Bonn, 2000.
[Sphinx Tailoring MTTv2]	BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): SPHINX - Technische Grundlagen - Tailoring MTTv2, Version 1.2, Bonn, 15. August 2000.
[TESTA Betriebs-handbuch CA]	Freistaat Thüringen, KoopA ADV, Deutsche Telekom: TESTA Deutschland Betriebshandbuch TESTA CA, Version 2.1.
[TESTA Betriebshandbuch Nutzer]	Freistaat Thüringen, KoopA ADV, Deutsche Telekom: TESTA Deutschland Betriebshandbuch für Nutzer, Mai 2001.
[TESTA CA Be-triebshandbuch Verwaltungs-PKI]	Freistaat Thüringen, KoopA ADV, Deutsche Telekom: TESTA Deutschland Betriebshandbuch Verwaltungs-PKI, Version 2.0.
[X.500 ff 1997]	ITU-T X.500 – International Telecommunication Union - Telecommunication Sector: ITU-T Recommendation X.500 ff – Information Technology - Open Systems Interconnection - The Directory, 1997: • X.500: Overview Of Concepts, Models, and Services. • X.501: Models. • X.509: Authentication Framework. • X.511: Abstract Service Definition. • X.518: Procedures For Distributed Operation. • X.519: Protocol Specifications. • X.520: Selected Attribute Types. • X.521: Selected Object Classes. • X.525: Replication. • X.530: Use of Systems Management for Administration of the Directory.
[X.500 ff 2001]	ITU-T X.500 ff – International Telecommunication Union - Telecommunication sector: ITU-T X.500 ff Information Technology - Open Systems Interconnection - The Directory, 2001. Für die Teile des Standards siehe [X.500 ff 1997].

Glossar

Das folgende Verzeichnis enthält in alphabetischer Reihenfolge Abkürzungen und Erläuterungen zu Begriffen. Dadurch können Abkürzungen unmittelbar erklärt werden. Es enthält auch Abkürzungen aus dem Literaturverzeichnis. Abkürzungen, die in Parametern oder Variablen von Prozessspezifikationen verwendet werden, sind **nicht** enthalten.

AD	Abkürzung für → Austauschdienst
AIA	Abkürzung für Authority Information Access, Verweis in Zertifikaten auf Entries, in denen CA-Zertifikate bereitgestellt werden.
A-DIT	Abkürzung für → Austausch-DIT; Directory Information Tree
AP	Abkürzung für Aktualisierungsprozess
ARL	Abkürzung für Authority Revocation List, → Sperrliste, die nur Verweise auf Zertifikate von Zertifizierungsinstanzen enthält.
Attribut	Bezeichnet den Speicherplatz für Werte eines Bestimmten Typs, z. B. *Surname* oder *OrganizationalUnitName.* Attribute treten in zwei Rollen auf: • als Bestandteile eines eindeutigen Namens (Distinguished Name). Der Distinguished Name besteht aus einer Reihe von Attributen, deren Reihenfolge festgelegt ist. In der Reihenfolge können an unterschiedlichen Stellen Attribute gleichen Typs auftreten. • als Speicherplatz für Werte *in einem* → Entry. Ein Entry kann verschiedene Attribute enthalten. Ein Attribut kann so definiert werden, dass es nur einen einzelnen Wert (singlevalued) oder mehrere Werte des Typs aufnehmen kann (multivalued).
Attribut-Typ	Attribut-Typen dienen der Spezifikation von Attributen für das → Directory-Schema. Mit ihnen wird die Semantik und die Codierung von Werten bestimmt. Sie werden benutzt, um → Objektklassen zu definieren. Ein → Attribut ist die Instanz eines Attribut-Typs in einem → Entry oder Distinguished Name.
Austauschdienst	Einer der drei → Verzeichnisdienste des Verzeichnisdienstkonzepts. Der Austauschdienst wird verwendet, um Daten zwischen den → Domänen zu übermitteln.
Austausch-DIT	Abkürzung für den gemeinsamen (einheitlichen) Directory Information Tree (→ DIT) der drei Dienste des Verzeichnisdienstkonzepts.
Authentizität	Eigenschaft einer Information (z. B. des Inhalts einer E-Mail): sie stammt tatsächlich von der Person, die sich als Absender bezeichnet.
Binary	Der Zusatz ";binary" zu einem Attribut-Namen kennzeichnet ein Codierungs-Format zum Einstellen von Daten in den oder Abruf aus dem Verzeichnisdienst.
