Verzeichnisdienstkonzept Version 2.3.2

Editor: Dr. Keutel i.A.d.

Bundesärztekammer, Berlin

	Datum	Name, Abteilung, Firma
Autor, Ansprechpartner		Georgios Raptis (Kap. 1,2), Dr. Keutel (Kap. 3-9)
Status (HPC-Projektbüro)	12.05.11	Freigegeben

Versionshistorie

Version	Datum	Bearbeiter	Änderungen	Bemerkungen
0.1	05.12.05	DL	Änderungen an oder Anmerkungen zum directory-concept sind gelb markiert. Übernahmen aus dem Lastenheft sind kursiv. Änderungen an übernommenen Vorgaben aus dem Lastenheft sind ausschließlich in der internen Wordversion im Änderungsmode sichtbar.	Dokument initialisiert, Input directory-concept 0.3 von Dr. Keutel und Lastenheft Verzeichnisdienst und Grobkonzept Zertifikatssuche. Das Lastenheft wurde vom Projektbüro eArztausweis der Bundesärztekammer erarbeitet.
0.2	06.12.05	RS	QS	
0.9	06.03.06	JK	Einarbeiten aller Änderungen, insbesondere: - 2 implementierbare Varianten - Objektklasse hpcPerson - HPC-eigene Attribute - LDAP-Beispiele - Object Identifier - Suche nach keyUsage - Diskussion von certificate-Match / componentMatch - ...	
0.9.2	14.03.06	JK	Korrekturen: - Signer ---> Objektklasse person - Klarstellung der Varianten 1 und 2 - Speicherung von CRLs	
0.9.3	23.03.06	Raptis	Überarbeitung	
0.9.4	24.03.06	Schladweiler, Raptis	QS, explizite Behandlung von „Rastersuchabfragen“, Verwaltung von Suchrechten	

0.9.5	14.02.07 02.03.07	Schladweiler, Raptis	aktuelle Arbeitsversion zur QS, Einarbeitung Kommentare aus Audit	Aktuelle Version ist inhaltsgleich mit der Version 0.9.4, es wurden nur Präzisierungen und editorische Anpassungen vorgenommen. Die Verwendung der BAN (bundeseinheitlichen Arztnummer) und die Benamung entsprechender Attribute wurde konsequent ersetzt durch eAInhaberID. Inhaltliche Änderungen sind davon nicht betroffen.
2.3.1	10.03.09 29.05.09	Georgios Raptis	Konsolidierung zum Paket V2.3.1	Neue RFCs, Common-PKI2.0,
2.3.2	12.05.11	Dirk Schladweiler	Aktualisierung der Referenzen wegen Ki-SiKo	

Fertigstellungszustand				
Lfd Nr.	**Probleme / Offene Punkte / Defizite**	**Ursachen**	**Maßnahmen / Lösungen**	**Kapitel-verweis**

Inhalt

Abbildungsverzeichnis

1 Gegenstand des Konzeptes

Die Bundesärztekammer, als Arbeitsgemeinschaft der Landesärztekammern, plant die Zulassung interessierter Zertifizierungsdiensteanbieter, welche diese unter Einhaltung verschiedener Kriterien zur Ausgabe der elektronischen Arztausweise berechtigt.

Der elektronische Arztausweis enthält verschiedene Schlüssel und Zertifikate, bspw. für die digitale Signatur, die Authentifizierung, die Verschlüsselung und für die Card-2-Card-Authentication zur elektronischen Gesundheitskarte des Patienten.

Gegenstand des Konzeptes ist die Spezifikation eines Verzeichnisdienstes. Die Spezifikation muss von zugelassenen Zertifizierungsdiensteanbietern implementiert werden, um die Zertifikate der elektronischen Arztausweise nachprüfbar und ggf. abrufbar zu halten.

In der Phase der Test- und Pilotierung des elektronischen Arztausweises werden Signaturzertifikate auf fortgeschrittenem Niveau eingesetzt. Die Anforderungen an die Verzeichnisdienste in der Test- und Pilotierungsphase unterscheiden sich nicht von denen der Wirkbetriebsphase, in welcher obligatorisch mit Signaturzertifikaten und Attributzertifikaten auf qualifiziertem Niveau gearbeitet werden muss. Im Folgenden wird der Terminus „qualifizierte Zertifikate“ synonym für Signatur- und Attributzertifikate und „nicht-qualifizierte Zertifikate“ für die Verschlüsselungs- und Authentisierungszertifikate verwandt.

Für die Nachprüfbarkeit von Zertifikaten soll das OCSP-Protokoll verwendet werden. Dies gilt auch für die nicht-qualifizierten Zertifikate. Für qualifizierte Zertifikate soll das Zertifikat nach entsprechender Anfrage in der Response mitgeliefert werden.

Zertifikate sollen über LDAP such- und abrufbar gehalten werden. Die Spezifikation soll die einheitliche Implementierungsgrundlage für verschiedene Trustcenter sein. Außerdem soll der LDAP-Pfad zu jedem Zertifikat oder CRL eindeutig und immer gleichartig aufgebaut sein.

2 Allgemeine und technische Anforderungen

2.1 Einleitende Anforderungen

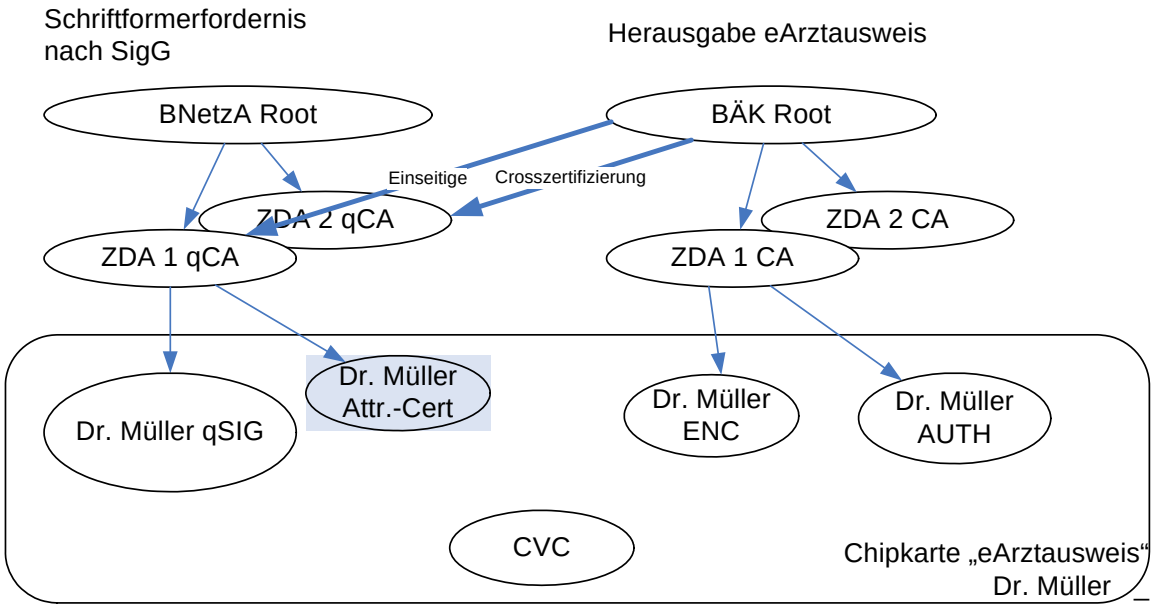
Teil einer PKI ist der Verzeichnisdienst. In der Telematik-Plattform erfüllt der Verzeichnisdienst folgende Aufgaben (Liste nicht abschließend):

- Bei Erhalt eines unterschriebenen eRezeptes: Überprüfung des Status des Signaturzertifikats und ggf. eines qualifizierten Attributzertifikats zum Zwecke der Überprüfung der Gültigkeit der Signatur
- Wenn ein Arzt Zugang in die Telematik-Infrastruktur erlangen möchte: Überprüfung der Gültigkeit des Authentisierungszertifikates von einem zentralen Dienst der Telematik-Infrastruktur
- Wenn etwas für einen Arzt verschlüsselt werden soll (z.B. Erstellung eines Tickets für einen Arzt durch einen Patienten): Bereitstellung des Verschlüsselungszertifikates.

Da qualifizierte Signaturzertifikate und ggf. qualifizierte Attributzertifikate auf die eArztausweise aufgebracht werden, muss der Verzeichnisdienst die Anforderungen des Signaturgesetzes und die daraus ergebenden technischen Anforderungen erfüllen.

Für die Struktur der PKI liegt das „Rahmenvertragsmodell“ der Bundesärztekammer zugrunde. Es gibt damit ein Root-Zertifikat der Bundesärztekammer, das CA-Zertifikate für kommerzielle zugelassene Trustcenter ausstellt. Von diesen CA-Zertifikaten werden die nichtqualifizierten Authentisierungs- und Verschlüsselungszertifikate der Ärzte abgeleitet. Zusätzlich existiert auf jeden eArztausweis ein qualifiziertes Signatur- sowie ggf. ein qualifiziertes Attributzertifikat, die von einem qualifizierten CA-Zertifikat eines ZDA ausgestellt wurden und zu einem Root-Zertifikat der Bundesnetzagentur validiert werden können. Das Root-Zertifikat der Bundesärztekammer zertifiziert mit Hilfe von Cross-Zertifikaten die qualifizierten CA-Zertifikate der zugelassenen ZDA. Ein Validierungspfad für die Signatur- und Attributzertifikate kann somit auch bis zum Root-Zertifikat der Bundesärztekammer gebildet werden. Es ist damit für alle Zertifikate ersichtlich, dass sie von einem eArztausweis stammen und den Anforderungen aus SGB V §291a erfüllen.

