

Zertifizierungs- infrastruktur für die PKI-1-Verwaltung

Verzeichnisdienstkonzept Anhänge

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

Dieses Dokument einschließlich aller Teile ist urheberrechtlich geschützt.
Die unveränderte Weitergabe (Vervielfältigung) des Dokuments ist ausdrücklich
erlaubt.

Jede weitergehende Verwertung außerhalb der engen Grenzen des
Urhebergesetzes ist ohne Zustimmung des Bundesamtes für Sicherheit in der
Informationstechnik unzulässig und strafbar.

© 2002 Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 183, 53175 Bonn

Telefon: 0228/9582-0

-

Telefax: 0228/9582-405

Inhaltsübersicht Anhänge

Änderungshistorie	A-1
Anhang A: Hinweise zu den Spezifikationen	A-1
A.1 Status und Anpassungsmöglichkeiten bei der Implementierung	A-1
A.2 Notationen	A-1
Anhang B: Plattformen und Betriebsumgebung	B-1
B.1 Implementierungsplattformen	B-1
B.2 Fehlerbehandlung	B-1
B.3 Monitoring	B-3
B.4 Inhalt der Log-Dateien	B-3
Anhang C: LDIF-Dateien des Verzeichnisdienstkonzepts	C-1
C.1 Namensregeln für LDIF-Dateien im VDK	C-1
C.2 LDIF-Datei-Header	C-3
C.3 Konventionen für den Inhalt der LDIF-Dateien	C-5
Anhang D: Spezifikation "Aktualisierungsprozess VDV"	D-1
D.1 Periodischer Rahmenprozess Domäne	D-1
D.2 Teilprozess Domäne	D-5
D.3 Periodischer Rahmenprozess VDV	D-26
D.4 Teilprozess Verzeichnisdienst der Verwaltung	D-29
Anhang E: Spezifikation "Aktualisierungsprozess Austauschdienst"	E-1
E.1 Teilprozess Austauschdienst	E-2
Anhang F: Spezifikation "Aktualisierungsprozess Domäne"	F-1
F.1 Abrufender Rahmenprozess Domäne	F-1
F.2 Annahme von Verbindungen der Domänen	F-7
Anhang G: Fragebogen-Antworten der Domänen	G-1

Änderungshistorie

Version	Datum	Status, Änderungen	Autoren
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

Anhang A: Hinweise zu den Spezifikationen

A.1 Status und Anpassungsmöglichkeiten bei der Implementierung

In den folgenden Anhängen sind die im Rahmen des Dokuments getroffenen Entwurfsentscheidungen so weit präzisiert, dass sie als eine Spezifikation für die technische Implementierung dienen können. Sie bildet die grundlegenden Konzepte wie auch die im Editorial Board abgestimmten Detail-Entscheidungen ab. Einzelne kleinere Fragestellungen müssen noch während der Implementierung in Abstimmung mit den Entwicklern festgelegt werden. Sie betreffen beispielsweise die Plattformen, sind abhängig von der Implementierungsstrategie, oder betreffen Fragen der Handhabung und operativen Betriebs.

Während der Erarbeitung der Spezifikation wurden eine Reihe von Implementierungsentscheidungen getroffen, die zum gegenwärtigen Stand des Projekts sinnvoll erschienen. Soweit sich während der Implementierung herausstellt, dass mit anderen Maßnahmen effizienter die gleichen Ziele erreicht werden können, sind Anpassungen möglich. Es ist jedoch zu fordern, dass die Vorgaben der Entwurfsentscheidungen eingehalten, die Flexibilität und Übertragbarkeit der Lösung nicht eingeschränkt und das Sicherheitsniveau erhalten wird (äquivalente Mechanismen). Alle Änderungen müssen in der Spezifikation entsprechend nachgepflegt werden.

A.2 Notationen

Zur Spezifikation werden Tabellen zur Prozessbeschreibung verwendet. Die Abläufe in Prozessen werden wie in der folgende Tabelle beschrieben:

Nr.	Funktionalität und Bedingungen	Verzweigung
...	...	
2	Zeigt Eingabefenster mit Abfrage der <ul style="list-style-type: none"> • Felder: Account, Passwort; und • Buttons: o.k., Abbruch Nach Betätigung eines der Buttons durch den Benutzer	

Nr.	Funktionalität und Bedingungen	Verzweigung
2.1	<ul style="list-style-type: none"> ➤ case: Account = LEER Anzeige der Fehlermeldung "Benutzerkennung erforderlich" und weiter bei #2 	#2
2.2	<ul style="list-style-type: none"> ➤ case: Passwort = LEER Fehlerbehandlung 	Fehlerbehandlung: schwerer Fehler
2.3	<ul style="list-style-type: none"> ➤ case: "Abbruch" Prozess terminiert (ggf. return mit Rückgabewerten) 	terminate
3	...	

Tabelle 9: Beispiel-Schritte aus einer Prozessbeschreibung

Hinweise zur Beschreibungsform:

- Innerhalb des Ablaufs hat jeder Schritt eine eindeutige Nummer, die als Ziel eines Sprunges, Aufrufs oder Returns (von einem aufgerufenen Prozess) genutzt werden kann.
- In jedem **case-Absatz** definiert der "case" die Bedingung, unter der die Anweisungen dieses Absatzes ausgeführt werden. In der Spalte Verzweigung wird kann auf ein "Sprungziel" für dieses Bedingung verwiesen werden. Der Ablauf folgt diesem Sprungziel, wenn die definierte Bedingung den Wert "wahr" annimmt.
- "return" zeigt einen Rücksprung zu einem aufrufenden Ablauf an.
- Im Default-Fall (keiner der case-Fälle trifft zu) wird der Ablauf mit dem nächsten Schritt fortgesetzt. Gewöhnlich ist dies der "good case" oder Standard-Ablauf.
- "terminate" zeigt an, dass der aktuelle Ablauf terminiert. Implikationen und Details der Schritte für eine geordnete Terminierung sind ggf. in Komponenten-Spezifikationen weiter zu konkretisieren.

Anhang B: Plattformen und Betriebsumgebung

B.1 Implementierungsplattformen

Die Aktualisierungsprozesse sind gemäß der Vorgaben von Kapitel 6 und zu den einzelnen Aktualisierungsprozessen plattformübergreifend zu implementieren.

Die Implementierung ist so zu gestalten, dass die Domänen bei Bedarf auf einfache Weise gegebenenfalls erforderliche Anpassungen oder Erweiterungen vornehmen können.

Die Mechanismen zur Erstellung von Log-Dateien und zum Versenden von Meldungen an das Monitoring sind so zu modularisieren, dass eventuell notwendige betriebssystemspezifische Anpassungen an einer Stelle zusammengefasst werden.

B.2 Fehlerbehandlung

Die Fehlerbehandlung der Aktualisierungsprozesse unterscheidet zwischen folgenden Stufen:

Name der Stufe	Kennzeichen	Reaktion
Warnung	Es tritt ein Konsistenzproblem auf, dass vom Prozess-Schritt aber entweder behoben oder ignoriert werden kann. Das Monitoring muss dem Problem nachgehen. Beispiel: ein Attribut-Typ soll nur einmal im DIT-DN enthalten sein, es gibt aber eine Regel, die beim mehrfachen Auftreten eine Auswahl treffen kann.	Folgende Aktionen werden beim Auftreten einer Warnung ausgeführt, sofern nicht ausdrücklich anders spezifiziert: <ul style="list-style-type: none"> • Inkrementieren einer Variablen <code>Warning_Counter := Warning_Counter + 1</code> • Eintrag in Log-File • Meldung an Monitoring am Ende des Prozesses
Fehler	Für die Bearbeitung eines Entry sind zwingende Bedingungen nicht erfüllt. Der Entry kann aber ohne Probleme übersprungen werden	Folgende Aktionen werden beim Auftreten eines Fehlers ausgeführt, sofern nicht ausdrücklich anders spezifiziert: <ul style="list-style-type: none"> • Inkrementieren einer Variablen <code>Setze Error_Counter := Error_Counter + 1</code> • Eintrag in Log-File • Meldung an Monitoring am Ende des Prozesses

Name der Stufe	Kennzeichen	Reaktion
schwerer Fehler	Es bestehen grundsätzliche Probleme, den Prozess auszuführen oder eine Ausführung könnte zu Folgeproblemen für PKI-Anwendungen führen.	Folgende Aktionen werden beim Auftreten eines schweren Fehlers ausgeführt, sofern nicht ausdrücklich anders spezifiziert: <ul style="list-style-type: none"> • Eintrag in Log-File • Es erfolgt eine entsprechende Meldung "Prozessabbruch" an das Monitoring. • alle erforderlichen Schritte zu einem sauberen Abschluss des Prozesses werden ausgeführt, z. B. geöffnete Dateien schließen • Der Prozess wird beendet

Tabelle 10: Fehlerstufen im Aktualisierungsprozess

Alle Fehlermeldungen werden in die Log-Datei des entsprechenden Aktualisierungsprozesses eingetragen (vgl. Abschnitt "Inhalt der Log-Dateien").

Eine zusammenfassende Fehlermeldung über alle aufgetretenen Fehler wird am Ende des jeweiligen Teils des Aktualisierungsprozesses erzeugt, entweder in der Domäne oder beim Betreiber des Verzeichnisdienstes der Verwaltung, Austauschdienstes oder Veröffentlichungsdienstes. Die zusammenfassende Fehlermeldung enthält folgende Informationen:

- Zeit,
- Prozess, Teilprozess,
- maximale Fehlerstufe,
- LDIF-Datei-Name, Anzahl der Fehler und Warnungen im Log-File.
- Bei schweren Fehlern wird die auslösende Ursache ergänzt.