BSI	Abkürzung für Bundesamt für Sicherheit in der Informationstechnik.
BYBN	Abkürzung für Bayrisches Behördennetz.
CA	Abkürzung für Certification Authority.
CCI	Abkürzung für Schlumberger/Sema-Competence Center Informatik GmbH.

CDP	Abkürzung für → CRL Distribution Point. 1) Im Directory kann es CDP-Entries geben, die Sperrlisten beinhalten. Unter bestimmten Umständen kann dies die Verwaltung der Sperrlisten oder den Zugriff darauf erleichtern. 2) Im Zertifikat kann ein CDP angegeben sein, der direkt auf den Speicherort der Sperrliste (nämlich den CDP im Verzeichnis) verweist. Dies kann Clients das Auffinden der zugehörigen Sperrliste erleichtern.
Chaining	Verbindung zwischen zwei Directory-Servern, über die der eine Server Anfragen, die er nicht beantworten kann, an den anderen weiterreicht. Dabei erfolgt die Verbindung zwischen der Servern, der Client steht immer nur mit dem ursprünglichen abgefragten Dienst in Verbindung (und erhält über diesen ggf. auch das Suchresultat). Im Rahmen des X.500-Standards (→ X.500 ff.) werden Mechanismen zum Chaining definiert. Viele Directory-Server unterstützen diese allerdings nicht, sondern verwenden eigene (proprietäre) Lösungen (zu Alternativen siehe auch → Verbindung zwischen Verzeichnisdiensten).
cn	Abkürzung für Common Name (Attribut-Typ).
CRL	Abkürzung für Certificate Revocation List, → Sperrliste mit Verweisen auf gesperrte Zertifikate von Teilnehmern und CAs.
D-DIT	Abkürzung für "Directory Information Tree der Domäne"
Dienste des Verzeichnisdienst-konzepts	Zusammenfassend für die drei Dienste, die im Verzeichnisdienstkonzept spezifiziert werden: → zentraler Verzeichnisdienst der Verwaltung, → Austauschdienst und → Veröffentlichungsdienst. Siehe auch → Verzeichnisdienst der PKI-1-Verwaltung.
Digitale Signatur	Konzept zur Sicherung der → Integrität und → Authentizität von E-Mails und elektronischer Dokumente. Anhand der digitalen Signatur kann der Empfänger unter Anwendung des Signaturprüfschlüssels feststellen, ob eine elektronische Nachricht authentisch und integer ist.
Directory	Synonym für → Verzeichnisdienst.
Directory-Schema	Das Directory-Schema beschreibt mit den → Objektklassen und → Attribut-Typen, welche Informationen die → Entries der einzelnen Objekttypen enthalten.
DIT	Abkürzung für Directory Information Tree. Bezeichnet die Struktur, in der die → Entries im Directory abgelegt werden. Der DIT wird durch eine Folge von Namen aufgespannt, die jeweils relativ zum übergeordneten Knoten eindeutig sein müssen. Jeder Entry im DIT wird durch seinen DIT-Distinguished Name eindeutig gekennzeichnet. Der DIT-DN entspricht damit einem Datenbankschlüssel für die Einträge im → Directory.
DIT-DN	Abkürzung für Directory Information Tree Distinguished Name, eindeutiger Name (und Identifier) eines → Entries im Directory. Siehe auch → DIT und → LDAP-Schreibweise von DIT-DNs. Zur Unterscheidung siehe → Subject-DN und → Issuer-DN. Der DIT-DN eines Teilnehmer-Entries und sein Subject-DN im Zertifikat können übereinstimmen, müssen dies aber nicht unbedingt.
DNS	Abkürzung für Domain Name System
Domäne	→ Domäne einer PKI, → Domäne eines Verzeichnisdienstes.
Domäne einer PKI	Der Bereich, für den eine PKI Zertifikate ausstellt (meist eine oder mehrere Organisationen, aus denen sich auch ein abgegrenzter Namensbereich ergibt).
Domäne eines Verzeichnisdienstes	Der Bereich, für den ein Verzeichnisdienst Zertifikate (und ggf. weitere Informationen) verwaltet (meist eine oder mehrere Organisationen, aus denen sich auch ein abgegrenzter Namensbereich ergibt). Die Domäne eines Verzeichnisdienstes kann aus der Sicht des Verzeichnisdienstkonzepts die → Zuständigkeitsbereiche mehrerer → Vertrags-CAs umfassen.