Abbildung 2.1-1: Zertifizierungsstruktur



2.2 Grundsätze

Für die nicht-qualifizierten Zertifikate (Verschlüsselung, Authentisierung) werden die selben Sicherheitsanforderungen wie für die qualifizierten Zertifikate gefordert. Ausnahmen von dieser Regel (z.B. HSM dürfen für OCSP-Antworten für nicht-qualifizierte Zertifikate eingesetzt werden) werden explizit in den jeweiligen Konzepten definiert.

Es werden nur Verschlüsselungszertifikate im Verzeichnisdienst über das LDAP-Protokoll öffentlich (in einem Intranet) abrufbar gehalten.

Alle Zertifikate müssen grundsätzlich nachgeprüft werden können. Die Nachprüfbarkeit der Zertifikate wird über das OCS-Protokoll realisiert. Qualifizierte Signatur- und Attributzertifikate werden über OCSP-Responder soweit zulässig abrufbar und (stets) nachprüfbar gehalten. Es muss möglich sein, in einer einzigen OCSP-Abfrage und zugehöriger OCSP-Antwort gleichzeitig ein qualifiziertes Signatur- und ein qualifiziertes Attributzertifikat abzurufen und nachzuprüfen.

Authentisierungszertifikate werden nicht abrufbar gehalten. SubjectDNs[1] und LDAP-DNs sind über alle ZDAs einmalig. (Ausnahme: nicht-qualifizierte CRL-Signer-Zertifikate, s. [baek-Certs])

Zertifikate, die abgelaufen sind oder gesperrt wurden, können vom LDAP-Server gelöscht werden. Ein Client kann jedoch nicht davon ausgehen, dass alle im LDAP befindlichen Zertifikate gültig sind. Die Bereinigung des LDAP-Servers von ungültigen Zertifikaten kann in re-

[1] Ausnahme: Die SubjectDNs der AUT-, ENC- und qSIG-Zertifikate desselben eArztausweises müssen gleich sein.

gelmäßigen oder unregelmäßigen Abständen durchgeführt werden; sie liegt im Ermessen des Betreibers. Evtl. gehaltene Signaturzertifikate sollen nicht „bereinigt“ werden

Es gibt über die verschiedenen zugelassenen Zertifizierungsdiensteanbieter hinweg keine zentrale Datenhaltung. Die Adresse des zuständigen Verzeichnisdienstes für die Überprüfung eines Zertifikates (OCSP-Server) ist im entsprechenden Zertifikat und in einer TSL der Bridge-CA der gematik enthalten.

2.3 OCSP-Server

Ein OCSP-Server stellt die „Nachprüfbarkeit“ (s. Begriff im SigG) der Zertifikate sicher. D.h., wenn man das Zertifikat oder relevante Teile davon kennt, kann man seinen Status abfragen. Der Status eines qualifizierten Zertifikates im Kontext der eArztausweise kann lauten:

- „good“: D.h. das Zertifikat ist vorhanden und nicht gesperrt. Als Nachweis dafür muss der OCSP-Responder den Hashwert (Hash-Algorithmus gemäß [extern8] und jeweils aktuellem [externAlgCat][2]) des DER-kodierten Zertifikats liefern.
- „unknown“, D.h. das Zertifikat ist nicht bekannt.
- „revoked at <date and time>“, d.h. das Zertifikat ist bekannt und wurde am Zeitpunkt <date and time> gesperrt.

Es ist ersichtlich, dass der OCSP-Responder keine Informationen über die Gültigkeit eines Zertifikates liefert, sondern nur über deren Status. So antwortet ein OCSP-Responder z.B. mit „good“ für ein abgelaufenes Zertifikat, das vorhanden und nicht gesperrt ist, welches aber zum Zeitpunkt der Anfrage nicht mehr gültig ist. Es ist Aufgabe des Clients die Gültigkeit eines Zertifikates zu einem bestimmten Zeitpunkt auf Grund der Informationen, die er vom Verzeichnisdienst bekommt und des zugrunde liegenden Gültigkeitsmodells zu ermitteln. Dem OCSP-Server „unbekannte“ Zertifikate sind ungültig, auch wenn sie mathematisch gültig sind (wie auch bei den qualifizierten Zertifikaten).

Bei Signaturzertifikaten und Attributzertifikaten muss der OCSP-Responder auf Verlangen und soweit zulässig das Zertifikat liefern. Dies resultiert aus den Anforderungen der noch offenen Spezifikation des eRezeptes (Signaturzertifikat soll nicht im signierten eRezept enthalten sein, nur dessen IssuerDN und Seriennummer). Der Client, der die Signatur eines eRezeptes prüfen möchte, kann aus dem Rezept (nach gegenwärtigem Meinungsstand) nur die Seriennummer des signierenden Zertifikats und seinen Aussteller extrahieren. Diese Informationen sind ausreichend, um eine OCSP-Anfrage zu starten und in einem Arbeitsschritt sowohl das Signaturzertifikat als auch dessen Status zu bekommen. Voraussetzung dafür ist, dass die „statischen“ Root- und CA-Zertifikate dem Client vorliegen.

[2] soweit dies von der Bundesnetzagentur für die qualifizierten Zertifikate gefordert wird

2.4 Struktur des öffentlichen Verzeichnisdienstes aus Sicht des OCSP-Responders

Es existiert kein zentraler OCSP-Responder. Jedes zugelassene Trustcenter betreibt seine eigene OCSP-Responder. Ein Anwender (d.h. eine Applikation) muss das Zertifikat haben, dessen Status er erfahren möchte (Ausnahme: Signatur- und Attributzertifikate). Die Information, welcher OCSP-Responder für das Zertifikat anzufragen sei, ist in der „AuthorityInfoAccess“-Extension im Zertifikat oder ggf. in einer TSL enthalten.

- Zugelassene Zertifizierungsdiensteanbieter müssen Signatur- und Attributzertifikate in der OCSP-Response auf Nachfrage mitliefern können. Für Authentisierungszertifikate ist dies nicht zulässig, für Verschlüsselungszertifikate ist dies optional. Clients müssen solche OCSP-Responses verarbeiten können.
- Es ist zulässig für die Nachprüfbarkeit und ggf. Abrufbarkeit von nicht-qualifizierten Zertifikaten, ein HSM für die Signatur der OCSP-Responses zu verwenden. Das HSM muss mindestens nach CC EAL4 „hoch“ oder FIPS 140-2 Level 3 oder vergleichbar sicherheitsevaluiert sein. Der ZDA ist für die Sicherheit eines HSM-betriebenen OCSP-Servers verantwortlich. Ein nach SigG bestätigtes HSM ist selbstverständlich für sämtliche Zertifikatsklassen zulässig und empfohlen.
- Für die übergreifende Suche nach Signaturzertifikaten und Attributzertifikaten über OCSP ist insbesondere im Umfeld der §291a-Anwendungen folgendes vorgesehen:
    - Die gematik setzt Trusted Service Lists als Teil einer Bridge-CA-Architektur für das Gesundheitswesen. Sie sind auch dafür geeignet, eine Zuordnung zwischen OCSP-Responder und Issuer-Zertifikat herzustellen. Die Clientsoftware kann die aus dem eRezept erhaltene Information des IssuerDN benutzen, um aus der hinterlegten TSL (Trusted Service List) den zugehörigen OCSP-Responder des entsprechenden ZDA zu identifizieren. Mittels der im eRezept enthaltenen (Zertifikats-) Seriennummer wird sodann eine OCSP-Anfrage an den benannten Responder gestellt. Dieser liefert mit der OCSP-Response das zugehörige Zertifikat an den Client.
    - In einem Umfeld außerhalb der Telematik-Infrastruktur kann die TSL der gematik für die Lokalisierung des zuständigen OCSP-Responders eingesetzt werden, oder aber (bei gem. [extern8] obligatorisch vorhandenem Signaturzertifikat in der Signatur) die URL des OCSP-Responders aus der authorityInfoAccess verwendet werden.

Als Gültigkeitsmodell für die qualifizierte Attribut- und Signaturzertifikate gilt das Kettenmodell; für alle nicht-qualifizierte Zertifikate (auch für Authentisierungs- und Verschlüsselungszertifikate) wird das mit der gematik abgesprochene und in der gemeinsame Policy der Leistungsträger beschriebene „Kompromissmodell“ festgelegt (s. [baekValidityModel]). D.h. ein OCSP-Responder muss für ein nicht-gesperrtes bekanntes Zertifikat mit „good“ antworten, auch wenn das CA-Zertifikat inzwischen gesperrt wurde (auch wenn der Sperrgrund möglicherweise „unspecified“ lautet oder nicht ermittelt werden kann).