Die zusammenfassende Ergebnismeldung des Prozesses wird an das Monitoring übermittelt, wenn im Prozess eine Warnung, ein Fehler oder ein schwerer Fehler aufgetreten ist. Für die Meldungen an das Monitoring wird ein geeigneter Mechanismus implementiert, von dem erwartet werden kann, dass er auf allen geforderten Plattformen eingesetzt oder leicht angepasst werden kann (siehe auch B.1). Er sollte in Standard-Werkzeuge zur Systemadministration eingebunden werden können, die in den Domänen zu erwarten sind.

B.3 Monitoring

Jede Domäne soll ein Monitoring des Aktualisierungsprozesses realisieren. Jede teilnehmende Domäne und die Betreiber der Dienste des Verzeichnisdienstkonzepts müssen sicherstellen, dass es eine zuständige Monitoring-Gruppe gibt. Für die Monitoring-Gruppe müssen in einem Rollenkonzept Zuständigkeiten und Verantwortlichkeiten festgelegt werden. Mitglieder der Monitoring-Gruppe müssen auf die Fehlermeldungen des Aktualisierungsprozesses reagieren.

Die Domäne und die Betreiber der Dienste des Verzeichnisdienstkonzepts müssen sicherstellen, dass überwacht wird, ob der oder die Rahmenprozesse für die Aktualisierung aktiv sind. Auf Störungen muss gemäß der Vorgaben für die Datenqualität reagiert werden.

B.4 Inhalt der Log-Dateien

In der Log-Datei eines Prozess-Laufs werden folgende Informationen festgehalten:

- Jeder Start und Abschluss eines Prozessabschnitts,
- alle Warnungen und Fehlermeldungen mit Ursache. Warnungen und Fehlermeldungen für Operationen auf Entries enthalten außerdem den DIT-DN des Entries, an dem der Fehler aufgetreten ist.
- die zusammenfassende Schlussmeldung an das Monitoring.

Jeder Eintrag wird mit Datum und Uhrzeit gekennzeichnet.

Es wird eine gesonderte Log-Datei über alle Prozess-Läufe erstellt (Übersichts-Log). In ihr werden für jeden Prozess-Lauf der Prozess-Start und die zusammenfassende Ergebnismeldung des Aktualisierungsprozesses gespeichert (Erfolgsmeldung oder Fehlermeldung im gleichen Wortlaut, wie sie an das Monitoring gemeldet wird).

Anhang C: LDIF-Dateien des Verzeichnisdienstkonzepts

Die LDIF-Dateien müssen so bearbeitet werden, dass sie nach der Ankunft beim Verzeichnisdienst der Verwaltung möglichst direkt verwendet werden können. Außerdem soll auch die Implementierung des Prozessabschnitts zum Einstellen der Entries möglichst einfach gehalten werden. Dazu sollen alle prozessrelevanten Informationen möglichst direkt verfügbar sein. Außerdem sollte der Prozessabschnitt entscheiden, ob ein Entry ergänzt oder geändert werden muss. Diese beiden Kategorien sollen in der LDIF-Datei nicht unterschieden werden. Dagegen müssen Entries mit Lösch-Befehlen eindeutig erkennbar sein.

Die Namensregeln und der Aufbau von LDIF-Dateien, die im Austauschdienst für den Aktualisierungsprozess der Domäne bereitgestellt werden, entsprechen denen, die dem Veröffentlichungsdienst der Verwaltung zugeliefert werden.

C.1 Namensregeln für LDIF-Dateien im VDK

Die Namen der LDIF-Dateien sollen aussagekräftig sein bezüglich der Quelle, des Inhalts und des Erzeugungsdatums. Ein Aufbau der Namen mit festen Längen für die einzelnen Bestandteile erlaubt es, einfache Auswahlmechanismen auf die Dateinamen anzuwenden.

Die folgende Tabelle beschreibt die Namensanteile und deren Format. Das zusammengesetzte Namensformat wird im Anschluss an die Tabelle dargestellt.

Namensanteile	Zweck	Format der Namensanteile
Quelle der Daten		
<ul style="list-style-type: none"> Domäne 	Der Dateiname soll erkennen lassen, aus welcher Domäne die enthaltenen LDIF-Entries stammen. Der Domänenname kann bei Bedarf zu Konsistenzprüfungen bezüglich der Datenquelle herangezogen werden.	[Domänen-Kennzeichen] <ul style="list-style-type: none"> String der Länge 8 wird vom Betreiber des VDV in Abstimmung mit dem Betreiber der Domäne vereinbart.

Namensanteile	Zweck	Format der Namensanteile
<ul style="list-style-type: none"> • einzelner Verzeichnisdienst der Domäne 	Innerhalb einer Domäne können mehrere Verzeichnisdienste betrieben werden, die als Quelle von Daten für den Aktualisierungsprozess dienen. Die Namen der Dateien unterschiedlicher Verzeichnisdienste müssen zu unterscheiden sein.	[VD-Kennzeichen] <ul style="list-style-type: none"> • String der Länge 5 • wird vom Betreiber der Domäne intern
Inhalt		
<ul style="list-style-type: none"> • Typ der Entries 	dient zur Unterscheidung zwischen Dateien mit Entries von CAs bzw. CDPs und Dateien mit Entries von Teilnehmern. Dieser Parameter überschneidet sich mit teilweise mit Abk_Teilbaum, verbessert aber die Unterscheidung.	[TypKennzeichen] aus "CA" "EE" <ul style="list-style-type: none"> • CA steht für alle CA- und CDP-Entries • EE steht für End-Entity-Entries • Wird vom Aktualisierungsprozess gemäß Konfiguration / Aufruf festgelegt
<ul style="list-style-type: none"> • Abk_Teilbaum 	ein Kürzel, dass zur Unterscheidung dient , falls die Domäne verschiedene Teilbäume durch jeweils unabhängige Prozesse aktualisieren will (z. B. aus Gründen des Aufbaus des Verzeichnisdienstes der Domäne oder zur Aufteilung in Teilbäume zur Lastverteilung kann es sinnvoll sein, den Aktualisierungsprozess per Teilbaum durchzuführen).	[Teilbaum] <ul style="list-style-type: none"> • String der Länge 5 • Wird vom Betreiber der Domäne intern festgelegt
<ul style="list-style-type: none"> • Datenumfang 	kennzeichnet, ob die Daten für einen Vollabgleich oder nur die Differenz seit dem letzten Lauf enthalten ist.	[Datenumfang] <ul style="list-style-type: none"> • String der Länge 4 • Wertebereich: aus "voll" "diff" • wird vom Aktualisierungsprozess abhängig vom Modus gesetzt
<ul style="list-style-type: none"> • Bearbeitungsstatus der LDIF-Entries 	Unterscheidet verschiedene Dateien eines Prozesslaufs, je nachdem welcher Bearbeitungsschritt abgeschlossen wurde.	[Bearbeitungsstatus] <ul style="list-style-type: none"> • Format: String der Länge 7 Wertebereich aus: <ul style="list-style-type: none"> • "initial": Abschluss der Dateiinitialisierung, • "retrRes": Abfrage der Werte aus dem lokalen Directory beendet (retrieval result), • "convtd": Umsetzung der Werte abgeschlossen (converted), • "genDeIS" bei Vollabgleich generiertes File mit Löschbefehlen (generated deletion für Subtree) • "genDeIA": bei Vollabgleich generiertes File mit Löschbefehlen (generated deletion für gesamten Austausch-DIT) Die Kennzeichen werden vom Aktualisierungsprozess im Prozessverlauf gesetzt
Erzeugungszeit		
<ul style="list-style-type: none"> • Datum und Zeit 	gibt den Zeitpunkt des Prozessstarts an. Dabei ist die Uhr des Verzeichnisdienstes der Domäne ausschlaggebend	[Erzeugungszeit] <ul style="list-style-type: none"> • Format: String der Länge 15 mit dem Aufbau JJJJMMTT-hhmmss • Zeitangabe auf Sekundengenauigkeit, Wert wird aus Zeitsynchronisation mit Verzeichnisdienst der Domäne entnommen. Wird vom Aktualisierungsprozess zu Beginn des Prozesslaufs festgestellt und nicht mehr geändert

Tabelle 11: Namensteile für Namen von LDIF-Dateien

Der Dateiname einer LDIF-Transfer-Datei ist so zu wählen, dass einfache Auswahl-Mechanismen für den Rück-Import in die Domänen möglich sind. Die Länge der Namensteile wird deshalb festgelegt, um mit der Wildcard "?" bereits auf den Dateinamen effizient filtern zu können. Als Haupt-Unterscheidungsmerkmal ist die Domäne und der Typ der Entries (CA / EE) relevant. Der Aufbau ergibt sich dann wie folgt:

- "[Domänen-Kennzeichen]-[TypKennzeichen]-[VD-Kennzeichen]-[Teilbaum]-[Erzeugungszeit]-[Datenumfang]-[Bearbeitungsstatus].LDIF"
- **Summe der Länge: 57 Zeichen** (mit .LDIF)

Dateinamen dürfen nur kleine Buchstaben, Zahlen, "-" (minus) und "_" (Underscore) enthalten. Weitere Sonderzeichen, Umlaute oder Blanks sind nicht zulässig. Namensbestandteile, die fehlen oder kürzer als die Vorgabe sind, werden mit "_" (Underscore) aufgefüllt.

