Informations
Technik
Zentrum Bund

DVDV
Deutsches
Verwaltungsdiensteverzeichnis

Beschreibung der Zertifikatsinfrastruktur im

Deutschen Verwaltungsdiensteverzeichnis (DVDV)

Version 1.8 | Februar 2019

Das vorliegende Dokument wurde durch die ehemalige Bundesstelle für Informationstechnik (BIT) (seit dem 01.01.2016 ITZBund) erstellt.

Alle Angaben wurden mit größter Sorgfalt recherchiert. Trotzdem können wir für die Richtigkeit keine Gewähr übernehmen. Änderungen vorbehalten.

Diese Informationsschrift ist auch im Internet unter www.dvdv.de verfügbar.

Ansprechpartner:

Koordinierende Stelle DVDV
Informationstechnikzentrum Bund (ITZBund)
E-Mail: dvdv@itzbund.de

Inhaltsverzeichnis

Abbildungs- / Tabellenverzeichnis

1. Einleitung

Das Deutsche Verwaltungsdiensteverzeichnis ist eine E-Govenment-Infrastrukturkomponente die zentral zur Verfügung gestellt wird, um die elektronische Kommunikation (Maschine - Maschine - Kommunikation) zwischen Behörden auf eine effiziente und effektive Art und Weise zu ermöglichen.

Zur Absicherung dieser elektronischen Kommunikation werden Sicherheitsmechanismen wie Verschlüsselung, Authentisierung und elektronische Signatur eingesetzt.

Die Grundlage zur Nutzung dieser Sicherheitsmechanismen sind „elektronische Ausweise“, so genannte Zertifikate.

Dieses Dokument informiert darüber, ob und wenn ja, welche Zertifikate die Verfahrensbeteiligten benötigen. Es liefert Informationen über die zu nutzende Zertifizierungsstelle und Bezugsadressen. Weiterhin liefert es die nötigen Konfigurationsparameter für die einzusetzenden technischen Komponenten.

Es wird Grundverständnis von OSCI-Transport und den Kommunikations-prozessen im Meldewesen vorausgesetzt.[1]

[1] siehe hierzu: OSCI-Transport 1.2 – Entwurfsprinzipien, Sicherheitsziele und –mechanismen – weitere Informationen unter www.osci.de

2. DVDV

Für die elektronische Adressierung der verschiedenen Dienste der Behörden wird ein Verwaltungsdiensteverzeichnis benötigt. In diesem sind die technischen Verbindungsparameter (so auch die Zertifikate) aller Dienste (wie z. B. die elektronische Rückmeldung) der (Melde-)Behörden in Deutschland hinterlegt. Ein solches Diensteverzeichnis steht mit dem Deutschen Verwaltungsdiensteverzeichnis (DVDV) zur Verfügung.

Der Kern des DVDV ist der zentrale DVDV-Bundesmaster[2], der durch das ITZBund bereitgestellt wird. Es stellt das DVDV-Referenzsystem dar. Änderungen erfolgen ausschließlich an diesem zentralen System und werden von dort zu den DVDV-Landesservern[3] repliziert.

Um die Sicherheit dieses Systems zu gewährleisten, sind nur die DVDV-Pflegeclients zum Zugriff zugelassen (lesend und schreibend). Für die Replikation von dem Bundesmaster auf die Landesserver sind lediglich Kommunikationsverbindungen vom Bundesmaster auf die Landesserver zugelassen.

Über den DVDV-Pflegeclient pflegen die zuständigen Stellen Änderungen in das DVDV ein. Für jedes Bundesland ist eine „Pflegende Stelle“ vorgesehen, die die Daten für das jeweilige Bundesland verändern kann. Die Veränderungen der Daten auf dem DVDV-Bundesmaster werden über Replikationsmechanismen an die DVDV-Landesserver automatisiert weitergegeben.

Um die Sicherheit des DVDV-Systems zu gewährleisten, sind das zentrale System und die Pflegeclients nur an das DOI-Netz[4], nicht aber an das Internet angeschlossen.

Die Überprüfung der Gültigkeit von Zertifikaten die in dem Verfahren DVDV eingesetzt werden ist eine Dienstleistung der jeweiligen Zertifizierungsstelle, bei der das Zertifikat angefordert wurde.