Der OCSP-Responder muss konform zur Common-PKI Spezifikation v2.0 inkl. SigG-Profil (Part 9). Das SigG-Profil (Part 9) gilt explizit auch für die nicht-qualifizierten Authentisierungs- und Verschlüsselungszertifikate.

Ein Client muss eine OCSP-Anfrage stellen, wenn die Gültigkeit eines Zertifikats zu einem bestimmten Zeitpunkt ermittelt werden soll. Es reicht nicht aus, zu prüfen, ob ein mathematisch gültig signiertes Zertifikat nicht in der CRL aufgeführt ist, weil es sein könnte, dass das Zertifikat „nicht bekannt“ ist (wenn z.B. die zugehörige Chipkarte abgefangen und missbräuchlich genutzt wurde). Dies gilt auch für die Authentisierungs- und Verschlüsselungszertifikate, wenngleich sie bei bekanntem Status auch in einer CRL aufgenommen werden dürfen und müssen. Wurde allerdings einmal der Status eines Zertifikats als „good“ ermittelt, darf für nachfolgende Validierungen eine CRL eingesetzt werden.

2.5 Struktur des öffentlichen Verzeichnisdienstes aus Sicht des LDAP-Servers

Qualifizierte Signaturzertifikate, qualifizierte Attributzertifikate und Authentisierungszertifikate werden nicht in **öffentlichen** LDAP-Servern bereitgestellt. Folgende Gründe sind dafür maßgebend:

- ein signiertes Dokument muss laut Common-PKI-Spezifikation das Signaturzertifikat enthalten; somit besteht kein Verwendungszweck für ein öffentliches Verzeichnis von Signaturzertifikaten. Für den Abruf von Signatur- und ggf. Attributzertifikaten für eRezept-Anwendungen (Zertifikat entgegen der Common-PKI-Spezifikation nicht im Container enthalten) kann ein OCSP-Responder verwendet werden.
- Bei einer Authentisierung wird das Authentisierungszertifikat des Arztes dem authentisierenden Dienst zwingend zugeschickt. Somit besteht kein Verwendungszweck für ein öffentliches Verzeichnis von Authentisierungszertifikaten.
- Das von den Datenschutzgesetzen abgeleitete Gebot der Datensparsamkeit würde verletzt, wenn Daten ohne ersichtlichen Zweck bereitgestellt würden. Der Arzt kann mit dem vorliegenden Modell seine Zertifikate nur den Geschäftpartnern und Patienten bekannt machen, mit denen er (Geschäfts)-beziehungen unterhält.

Das LDAP-Schema soll jedoch grundsätzlich ohne größere Änderungen auf diese Zertifikatsklassen erweiterbar sein. Deshalb werden in diesem Konzept zwei Realisierungsvarianten betrachtet. Variante 1 muss von allen ZDAs realisiert werden und geht davon aus, dass nur Verschlüsselungszertifikate im LDAP bereitgestellt werden. Variante 2 geht davon aus, dass auch Signatur- und/oder Attribut- und/oder Authentisierungszertifikate im LDAP bereitgestellt werden und muss von den ZDAs zunächst nicht umgesetzt werden, sondern kann bei Bedarf in der Zukunft betrachtet werden, wenn geänderte Anforderungen dies erfordern. Textbausteine, die sich auf Variante 2 beziehen, werden als grau unterlegt gekennzeichnet.

Andere Zertifikate technischer Natur müssen in den dezentralen Verzeichnisdiensten der zugelassenen Trustcenter publiziert werden. Solche Zertifikate sind:

- Root-Zertifikate
- CA-Zertifikate
- Cross-Zertifikate (obligatorisch auch in einem eigenen caCertificate-Attribut). Es gibt zwei Arten von Cross-Zertifikaten:
    - Cross-Zertifikate, mit welchen sich 2 Root-Zertifikate der Bundesärztekammer gegenseitig zertifizieren (analog der Cross-Zertifizierung von Root-Zertifikaten der Bundesnetzagentur)
    - Cross-Zertifikate, die (einseitig) qualifizierte CA-Zertifikate der zugelassenen ZDA zertifizieren.
- CRL-Signer-Zertifikate
- OCSP-Signer-Zertifikate
- TSS-Signer-Zertifikate

Sperrlisten (CRLs) müssen ebenso im LDAP eingestellt werden. Es werden ausschließlich indirekte CRLs ausgestellt. Der Speicherort der CRL ist in den Zertifikaten in der „CRL Distribution Point"-Extension enthalten.

Jeder zugelassene Zertifizierungsdiensteanbieter muss alle Root- und Cross-Zertifikate (für die Kettenbildung zwischen BÄK-Root-Zertifikaten) der Bundesärztekammer sowie „seine" CA-, CROSS-, CRL-Signer und OCSP-Zertifikate auch in seinem LDAP-Tree auf die mit diesem Konzept vereinbarten Knoten publizieren.

2.6 Allgemeine Anforderungen an die Struktur des Directory-Tree im LDAP-Server

Der LDAP-DN eines Zertifikates soll dem SubjectDN entsprechen. Alle Knoten (d.h. Country, ggf. Organization, ggf. serialNumber) müssen als Objekte vorhanden sein. CRLs müssen logischerweise im Knoten des CRL-DP untergebracht sein, auch wenn der CRL-Signer inzwischen ausgetauscht wurde.

Der SubjectDN aller Zertifikatsklassen wird im Dokument [baekCerts] der Bundesärztekammer beschrieben.

Für Attributzertifikate wird die entsprechende Spezifikation der Bundesärztekammer verwendet. Es werden Attribut-Zertifikate in der Version 1 ohne eigenes SubjectDN (CHOICE: baseCertificateID) verwendet.

2.7 Zertifikatssuche

Es besteht innerhalb der Telematikinfrastruktur die Anforderung, Zertifikate (resp. auch öffentliche Schlüssel) für eine gerichtete Kommunikation auszuwählen. Es muss demzufolge

eine Möglichkeit bestehen, über mehrere ZDAs hinweg – da ein Arzt auch von mehreren ZDAs aktive eArztausweise besitzen kann – nach Zertifikaten der Ärzte zu suchen und diese für die Verwendung zu downloaden. Die Grundlage für diese Zertifikatssuche soll das LDAP-Protokoll bilden. Als Suchparameter sind mindestens alle ohne Authentifizierung lesbaren Attribute erlaubt und geeignet zu indizieren. Als Response soll das Zertifikat geliefert werden.

3 Einleitung

Dieses Papier spezifiziert einen Verzeichnisdienst, der im Rahmen der Einführung des "elektronischen Arztausweis" implementiert werden soll. Basis ist das "Lastenheft Verzeichnisdienst, Version 0.1.2". Auszüge davon sind in den Kap. 1 und 2 dieses Dokumentes enthalten.

Dieses Lastenheft definiert den Verzeichnisdienst als Menge von 2 Diensten:

- LDAP-Service
- OCSP-Service

Es ist nicht Gegenstand dieses Konzeptes, den OCSP-Service / -Responder zu spezifizieren (s. [baekOCSP]). Jedoch wird eine Möglichkeit dargestellt, wie man OCSP-Responder lokalisieren kann.

Die Zertifikatsstruktur ergibt sich aus dem Papier "Zertifikatsprofile für X.509 Basiszertifikate" [baekCerts].

Es werden auch Aussagen getroffen, wie man per LDAP Zertifikate suchen kann. Hierbei werden 2 Varianten spezifiziert:

Variante 1 beschreibt die Zertifikatssuche unter der Voraussetzung, dass nur die Verschlüsselungs-Zertifikate im Directory veröffentlicht werden. Dies ist gemäß den aktuellen Anforderungen ausreichend. Die Unterstützung dieser Variante 1 ist Pflicht - es sei denn, Variante 2 soll aufgrund geänderter Anforderungen unterstützt werden und die Realisierung ist technisch möglich (Abstimmung mit der BÄK).

Variante 2 beschreibt die Zertifikatssuche unter der Voraussetzung, dass mehrere Zertifikate pro User im Directory veröffentlicht werden. Um hier gezielt suchen zu können, ist die Unterstützung relativ neuer LDAP-Standards nötig, die noch längst nicht alle LDAP-Server-Hersteller implementiert haben. Daher ist diese Variante 2 nicht zwingend umzusetzen.

D.h. ZDA müssen jetzt:

- nur die Verschlüsselungszertifikate im Directory veröffentlichen - dann müssen sie die in Variante 1 beschriebenen Schema-Erweiterungen oder die neuen LDAP-Standards unterstützen

Zukünftig könnte es aufgrund geänderter Anforderungen notwendig werden

- mehrere Zertifikate pro User im Directory zu veröffentlichen - dann müssen sie die neuen LDAP-Standards unterstützen. Eine solche Entscheidung wird nach Abstimmung mit der BÄK getroffen und setzt voraus, dass die technische Realisierung möglich ist.

4 Konventionen

Die Schlüsselwörter MÜSSEN, SOLLTEN, KÖNNEN etc. sind zu interpretieren wie im "Best Current Practise" - Papier der IETF BCP 14 (gleich RFC2119) ([extern6]).

Es gilt also der gleiche Satz, wie er den meisten IETF-RFCs vorangestellt ist:

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", “SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this

document are to be interpreted as described in BCP 14 [RFC2119].