Zu jedem Prozess-Lauf wird eine Log-Datei erzeugt. Der Name der Log-Datei wird mit Ausnahme der Datei-Extension genauso gebildet wie der Name der LDIF-Datei. Die Datei-Extension lautet .LOG.

C.2 LDIF-Datei-Header

Jede LDIF-Datei des Verzeichnisdienstkonzepts beginnt mit spezifischen Header-Informationen, die die Status- und Konsistenz-Prüfungen erleichtern. Die einzelnen Zeilen werden als Kommentar eingetragen, um die Kompatibilität mit Standard-LDIF-Dateien zu erhalten. Es werden die Header-Informationen eingetragen, die in der folgenden Tabelle aufgeführt sind. Die Formate entsprechen denen der Namensteile des Dateinamens, soweit keine anderen Regeln angegeben sind.

Header-Information	Zweck, Format, Werte	Beispiel
Version	Unterscheidung von LDIF-Dateien des Verzeichnisdienstkonzept in verschiedenen Ausbaustufen. festgelegter Wert der Ausbaustufe 1: "LDIF_for_VDV.01"	Version:LDIF_for_VDV.01
Domäne	wie bei Dateiname	Domäne:Bayern

Header-Information	Zweck, Format, Werte	Beispiel
VD-Kennzeichen	wie bei Dateiname	VD-Kennzeichen:Polizei
Typkennzeichen	wie bei Dateiname	Typkennzeichen:CA
Teilbaum	Angabe des Teilbaums (des Wurzelknotens), aus dem alle Entries der LDIF-Datei stammen. Format: DIT-DN, String variabler Länge, Wird aus dem Konfigurationsfile aus "DN_SelectedSubTree" übernommen	Teilbaum:ou=Freistaat Bayern, o=PKI-1-Verwaltung, c=de
Datenumfang	wie bei Dateiname	Datenumfang:diff
Bearbeitungsstatus	wie bei Dateiname	Bearbeitungsstatus:ValConv
Erzeugungszeit	[Erzeugungszeit], Wert wird aus Zeit-synchronisation mit Verzeichnisdienst der Domäne entnommen. Hinweis: Im Rahmen der Implementierung kann eine Anpassung an das technische Format erfolgen, dass auf allen Plattformen am einfachsten nutzbar ist.	Erzeugungszeit:20021103-234358 {für 3.11. 2002, 23:47:58 Uhr)
EE_A-DIT-DN-root	DN, Ziel-Teilbaum im A-DIT für Teilnehmer-Entries, wie in Tabelle 15, leer, falls keine Teilnehmer-Entries. Wird zur Konsistenzprüfung beim Eingang im VDV verwendet	EE_A-DIT-DN-root:o=Bayern,c=DE
Dir_Constraints	Kennzeichnung für Windows 2000 Quellen, wie in Tabelle 15, wird zur Konsistenzprüfung beim Eingang im VDV verwendet	Dir_Constraints:W2K
CA_Subject_DN_root	DN, Ziel-Teilbaum im A-DIT für CA-Entries (bei Windows 2000 Quellen), wie in Tabelle 15, leer, falls Teilnehmer-Entries. wird zur Konsistenzprüfung beim Eingang im VDV verwendet	CA_Subject_DN_root:ou=Freistaat Bayern,o=PKI-1-Verwaltung,c=DE

Tabelle 12: Kennzeichen in LDIF-Datei-Headern des Verzeichnisdienstkonzepts

```
...
#Domäne:Bayern
#VD-Kennzeichen:Polizei
#Typkennzeichen:CA
#Teilbaum:ou=Freistaat Bayern,o=PKI-1-Verwaltung,c=de
#Datenumfang:diff
#Bearbeitungsstatus:convtd
#Erzeugungszeit:20021103-234358
#Dir_Constraints:W2K
#CA_Subject_DN_root:ou=Freistaat Bayern,o=PKI-1-Verwaltung,c=DE
..
```

Abbildung 17: Beispiel für den Datei-Header in einer LDIF-Datei

Die Reihenfolge der Kennungen wird nicht festgelegt

Implementierungshinweis:

Die Werte der einzelnen Parameter im Datei-Header können Umlaute und andere Sonderzeichen enthalten. Da ein plattformübergreifender Transfer notwendig ist, muss die Implementierung sicherstellen, dass diese Sonderzeichen auf alle Plattformen korrekt zur Verfügung stehen und verarbeitet werden können. Eine mögliche Realisierung besteht darin, den Datei-Header als einen "Pseudo-Entry" zu implementieren. Dadurch kann die u.U. lokal verfügbare UTF-8 Unterstützung verwendet werden.

C.3 Konventionen für den Inhalt der LDIF-Dateien

Für die Ausbaustufe 1 ist der Wurzelknoten der jeweiligen Domäne (betrifft nur die oberste Ebene der Domänen: "o=") nicht in der LDIF-Datei enthalten, die an den Verzeichnisdienst der Verwaltung übertragen wird. Dies bedeutet, dass der jeweilige Wurzelknoten für den CA-Subtree und Teilnehmer-Subtree im VDV beim Beitritt einer Domäne zu den Diensten des VDKs manuell eingerichtet werden muss.

Die Domänen verwenden zur Pflege ihrer lokalen Ausschnitte aus dem Austausch-DIT die gleichen LDIF-Dateien (vgl. unten "Aktualisierungsprozess Domäne"). Domänen, die einen zusätzlichen Teilbaum (o=) aus dem Austausch-DIT vom Austauschdienst importieren wollen, müssen den Wurzelknoten dieses Teilbaums deshalb ebenfalls manuell einrichten.

Alle Entries in der LDIF-Datei, die zum Verzeichnisdienst der Verwaltung neu hinzugefügt oder geändert werden müssen, erhalten als Kommando "changetype:add". Der Changetype "modify" wird gegebenenfalls vom Aktualisierungsprozess bei der Umsetzung von Werten ergänzt oder angepasst.

Konsistent mit den Regeln für die Löschung von Entries darf der "changetype:delete" in LDIF-Dateien nur für Teilnehmer-Entries enthalten sein. Auf der Seite des Verzeichnisdienst der Verwaltung wird dies geprüft.

Anhang D: Spezifikation "Aktualisierungsprozess VDV"

In diesem Anhang werden die Konfigurationsparameter und Prozess-Schritte des Aktualisierungsprozesses von der Domäne zum Verzeichnisdienst der Verwaltung (VDV) spezifiziert. Er zerfällt in folgende Prozessabschnitte

- periodischer Rahmenprozess in der Domäne,
- Teilprozess Domäne,
- Periodischer Rahmenprozess VDV und
- Teilprozess Verzeichnisdienst der Verwaltung.

Auf die Spezifikation des "Teilprozess Verzeichnisdienst der Verwaltung" wird in der Spezifikation des Aktualisierungsprozesses vom Austauschdienst zur Domäne zurückgegriffen.

D.1 Periodischer Rahmenprozess Domäne

Der Rahmenprozess der Domäne wird nur in seinen allgemeinen Abläufen spezifiziert. Realisierungsdetails und eine differenzierte Berücksichtigung weiterer Fehlerfälle bleibt der Feinspezifikation bzw. Implementierung vorbehalten.

Die Fehlerbehandlung und das Monitoring erfolgen gemäß der Entwurfsentscheidungen. Die Domäne muss dafür Sorge tragen, dass die entsprechenden Rollen durch Personal besetzt sind. Die Sicherheitsanforderungen müssen umgesetzt sein, d.h., dass der Teilprozess in einem Bereich konfiguriert und betrieben wird, auf den Unberechtigte keinen Zugriff haben.

D.1.1 Vorbedingungen

Für den Rahmenprozess müssen folgende Vorbedingungen erfüllt sein:

- Zugriff auf die Konfigurationsdatei für den Rahmenprozess

- Zugriff auf die Systemzeit des Servers, auf dem der Rahmenprozess läuft (Systemtime)

D.1.2 Invariante

Während der Rahmenprozess der Domäne aktiv ist, gilt folgende Invariante:

- Der Teilprozess der Domäne wird alle "restartAfterMinutes" gestartet.
- Wenn "nextFullUpdate" erreicht wurde und "DayTimeOfFullUpdate" erfüllt ist, dann wird der Teilprozess der Domäne im Modus "Full" gestartet.
- Wenn ein Start des Teilprozesses der Domäne erfolgen soll, der Teilprozess aber bereits aktiv ist oder der Startzeitpunkt nicht in dem für den Modus "voll" zulässigen Zeitraum liegt, wird der Start verzögert. Werden Obergrenzen der Verzögerung überschritten, erfolgt eine Meldung an das Monitoring.
- Wenn ein Start des Teilprozesses der Domäne erfolgen soll, aber nicht möglich ist, erfolgt eine Fehlermeldung an das Monitoring.

D.1.3 Aufruf des Rahmenprozesses

Der Prozess wird manuell oder beim Hochfahren des Systems automatisch gestartet.