Für weitere (Hintergrund-) Informationen zum Aufbau und der Funktionsweise des Deutschen Verwaltungsdiensteverzeichnisses wird auf das Dokument „DVDV Verfahrensbeschreibung“ verwiesen.[5]

[2] In der Vergangenheit wurde der DVDV-Bundesmaster auch Replikationsmaster oder DVDV-Master genannt.
[3] In der Vergangenheit wurde die DVDV-Landesserver auch Produktionsmaster oder DVDV-Landesmaster genannt.
[4] Deutschland-Online Infrastruktur (DOI) – ehemals TESTA
Weitere Informationen:
http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_BIT/Leistungen/IT_Produkte/VerbindungsnetzDOI/verbindungsnetzdoi_node.html
[5] Steht im Internet unter www.dvdv.de zum Download bereit.

3. Verfahrensbeteiligte

Im DVDV-Kontext werden verschiedene Verfahrensbeteiligte unterschieden:

1. „**Behörden“ oder auch „DVDV-Nutzer“** sind zum Beispiel Meldebehörden.

2. **„Provider“** im Sinne von DVDV sind Institutionen, die zur Realisierung von Onlinediensten die notwendigen Infrastruktursysteme betreiben:

   - Ein Provider kann der Betreiber einer oder mehrerer Clearingstellen sein, die die Kommunikation stellvertretend für alle angeschlossenen Meldebehörden übernehmen.

   - Ein Provider kann ein kommunales Rechenzentrum sein, das diese Aufgabe für eine oder einen Teil der bei Ihnen tätigen Meldebehörden übernommen hat.

   - Ein Provider kann der Betreiber eines Intermediäres oder einer anderen OSCI-Infrastrukturkomponenten sein.

3. **„Pflegende Stellen“** Für jedes Bundesland ist eine „Pflegende Stelle“ vorgesehen, die die Daten für das jeweilige Bundesland verändern kann. Die Benennung dieser Stellen erfolgt durch die jeweiligen Melderechtsreferenten.

4. Benötigte Zertifikate im DVDV

Im Folgenden wird beschrieben, welche Verfahrensbeteiligten, in welcher Konstellation, welche Zertifikate für welche OSCI-Infrastrukturkomponente benötigen.

Die benötigten Zertifikate können hier gemäß ihrer Bestimmung in zwei funktionale Gruppen unterteilt werden:

- Die erste Gruppe der Zertifikate wird für die DVDV-Server und Governikus-Server benötigt; sowohl auf dem Bundesmaster als auch auf dem jeweiligen Landesserver (Zertifikate 1 bis 3)

- Die zweite Gruppe der Zertifikate (Zertifikat 4 und 5) wird für den Einsatz des Pflegeclients benötigt.

Die verwendeten DOI Zertifikate sind sowohl zum Signieren als auch zum Verschlüsseln der Nachrichten geeignet (Kombi-Zertifikat). Es können folgende Zertifikatsformate verwendet werden:

- *.cer (DER-kodiert) und / oder

- *.cer (base64).

Zertifikate im Format Base64 werden in die entsprechende DER-Kodierung überführt.