5 OCSP-Service

Es existiert kein zentraler OCSP-Responder. Jedes zugelassene Trustcenter betreibt seine eigene OCSP-Responder.

Die Gültigkeit eines Zertifikates, das man bereits besitzt, per OCSP zu überprüfen ist einfach: Das Zertifikat enthält den zuständigen OCSP-Server in der „AuthorityInfoAccess"-Extension. Im Kontext der Telematik-Infrastruktur müssen Clients die Trusted Service Lists der Bridge-CA der gematik auswerten und den zuständigen OCSP-Responder prioritär aus der TSL extrahieren und anfragen. Dies ist aufgrund der Sicherheitsanforderungen des mit der gematik abgestimmten Gültigkeitsmodells („Kompromissmodell") notwendig.

Alternativ kann folgende Möglichkeit realisiert werden:

Die Ausstellung einer signierten TSL, die von der Root-Instanz der BÄK ausgestellt wurde. Diese enthält ebenso die Zuordnung aller zugelassenen Issuer <---> OCSP-URL, so dass ein Client anhand der Einträge in der Liste weiß, welchen OCSP er für ein bestimmtes Zertifikat anfragen soll. Diese Liste könnte z.B. an einem CA-Eintrag der Root-Instanz abgelegt werden. So kann jeder Client diese Liste per LDAP abrufen.

Vor Implementierung dieses Verfahrens sind noch weitere Abstimmungen mit der BÄK notwendig.

6 LDAP-Service

6.1 Anforderungen

Es bestehen folgende spezielle Anforderungen an den LDAP-Service:

- MUSS: Speicherung von Root-Zertifikaten, CA-Zertifikaten, Cross-Zertifikaten, CRL-Signer-Zertifikaten, OCSP-Signer-Zertifikaten und TSS-Signer-Zertifikaten (Root-und Cross-Zertifikate der BÄK, jeweils „eigene“ relevante CRL-Signer-, OCSP-Signer-, TSS-Signer- und CA-Zertifikate, sowohl qualifiziert als auch nicht-qualifiziert. Die Speicherung von qualifizierten Trustcenter-Zertifikaten ist keine Speicherung im Sinne der Abrufbarkeit nach dem SigG und ist somit nicht bestätigungsrelevant. Clients MÜSSEN (nur bei Bedarf!) die Verzeichnisdienste der BNetzA für das vertrauenswürdige Abrufen und Nachprüfen solcher Zertifikate nach SigG verwenden.
- MUSS: Speicherung des Verschlüsselungs-User-Zertifikates.
- KANN: Es ist möglich, dass pro User mehrere Zertifikate (AUTH, ENC, qSIG) gespeichert werden (nach Abstimmung mit der BÄK).
- MUSS: Speicherung von Attribut-Zertifikaten[3].
- Speicherung von CRLs - MUSS sowohl an den CA-Einträgen als auch an CRL DPs möglich sein.
- Es MUSS möglich sein, nach Zertifikaten anhand Aussteller und Zertifikatsnummer zu suchen.
- Es MUSS möglich sein, nach Zertifikaten anhand Nachname, Vorname und Titel (falls vorhanden) zu suchen.
- Es SOLLTE möglich sein, nur das angeforderte Zertifikat - z.B. das Signaturzertifikat - auszulesen.
- Es SOLLTE möglich sein, nach Zertifikaten anhand der gewünschten KeyUsage (z.B. ENC) zu suchen.

6.2 Grundsätzliches Vorgehen

Diese Spezifikation orientiert sich vorrangig an verabschiedeten Internet-RFCs der Kategorie "Standards Track". Z.T. wird auch auf Internet-Drafts verwiesen - aber auch hier nur auf sol-

[3] Attributzertifikate werden vorerst nicht publiziert, genauso wie Signaturzertifikate. Jedoch muss der LDAP Attributzertifikate (im Knoten des zugehörigen Signaturzertifikates) aufnehmen können, für den Fall, dass sie in der Zukunft benötigt werden. Eine Vorlaufzeit von 6 Monaten für die Aufnahme von Attributzertifikaten im LDAP kann vorausgesetzt werden.

che, die der "Intended Category: Standard Track" angehören und kurz vor der Verabschiedung als RFC stehen.

Darüber hinaus gilt natürlich Common-PKI v2.0 [extern8] als gesetzter Standard.

Es wird auf die neuen Standards (Stand: Ende 2006) gesetzt, die in der LDAP-Welt gelten. Hier kann insbesondere davon ausgegangen werden, dass sie zügig in LDAP-Produkten (Client und Server) umgesetzt werden; speziell wird OpenLDAP das sehr schnell unterstützen.

Speziell sind das - neben der allgemeinen Roadmap der IETF-Working-Group LDAPbis [extern1] - die folgenden Standards:

- RFC3377: LDAP V3 Technical Specification [extern2] (diese beinhaltet insbesondere die Gültigkeit der RFCs RFC2252, RFC2253, RFC2254, RFC2255, RFC2256, RFC2829 und RFC2830)
- RFC4523: LDAP schema definitions for X.509 Certificates [extern3]
- RFC3687: LDAP and X.500 Component Matching Rules [extern4]
- RFC3876: Returning Matched Values with LDAP [extern5]

Als Ausnahme muss hier die Verwendung der Standards für Attribut-Zertifikate gelten: X.509 hat schon seit Jahren das Attribut attributeCertificateAttribute und die Objektklasse pmiUser spezifiziert; der entsprechende LDAP-RFC steht weiter aus (die letzte Veröffentlichung scheint [extern9] aus dem Juni 2002 zu sein). Trotzdem wird in der Praxis fast immer mit den Definitionen dieses Drafts gearbeitet.

Des Weiteren wird als allgemeines Prinzip formuliert, dass die subjectDNs der Zertifikate (User, CAs) gleich den Directory-DNs sein MÜSSEN. Das ermöglicht speziell eine Vereinfachung von Suchen. Auch entspricht es dem allgemeinen Verständnis, dass die subjectDNs die Identität des Objektes (z.B. der Person, der CA, ...) enthalten und damit auch so im Directory abgelegt werden.

6.3 Topologie

Der LDAP-Service wird als verteilter Dienst implementiert - d.h. verschiedene Anbieter, die Zertifikate für den elektronischen Arztausweis ausstellen, MÜSSEN jeweils einen LDAP-Service nach den Vorgaben dieses Papiers betreiben.

Der LDAP-Server eines Anbieters MUSS Referenzen auf alle anderen LDAP-Server im Umfeld "elektronischer Arztausweis" eingetragen haben - sogenannte Referrals (siehe RFC2251

[extern7] - eine Folge von ldap(s)-URLs). D.h. die LDAP-Server müssen bei Anfragen, die sie nicht oder nur teilweise erfüllen können (z.B. "Nachname gleich Meier"), sowohl ihre eigenen Treffer als auch Referrals auf die anderen LDAP-Server zurückgeben.

Clients, die einen LDAP-Server kontaktieren und auf spezielle Suchen (z.B. "Nachname gleich Meier") sowohl Treffer als auch Referrals zurückerhalten, SOLLTEN in der Lage sein, diese Referrals zu verfolgen. (Hinweis: Das wurde nicht als "MÜSSEN" spezifiziert, da u. U. vorausgesetzt werden kann, dass der Client bereits weiß, dass er den richtigen LDAP-Server kontaktiert, und ihn somit die Treffer bei anderen Servern nicht interessieren.)

Clients SOLLTEN damit umgehen können, LDAP-Server, die sie wegen Referrals kontaktieren, möglicherweise nicht erreichen zu können. In diesem Fall sind akzeptable Timeouts (z.B. 5 s) vorzusehen.

LDAP-Server MÜSSEN aus dem Netz der Telematik-Infrastruktur frei erreichbar sein.

LDAP-Server für Verschlüsselungszertifikate DÜRFEN NICHT aus dem Internet erreichbar sein.

Anmerkung: Es muss eine dedizierte (nicht-internet) Zugriffsmöglichkeit für die Kammermitarbeiter geben. Nach erfolgreicher Authentifizierung müssen diese Suchen usw. durchführen können. Ob dieser Zugriff von der Telematik-Infrastruktur oder über andere Kommunikationswege (zusätzliches eigenes VPN) muss anhand der Zugriffsmöglichkeiten der Ärztekammern in der TI realisiert werden und ist daher noch offen.

6.4 LDAP-Protokoll

Zu dieser Spezifikation konforme LDAP-Server und -Clients MÜSSEN:

- LDAP V3 sprechen
- als Zeichensatz UTF-8 verwenden
- multi-valued RDNs unterstützen (d.h. einen RDN mit mehreren Typ-Wert-Paaren)
- alle in RFC2251 spezifizierten Operationen unterstützen
- die Attribute commonName, Nachname, Vorname, Seriennummer und ggf. "persönlicher Titel" am Personeneintrag speichern und so indizieren, dass danach performant gesucht werden kann
- administrative Limits unterstützen, speziell die Begrenzung der Suchmenge auf z. B. 10 Treffer. Dieses Limit muss konfigurierbar sein.