Domänen-PKI	Die PKI einer → Domäne (also alle Zertifizierungsstellen und SubCAs, die in dieser Domäne betrieben werden).

Email	Abkürzung für das Attribut, das die E-Mail-Adresse enthält.
Entry	Die Informationen zu einem Objekt (Teilnehmer oder Zertifizierungsinstanz) werden in einem sogenannten Entry im Verzeichnisdienst gespeichert. Der Entry umfasst, quasi als Container, mehrere → Attribute. In den Attributen werden die einzelnen Werte abgelegt, die dem Objekt zugeordnet sind, beispielsweise die E-Mail-Adresse, der Nachname oder das Zertifikat eines Teilnehmers. Jeder Entry wird eindeutig durch einen eindeutigen Namen im Directory adressiert, dem sogenannten DIT Distinguished Name → DIT-DN.
Extranet	Extranet steht für das "restliche" Internet im Unterschied zum → Intranet der öffentlichen Verwaltung.
gn	Abkürzung für Given Name (Attribut-Typ).
HTTP	Abkürzung für Hypertext Transfer Protocol. Protokoll, das zur Übertragung von Webseiten genutzt wird.
HTTPS	Protokoll zur Absicherung der Übertragung von Webseiten (basiert auf → HTTP und verwendet → SSL).
IETF	Abkürzung für Internet Engineering Task Force, Standardisierungsgremium (www.ietf.org).
Integrität	Eigenschaft einer Information (z. B. dem Inhalt einer E-Mail), dass (unzulässige) Veränderungen an ihr nicht vorgenommen wurden. Wurde eine E-Mail während der Übertragung nicht verändert, so ist sie integer. Die Integrität einer signierten elektronischen Nachricht kann vom Empfänger durch die Überprüfung ihrer → digitalen Signatur mit dem Signaturprüfschlüssel des Absenders festgestellt werden.
Intranet	Abgeschlossenes IT-Netzwerk, auf das nur bestimmte Teilnehmer Zugriff haben. Unter dem "Intranet der Verwaltung" wird das gemeinsame Netz der deutschen Behörden verstanden (entspricht → TESTA D Netz), das gegen das restliche Internet (→ Extranet) abgegrenzt ist. Alle Mitarbeiter angeschlossener Behörden können auf den im Intranet bereitgestellten → zentralen Verzeichnisdienst der Verwaltung zugreifen.
Issuer DN	Issuer Distinguished Name, eindeutiger Name des Ausstellers eines Zertifikats, im Zertifikat enthalten. Zur Unterscheidung siehe → Subject-DN und → DIT-DN.
ITU-T	Abkürzung für International Telecommunication Union - Telecommunication Sector, internationale Standardisierungsorganisation für Telekommunikation, vormals Comité Consultatif International Télégraphique et Téléphonique (CCITT)
IVBB	Abkürzung für Informationsverbund Berlin-Bonn.
KoopA	Abkürzung für Kooperationsausschuß automatisierte Datenverarbeitung der Behörden des Bundes, der Länder und des kommunalen Bereichs"
l	kleines "L" als Abkürzung für Locality (Attribut-Typ).
LDAP	Abkürzung für Lightweight Directory Access Protocol (standardisiert durch → RFCs im Unterschied zum Directory Access Protocol (DAP) des → X.500-Standards). LDAP legt lediglich fest, mit welchen Kommandos eine Information abgefragt oder geändert werden kann, macht aber keine Aussagen über die Ablage der Daten. Auch "echte" X.500 Server oder Standard-Datenbanken können LDAP "sprechen".
LDAP-Proxy	Ein Proxy, der LDAP-Anfragen weiterreicht. Dies wird insbesondere dann verwendet, wenn Firewalls zwischen dem Client und dem abzufragenden LDAP-Server stehen, die LDAP sperren. Mittels des Proxies kann eine Öffnung des Firewalls für alle Clients umgangen werden (zu Alternativen siehe auch → Verbindung zwischen Verzeichnisdiensten).

LDAP-Schreibweise von DIT-DNs	Die LDAP-Schreibweise von → DIT-DNs beginnt beim Blatt-Entry und folgt den Knoten aufsteigend zur Wurzel des DIT, also beispielsweise "cn=Peter Mustermann, o=Muster GmbH, c=DE".
LDIF	Abkürzung für → LDAP Data Interchange Format. Spezifiziert in RFC 2849, bietet eine Möglichkeit, Datenaustausch zwischen Directories dateibasiert vorzunehmen.