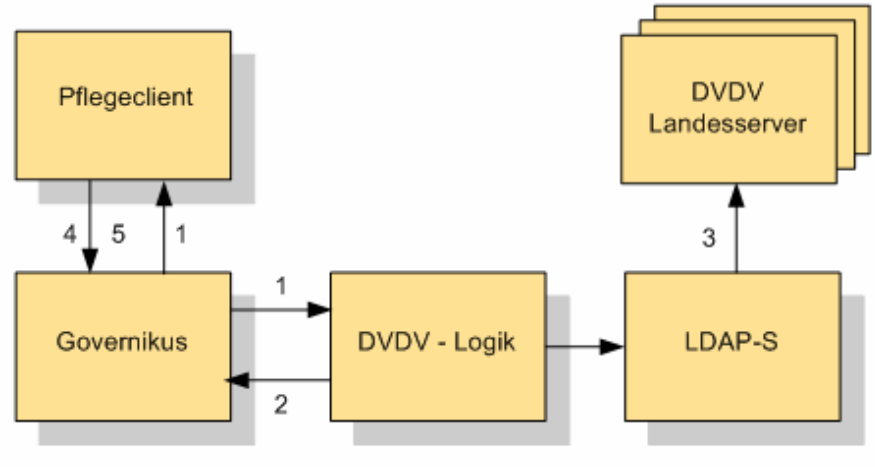

Abbildung 1 Zertifikate DVDV am Beispiel der Zertifikate im ITZBund

1. Für den OSCI-Intermediär Server – in diesem Fall Governikus - wird ein Software-Zertifikat zum Signieren und Verschlüsseln genutzt. Dieses so genannte Intermediär-Zertifikat wird für den Empfang der Daten (OSCI-Rollen Empfänger und Leser) und für das Senden (OSCI-Rollen Autor und Sender) eingesetzt. Dieses Zertifikat müssen Sie beschaffen. Je nach - aus Netzwerksicht betrachteter Erreichbarkeit Ihres Intermediäres - kann es sich hier um ein Zertifikat der DOI-CA handeln, oder aber bei der

Verfügbarkeit Ihres Intermediäres zum Beispiel im Internet kann jede Zertifizierungsstelle gewählt werden, die eine Überprüfung der Zertifikate anbietet.

Was die Namenskonvention für die Beantragung des Zertifikats betrifft, schlagen wir für den einzutragenden Namen im OU Feld folgendes vor:

Rolle und Name: "INTERMED-HE"

→ Als Beispiel für den Namen des Zertifikats für den Intermediär in Hessen. Die offiziellen Kürzel der Bundesländer sind unter Punkt 2 aufgelistet.
Das Zertifikat des Governikus in der BIT hat im OU Feld den Eintrag: "INTERMED-BIT"

Wenn Sie ein solches Zertifikat bei der DOI-CA beantragen möchten, gehen Sie bitte gemäß der Beschreibung im „DOI104 Handbuch Teilnehmer Oeffentliche Verwaltung v20“[6] vor.

2. Für den DVDV-Server wird EIN Zertifikat für die Signatur und zur Verschlüsselung eingesetzt. Dieses Zertifikat dient zum einen der sicheren Kommunikation zwischen dem DVDV Server und dem Governikus-Server bzw. dem Intermediär, als auch zur Kommunikation zwischen den Pflegeclients und dem DVDV-Server. Dieses Zertifikat müssen Sie beschaffen. Je nach - aus Netzwerksicht betrachteter Erreichbarkeit Ihres Intermediärs - kann es sich hier um ein Zertifikat der DOI-CA handeln, oder aber bei Verfügbarkeit im Internet kann jede Zertifizierungsstelle gewählt werden, die eine Überprüfung der Zertifikate anbietet. Was die Namenskonvention betrifft schlagen wir folgendes vor:

Rolle und Name: "DVDV-LS-HE"

→ Als Beispiel für den Namen für das Zertifikat des Applikation-Server (Landes-slave)in Hessen.
Das Zertifikat des Governikus in der BIT hat im OU Feld den Eintrag: "DVDV-AS-BIT"

Kürzel:	
Baden-Württemberg	BW
Freistaat Bayern	BY
Berlin	BE
Brandenburg	BB
Freie Hansestadt Bremen	HB
Freie und Hansestadt Hamburg	HH
Hessen	HE
Mecklenburg-Vorpommern	MV
Niedersachsen	NI
Nordrhein-Westfalen	NW
Rheinland-Pfalz	RP
Saarland	SL
Freistaat Sachsen	SN
Sachsen-Anhalt	ST
Schleswig-Holstein	SH
Freistaat Thüringen	TH

[6] Das Handbuch finden Sie im Internet unter www.dvdv.de im Download-Bereich.

Wenn Sie ein solches Zertifikat bei der DOI-CA beantragen möchten, gehen Sie bitte gemäß der Beschreibung im „DOI104 Handbuch Teilnehmer Oeffentliche Verwaltung v20“ vor.