Zu dieser Spezifikation konforme LDAP-Server und -Clients SOLLTEN:

- eine der beiden folgenden Varianten, gezielt nach Zertifikatsinhalten zu suchen, unterstützen:

  - Matching Rules certificateMatch und certificateExactMatch aus [extern3] inkl. der zugehörigen Assertions CertificateAssertion und CertificateExactAssertion - im Minimum sollten die Zertifikats-Felder Issuer, serialNumber und keyUsage durchsuchbar sein.
  - Component Matching [extern4] - im Minimum sollten die Zertifikats-Felder Issuer, serialNumber und keyUsage durchsuchbar sein.
- bei Suchen nach Zertifikaten mit bestimmter KeyUsage nur die darauf passenden Zertifikate anfordern und zurückgeben - d.h. "matchedValuesOnly" ([extern5]) unterstützen

Zu dieser Spezifikation konforme LDAP-Clients MÜSSEN:

- bei Suchen nach Zertifikaten mit bestimmter KeyUsage damit rechnen, dass der Server trotzdem ALLE Zertifikate des passenden Eintrages zurückliefert, und daher dann lokal die Zertifikate parsen und das mit der richtigen KeyUsage auswählen

Hinweis: Im Kapitel 7 - Zertifikatssuche - werden 2 Varianten beschrieben, wie nach Zertifikaten gesucht werden kann:

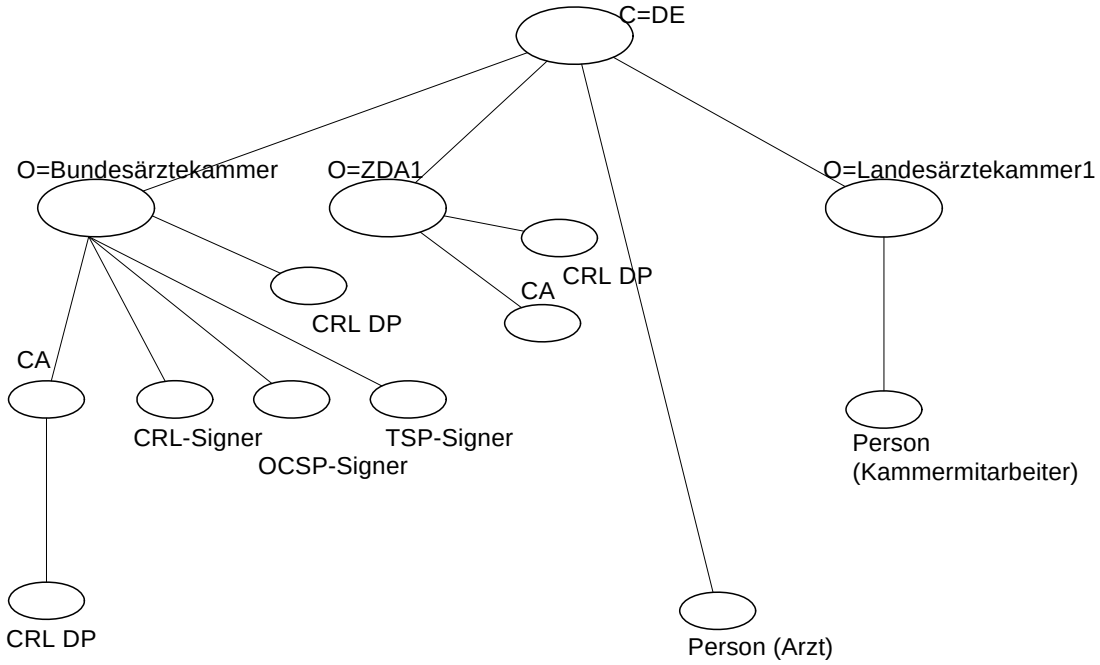
- "klassische" Suche (Suche in speziellen Attributen)
- Suche unter Benutzung der "modernen" Methoden (certificate- oder componentMatching)

Es ist serverseitig ausreichend, eine der beiden Varianten zu implementieren. Wird nur Variante 1 ("klassische Suche") implementiert, ist es nicht notwendig, certificateMatch, componentMatch und matchedValuesOnly zu unterstützen. Clients MÜSSEN beide Varianten unterstützen.

6.5 Struktur des Baums

Folgende DIT-Struktur wird definiert:

Abbildung 6.5-1: DIT



Administrative point ist damit für alle LDAP-Server "c=DE". Das entspricht zwar nicht der hohen Theorie (X.501 etc.), aber da jeder LDAP-Server sowohl CAs als auch Personen speichert und deren DNs erst bei c=DE zusammenlaufen, ist dies notwendig.

6.6 Naming

Personen-Einträge liegen direkt unterhalb c=DE. Sie erhalten mehrere Naming-Attribute ("multiple RDNs") - sowohl um sie eindeutig zu machen als auch um PKI-Client-Software zu unterstützen, die nur die Bestandteile des subjectDN anzeigt. Ein typischer Eintrag sieht wie folgt aus:

cn=Max Mustermann+sn=Mustermann+givenName=Max+title=Prof. Dr.+serialNumber=12345678, c=DE

Es ist wichtig, die Eindeutigkeit von DNs über die verschiedenen Directories zu gewährleisten: Es sollten nicht im Umfeld "elektronischer Arztausweis" mehrere Personen mit gleichem DN (bei verschiedenen ZDAs) existieren. Das führt zu Verwirrung, macht Probleme bei Authentisierungen etc.. Das Zertifikatsprofil macht hier Vorgaben, die eindeutige DNs gewährleisten; (pro ZDA wird ein fester Nummernkreis als Prefix für das serialNumber-Attribut festgelegt, s. [baekConfigData]).

Hinweis: Die serialNumber ist NICHT die Zertifikats-Nummer, sondern eine beliebige Zahl, die NUR dazu dient, den DN eindeutig zu machen.

CAs und Sperrlisten-Verteilpunkte (CRL DPs) werden mit "cn" als namensgebendem Attribut versehen.

6.7 Schema

6.7.1 ObjectIdentifier

Die Bundesärztekammer hat bei der IANA [extern10] eine Enterprise Number [extern11] beantragt [extern12] und erhalten:

```
24796
  Bundesärztekammer
    Georgios Raptis
      georgios.raptis@baek.de
```

Sollten Schema-Erweiterungen notwendig sein (z.B. zur Speicherung von zusätzlichen Attributen), so wird in diesem OID-Branch gearbeitet:

- `1.3.6.1.4.1.24796.4.*`: Attribute
- `1.3.6.1.4.1.24796.6.*`: Objektklassen
- `1.3.6.1.4.1.24796.15.*`: Name Forms

Der Präfix für LDAP-Schreibweisen wird "hpc" heißen.

Beispiel: Das Attribut "eAInhaberID" könnte hinterlegt sein im Attribut hpcEAInhaberID mit dem OID 1.3.6.1.4.1.24796.4.2. Definition s.u., eine Auflistung aller OIDs ist in [baekConfigData] enthalten.

6.7.2 Attribute

Es werden, wenn irgend möglich, die Standard-Attribute verwendet. Speziell:

Eigenschaft	LDAP-Attribut-Typ	Bemerkung	RFC
Benutzer-Zertifikate	userCertificate	In diesem Attribut werden ALLE Benutzer-Zertifikate (AUTH, ENC, qSIG) gespeichert.	2256
Root-Zertifikate	caCertificate		2256
CA-Zertifikate	caCertificate		2256
Cross-Zertifikate	caCertificate	Die Bundesnetzagentur verwendet caCertificate für die Cross-Zertifikate zur Kettenbildung - daher werden hier zur Wahrung der Kompatibilität keine Attribute des Typs crossCertificatePair verwendet.	2256
CRL-Signer-Zertifikate	userCertificate		2256
OCSP-Signer-Zertifikate	userCertificate		2256
TSS-Signer-Zertifikate	userCertificate		2256
Sperrlisten	certificateRevocationList authorityRevocationList	wegen Kompatibilität zur Bundesnetzagentur: keine Verwendung von authorityRevocationList	2256 2256
Attribut-Zertifikate	attributeCertificateAttribute		[extern9]
Nachname	sn		2256
Vorname	givenName		2256
Titel	title		2256
Name	cn		2256
Seriennummer	serialNumber	dient zur Eindeutigmachung des DNs; ist NICHT notwendig gleich der Zertifikats-Seriennummer	2256
Land	c		2256
PLZ	postalCode		2256

Straße	street		2256
Ort	l		2256

Zusätzlich werden folgende HPC-eigene Attribute definiert:

Eigenschaft	LDAP-Attribut-Typ	Bemerkung
Fachrichtung	hpcField	Die Verwendung liegt im Ermessen der Ärztekammer
eA-Inhaber-Identifier	hpcEAInhaberID	enthält die bundesweit einheitliche ID des Inhabers des eArztausweises
Seriennummer des Verschlüsselungszertifikates	hpcEncCertificateSerialNumber	siehe Kapitel 7
Issuer des Verschlüsselungszertifikates	hpcEncCertificateIssuer	siehe Kapitel 7

Bemerkungen:

- Attribut für Titel ("Dr." etc.): RFC2256 sagt:

This attribute contains the title, such as "Vice President", of a person in their organizational context. The "personalTitle" attribute would be used for a person's title independent of their job function.