D.1.4 Konfigurationsparameter

Name	Format	Zweck	Default / Beispiel / Bemerkung
restartAfterMinutes	numerisch	legt die Periode fest, nach der der nächste automatische Start des Aktualisierungsprozesses in der Domäne mit "diff" durchgeführt wird	restartAfterMinutes=30 führt zu einem Prozess-Lauf je halber Stunde. Der Wert darf nicht größer als 1440 (1 Tag) sein, um die geforderte Servicequalität sicherzustellen.
restartFullUpdateAfterDays	numerisch	legt die Periode fest, nach der der nächste automatische Start des Aktualisierungsprozesses in der Domäne mit "voll" durchgeführt wird	restartFullUpdateAfterDays = 31 führt zu einem Vollabgleich etwa alle 31 Tage
DayTimeOfFullUpdate • not_before • not_after	Feld mit 2 Tageszeiten	legt fest, zu welcher Tageszeit der Vollupdate durchgeführt werden soll	DayTimeOfFullUpdate = {not_before=18:00; not_after=5:00}

Name	Format	Zweck	Default / Beispiel / Bemerkung
nextFullUpdate	Datum-Zeit	legt den nächsten Startzeitpunkt für einen Vollabgleich fest. Wird nach Vollabgleich anhand von restartFullUpdateAfterDays und DayTimeOfFullUpdate.not_before bestimmt	2002.09.07-18:00:00
Log- und Monitoring-parameter	wie erforderlich	legen fest, wie Meldungen an das Monitoring übertragen werden, z.B. eine E-Mail-Adresse, das Verzeichnis, in dem die Prozessspezifischen und die Gesamt-Log-Datei zu speichern sind, die Anzahl der Prozess-Log-Dateien und die Anzahl der Einträge im Gesamt-Log.	Implementierungsabhängig, die Parameter können vom Rahmenprozess und vom Teilprozess in der Domäne gemeinsam genutzt werden

Tabelle 13: Konfigurationsparameter des Rahmenprozesses in der Domäne zur Steuerung der lokalen Teilprozesse zur Aktualisierung des VDV.

D.1.5 Prozess-Schritte

Hinweise zur Implementierung:

- In der folgenden Spezifikation wird angenommen, dass jedem Teilprozess der Domäne "TP_D_updates_VDV" genau ein Rahmenprozess zugeordnet ist und sich die Zuordnung aus dem Kontext der Installation ergibt. Wenn dies nicht der Fall ist, sind die entsprechenden Konfigurationsparameter zu ergänzen.
- Der Prozess muss sicherstellen, dass ein Vollabgleich nur in dem Zeitabschnitt des Tages läuft, der durch DayTimeOfFullUpdate.not_before und DayTimeOfFullUpdate.not_after konfiguriert ist. Dazu wird intern bei Bedarf ein spezifischer neuer Startzeitpunkt berechnet (next_trial), der innerhalb der nächsten 24 Stunden liegt. Ab einer Verzögerung von 24 Stunden wird das Monitoring informiert.
- Falls der aufzurufende Teilprozess TP_D_updates_VDV bereits aktiv ist, wird der nächste Versuch nach 30 Minuten gestartet. Ab einer Verzögerung von mehr als 60 Minuten (3 Versuch nicht erfolgreich) wird das Monitoring informiert. Dazu muss "delayBecauseActive" als persistenter Parameter realisiert werden.

- Der Parameter "nextFullUpdate" wird nicht in diesem Rahmenprozess, sondern nach erfolgreichem Abschluss des Teilprozesses der Domäne (unten) aktualisiert.

Nr.	Funktionalität und Bedingungen	Verzweigung
1	(Prozess wurde aufgerufen und alle Konfigurationsparameter sind gesetzt)	
2	<ul style="list-style-type: none"> • (delayBecauseActive ist persistent oder einzulesen) • setze next_trial := 0 • Teste, ob der zugeordnete Teilprozess TP_D_updates_VDV bereits aktiv ist. 	
2.1	<ul style="list-style-type: none"> ➤ case: Ist bereits aktiv: setze delayBecauseActive := delayBecauseActive := +30 schreibe Meldung mit delayBecauseActive in Übersichts-Log setze next_trial := Systemtime +30 min weiter bei #7 	weiter bei #7
3	Überprüfe, ob Vollabgleich anzustoßen ist.	
3.1	<ul style="list-style-type: none"> ➤ case: Systemtime < nextFullUpdate: (kein Vollabgleich) weiter bei #6 	#6
3.2	<ul style="list-style-type: none"> ➤ case: Systemtime >= nextFullUpdate UND Stunde+Minute von Systemtime liegt in (DayTimeOfFullUpdate.not_before, DayTimeOfFullUpdate.not_after): dann weiter bei #4 (Vollabgleich anstoßen) 	#4
3.3	<ul style="list-style-type: none"> ➤ case: Systemtime >= nextFullUpdate UND Stunde+Minute von Systemtime liegt nicht in (DayTimeOfFullUpdate.not_before, DayTimeOfFullUpdate.not_after): dann weiter bei #5 (Vollabgleich verzögern) 	#5
4	(Vollabgleich anstoßen)	
	<ul style="list-style-type: none"> • delayBecauseActive := 0 • Aufruf von TP_D_updates_VDV (Konfigurationsdatei, Scope ist "voll", "automatisch") 	
4.1	<ul style="list-style-type: none"> ➤ case: Aufruf nicht erfolgreich melde schweren Fehler an Monitoring (qualifizierte Meldung mit Prozesskennung) schreibe qualifizierte Meldung in Übersichts-Log Bestimme next_trial := Sytemtime + 30 weiter bei #7 	weiter bei #7
4.2	<ul style="list-style-type: none"> ➤ case: Aufruf erfolgreich weiter bei #8 	#8
5	(Vollabgleich ist erforderlich, aber Systemzeit nicht im zulässigen Zeit-Slot, daher verschieben. ggf. Hinweis an Monitoring, nächsten möglichen Zeitpunkt bestimmen und Differenzabgleich anstoßen)	
	<ul style="list-style-type: none"> • bestimme next_trial := nächstes mögliches DayTimeOfFullUpdate.not_before 	
6	(Differenzabgleich anstoßen)	
	<ul style="list-style-type: none"> • delayBecauseActive := 0 • Aufruf von TP_D_updates_VDV (Konfigurationsdatei, Scope ist "diff", "automatisch") 	

Nr.	Funktionalität und Bedingungen	Verzweigung
6.1	<ul style="list-style-type: none"> ➤ case: Aufruf nicht erfolgreich melde schweren Fehler an Monitoring (qualifizierte Meldung mit Prozesskennung) schreibe qualifizierte Meldung in Übersichts-Log Bestimme next_trial := Sytemtime + 30 weiter bei #7 	weiter bei #7
6.2	<ul style="list-style-type: none"> ➤ case: Aufruf erfolgreich weiter bei #8 	#8
7	(nach mehr als einer Stunde Verzögerung Meldung an Monitoring)	
7.1	<ul style="list-style-type: none"> • Überprüfe delayBecauseActive und Verzögerung des Vollabgleichs ➤ case: delayBecauseActive > 60: melde schweren Fehler an Monitoring (qualifizierte Meldung mit Prozesskennung) schreibe qualifizierte Meldung in Übersichts-Log weiter mit nächstem case 	weiter mit nächstem case
7.2	<ul style="list-style-type: none"> ➤ case: Systemtime >= Systemtime + 24h melde schweren Fehler an Monitoring (qualifizierte Meldung mit Prozesskennung) schreibe qualifizierte Meldung in Übersichts-Log weiter mit nächstem Schritt 	weiter mit nächstem Schritt
8	(Neustart sicherstellen: früherer Zeitpunkt aus next_trial und restart-Konfiguration) <ul style="list-style-type: none"> • (delayBecauseActive ist persistent oder zu schreiben) • bestimme next_trial := min ((next_trial), (Systemtime + restartAfter-Minutes)) • Veranlasse den Neustart des Prozesses zum Zeitpunkt next_trial 	weiter mit #1
8.1	<ul style="list-style-type: none"> ➤ case: Neustart konnte nicht erfolgreich veranlasst werden: melde schweren Fehler an Monitoring (qualifizierte Meldung mit Prozesskennung) schreibe qualifizierte Meldung in Übersichts-Log Abbruch des Prozesses. 	schwerer Fehler

Tabelle 14: Prozessschritte aus dem Rahmenprozess der Domäne für die Aktualisierung des VDV

D.2 Teilprozess Domäne

Der "Teilprozess Domäne" wird auf einem Server in der Domäne ausgeführt. Er liest die relevanten Entries aus dem Verzeichnisdienst der Domäne, bereitet sie auf und überträgt sie an den Verzeichnisdienst der Verwaltung.

Die Fehlerbehandlung und das Monitoring erfolgen gemäß der Entwurfsentscheidungen. Die Domäne muss dafür Sorge tragen, dass die entsprechenden Rollen durch Personal besetzt sind. Die Sicherheitsanforderungen müssen umgesetzt sein, d.h., dass der Teilprozess in einem Bereich konfiguriert und betrieben wird, auf den Unberechtigte keinen Zugriff haben.

D.2.1 Vorbedingungen Teilprozess Domäne

Folgende Vorbedingungen und Annahmen müssen erfüllt sein, damit der Aktualisierungsprozess für den Verzeichnisdienst der Verwaltung auf der Seite der Domäne erfolgreich durchgeführt werden kann:

- Der Teilprozess ist korrekt konfiguriert und kann seine Konfigurationsdatei lesen und schreiben
- Der Teilprozess kann auf die Konfigurationsdatei des Rahmenprozesses des Domäne lesend und schreibend zugreifen.
- Der Verzeichnisdienst der Domäne ist in den relevanten Ausschnitten voll lesend zugreifbar.
- Für den Verzeichnisdienst der Domäne ist Schema-Konformität gegeben, wie sie nach Kapitel 5 gefordert ist.
- Es wird erwartet, dass der Aktualisierungsprozess zur Zeitsynchronisation auf einen Hilfs-Entry im Verzeichnisdienst der Domäne schreibend und lesend zugreifen kann (Konfigurationsparameter: DN_TimeSyncEntry).
- Für die Uhr des Servers des Verzeichnisdienstes wird angenommen, dass sie auch nach Störfällen monoton steigend wiederhergestellt wird.
- In den Datensätzen, die in den Verzeichnisdienst der Verwaltung und den Veröffentlichungsdienst übertragen werden sollen, sind das Attribut oder die Attribute, auf die "AT_VDV_visible" und "AT_VoeD_visible" verweisen, mit den geforderten Werten belegt.
- Die Datensätze, die gegenüber dem letzten Prozess-Lauf verändert wurden, sind wie folgt gekennzeichnet: das Attribut, auf das "AT_LastModified" verweist, enthält den Zeitpunkt der letzten Änderung.
- Der Teilprozess kann auf ein Zertifikat und den zugehörigen geheimen Schlüssel zugreifen, um eine SSH-Verbindung zum Verzeichnisdienst der Verwaltung aufzubauen.