MTT	MailTrusT, Standard für Formate und Dienste von → PKIs und Anwendungen, die PKIs nutzen, z. B. zur Verschlüsselung von E-Mails.
multivalued	→ Attribut, das mehrere Wert enthalten kann, z. B. mehrere Namen von Organisational Units (zum Unterschied siehe → singlevalued)
nachgeordnete CA	CA, die nicht → Vertrags-CA ist, aber zur Zertifizierungshierarchie der PKI-1-Verwaltung gehört. Der öffentliche Schlüssel der nachgeordneten CA muss dazu direkt oder indirekt von einer Vertrags-CA zertifiziert sein.
Namensgebendes Attribut	Das "unterste" → Attribut des DIT-DN, das den Namen des → Entries von den anderen Entries auf der gleichen Ebene unterscheidet, wird als namensgebendes Attribut oder → Relative Distinguished Name bezeichnet.
Nutzer	Nutzer im Sinne des Verzeichnisdienstkonzepts sind Behörden, die das IVBB bzw. die PKI-1-Verwaltung (oder eine andere Infrastruktur) nutzen.
o	Abkürzung für Organization (Attribut-Typ).
Objektklasse	Die Objektklasse legt fest, um welchen Typ von → Entry es sich handelt. Eine Objektklasse fasst mehrere → Attribut-Typen zusammen. Jeder Entry kann aus mehreren Objektklassen gebildet werden. Er muss jedoch mindestens eine → strukturelle Objektklasse mit dem → namensgebenden Attribut enthalten.
OCSP	Abkürzung für Online Certificate Status Protocol, Standard zur Abfrage des Sperrstatus von einzelnen Zertifikaten (im Verzeichnisdienstkonzept nicht berücksichtigt).
Öffentlicher Schlüssel	Der öffentliche Schlüssel ist der öffentliche Teil des → Schlüsselpaars. Verschlüsselungsschlüssel und Signaturprüfschlüssel sind öffentliche Schlüssel und werden i.d.R. in Zertifikaten authentisch zur Verfügung gestellt.
ou	Abkürzung für Organizational Unit Name (Attribut-Typ).
PCA	→ PCA-1-Verwaltung.
PCA-1-Verwaltung	Wurzelzertifizierungsinstanz der → PKI-1-Verwaltung, betrieben vom → BSI.
PKI	Public Key Infrastruktur, Infrastruktur zur Bereitstellung von öffentlichen Schlüsseln, Zertifikaten und Sperrinformationen. Zur Infrastruktur zählen alle Voraussetzungen für die Dienste, mit denen die Leistungen erbracht werden, z. B. auch der → Verzeichnisdienst.
PKI-1-Verwaltung	PKI der öffentlichen Verwaltung der Bundesrepublik Deutschland. Sie umfasst alle → PKIs, die durch die → PCA-1-Verwaltung für die öffentliche Verwaltung zertifiziert werden.
PKI-Domäne	→ Domänen-PKI
PKI-Informationen	Oberbegriff für Teilnehmer-Zertifikate, CA-Zertifikate und Sperrlisten
Privater Schlüssel	Der private Schlüssel ist der private Teil des → Schlüsselpaars. Er ist nur dem Besitzer des zugehörigen Zertifikats bekannt.
Proxy	Hier: → LDAP-Proxy.
PSE	Abkürzung für Personal Secure Environment, wird als Bezeichnung für einen gesicherten Speicher- und / oder Verarbeitungsbereich für Schlüsselinformationen und sicherheitskritische Parameter verwendet.

Referral	Information eines Directory-Servers an einen Client, den gesuchten Eintrag bei einem anderen Server zu suchen. Die Rückantwort des Servers enthält im Referral den Namen des anderen Servers und ggf. auch die passende Such-Anfrage. Im Anschluss baut der Client eine neue Verbindung zum genannten Server auf und sucht erneut. Der Mechanismus muss von Client und Server unterstützt werden. Er ist Bestandteil des LDAPv3-Standards (zu Alternativen siehe auch → Verbindung zwischen Verzeichnisdiensten).
Relative Distinguished Name	Der Relative Distinguished Name ist ein Namensteil des DIT Distinguished Name, der auf einer Ebene des DIT Eindeutigkeit sicherstellt. Für den Wert eines Relative Distinguished Names eines Entries ist gefordert, dass er sich von allen anderen Relative Distinguished Names auf der gleichen Ebene seines Teilbaums unterscheidet.