D.h. eigentlich müsste personalTitle genommen werden. Da aber bestehende Implementierungen, speziell die zu Common-PKI konformen, title benutzen, wird auch hier title vorgegeben - mit dem Bewusstsein, hier semantisch leicht unsauber zu sein.

- X.520 und Common-PKI beschränken die Länge des Attributes cn auf 64 - die LDAP-Standards haben diese Längenbeschränkung nicht mehr. Zu dieser Spezifikation konforme LDAP-Server und -Clients SOLLTEN voraussetzen, dass die Länge aller Attribute inkl. cn beliebig lang sein kann. Es ist nicht Teil dieser Directory-Spezifikation, diese Längenbeschränkung zu diskutieren - ggf. macht hierzu das Zertifikatsprofil Vorgaben.

Formale Definition der HPC-eigenen Attribute:

Fachrichtung: Die Syntax ist DirectoryString.

```
( 1.3.6.1.4.1.24796.4.1 NAME 'hpcField' EQUALITY caseIgnoreMatch
```

```
      SUBSTR caseIgnoreSubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

eAInhaberID: Die Syntax ist PrintableString.

```
( 1.3.6.1.4.1.24796.4.2 NAME 'hpcEAInhaberID' EQUALITY caseIgnoreMatch
      SUBSTR caseIgnoreSubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.44 )
```

Seriennummer des Verschlüsselungszertifikates: Die Syntax ist Integer.

```
( 1.3.6.1.4.1.24796.4.3 NAME 'hpcEncCertificateSerialNumber' EQUALITY integerMatch
      ORDERING integerOrderingMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 )
```

Bemerkung: integerOrderingMatch ist NICHT in den Standard-LDAP-RFCs (speziell RFC2252 [extern16]) definiert, sondern in einem eigenen RFC: RFC3698 [extern13], der auch "Standards Track ist".

Issuer des Verschlüsselungszertifikates: Die Syntax ist DistinguishedName.

```
( 1.3.6.1.4.1.24796.4.4 NAME 'hpcEncCertificateIssuer' EQUALITY distinguishedName-
Match
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

6.7.3 Indizes

Im Minimum MÜSSEN indiziert sein:

- sn: equal, substrings
- givenName: equal, substrings
- title: equal, substrings
- cn: equal, substrings
- objectClass: equal
- l: equal, substrings
- postalCode: equal, substrings

- street: equal, substrings

Es SOLLTEN indiziert sein:

- userCertificate: bzgl. Certificate-Matching Rules oder Component Matching (speziell: wichtige Zertifikatsbestandteile (issuerDN, Zertifikatsnummer, KeyUsage))
- userCertificate: present
- Fachrichtung: equal
- hpcEAInhaberID: equal
- wenn verwendet: Issuer und Seriennummer des Verschlüsselungszertifikates: equal

6.7.4 Objektklassen

Es werden, wenn möglich, Standard-Objektklassen verwendet. Speziell besteht vorerst keine Notwendigkeit, die in ISIS-MTT [extern8] spezifizierte Objektklasse pkiCaData zu verwenden.

Es wird eine Objektklasse definiert, die die HPC-eigenen Attribute enthält:

```
( 1.3.6.1.4.1.24796.6.1 NAME 'hpcPerson' SUP top AUXILIARY MAY ( serialNumber $
hpcField $ hpcEAInhaberID $ hpcEncCertificateSerialNumber $ hpcEncCertificateIssuer
) )
```

Objekt	LDAP-Objektklasse	Bemerkung	RFC
Personen	person organizationalPerson inetOrgPerson pkiUser pmiUser hpcPerson		2256 2256 2798 2587 [extern9] HPC-eigen
CAs	applicationProcess pkiCA		2256 2587
Signer	person pkiUser		2256 2587

CRL DP	crlDistributionPoint		2256
Firmen	organization	o als naming attribute	2256

Bemerkungen:

- Personen:
  - Die Objektklasse pkiUser SOLLTE dann und nur dann verwendet werden, wenn die entsprechende Person mindestens ein Zertifikat hat. Sie ist nicht unbedingt nötig, da auch inetOrgPerson bereits das Attribut userCertificate erlaubt - sie sollte aber verwendet werden, um anzuzeigen, dass ein Zertifikat vorhanden ist. (D.h. eine Suche mit im Filter enthaltenem "objectClass=pkiUser" gibt nur Personen mit Zertifikaten zurück. Natürlich kann das auch mit "userCertificate=*" erreicht werden - doch dazu muss userCertificate speziell ("present") indiziert sein.)
  - Die Attribute cn, sn und givenName MÜSSEN gefüllt sein.
  - Die Attribute l, postalCode und street SOLLTEN gefüllt sein.
  - Um einer Person das Attribut serialNumber geben zu können, ist die Verwendung einer zusätzlichen Objektklasse notwendig - die Standard-Personen-Objektklassen erlauben das nicht. Es wird empfohlen, obige HPC-Objektklasse hpcPerson zu verwenden. Es können aber auch die aus ISIS-MTT bekannte Objektklasse pkiUserData oder die von einigen PKI-Produkten (speziell Entrust) verwendete Objektklasse uniquelyIdentifiedUser [extern14] verwendet werden.
- CAs:
  - Es SOLLTE die Kombination applicationProcess (als structural object class) und pkiCA (als auxiliary object class) verwendet werden.
- CRL-Signer-Zertifikate, OCSP-Signer-Zertifikate und TSS-Signer-Zertifikate werden an speziellen Objekten (objectclass person und pkiUser) im Attribut userCertificate abgelegt - es ist hier also keine spezielle Objektklasse notwendig.
- Sperrlisten KÖNNEN an CA-Einträgen und MÜSSEN an CRL DPs (eingetragen im Zertifikat) abgelegt werden.

6.7.5 Name Forms

LDAP-Server KÖNNEN Name Forms unterstützen. LDAP-Server, die mit Name Forms arbeiten (z.B.X.500-konforme Server), MÜSSEN erlauben:

- cn (Pflicht) und sn, givenName, title und serialNumber (optional) für Personenobjekte (inetOrgPerson)
- cn (Pflicht) für CAs und Signer (applicationProcess)
- cn (Pflicht) für CRL DPs (crlDistributionPoint)
- o (Pflicht) für Firmen (organization)

6.7.6 Content Rules

LDAP-Server KÖNNEN Content Rules unterstützen. LDAP-Server, die mit Content Rules arbeiten (z.B.X.500-konforme Server), MÜSSEN erlauben:

- pkiUser und pmiUser als auxiliary object class für inetOrgPerson
- pkiCA als auxiliary object class für applicationProcess

6.7.7 Structure Rules

LDAP-Server KÖNNEN Structure Rules unterstützen. LDAP-Server, die mit Structure Rules arbeiten (z.B.X.500-konforme Server), MÜSSEN erlauben:

- Land (country) als root-Structure-Rule
- Firma (organization) als Unterknoten von country
- CAs und Signer (beide applicationProcess) als Unterknoten von Firmen
- Personen (inetOrgPerson) als Unterknoten von Country oder Firmen

Das entspricht der im Abschnitt "Struktur des Baumes" dargestellten Baumstruktur.

6.8 LDAP-Read-Only-Server

LDAP-Server KÖNNEN ihren Service (der ja frei im Netz der Telematik-Infrastruktur steht) aus Sicherheitsgründen als Read-Only-Server anbieten. Voraussetzung ist natürlich, dass über diesen Weg keine Schreiboperationen durchgeführt werden sollen.

Ansonsten sei hier nur auf den späteren Abschnitt "Zugriffsrechte" hingewiesen.

6.9 LDAP-Protokoll-Verschlüsselung über SSL/TLS

Zu dieser Spezifikation konforme LDAP-Server MÜSSEN die Möglichkeit anbieten, per "LDAP über SSL/TLS" zuzugreifen. Es ist der Standard-Port 636 zu nutzen.

LDAP-Server KÖNNEN zusätzlich die Möglichkeit anbieten, per start_tls SSL/TLS auf dem Standard-Port 389 zu fahren.

Grund für diese Forderung ist, dass u.U. auch Update-Operationen oder Abfragen geschützter Felder über den Weg über das Intranet kommen können, z.B. das Auslesen von sensiblen Personendaten durch Kammermitarbeiter o.ä.. Da in diesem Falle sich Clients u.U. noch mit "Name/Passwort" authentisieren (siehe Abschnitt "Authentisierungen"), sollten diese Authentisierungsinformationen nicht im Klartext über das Internet gehen.

Außerdem kann dies eine Anforderung von Anwendungen der Telematik-Infrastruktur sein.

Die das SSL-Zertifikat des LDAP-Servers ausstellende CA SOLLTE eine der allgemein vertrauenswürdigen CAs (z.B. aus der Bridge-CA-Liste) sein.

6.10 Authentisierung

LDAP-Server MÜSSEN eine Authentisierung via "Bind with simple credentials" anbieten. D.h. hier wird mit dem DN eines Eintrages und dem in diesem Eintrag hinterlegten Password verbunden.

Eine solche Authentisierung SOLLTE via LDAP-SSL passieren, wenn der Weg vom Client zum Server in der DMZ bleibt; im Falle einer Authentisierung über das Internet MUSS LDAP-SSL benutzt werden.