3. Für den mittels LDAP-S angebotenen Replikationsprozess wird ein weiteres Zertifikat für die SSL-Verschlüsselung benötigt. Bei diesem automatisierten Replikationsprozess werden die Daten aus dem LDAP des DVDV-Bundesmasters beim ITZBund zu den LDAP-Slaves in den Ländern repliziert. Dieses Zertifikat erhalten Sie vom ITZBund. Beantragung unter: dvdv@itzbund.de

4. Die Pflegenden Stellen im DVDV benötigen ein "Authentisierungs-Zertifikat". Mit diesem Smartcard-Zertifikat authentisieren sich die pflegenden Stellen gegenüber dem DVDV-Server. Dieses Zertifikat erhalten Sie bei der DOI-CA. Das Kartenlesegerät für das Smartcard Zertifikat müssen Sie beschaffen. Welche Kartenlesegeräte mit dem von Ihnen verwendeten Intermediär kompatibel sind, erfahren Sie bei den Herstellern der Intermediär-Software. Der öffentliche Schlüssel diese Zertifikats muss an das ITZBund übersendet werden, damit der entsprechende Pflegeclient von einem Mitglied der Root-Gruppe als Pflegende Person in das Berechtigungskonzept eingetragen werden kann.
   Wenn Sie ein solches Zertifikat bei der DOI-CA beantragen möchten, so müssen Sie einen schriftlichen Antrag an das Trust Center der T-Systems senden. Das benötigte Formblatt „TESTA Zertifizierungsantrag DVDV pflegende Stellen“ finden Sie im Internet unter www.dvdv.de im Download-Bereich.

5. Für die Applikation DVDV wird ein weiteres Software-Zertifikat benötigt, welches die Funktion übernimmt, die PIN Eingabe des Smartcard-Zertifikats, welches unter 4 beschrieben ist, zu signieren. Dieses Zertifikat bietet Ihnen rein lesenden Zugriff auf den Datenbestand des DVDV. Für den schreibenden Zugriff auf den Datenbestand im DVDV benötigen Sie das unter 4 beschriebene Zertifikat. Dieses Zertifikat erhalten Sie vom ITZBund.

6. Im Datenbestand des DVDV werden je nach eingerichtetem Dienst Zertifikate hinterlegt. Für den Dienst Meldewesen können und werden dementsprechend "Zertifikate für das Meldewesen" im DVDV hinterlegt. Hierbei handelt es sich z. B. für den Dienst „Meldewesen“ um ein Zertifikat für den Intermediär des Fachverfahren und um ein Zertifikat für das Fachverfahren der jeweiligen Meldebehörde. Diese Zertifikate werden mit der Erstbefüllung (wenn die Daten-erfassung mittels Access Tool der KDO erfolgte) oder mit Hilfe des Pflegeclients im DVDV hinterlegt und können dann abgefragt werden. Sie werden von den Fachverfahren / Clients benötigt, um z. B. eine Rückmeldung durchführen zu können.
   Wenn Sie ein solches Zertifikat bei der DOI-CA beantragen möchten, gehen Sie bitte gemäß der Beschreibung im „DOI104 Handbuch Teilnehmer Oeffentliche Verwaltung v20“ vor.

Für die Zertifikate die für die Kommunikation zwischen Ihrem DVDV-Landesserver und der EWO-Software benötigt werden, wenden Sie sich an Ihren EWO Hersteller.

Für die Verfahrensbeteiligten ‚Behörden’ und ‚Provider’ erfolgt die Zuordnung in Tabellenform.

4.1. Zertifikate für Behörden und Provider

Verfahrens-beteiligte	**Benötigte Zertifikate mit Zuordnung zu den OSCI-Rollen**		
Behörden mit Zuordnung zu	Autor / Sender (Senden), Empfänger / Leser (Empfangen)	Intermediär	Bemerkung
einer Clearingstelle (OSCI-Rollen Autor / Sender, Intermediär, Empfänger / Leser)	-	-	Die Kommunikation zwischen Clearingstelle und Meldebehörde steht nicht im Fokus dieser Betrachtung.
zu einem kommunalen Rechenzentrum oder anderen Dienstleistern (OSCI-Rolle Intermediär)	Ein Zertifikat der DOI-CA, es sei denn ein anderer Dienstleister übernimmt die OSCI-Rollen Autor / Sender, Empfänger / Leser.	-	
zu einem kommunalen Rechenzentrum oder anderen Dienstleistern (OSCI-Rollen Autor / Sender Empfänger / Leser)		Ein Zertifikat der DOI-CA, es sei denn ein anderer Dienstleister übernimmt die OSCI-Rolle Intermediär.	
keinem Dienstleister, sind als Provider zu sehen, wenn sie alle OSCI-Rollen selber betrieben.			