-
- Der Teilprozess kennt den öffentlichen Schlüssel des Eingangsbereichs beim VDV.

D.2.2 Nachbedingungen Teilprozess Domäne

Im Falle eines erfolgreichen Abschlusses aller Prozessabschnitte auf der Seite der Domäne gelten folgenden Bedingungen:

- Die Datensätze, die im Verzeichnisdienst der Domäne entsprechend gekennzeichnet waren, wurden in einer LDIF-Datei zusammengestellt.
- Der Wurzelknoten der Domäne (o=) ist nicht in der Datei enthalten.
- Alle neuen oder zu ändernden Entries haben den "changetype:add", alle zu löschenden Entries haben den "changetype:delete".
- Die Datensätze wurden, falls erforderlich, an die Namensstruktur und das Schema des Austausch-DIT angepasst.
- Die LDIF-Datei hat den Bearbeitungsstatus "convtd" (vgl. Tabelle 11)
- Die Datei wurde erfolgreich an den Empfangs-Server beim Verzeichnisdienst der Verwaltung übertragen.
- Es wurden Log-Einträge und bei Bedarf Meldungen an das Monitoring und Audit erzeugt.
- Der Konfigurationsparameter des Teilprozesses "startTimeOfLastSuccessfulRetrieval" wurde auf den Anfangszeitpunkt des Prozesses gesetzt (zur Fortschaltung für den nächsten Differenz-Abgleich).
- Im Falle eines Vollabgleichs wurde der Konfigurationsparameter des Rahmenprozesses "nextFullUpdate" für den nächsten Vollabgleich fortgeschaltet.

D.2.3 Konfigurationsparameter

In dieser Spezifikation werden Konfigurationsparameter eingesetzt um:

- den Aktualisierungsprozess auf die Anforderungen und Gegebenheiten der Domäne anzupassen,

- flexibel für Varianten auch für solche Domänen zu halten, die erst später der PKI-1-Verwaltung beitreten oder über deren Verzeichnisdienst-Aufbau noch keine Angaben vorliegen, und
- die Implementierung zu vereinfachen, indem einige Ersetzungsregeln mit über Parameter gesteuert werden, z. B. indem die Objektklasse eines Entry-Typs nach den Gegebenheiten der Domäne eingestellt wird.

Hinweise zur Implementierung:

- Einige der im folgenden festgelegten Konfigurationsparameter dienen der Vereinfachung der Implementierung des Aktualisierungsprozesses. Sofern in einer Domäne mehrere Varianten unterstützt werden müssen, kann es daher in der Ausbaustufe 1 erforderlich sein, den Aktualisierungsprozess jeweils mit unterschiedlichen Konfigurationsparametern aufzurufen.
- Unabhängig von der jeweiligen Plattform müssen DIT-DNs Umlaute enthalten können!
- Es wird keine Ordnung auf den Werten der Attribute vorausgesetzt, die die Replikation steuern. Eine solche Ordnung entsteht zwar in Bayer, nicht aber beim IVBB. Deshalb müssen alle zulässigen Werte in den Feldern "Val_VoeD_visible" und "Val_VDV_visible" eingetragen werden. Die Konfiguration muss berücksichtigen, dass alle Entries mit Werten aus "Val_VoeD_visible" implizit auch in den VDV eingestellt werden. Es ist daher ausreichend, wenn entsprechende Entries nur über einen Wert in "Val_VoeD_visible" ausgewählt werden.

Name	Format	Zweck	Anmerkung / Default / Beispiel
startTimeOfLast-SuccessfulRetrieval	Date & Time (Sekunden)	Hält die genaue Zeit fest, zu der der letzte erfolgreiche Durchlauf des Prozesses begann.	
DNS_Domain_Dir	String (DNS-Name)	DNS-Name des Verzeichnisdienstes, aus dem die Daten abgefragt werden sollen	
Port_Domain_Dir	Zahl	Port des Verzeichnisdienstes, aus dem die Daten abgefragt werden sollen	

Name	Format	Zweck	Anmerkung / Default / Beispiel
FNP_xxx • einzelne Parameter gemäß Tabelle 11 oben	gemäß Bedarf	FNP steht für fileNameParameter. Zur Konstruktionsregel siehe oben	
DN_TimeSyncEntry	String: DIT-DN	enthält den DIT Distinguished Name des Hilfs-Entries, über den der Aktualisierungsprozess die aktuelle Zeit des Verzeichnisdienst-Servers feststellt.	
DN_SelectedSubTree	String: DIT-DN	der Parameter gibt den DN des Wurzelknotens für den Teilbaum an, für den der Aktualisierungsprozess durchgeführt werden soll (search-root)	"dc=certificates, dc=pki, dc=Bayern, dc=de"
Proc_Name_D-Preprocessing	String: {LEER [voller Prozedur-name]}	Name der Prozedur, die das domänenspezifische Preprocessing durchführt (Interface zu spezifizieren)	
EE_D-DIT-DN-root	String: DIT-DN	steht für "End Entity Domänen DIT root". Der Parameter gibt die hohen relative Distinguished Names von Teilnehmer-Entries an, die durch EE_A-DIT-DN-root im Umsetzungsprozess für den Austausch-DIT ersetzt werden.	"dc=certificates, dc=pki, dc=Bayern, dc=de" In der Regel der gleiche Wert wie "DN_SelectedSubTree". Abweichungen sind nur sinnvoll, wenn die Domäne ein eigenes Preprocessing durchführt.
EE_A-DIT-DN-root	String: DIT-DN	steht für "End Entity Austausch-DIT root". Wert, mit dem in jedem DN von Teilnehmer-Entries die EE_D-DIT-DN-root substituiert wird.	"ou=certificates, o=Bayern, c=DE"
rank_D-DIT-ou_for_A-DIT	Zahl	kennzeichnet, welches ou aus dem DDIT-DN in den ADIT-DN übernommen werden soll (höchstes ou bekommt die Nummer 1)	
Dir_Constraints	String: {"none" "W2K"}	zur Unterscheidung, ob spezielle Umsetzungsregeln für Windows 2000 für Objektklassen, Attribut-Typen oder Werte angewendet werden müssen	
CA_Subject_DN_root	String: DIT-DN	für Win2K-Umgebungen, enthält alle Namensbestandteile des Subject-DN in der Domäne für alle CAs außer dem untersten CN, wird verwendet um den DIT-DN für den Austausch-DIT zu bilden (Entspricht bei korrekter Namensgebung der Wurzel des A-DIT für die CAs). Wird nur verwendet, wenn Dir_Constraints="W2K" hat.	

Name	Format	Zweck	Anmerkung / Default / Beispiel
Log- und Monitoringparameter (Liste ist im Rahmen der Implementierung zu ergänzen)	wie erforderlich	legen fest, wie Meldungen an das Monitoring übertragen werden, z.B. eine E-Mail-Adresse, das Verzeichnis, in dem die Prozessspezifischen und die Übersichts-Log-Datei zu speichern sind, die Anzahl der aufzubewahrenden Prozess-Log-Dateien und die Anzahl der Einträge im Übersichts-Log.	Implementierungsabhängig, die Parameter können vom Rahmenprozess und vom Teilprozess in der Domäne gemeinsam genutzt werden
OC_Person	String	enthält den Namen der strukturellen Objektklasse, die in der Domäne für Entries von Personen verwendet wird.	Verwendung für Umsetzungsregeln, OC_Person=inetOrgPerson
OC_CA	String	enthält den Namen der Hilfs-Objektklasse, die in der Domäne für Entries von CAs verwendet wird.	Verwendung für Umsetzungsregeln, OC_CA=certificationAuthority
OC_CDP	String	enthält den Namen der strukturellen Objektklasse, die in der Domäne für Entries von CDPs verwendet wird.	Verwendung für Umsetzungsregeln, OC_CDP=cRLDistributionPoint
AT_userEMail	String	enthält Namen des einwertigen Attributes, das die namensgebende E-Mail-Adresse enthält. (Falls Parameter LEER, wird Standard-Verfahren verwendet.)	Verwendung für Umsetzungsregeln, Beispiel: AT_userEMail=mail
AT_userCertificate	String	enthält den Namen des Attributtyps, der in der Domäne für die Speicherung von Teilnehmerzertifikaten verwendet wird.	Verwendung für Umsetzungsregeln, AT_userCertificate=userCertificate
AT_VDV_visible	String	enthält den Namen des Attribut-Typs, in dem die Steuerinformation für die Replikation in den Verzeichnisdienst der Verwaltung enthalten ist.	
Val_VDV_visible	Array of Strings	enthält einen oder mehrere alternativ zulässige Wert des Attributs, auf das AT_VDV_visible verweist	Es wird keine Ordnung auf den Werten vorausgesetzt, die die Replikation steuern. Deshalb müssen alle zulässigen Werte in diesem Feld eingetragen werden.
AT_VoeD_visible	String	enthält den Namen des Attribut-Typs, in dem die Steuerinformation für die Replikation in den Veröffentlichungsdienst enthalten ist.	
Val_VoeD_visible	Array of Strings	enthält einen oder mehrere alternativ zulässige des Attributs, auf das AT_VoeD_visible verweist	Es wird keine Ordnung auf den Werten vorausgesetzt, die die Replikation steuern. Deshalb müssen alle zulässigen Werte in diesem Feld eingetragen werden.