Über welche Verfahren sich die CAs mit den LDAP-Servern verbinden und authentisieren, ist nicht Gegenstand dieser Spezifikation und obliegt den ZDAs.

LDAP-Server MÜSSEN eine LDAP-SSL-Client-Authentication ermöglichen. Diese Authentisierung MUSS benutzt werden, wenn über das Intranet via LDAP (ohne SSL) für Updates oder für Abfragen zugegriffen wird. Es KANN für diese Fälle auch Name/Password verwendet werden, aber NUR via LDAP-SSL-Verschlüsselung.

Wenn LDAP-SSL-Client-Authentication durchgeführt wird, MÜSSEN die LDAP-Server auf Gültigkeit des präsentierten Client-Zertifikates prüfen, inkl. CRL-Prüfung.

Die Gültigkeitsprüfung muss konform zum verwendeten Gültigkeitsmodell sein, d.h. unter Umständen ist die Prüfung der Gültigkeit des CA-Zertifikats entsprechend zu gestalten oder ganz zu unterlassen.

LDAP-Clients, die für administrative Funktionen verwendet werden (z.B. von Ärztekammermitarbeiter für Suchoperationen mit der eAInhaberID) MÜSSEN in der Lage sein, mit dem

auf der Karte vorhandenen AUTH-Schlüsselpaar eine SSL-Client-Authentication durchzuführen.

6.11 Zugriffsrechte

Grundsätzlich sind die meisten oben aufgeführten Objekte und Attribute frei lesbar. Ausnahmen sind natürlich evtl. vorhandene Password-Felder ~~sowie der "Hash der bundeseinheitlichen Arztnummer eAInhaberID"~~ und ggf. weitere, zu definierende, Attribute.

Die eAInhaberID sowie die Telematik-ID DÜRFEN NICHT im LDAP gespeichert sein. Eine Suche von nicht-öffenltichen Informationen durch Mitarbeiter der Ärztekammern wird über den KammerClient realisiert.

Zugriffsrechte werden anhand von Gruppen (üblicherweise Objektklasse groupOfUniqueNames) administriert. So MÜSSEN autorisierte Kammermitarbeiter einer bestimmten Gruppe – der jeweiligen Landesärztekammer - zugeordnet werden; diese Gruppe hat dann Such-Rechte auf den eAInhaberID der EndEntitäten aus der gleichen Gruppe und DARF NICHT auf eAInhaberID von Mitgliedern anderer Kammerbezirke suchen können. In diesem Kontext muss möglich sein, die Zuordnung eines LDAP-Knotens zur administrativen Gruppe durch den ZDA zu ändern, wenn die Kammerzugehörigkeit eines Arztes geändert wird. Der ZDA kann die hier beschriebenen Zugriffsregeln wahlweise mit anderen Mechanismen durchsetzen (es handelt sich um eine funktionale Anforderung)

Das Attribut eAInhaberID DARF generell NICHT suchbar sein, außer für die o.g. Gruppen von autorisierten Kammermitarbeitern, erst nach Authentisierung.

Jeder Personeneintrag darf durch die zugehörige Person ("self") komplett ausgelesen werden.

6.12 Weiteres zur Sicherheit

ZDAs haben die für den Betrieb von Verzeichnisdiensten und den Schutz von Personendaten üblichen Sicherheitsvorgaben umsetzen, insbesondere:

- Vermeidung von Denial-of-Service-Attacks
- Datenschutzkonzept
- Vermeidung von "Auswertungsläufen"
- Protokollierung (Logfiles)

Speziell müssen hier natürlich die Vorgaben des Bundesdatenschutzgesetzes eingehalten werden. Falls Signaturzertifikate über LDAP angeboten werden sollten (derzeit nicht vorgesehen), dann kann der LDAP-Server als bequeme, „unsichere“ Download-Möglichkeit ange-

sehen werden; ein SigG-konformer Client MUSS ein vom LDAP abgerufenes Zertifikat über OCSP prüfen. Somit kann der LDAP-Server als nicht bestätigungsrelevant betrachtet werden. Die Abrufbarkeit von Signatur- und Attributzertifikaten im Sinne des SigG wird über den OCSP-Responder realisiert.

7 Zertifikatssuchen

Der Verzeichnisdienst wird u.a. zur Suche nach Zertifikaten benutzt. Hierbei ist es insbesondere notwendig, dass Zertifikate anhand von

- Issuer + Seriennummer
- keyUsage

identifiziert werden können.

Die Treffermenge einer Suchabfrage MUSS serverseitig auf einen konfigurierbaren Wert (aktuell: 10) beschränkt werden, um „Rastersuchanfragen“ zu unterbinden.

Im Folgenden werden 2 Varianten beschrieben:

- Variante 1 geht davon aus, dass nur die Verschlüsselungs-Zertifikate im Directory gespeichert werden. Dann können Issuer und Seriennummer in eigenen Attributen abgespeichert werden, und es kann danach "klassisch" gesucht werden.
- Variante 2 geht davon aus, dass mehrere Zertifikate pro User - also in einem Eintrag - gespeichert werden. In diesem Falle müssen die neueren LDAP-Standards bzgl. certificateMatch / componentMatch unterstützt werden.

Zu dieser Spezifikation konforme Server MÜSSEN:

- mindestens die Verschlüsselungszertifikate im Directory speichern
- dort mit Mitteln aus Variante 1 ODER Variante 2 die Zertifikatssuche unterstützen

Zu dieser Spezifikation konforme Server KÖNNEN:

- mehrere Zertifikate pro User (Eintrag) im Directory speichern
- in diesem Falle MÜSSEN sie die neueren LDAP-RFCs (Variante 2) unterstützen

Zu dieser Spezifikation konforme Clients MÜSSEN beide Varianten unterstützen - d.h. wenn eine Suche mit Variante 1 nichts findet, MUSS Variante 2 benutzt werden.

7.1 Variante 1: "klassische" Suche

Sollten LDAP-Server die Standards Certificate-Matching und/oder Component-Matching (noch) nicht unterstützen, muss wie folgt implementiert werden:

- Es wird für Personen NUR das Verschlüsselungszertifikat im Directory abgespeichert.
- Abspeicherung der Seriennummer des Verschlüsselungszertifikates im Attribut hpcEncCertificateSerialNumber

- Abspeicherung des Issuer des Verschlüsselungszertifikates im Attribut hpcEncCertificateIssuer

Damit kann dann leicht das passende Zertifikat gesucht werden, z.B. mit dem LDAP-Filter

(&(hpcEncCertificateSerialNumber=123)(hpcEncCertificateIssuer=cn=ZDA CA für Ärzte 1:PN,o=ZDA,c=DE))

; natürlich müssen beide Attribute indiziert sein, damit die Suchen schnell beantwortet werden.

Hinweis: Es ist möglich, dass LDAP-Server-Produkte nicht certificateMatch / componentMatch, aber matchedValuesOnly unterstützen. Es nützt aber in diesem Falle nicht viel: Es wird ja eh nur ein Wert, eben das Verschlüsselungszertifikat, gespeichert.

7.2 Variante 2: certificateMatch / componentMatch

Hier wird davon ausgegangen, dass LDAP-Clients und -Server das X.509-Zertifikats-Schema (certificateMatch - [extern3]) und/oder den RFC 3687 (componentMatch - [extern4]) unterstützen und so auf Zertifikatsfeldern direkt suchen können.

LDAP-Server, die das unterstützen, können auch mehrere Zertifikate pro Personeneintrag speichern; durch Verwendung obiger Matching Rules kann ja immer der richtige Personeneintrag gefunden werden.

Die Unterstützung von RFC 3876 ("matched values" - [extern5]) ist optional. Wenn LDAP-Server das unterstützen, so zeigen sie das in der Root-DSE an:

```
$ ldapsearch -x -h 127.0.0.1 -b "" -s base 'objectclass=*' +
...
supportedControl: 1.2.826.0.1.3344810.2.3
...
```

Genau dieses Control benutzen Clients auch in Suchen, wenn sie nur passende Werte zurückbekommen wollen - z.B. das ENC-Zertifikat, wenn mit keyUsage=keyEncipherment gesucht wurde.

Wie oben bereits ausgeführt: Clients MÜSSEN damit rechnen dass dieses Control nicht unterstützt wird, und müssen ggf. am Client das passende Zertifikat ausfiltern.

8 LDAP-Issues

8.1 multi-valued RDNs

Wie spezifiziert, werden RDNs mit mehreren Typ-Wert-Paaren benutzt, z.B.:

dn: cn=Jochen Keutel+sn=Keutel+givenName=Jochen+serialNumber=9876543210+title=Dr., c=DE

Heutige Produkte sollten damit keine Probleme haben. Speziell sollte klar sein, dass hier die Matching Rules bzgl. distinguishedNames angewendet werden und nicht etwa ein "String-Compare"; so ist z.B. obiger DN gleich dem Folgenden:

dn: title=Dr.+serialNumber=9876543210+cn=Jochen Keutel+sn=Keutel+givenName=Jochen, c=DE

D.h.: die Reihenfolge der Typ-Wert-Kombinationen in einem RDN ist nicht relevant! (ein RDN ist als SET - nicht als SEQUENCE - von Typ-Wert-Kombinationen definiert.). Für den Aufbau des RDNs **im Zertifikat** gelten jedoch die DER (strikte wohldefinierte Reihenfolge in der ASN.1-Kodierung).