Tabelle 1 Benötigte Zertifikate für Behörden

Verfahrens-beteiligte	**Benötigte Zertifikate mit Zuordnung zu den OSCI-Rollen**		
Provider, die die	Autor / Sender (Senden), Empfänger / Leser (Empfangen)	Intermediär	Bemerkung
OSCI-Rolle Intermediär übernehmen	-	Software-Zertifikat der DOI-CA.	Auch Sekundär-Systeme sind mit Zertifikate auszustatten.
OSCI-Rollen Autor / Sender, Empfänger / Leser übernehmen	Ein Zertifikat der DOI-CA.	-	Auch Sekundär-Systeme sind mit Zertifikate auszustatten. Für OSCI-Infra-struktur-komponenten für

			unterschiedliche Dienste sollten unterschiedliche Zertifikate verwendet werden.
OSCI-Rollen Autor / Sender, Intermediär, Empfänger / Leser (z. B. Clearingstellen) übernehmen	Ein Zertifikat der DOI-CA.	Ein Zertifikat der DOI-CA.	Auch Sekundär-Systeme sind mit Zertifikate auszustatten.

Tabelle 2 Benötigte Zertifikate für Provider

4.2. Zertifikate für den Pflegende Stellen

‚Pflegende Stellen' benötigen für die Arbeit mit dem Pflegeclient ein Zertifikat der DOI-CA (Trägermedium: Smartcard) und Chipkarten-Lesegerät.
Weiterhin wird ein Software-Zertifikat benötigt, um die OSCI-Kommunikation zwischen Pflegeclient und DVDV-Bundesmaster beim ITZBund abzusichern. Das Software-Zertifikat wird vom ITZBund kostenlos zur Verfügung gestellt.

4.3. Zertifikat zur LDAP-Replikation

Die Replikation der Daten vom DVDV-Bundesmaster im ITZBund zu den DVDV-Landessservern erfolgt mittels LDAP über SSL (LDAP-S). Das dafür benötigte Zertifikat wird vom ITZBund kostenlos zur Verfügung gestellt. Jeder DVDV-Landessserver (Slave) ist also im Besitz des Zertifikates. Die Beantragung erfolgt via E-Mail unter: dvdv@itzbund.de

5. Die Zertifizierungsstelle „CA DOI Deutschland“

Ihr Zertifikat für die Anwendung im Meldewesen und den Pflegeclient erhalten Sie von der Zertifizierungsstelle (CA)[7] „CA DOI Deutschland“ (DOI-CA)[8], welche bei T-Systems im Telekom Trust Center betrieben wird und in die „Verwaltungs-PKI“ des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) integriert ist.
Mit der DOI-CA können Zertifikate für Verschlüsselung, Authentifikation und die Erstellung fortgeschrittener Signaturen erstellt werden. Bei den Zertifikaten handelt es sich nicht um Personen- sondern um Gruppenzertifikate, d. h. die Zertifikatsinhaber sind z. B. die einzelnen Meldebehörden, nicht jedoch einzelne Mitarbeiter

5.1. Die Registrierung

Da die DOI-CA von vielen Institutionen genutzt wird, wurde diese gem. eines zweistufigen hierarchischen Domänenkonzeptes in verschiedene Zuständigkeitsbereiche (Master- und Sub-Domänen) unterteilt.