Name	Format	Zweck	Anmerkung / Default / Beispiel
base_search_filter	String	optional: Definition eines Suchfilters für die zu abzufragenden Entries. Falls leer wird der Suchfilter aus Val_VDV_visible und Val_VoeD_visible konstruiert.	Dient dazu, spezielle Suchfilter in der Domäne zu konfigurieren.
AT_LastModified	String	enthält den Namen des Attribut-Typs, das in jedem Entry den letzten Zeitpunkt der Veränderung speichert.	
AT_internal-Notification	String	enthält den Namen des Attribut-Typs, das zur Kennzeichnung von Einträgen für die interne Kommunikation im VDK genutzt wird	Verwendung für Umsetzungsregeln
DNS_VDV_Receiver	String (DNS-Name)	DNS-Name des Empfänger-Servers beim VDV	
Port_VDV_Receiver	Zahl	Port des Empfänger-Servers beim VDV	
File-Location_VDV-Receiver	String	Unterverzeichnis im Server des Empfänger beim VDV, in dem die LDIF-Dateien abgelegt werden sollen	
PSE-Location	String	Stelle, an der die PSE zur Sicherung der SSH Verbindung in der Domäne abgelegt ist	
PasswordConnection PSE	zu klären	Passwort zur Verwendung der PSE aus PSE-Location Implementierungshinweis: möglicherweise sollte das Passwort separat abgelegt werden können, um den Zugriff besser begrenzen zu können.	
audit_mail_address	String: E-Mail-Adresse	Dient zur Benachrichtigung der Rolle "Audit", wenn Log-Dateien gelöscht werden können.	
Archival_Period_Days	Zahl	Anzahl der Tage, nach denen archivierte Dateien gelöscht werden können	Default: 62 (2 Monate)

Tabelle 15: Konfigurationsparameter des Teilprozesses der Domäne für die Aktualisierung des Verzeichnisdienstes der Verwaltung

D.2.4 Aufruf des Teilprozesses

Der Teilprozess der Domäne kann durch den Rahmenprozess automatisch oder durch manuellen Aufruf gestartet werden.

Im Rahmen der Implementierung ist sicherzustellen, dass der Prozess beim Aufruf erkennt, ob er bereits für den gleichen "DN_SelectedSubTree" läuft. In

diesem Fall muss der erneute Aufruf mit geeigneter Fehlermeldung (Monitoring und gegebenenfalls manueller Bediener) gemeldet werden und abrechnen.

Der Aufruf des Teilprozesses erfolgt mit den Parametern:

- Konfigurationsdatei: Es muss möglich sein, den Teilprozess auf einem Server für unterschiedliche Teilbäume des Domänen-DIT auszuführen. Abhängig von der Implementierung muss daher die Konfigurationsdatei beim Aufruf übergeben werden.
- Scope ist "diff" oder "voll" (entspricht Bestandteil "Datenumfang" des Dateinamens)
- Aufruf ist "automatisch" oder LEER (der Rahmenprozess ruft immer mit "automatisch" auf)

D.2.5 Prozessabschnitte

Alle Prozessabschnitte kennen die Parameter der jeweils vorhergehenden, soweit auf diese zugegriffen wird.

D.2.5.1 Prozessabschnitt "Initialisierung"

Der Prozessabschnitt führt einige vorbereitende Schritte durch. Dadurch wird sichergestellt, dass Aufruf- und Konfigurationsparameter gesetzt, der Prozess nicht gleichzeitig bereits mit der gleichen Konfigurationsdatei ausgeführt wird und die Systemzeit vom Verzeichnisdienst der Domäne übernommen wird. Letzteres stellt implizit sicher, dass der Verzeichnisdienst der Domäne zum Aufrufzeitpunkt verfügbar ist.

Hinweise zur Implementierung:

- Der Prozessabschnitt "Initialisierung" und die weiteren Abschnitte müssen Zeitangaben auf ein einheitliches Format umsetzen. Dabei muss berücksichtigt werden, dass sich die Formate zwischen Betriebssystemen, Verzeichnisdienst-Produkten und gegebenenfalls auch domänenspezifischen Realisie-

rungen von Attribut-Typen unterscheiden können. Sofern solche Unterschiede auftreten, muss die Implementierung konfigurierbar sein.

- Alle LDAP-Transaktionen werden mit dem Domain_Dir_Server durchgeführt.

Folgende Schritte werden durch den Prozessabschnitt ausgeführt:

Nr.	Funktionalität und Bedingungen	Verzweigung
1	Prüfe Aufrufparameter: <ul style="list-style-type: none"> • Scope ist "diff" oder "full" • Aufruf ist "automatisch" oder LEER • Konfigurationsdatei ist gesetzt • Setze AP-Server_StartTime := Systemzeit des Servers, auf dem der Teilprozess abläuft 	
1.1	➤ case: Fehler in Aufrufparametern: Prozess beenden gemäß Fehlerbehandlung	schwerer Fehler
2	Lese Konfigurationsparameter des Teilprozesses des Domäne	
2.1	➤ case: nicht verfügbar: Prozess beenden gemäß Fehlerbehandlung	schwerer Fehler
3	Lese folgende Konfigurationsparameter des Rahmenprozesses des Domäne <ul style="list-style-type: none"> • restartAfterMinutes • Log- und Monitoringparameter 	
3.1	➤ case: nicht verfügbar: Prozess beenden gemäß Fehlerbehandlung	schwerer Fehler
4	Konsistenzprüfungen für Konfigurationsparameter: Die folgenden Bedingungen dürfen nicht auftreten: <ul style="list-style-type: none"> • entsprechendes Tests für Log- und Monitoringparameter • Scope = "diff" UND startTimeOfLast-SuccessfulRetrieval = LEER • Einer der Parameter DNS_Domain_Dir, Port_Domain_Dir, alle aus der Liste der FNP, DN_TimeSyncEntry, DN_SelectedSubTree, EE_D-DIT-DN-root, EE_A-DIT-DN-root ist LEER • Dir_Constraints enthält anderen Wert als {"none" "W2K"} • Dir_Constraints = "W2K" UND CA_Subject_DN_root = LEER • Einer der Parameter OC_Person, OC_CA, OC_CDP, AT_userCertificate, AT_VDV_visible, Val_VDV_visible, Val_VoeD_visible, AT_LastModified ist LEER • (ggf. zu vervollständigen) 	
4.1	➤ case: es ist ein Konfigurationsfehler aufgetreten (eine der Bedingungen aus der Liste war erfüllt) Prozess beenden gemäß Fehlerbehandlung	schwerer Fehler (qualifizierte Meldung über die Ursache mit Parameter-Name(n))
5	Teste, ob der Teilprozess bereits für den gleichen DN_SelectedSubTree aktiv ist.	
5.1	➤ case: Ist bereits aktiv Prozess beenden gemäß Fehlerbehandlung	schwerer Fehler
6	Zeitsynchronisation mit Verzeichnisdienst <ul style="list-style-type: none"> • Bestimme die Adresse des Domain_Dir_Server aus DNS_Domain_Dir und Port_Domain_Dir • schreibe ein Attribut per LDAP-modify in DN_TimeSyncEntry (unter Veränderung von AT_LastModified durch Domain_Dir_Server) • lese AT_LastModified aus DN_TimeSyncEntry • bestimme Dir-Server_StartTimeOfProcess := AT_LastModified 	

Nr.	Funktionalität und Bedingungen	Verzweigung
6.1	<ul style="list-style-type: none"> ➤ case: Fehler in Zeitsynchronisation Prozess beenden gemäß Fehlerbehandlung 	schwerer Fehler
7	Setzen globaler Variablen <ul style="list-style-type: none"> • Setze Process_State auf "initial" • Setze Warning_Counter := 0 • Setze Error_Counter:= 0 • Setze NumberOfEntries := 0 Dateien vorbereiten <ul style="list-style-type: none"> • Bilde Dateinamen für Working_File für LDIF-Datei gemäß Regel mit Status ist "initial" • Schreibe den Header von Working_File gemäß festgelegter Header-Informationen • Bilde Dateinamen für Log_File gemäß Regel • Erzeuge Start-Eintrag in Log_File • Erzeuge Start-Eintrag in Übersichts-Log 	
7.1	<ul style="list-style-type: none"> ➤ case: Fehler in der Dateivorbereitung Prozess beenden gemäß Fehlerbehandlung 	schwerer Fehler

D.2.5.2 Prozessabschnitt "Datenabfrage"

Voraussetzung des Prozessabschnitts "Datenrecherche" ist der erfolgreiche Abschluss des Prozessabschnitts "Initialisierung"

Der Prozessabschnitt fragt die Daten des konfigurierten Teilbaums aus dem Verzeichnisdienst der Domäne ab. Dabei werden nur Entries berücksichtigt, die für die Bereitstellung im VDV oder Veröffentlichungsdienst gekennzeichnet sind. Je nach Datenumfang, den der Teilprozess bearbeiten soll, wird der Zeitpunkt der letzten Veränderung der Entries berücksichtigt. Das Abfrageergebnis wird an den Header der initialen LDIF-Datei angehängt. Jeder Entry des Abfrageergebnisses wird mit den "changetype:add" versehen.