Replikation	Kopie von Daten eines Verzeichnisdienstes (Datenquelle) auf einen oder mehrere weitere Verzeichnisdienste. Im Kontext von Datenbanken oder Verzeichnisdiensten wird im Allgemeinen davon ausgegangen, dass eine regelmäßige oder fallabhängig Aktualisierung der Replikationen erfolgt.
RFC	Abkürzung für Request for Comment, Standardisierungsdokumente der → IETF.
Schlüsselpaar	Zusammengehöriges Paar aus → privatem Schlüssel und → öffentlichem Schlüssel.
Secure Copy	eine auf das Kopieren von Dateien eingeschränkte → SSH-Verbindung.
Service-Level	Vereinbarung zu bestimmten Eigenschaften des Betriebes eines Dienstes (z. B. Verfügbarkeit, Reaktionszeiten auf bestimmte Vorfälle, Leistungen etc.).
Signaturprüfzertifikat	Zertifikat, das zur Signaturprüfung verwendet wird. (Es kann zulässig sein, es für weitere Zwecke zu verwenden.)
singlevalued	→ Attribut mit nur einem Wert (zum Unterschied siehe → multivalued)
sn	Abkürzung für Surname Name (Attribut-Typ).
Sperrliste	Liste, die Verweise (meist Seriennummern) auf gesperrte Zertifikate enthält und von der ausstellenden CA unterschrieben ist. Sie kann von Anwendern dazu verwendet werden, zu überprüfen, ob ein bestimmtes Zertifikat gesperrt oder gültig ist. Es gibt mehrere Typen von Sperrlisten: → CRL und → ARL.
SSH	Abkürzung für Secure Shell; entspricht einer SSL gesicherten Verbindung zwischen zwei Rechnern, in der Telnet zur Verfügung steht. Kann bei entsprechenden Zugriffsrechten zur Fernsteuerung des zweiten Rechners verwendet werden.
SSL	Abkürzung für Secure Socket Layer.
Steuerungsgremium der PKI-1-Verwaltung	Gegenwärtig wird geklärt, wie die an der PKI-1-Verwaltung beteiligten Domänen und CAs gemeinsam die Weiterentwicklung dieser PKI und des Verzeichnisdienstkonzepts steuern. Im Verzeichnisdienstkonzept wird für die zuständigen Gremien zusammenfassend "Steuerungsgremium der PKI-1-Verwaltung" verwendet.
Strukturelle Objektklasse	→ Objektklasse, die das → namensgebende Attribut (relative Distinguished Name) enthält.
Sub-CA	auch für → nachgeordnete CA.
Subject-DN	Subject Distinguished Name, eindeutiger Name des Inhabers eines Zertifikats, im Zertifikat enthalten. Zur Unterscheidung siehe → Issuer DN und → DIT DN.
Teilnehmer	Personen, die im Rahmen der PKI-1-Verwaltung Schlüssel und Zertifikate erhalten oder aus dem Verzeichnisdienst PKI-Informationen von CAs oder Teilnehmern abrufen.
TESTA	Abkürzung für Trans European Services for Telematics between Administration

TESTA D	Abkürzung für TransEuropean Services for Telematics between Administration Deutschland. TESTA D steht auch für das Kommunikationsnetz der öffentlichen Verwaltung. Im Rahmen von TESTA D wird auch der → Verzeichnisdienst der Verwaltung betrieben.
UNICODE	Zeichentabelle zur Umsetzung von bestimmten Zeichnen (Buchstaben, Zahlen) in numerische Äquivalente. Enthält insbesondere auch Umlaute und weitere Sonderzeichen.
UTF8	Codierungsvorschrift zur Codierung von UNICODE-Zeichen in Texten und Nachrichten
VCA	Abkürzung für → Vertrags-CA
VD	Abkürzung für Verzeichnisdienst
VDK	Abkürzung für Verzeichnisdienstkonzept
VDV	Abkürzung für → zentraler Verzeichnisdienst der Verwaltung
Verbindung zwischen Verzeichnisdiensten	Die Verbindung zwischen zwei Verzeichnisdiensten ist immer dann sinnvoll, wenn ein Server Anfragen bekommt, die er selber nicht beantworten kann, aber bekannt ist, dass ein anderer Server die entsprechenden Informationen hat. Dazu gibt es die Möglichkeiten: → Referral und → Chaining. Im Unterschied zu → Replikationen hält in den beiden genannten beiden Varianten der erste Server die eigentlich gesuchten Daten nicht selbst.