8.2 Aktueller Stand bzgl. certificateMatch / componentMatch

Standardisierung:

- componentMatch: aktueller Standard: RFC3687.
- certificateMatch: aktueller Standard: RFC 4523.
- matchedValuesOnly: aktueller Standard: RFC3876.

OpenLDAP (Stand 2006):

- lt. OpenLDAP-Faq-o-matic werden alle 3 Standards unterstützt. Das ist allerdings wohl nicht ganz korrekt; auf Nachfrage auf der Mailing-Liste openldap-software@openldap.org wurde bestätigt:
  - "Component matching is considered experimental in OpenLDAP Software. As indicated by ITS#4112 and -devel list discussions, it needs work." (K. Zeilenga)

- "Both certificateMatch and certificateExactMatch are implemented (they rely on OpenSSL), though I am not sure the latter fully supports the recently approved standard track assertion syntax (draft-zeilenga-ldap-x509). The test script appears to be using an experimental assertion syntax. The code likely needs some updating." (K. Zeilenga)
- "Looks like certificateMatch needs some work, too." (K. Zeilenga)

- D.h. wenn überhaupt, dann kann certificateMatch benutzt werden; Kurt Zeilenga sagte wenige Tage nach obigen Aussagen auf der Mailing-List ldapext@ietf.org:
  - "I believe this matching rule to be fully implemented as specified in draft-zeilenga-ldap-x509 in at least one implementation. (I note that I am not counting OpenLDAP's implementation as it is flawed in the current release, an issue I am currently working on addressing.)"
- Es ist also davon auszugehen, dass in wenigen Tagen/Wochen das certificateMatch in OpenLDAP voll unterstützt wird - Kurt Zeilenga arbeitet ja gerade daran.
- Derzeit (Stand 2006) unterstützt OpenLDAP noch nicht die in [extern3] definierte Form, die auf den Generic String Encoding Rules (GSER) [extern15] beruht.

Weitere Produkte (Stand 2006):

- Siemens DirX: Nach Auskunft des Herstellers wird derzeit keiner der genannten Standards unterstützt. Das ist insofern enttäuschend, als DirX als X.500-Implementierung gerade bzgl. Zertifikats-Matching-Rules schon weiter sein müsste - es gibt diese Matching Rules in X.509 bereits seit einigen Jahren.
- View500 (http://www.view500.com/) - ein Produkt der australischen Firma eB2Bcom (früher von Adacel; speziell der "Guru" Steven Legg steckt dahinter): Es werden lt. Aussage von Steven Legg auf ldapext@ietf.org alle hier genannten Standards unterstützt.

8.3 Beispiele für LDAP-Suchanfragen

8.3.1 LDAP-Filter zur Suche nach Zertifikaten mittels certificateExactMatch:

alte Form (z.Z. in OpenLDAP verwendet):

```
((userCertificate=1357$o=truetrust ltd,c=gb))
```

Form lt. [extern3] und den dort referenzierten GSER [extern15]:

```
(userCertificate={ serialNumber 1357, issuer "o=truetrust ltd,c=gb" })
```

8.3.2 LDAP-Filter zur Suche nach Zertifikaten anhand keyUsage

```
(userCertificate:certificateMatch:= { keyUsage { keyEncipherment } })
```

8.3.3 LDAP-Filter zur Suche nach anderen Zertifikatsfeldern

Die Assertion, die certificateMatch bestimmt, erlaubt nicht beliebige Suchen nach Zertifikatsfeldern. Z.B. kann nur gesucht werden nach Zertifikaten, die in der Extension subjectAltName ein Feld rfc822Name haben - aber nicht nach Inhalten dieses Feldes. Die Suche nach dem bloßen Vorhandensein geht mit certificateMatch:

```
{ subjectAltName builtinNameForm:rfc822Name }
```

zur Suche nach Inhalten hilft componentMatch:

```
(userCertificate:componentFilterMatch:=item:{
    component "toBeSigned.extensions.*.extnValue.content.(2.5.29.17).*.rfc822Name",
    rule caseIgnoreIA5Match, value "aaa@example.com" })
```

8.4 Beispiele für LDAP-Einträge

8.4.1 Person mit mehreren Zertifikaten

Hier wird vorausgesetzt, dass certificateMatch unterstützt wird - d.h. es ist nicht notwendig, hpcEncCertificateSerialNumber und hpcEncCertificateIssuer zu benutzen:

```
dn: cn=Jochen Keutel+sn=Keutel+givenName=Jochen+serialNumber=9876543210+title=Dr.,
c=DE
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: pkiUser
objectClass: hpcPerson
```

```
cn: Jochen Keutel
displayName: Keutel, Jochen
sn: Keutel
givenName: Jochen
title: Dr.
personalTitle: Dr.
serialNumber: 9876543210
telephoneNumber: +49 30 67819188
mobile: +49 177 6572720
mail: jochen@keutel.de
hpcField: Consulting
hpcEAInhaberID:: ...
userCertificate;binary:: MD1...
userCertificate;binary:: MD2...
```

8.4.2 Person mit einem Zertifikat unter Verwendung der HPC-eigenen Attribute

```
dn: cn=Jochen Keutel+sn=Keutel+givenName=Jochen+serialNumber=9876543210+title=Dr.,
c=DE
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: pkiUser
objectClass: hpcPerson
cn: Jochen Keutel
displayName: Keutel, Jochen
sn: Keutel
givenName: Jochen
title: Dr.
personalTitle: Dr.
serialNumber: 9876543210
telephoneNumber: +49 30 67819188
mobile: +49 177 6572720
mail: jochen@keutel.de
hpcField: Consulting
hpcEAInhaberID:: ...
hpcEncCertificateSerialNumber: 12345
```

```
hpcEncCertificateIssuer: cn=Keutel CA, dc=keutel, dc=de
userCertificate;binary:: MD1...
```

-

9 Referenzen

[baekCerts] Zertifikatsprofile für X.509 Basiszertifikate; Version 2.3.2; 12.05.11

[extern1] Zeilenga: RFC4510, Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, June 2006

[extern2] Hodges, Morgan: RFC3377: Lightweight Directory Access Protocol (v3): Technical Specification: http://www.ietf.org/rfc/rfc3377.txt, September 2002.

[extern3] Zeilenga: RFC4523, Lightweight Directory Access Protocol (LDAP) schema definitions for X.509 Certificates, June 2006

[extern4] Legg: RFC3687: Lightweight Directory Access Protocol (LDAP) and X.500 Component Matching Rules: http://www.ietf.org/rfc/rfc3687.txt, Februar 2004

[extern5] Chadwick, Mullan: RFC3876: Returning Matched Values with the Lightweight Directory Access Protocol version 3 (LDAPv3), September 2004

[extern6] Bradner, RFC2119 / BCP 14: Key words for use in RFCs to Indicate Requirement Levels, März 1997

[extern7] Wahl, Howes, Kille: RFC2251: Lightweight Directory Access Protocol (v3), Dezember 1997

[extern8] Common PKI Specification for Interoperable Applications, T7 & TeleTrusT, Version 2.0, 20.01.2009

[extern9] Chadwick, Legg: Internet X.509 Public Key Infrastructure LDAP Schema and Syntaxes for PMIs <draft-ietf-pkix-ldap-pmi-schema-00.txt>: Expired Draft: http://tools.ietf.org/wg/pkix/draft-ietf-pkix-ldap-pmi-schema/draft-ietf-pkix-ldap-pmi-schema-00.txt, 27. Juni 2002

[extern10] IANA: http://www.iana.org/

[extern11] IANA Enterprise Numbers: http://www.iana.org/assignments/enterprise-numbers

[extern12] Beantragung einer neuen IANA Enterprise Number: http://www.iana.org/cgi-bin/enterprise.pl

[extern13] Zeilenga: RFC3698: Lightweight Directory Access Protocol (LDAP): Additional Matching Rules, Februar 2004

[extern14] Oliva: Entrust Directory Schema Requirements For Entrust 6.0, Mai 2001: http://www.entrust.com/resources/download.cfm/21132/directory_schema_6.pdf

[extern15] Legg: RFC3641: Generic String Encoding Rules (GSER) for ASN.1 Types: http://www.ietf.org/rfc/rfc3641.txt, Oktober 2003

[extern16] Wahl, Coulbeck, Howes, Kille: RFC2252: Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions, Dezember 1997

[externAlgCat] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17.11.2008, veröffentlicht am 27.01.2009 im Bundesanzeiger Nr. 13 S. 346, Bundesnetzagentur. http://www.bundesnetzagentur.de/media/archive/15549.pdf.

[baekValidityModel] Gültigkeitsmodell der elektronischen Arztausweise und Laufzeit der Zertifikate; Version 2.3.1; 29.05.09

[baekOCSP] Funktionale Spezifikation der OCSP Responder für die PKI der eArztausweise; Version 2.3.2; 12.05.11

[baekConfigData] Konfigurationsdaten für die PKI der elektronischen Arztausweise, Version 2.3.4; 12.05.11