Im Anschluss an den Prozessabschnitt wird optional das domänenspezifische Preprocessing aufgerufen.

- Aufruf-Parameter sind der Name des Working-Files und der Scope des aufrufenden Aktualisierungsprozesses.
- Nach Rückkehr sind die Veränderungen in Working_File eingearbeitet bzw. ergänzt. Die Prozedur muss die Konventionen für die LDIF-Datei in diesem Prozessabschnitt einhalten. Etwa angehängte LDIF-Löschbefehle müssen mit "changetype:delete" gekennzeichnet sein.

Hinweise zur Implementierung:

- Auf den Steuerattributen zur Auswahl der Entries für den VDV und den Veröffentlichungsdienst wird keine Ordnung vorausgesetzt (wie sie in Bayern gegenwärtig besteht). Im IVBB können mehrere Werte angegeben werden. Deshalb muss der Suchfilter aus den Werten konstruiert werden, die in den String-Arrays "Val_VDV_visible" und "Val_VoeD_visible" enthalten sind. Sie enthalten alle zulässigen Werte des jeweiligen Attribut-Typs. Der Suchfilter wird gebildet, indem alle zulässigen Werte mit ODER-Bedingungen verknüpft werden. Sofern "base_search_filter" belegt ist, wird der enthaltene String als Suchfilter verwendet (vorrangig vor einem konstruierten). Der Umfang (full | diff) bestimmt implizit, ob eine Zeitgrenze verwendet wird. Diese muss bei Bedarf in allen Varianten dynamisch ergänzt werden.

Folgende Schritte werden durch den Prozessabschnitt ausgeführt:

Nr.	Funktionalität und Bedingungen	Verzweigung
1	Konstruktion des Basis-Suchfilters (aus Domain_Dir_Server)	
1.1	<ul style="list-style-type: none"> ➤ case: base_search_filter ist NICHT LEER: setze Searchfilter := base_search_filter weiter bei #2 	weiter bei #2
1.2	<ul style="list-style-type: none"> ➤ case: base_search_filter ist LEER: setze Searchfilter := alle Entries aus DN_SelectedSubTree mit Attribut (AT_VDV_visible = einem Wert aus Array Val_VDV_visible) ODER (AT_VoeD_visible = einem Wert aus Array Val_VoeD_visible) (siehe auch Implementierungshinweis oben) weiter bei #2 	weiter bei #2
2	Anpassung des Suchfilters nach Scope des Teilprozesses	
2.2	<ul style="list-style-type: none"> ➤ case: scope ist "diff": dann setze Searchfilter := SearchFilter UND (Attribut AT_LastModified >= startTimeOfLastSuccessfulRetrieval) weiter bei #2 	
3	Abfrage der Entries: • LDAP-Search in Domain_Dir_Server mit SearchFilter	
4	Teste Suchergebnis	
4.1	<ul style="list-style-type: none"> ➤ case: Suchergebnis war LEER (kein Entry gefunden: der Prozesslauf kann abgeschlossen werden. Weiter mit Prozessabschnitt ["LDIF-Übertragung", Schritt #4] 	Prozessabschnitt ["LDIF-Übertragung", Schritt #4]

Nr.	Funktionalität und Bedingungen	Verzweigung
4.2	<ul style="list-style-type: none"> ➤ case: ist nicht LEER, aber enthielt neben Entries auch Fehlermeldungen: <ul style="list-style-type: none"> * setze Error_Counter auf Anzahl der Fehler; * schreibe Log-Eintrag * weiter mit #3 	
5	Schreibe Suchergebnis in Working_File Kennzeichnung als "Positiv-Einträge" (zur Abgrenzung gegen Lösch-befehle) <ul style="list-style-type: none"> • Ergänze zu jedem Entry in Working_File "changetype:add" 	
6	Lokales Preprocessing aufrufen	
6.1	<ul style="list-style-type: none"> ➤ case: Proc_Name_D-Preprocessing ist nicht LEER: <ul style="list-style-type: none"> * Erzeuge Status-Eintrag in Log_File für Aufruf * call Proc_Name_D-Preprocessing (Working_File, scope) (Hinweis: nach Rückkehr sind die Veränderungen in Working_File eingearbeitet; siehe auch oben) 	
6.2	<ul style="list-style-type: none"> ➤ case: Bei Aufruf von lokalem Preprocessing: Aufruf nicht erfolgreich oder keine Rückgabe der Prozesskontrolle innerhalb von restartAfterMinutes/2: Prozess beenden gemäß Fehlerbehandlung 	schwerer Fehler
7	(Nach Rückkehr von lokalem Preprocessing) Bearbeitungsstatus fortschalten: <ul style="list-style-type: none"> • Setze Process_State auf "retrRes" • ändere Bearbeitungsstatus im Header von Working_File auf "retrRes" • ändere Dateiname von Working_File gemäß Regeln auf [..]"retrRes".LDIF • Erzeuge Status-Eintrag in Log_File 	
7.1	<ul style="list-style-type: none"> ➤ case: Fehler in diesem Schritt 	schwerer Fehler

D.2.5.3 Prozessabschnitt "Umsetzungen"

Voraussetzung des Prozessabschnitts "Umsetzungen" ist der erfolgreiche Abschluss des Prozessabschnitts "Datenabfrage" oder eine Eingabedatei, die durch das lokale Preprocessing erzeugt wurde und allen Bedingungen genügt, die in diesem Prozess-Status erreicht sind.

Die Aufgabe des Prozessabschnitts ist es, alle Entries auf die Namensregeln und das Schema des Austausch-DIT umzusetzen. Dazu wird jeder Entry aus dem Working_File gelesen. Der Entry wird mit allen Attributen einschließlich des Changetypes an den entsprechenden Prozessabschnitt übergeben. Die Umsetzungsregeln werden angewandt. Das zurückgegebene Ergebnis wird in eine neue Datei geschrieben. Diese Ergebnisdatei enthält ausschließlich Entries, deren Umsetzung gemäß der Umsetzungsregeln erfolgreich war.

Entries, die nicht umgesetzt werden können oder in denen Vorgaben nicht erfüllt werden, werden nicht übernommen (ignoriert, erzeugen aber einen Fehlereintrag in Log_File). Der Datenumfang aller Entries ist auf die Attribute reduziert, die im Verzeichnisdienst der Verwaltung bereitgestellt werden sollen. Der Changetype ist für alle Entries auf einen der Werte "add" oder "delete" gesetzt. Der Prozessabschnitt für die Umsetzung kann in "result" die folgenden Ergebnisse liefern:

- Umgesetzten Entry
- LEER
- schwerer Fehler, ggf. mit Error-Code. Diese Rückmeldung ist nötig, um eine ordnungsgemäßen Prozessabschluss zu ermöglichen.
(Hinweis: Warnungen und einfache Fehler werden lokal während der Umsetzung behandelt)

Folgende Schritte werden durch den Prozessabschnitt ausgeführt:

Nr.	Funktionalität und Bedingungen	Verzweigung
1	<ul style="list-style-type: none"> • Bilde Dateinamen für Output_File für gemäß Regel mit Status ist "convted" • Kopiere die Header aus Working_File in Output_File aber mit "Bearbeitungsstatus:convted" • Erzeuge Status-Eintrag in Log_File 	
2	Für jeden Entry aus Working_File:	
2.1	<ul style="list-style-type: none"> • Aufruf von "Prozessabschnitt Umsetzung Entry (gesamter Entry incl. changetype, result)" <ul style="list-style-type: none"> ➢ case: result ist LEER: weiter mit nächstem Entry (#2) 	#2
2.2	<ul style="list-style-type: none"> ➢ case: result ist nicht LEER und kein Fehler: * schreibe Entry in Output_File * inkrementiere NumberOfEntries * weiter mit nächstem Entry (#2) 	#2
2.3	<ul style="list-style-type: none"> ➢ case: result ist "schwerer Fehler" (ggf. mit Errorcode) Prozess beenden gemäß Fehlerbehandlung 	schwerer Fehler
3	Bearbeitungsstatus fortschalten:	
3.1	<ul style="list-style-type: none"> • Setze Process_State auf "convted" • Working_File := Output_File • Erzeuge Status-Eintrag in Log_File ➢ case: Fehler in diesem Schritt Prozess beenden gemäß Fehlerbehandlung 	schwerer Fehler

D.2.5.4 Prozessabschnitt "LDIF-Übertragung"

Voraussetzung des Prozessabschnitts "LDIF-Übertragung" ist der erfolgreiche Abschluss des Prozessabschnitts "Umsetzungen"

In diesem Prozessabschnitt wird die erzeugte LDIF-Datei über eine mit Secure Shell gesicherte Kommunikationsverbindung über das Intranet an den Verzeichnisdienst der Verwaltung übertragen. Der Außerdem sind einige Abschlussarbeiten auf der Seite der Domäne auszuführen. Unter anderem werden alte Ergebnisdateien, die lokal vorliegen, gemäß folgender Regeln gelöscht:

- Sofern die **Übertragung nicht erfolgreich** war, bleiben alle Dateien erhalten. Das erlaubt gegebenenfalls eine manuelle Übertragung an den Verzeichnisdienst der Verwaltung. Der Konfigurationsparameter "startTimeOfLast-SuccessfulRetrieval" wird allerdings nicht fortgeschaltet, so dass der nächste Lauf wieder beim gleichen Änderungszeitpunkt aufsetzt.
- Sofern die **Übertragung erfolgreich** war, wurde die LDIF-Datei Working_File auf den Server des VDV kopiert. In der Domäne wird Working_File und die zugehörige Log-Datei in das Archiv verlegt. Die LDIF-Dateien vorherigen erfolglosen Versuchen müssen nicht mehr übertragen werden, da alle Entries aus den vorherigen erfolglosen Prozessläufen auch im aktuellen Working_File berücksichtigt wurden. Nachdem Working_File und die Log-Datei archiviert wurden, können daher alle anderen Dateien im Arbeitsverzeichnis aus vorherigen erfolglosen Versuchen gelöscht werden.
- Sofern die **Übertragung erfolgreich** war und scope="full", werden im Archiv alle LDIF-Dateien gelöscht, die älter als einen Monat sind. Das Audit erhält einen Hinweis, wenn Log-Dateien gelöscht werden können (wg. Rollentrennung und Zugriffsbegrenzungen)

Hinweise zur Implementierung:

- Es wird vorgeschlagen, zur Sicherung der Verbindung SSH (mindestens Version 2) mit fest konfigurierten Schlüsseln einzusetzen. Ein äquivalentes

Verfahren ist möglich, muss aber in der Spezifikation entsprechend nachgepflegt werden.