Veröffentlichungsdienst	Einer der drei → Verzeichnisdienste des Verzeichnisdienstkonzepts. Der Veröffentlichungsdienst dient zur öffentlichen Bereitstellung bestimmter Daten im Internet (im Unterschied zum → zentralen Verzeichnisdienst der Verwaltung).
Verschlüsselungs-zertifikat	Verschlüsselungszertifikate sind Zertifikate, die zur Verschlüsselung von Mails oder Dateien geeignet sind. Dies schließt nicht aus, dass sie auch zur Signaturprüfung verwendet werden können, wenn dies im Zertifikat vorgesehen ist.
Vertrags-CA	Als Vertrags-CA wird eine CA bezeichnet, die die Beitrittsvereinbarung mit der → PCA abgeschlossen hat. Jede Vertrags-CA hat einen abgegrenzten → Zuständigkeitsbereich und kann einer → Domäne angehören. Die Vertrags-CA kann für ihren Zuständigkeitsbereich nachgeordnete CAs zulassen.
Verzeichnisdienst	Synonym für → Directory. Quelle für Informationen über Objekte. Für jedes Objekt wird im Verzeichnisdienst ein → Entry eingerichtet, der die Informationen enthält. Die Entries sind hierarchisch in einem → DIT organisiert. Objekte sind beispielsweise Personen, zu denen E-Mail-Adresse, postalische Adresse und Telefonnummer vorgehalten werden. Siehe auch → Verzeichnisdienst der PKI-1-Verwaltung.
Verzeichnisdienst der PKI-1-Verwaltung	Unter Verzeichnisdienst der PKI-1-Verwaltung werden drei Verzeichnisdienste zusammengefasst. Der → zentrale Verzeichnisdienst der Verwaltung und der Veröffentlichungsdienst dienen dem Zugriff von unterschiedlichen Teilnehmer-Kreisen auf PKI-Informationen. Der → Austauschdienst erlaubt eine effiziente Übermittlung von PKI-Informationen zwischen den Domänen zur Aktualisierung der lokalen Verzeichnisdienste. Da die Verzeichnisdienste für eine Public Key Infrastruktur (→ PKI) eingesetzt werden, müssen in ihnen die Zertifikate von Teilnehmern, die Zertifikate von Zertifizierungsinstanzen und die Sperrlisten bereitgestellt werden.
Verzeichnisdienst der Verwaltung	Synonym für → zentraler Verzeichnisdienst der Verwaltung
Verzeichnisdienst-konzept	Hier: das Konzept für eine Integration der verschiedenen Verzeichnisdienste der in der PKI-1-Verwaltung zusammengeschlossenen → Domänen-PKIs. Siehe auch → Verzeichnisdienst der PKI-1-Verwaltung.
VöD	Abkürzung für → Veröffentlichungsdienst
X.500 ff.	Serie von Standards der → ITU-T für → Verzeichnisdienste.

zentraler Verzeichnisdienst der Verwaltung	Einer der drei → Verzeichnisdienste des Verzeichnisdienstkonzepts. Der zentrale Verzeichnisdienst der Verwaltung dient zur Bereitstellung bestimmter Daten im → Intranet der Verwaltung und ist nicht aus dem Internet zugänglich (im Unterschied zum → Veröffentlichungsdienst).
Zuständigkeitsbereich einer CA	Der Zuständigkeitsbereich betrifft den Bereich, für den eine CA verantwortlich die Regelungen des Verzeichnisdienstkonzepts durchsetzen muss. Der Zuständigkeitsbereich einer CA umfasst den Teilnehmer-Kreis, für den die CA gemäß ihrer vertraglichen Regelungen mit der → PCA oder einer nachgeordneten CA Zertifikate ausstellen darf. Er ist beispielsweise durch Organisationsgrenzen oder einen Namensraum definiert. Der Zuständigkeitsbereich einer übergeordneten CA (z. B. der → Vertrags-CA) umfasst immer auch die Verantwortung für die Durchsetzung von Regeln für die nachgeordneten CAs. Im Unterschied zum Zuständigkeitsbereich wird der Begriff der → Domäne im VDK als logisch-technische Sicht verwendet. In einer Domäne können mehrere Zuständigkeitsbereiche zusammengefasst werden.

Anhänge