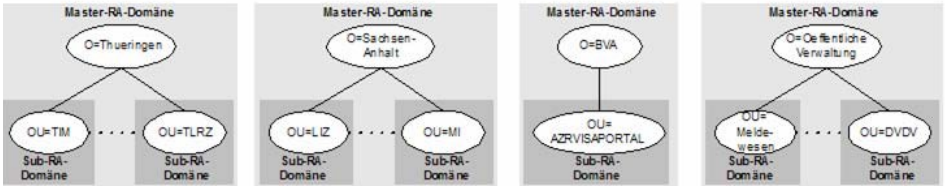

Abbildung 2 Master- und Sub-RA-Domänen der TESTA-CA

In den Ländern, in welchen bereits die DOI-CA genutzt wird, kann die vorhandene Registrierungs-Infrastruktur genutzt werden. Die Softwarezertfikate werden innerhalb der existierenden Domänen über die eingeführten Registrierungsprozesse der Länder ausgegeben. Dies bedeutet, dass die in den Ländern selbst ausgestellten Zertifikate für das Meldewesen den Master-Domänen der Länder, also z. B. O = Brandenburg, O = Sachsen-Anhalt entstammen.
Für die Meldebehörden aus den Ländern, welche die TESTA-CA nicht nutzen, ist eine separate Domäne eingerichtet worden. Die Registrierung wird hierbei durch das Telekom Trust Center durchgeführt. Dies wäre in diesem Fall die Masterdomäne O = Oeffentliche Verwaltung, mit der Sub-Domäne OU = Meldewesen.
Ebenso ist für die pflegenden Stellen eine Sub-Domäne OU = DVDV unterhalb von O = Oeffentliche Verwaltung eingerichtet worden. Auch die Zertifikate auf Smartcards für die pflegenden Stellen werden zentral vom Telekom Trust Center ausgegeben.
An dieser Stelle wird auf das Dokument „DOI104 Handbuch Teilnehmer Oeffentliche Verwaltung v20“[9] hingewiesen.

[7] CA = engl. Abkürzung für Certification Authority.
[8] Die benötigten Zertifikate werden gemäß IMK-Beschluss während der ersten Gültigkeitsdauer nur von der CA DOI Deutschland“ (DOI-CA) ausgestellt.
[9] Dokument steht im Internet unter www.dvdv.de zum Download bereit.

5.2. Konditionen für die Ausstellung der DOI-Zertifikate

Die Ausstellung der Zertifikate erfolgt auf Basis des Rahmenvertrags „TESTA Deutschland“ als Bestandteil des Deutschen Verwaltungsnetzes (DVN). Abhängig von der gewählten Variante zur Ausgabe der Zertifikate gelten folgende Konditionen:

- Bei Ausgabe der Zertifikate über die etablierten Registrierungsinfrastrukturen (Variante 1) fallen nur die entsprechenden Kosten gemäß TESTA-Rahmenvertrag an.

- Bei Ausgabe der Zertifikate über die zentrale Registrierungsstelle im Telekom Trust Center (Variante 2) fallen zusätzlich zu den Zertifikatskosten gemäß TESTA-Rahmenvertrag noch Kosten für die Bearbeitung der Anträge und Support im Telekom Trust Center an, so dass für Zertifikate, die über Variante 2 ausgegeben werden, Kosten von insgesamt 90,- Euro einmalig je Zertifikat mit 36 Monaten Gültigkeit anfallen.

Für die Nutzung der zentralen Registrierungsinfrastruktur hat die T-Systems Enterprise Services GmbH ein Handbuch mit detaillierten Erläuterungen zum Beantragungsprozess erstellt[10]. Zur Beantragung von Zertifikaten gem. dieser Variante gehen Sie bitte wie in dem Handbuch beschrieben vor. Die Web-Seiten zur Beantragung sind mit Benutzerkennung und Passwort geschützt, nutzen Sie bitte die Zugangsdaten, welche Ihnen von Ihrem zuständigen Melderechtsreferenten mitgeteilt wurden.

5.3. Ansprechpartner

Für allgemeine Fragen, Anregungen und Wünsche rund um das DOI-CA und Zertifikate steht Ihnen Frau Fournes bei der Telesec zur Verfügung:

Frau Gabriele Fournes
T-SYSTEMS INTERNATIONAL GMBH
Trust Center Solutions 2 (TCS 2)
E-Mail: Gabriele.Fournes@t-systems.com
E-Mail: tc.notary.leipzig@t-systems.com

5.4. Zentraler Zertifikats-Verzeichnisdienst der Verwaltungen

Zur Gewährleistung der Interoperabilität der verschiedenen CAs in und auch außerhalb der Verwaltungs-PKI wird auf der TESTA-D-Plattform ein zentraler Zertifikatsverzeichnisdienst betrieben.

[10] Steht im Internet unter www.dvdv.de zum Download bereit.

Dieser Zertifikats-Verzeichnisdienst gliedert sich u. a. in

- einen internen Verzeichnisdienst, der nur aus dem TESTA-Netz erreicht werden kann (zentrales Zertifikatsverzeichnis der Verwaltungen, ZZVD),

- einem Veröffentlichungsdienst (VöD), d. h. einer Teilmenge aus dem ZZVD, welche im Internet zur Verfügung gestellt wird.

Sperrlisten (CRL[11]) werden sowohl beim ZZVD als auch beim VöD vorgehalten.

OSCI-Intermediäre, die sich im DOI-Netz befinden, müssen sich die Sperrlisten vom ZZVD-Server laden. Intermediäre, die im Internet verortet sind, müssen für den CRL-Download den VöD-Server adressieren. Die Servicemodule der Intermediäre sind entsprechend zu konfigurieren.

[11] CRL = Abkürzung für Certificate Revocation List, Sperrliste mit Verweisen auf gesperrte Zertifikate von Teilnehmern und CAs

6. Konfiguration des OSCI-Intermediärs

Systemadministratoren, die sich für den Betrieb der Intermediäre verantwortlich zeigen, benötigen folgende Informationen um die Sperrlisten[12] herunterladen und verarbeiten, zu können.

Alle Sperrlisten der DOI-CA können auf folgenden Servern erreicht werden:

- im DOI-Netz: IP `192.168.251.182` oder DNS im DOI-Netz: `pki-directory.testa-de.net` (ZZVD im TESTA-Netz)
- im Internet: `x500.bund.de` (IVBB-Verzeichnis im Internet)
- im Internet: IP `217.237.168.75` (VöD DOI im Internet)

Der Port ist jeweils `389` (Standard LDAP), die Suchbasis entspricht immer den Angaben des CRL-DP (mit Ausnahme des Servernamens `Server]`).

6.1. Sperrlisten DOI-CA:

- `ldap:/"Server"//CN=CA TESTA Deutschland 03, OU=TESTA Deutschland, O=PKI-1-Verwaltung, C=DE?certificateRevocationList`
- `ldap:/"Server"//CN=CA TESTA Deutschland 04, OU=TESTA Deutschland, O=PKI-1-Verwaltung, C=DE?certificateRevocationList`
- `ldap:/"Server"//CN=CA TESTA Deutschland 05, OU=TESTA Deutschland, O=PKI-1-Verwaltung, C=DE?certificateRevocationList`
- `ldap:/"Server"//CN=CA TESTA Deutschland 06, OU=TESTA Deutschland, O=PKI-1-Verwaltung, C=DE?certificateRevocationList`

6.2. Sperrlisten PCA-1-Verwaltung:

- `ldap://"Server"/CN=PCA-1-Verwaltung-02,O=PKI-1-Verwaltung,C=DE?authorityRevocationList`

[12] Sperrliste (Certificate Revocation List - CRL) - Die TESTA-CA als Zertifizierungsstelle führt eine Liste, in der kompromittierte Zertifikate aufgeführt sind, die von ihr selbst ausgestellt wurden. Unter kompromittiert ist z. B. ein Missbrauch des Zertifikats durch seinen Besitzer, ein Verlust der SignaturCard oder ein Ausscheiden des Zertifikatsbesitzers aus einer Dienststelle zu verstehen.

- ldap://"Server"/cn=PCA-1-Verwaltung-03,o=PKI-1-Verwaltung,c=DE?certificateRevocationList

- ldap://"Server"/cn=PCA-1-Verwaltung-04,o=PKI-1-Verwaltung,c=DE?certificateRevocationList

- ldap://"Server"/cn=PCA-1-Verwaltung-05,o=PKI-1-Verwaltung,c=DE?certificateRevocationList