Folgende Schritte werden durch den Prozessabschnitt ausgeführt:

Nr.	Funktionalität und Bedingungen	Verzweigung
1	Baue SSH Verbindung zum Verzeichnisdienst der Verwaltung auf unter Verwendung von <ul style="list-style-type: none"> • DNS_VDV_Receiver • Port_VDV_Receiver • File-Location_VDV_Receiver • PSE-Location • PasswordConnectionPSE 	
1.1	➤ case: Verbindungsaufbau gescheitert: Working_File und zugehöriges Log-File wird nicht gelöscht. Prozess beenden gemäß Fehlerbehandlung	schwerer Fehler (mit qualifizierter Meldung über die Ursache)
2	(SSH-Verbindung erfolgreich) <ul style="list-style-type: none"> • Übertrage Working_File an File-Location_VDV_Receiver • Überprüfe erfolgreiche Übertragung durch Größenvergleich zwischen gesendetem Working_File und der Datei auf File-Location_VDV_Receiver nach beendeter Übertragung. 	
2.1	➤ case: Übertragung nicht erfolgreich: Working_File und zugehöriges Log-File wird nicht gelöscht. Prozess beenden gemäß Fehlerbehandlung (mit qualifizierter Meldung über die Ursache)	schwerer Fehler
3	(Übertragung war erfolgreich) <ul style="list-style-type: none"> • verlege Working_File und zugehöriges Log-File in Archive • setze in Konfigurationsdatei des Teilprozesses den Parameter startTimeOfLastSuccessfulRetrieval := Dir-Server_StartTimeOfProcess 	
3.1	➤ case: scope ist "diff" weiter bei Schritt #4	Schritt #4
4	(scope ist "full") <ul style="list-style-type: none"> • lese nextFullUpdate aus Konfigurationsdatei Rahmenprozess • bestimme nextFullUpdate := nextFullUpdate + restartFullUpdateAfterDays + DayTimeOfFullUpdate • schreibe nextFullUpdate in Konfigurationsdatei Rahmenprozess • falls im LDIF-Datei-Archiv Dateien vorhanden sind, die älter als Archival_Period_Days Tage sind: lösche diese Dateien • falls im Log-Archiv Dateien vorhanden sind, die älter als Archival_Period_Days Tage sind, generiere E-Mail an audit_mail_address mit Anzahl dieser Dateien, verbrauchtem Speicherplatz und verfügbarem Speicherplatz. 	
4.1	➤ case: Eine der Aktionen nicht erfolgreich <ul style="list-style-type: none"> * direkte Fehler-Meldung (mit qualifizierter Ursache) an das Monitoring * Eintrag in das Übersichts-Log 	
5	Auswertung und Warnungen bei kritischer Prozesslaufzeit <ul style="list-style-type: none"> • Bestimme AP-process-duration := Systemzeit des Servers - AP-Server_StartTime • Schreibe aktuelle Systemzeit des Servers und AP-process-duration in Log 	
5.1	➤ case: AP-process-duration > restartAfterMinutes/2: Fehlerbehandlung für "Fehler" und Eintrag in Übersicht-Log	

Nr.	Funktionalität und Bedingungen	Verzweigung
5.2	<ul style="list-style-type: none"> ➤ case: AP-process-duration > 80% von restartAfterMinutes: * Eintrag in Log_File * Eintrag in das Übersichts-Log * direkte Fehler-Meldung (mit qualifizierter Ursache) an das Monitoring 	
6	Log und Meldungen abschließen <ul style="list-style-type: none"> • Erstelle zusammenfassende Meldung gemäss Entwurfsentscheidungen "Fehlerbehandlung" und "Monitoring" (unter Berücksichtigung von NumberOfEntries, Warning_Counter und Error_Counter) • Schreibe zusammenfassende Meldung in Log_File • schreibe zusammenfassende Meldung in Übersichts-Log • Schliesse offen Dateien • Beende Prozess regulär 	
6.1	<ul style="list-style-type: none"> ➤ case: Eine Aktion nicht erfolgreich Prozess beenden gemäß Fehlerbehandlung 	schwerer Fehler (mit qualifizierter Meldung über die Ursache)

Tabelle 16: Prozess-Schritte der LDIF-Übertragung

D.2.5.5 Prozessabschnitt "Umsetzung Entry"

Der in Tabelle 17 spezifizierte Prozessabschnitt zur Umsetzung von DIT und Schema nimmt die Umsetzung des gesamten Entries vor. Er wird je Entry vom Rahmenprozess aufgerufen. Während des ganzen Prozessabschnitts bleibt der Ursprungs-Entry (D-DIT-Entry) verfügbar; die Ergebnisse der Umsetzung werden in result geschrieben. Beide Datenstrukturen müssen für alle Unterprozessabschnitte les- und schreibbar sein.

Dann folgen diese Schritte:

- Umsetzung des changetype, wo erforderlich.
- Für Entries vom für CAs vorgesehen Objekttyp:
 - Falls der Entry zur Löschung markiert ist, Ausgabe einer Fehlermeldung (CAs werden nur manuell gelöscht).
 - Ansonsten Umsetzung von DIT und Schema nach Definition.
- Für Entries vom für CDPs vorgesehen Objekttyp:
 - Falls der Entry zur Löschung markiert ist, Ausgabe einer Fehlermeldung (CDPs werden nur manuell gelöscht).
 - Ansonsten Umsetzung von DIT und Schema nach Definition.

- Für Entries vom für Teilnehmer vorgesehen Objekttyp:
 - Falls der Entry zur Löschung markiert ist, Umsetzung nur des DITs (damit der Löschbefehl im A-DIT zugeordnet werden kann).
 - Ansonsten Umsetzung von DIT und Schema nach Definition.

Danach wird der umgesetzte Entry in der Variable "result" zurückgegeben (im Fehlerfalle bleibt result LEER).

1	Umsetzung changetype (zur Vereinheitlichung der Formate)		
1.1	<ul style="list-style-type: none"> ➤ case: changetype=modify: ersetze durch changetype:=add; gehe zu #2 		
1.2	<ul style="list-style-type: none"> ➤ case: changetype=delete: gehe zu #2 		
1.3	<ul style="list-style-type: none"> ➤ else: gebe Fehler aus; result:=LEER an aufrufenden Prozess; terminiere Prozessabschnitt 		
2	Umsetzung Objektklassen und Attributtypen		
2.1	<ul style="list-style-type: none"> ➤ case: Objektklasse des Entries =OC_CA und changetype=delete: gebe Warnung aus; gebe result:=LEER an aufrufenden Prozess; terminiere diesen Prozessabschnitt. 	Tabelle 19: Umsetzung Objektklassen und Attributtypen CA	
2.2	<ul style="list-style-type: none"> ➤ case: Objektklasse des Entries =OC_CA: führe Konstruktion von result gemäß Tabelle 19 durch; gehe zu #3. 		
2.3	<ul style="list-style-type: none"> ➤ case: Objektklasse des Entries = OC_CDP und changetype=delete: gebe Warnung aus; gebe result:=LEER an aufrufenden Prozess; terminiere diesen Prozessabschnitt. 		
2.4	<ul style="list-style-type: none"> ➤ case: Objektklasse des Entries = OC_CDP: führe Konstruktion von result gemäß Tabelle 20 durch; gehe zu #3. 		Tabelle 20: Umsetzung Objektklassen und Attributtypen CDP
2.5	<ul style="list-style-type: none"> ➤ case: Objektklasse des Entries = OC_TN führe Konstruktion von result gemäß Tabelle 21 durch; gehe zu #3. 		Tabelle 21: Umsetzung Objektklassen und Attributtypen Teilnehmer
2.6	<ul style="list-style-type: none"> ➤ else: result:=LEER an aufrufenden Prozess; terminiere diesen Prozessabschnitt. 		
3	Umsetzung Attributwerte		
3.1	<ul style="list-style-type: none"> ➤ case: Objektklasse des Entries = OC_CA oder OC_CDP: führe Konstruktion von result gemäß Tabelle 22 durch; gebe result an aufrufenden Prozess; terminiere diesen Prozessabschnitt. 	Tabelle 22: Umsetzung Attributwerte CAs und CDPs	
3.2	<ul style="list-style-type: none"> ➤ case: Objektklasse des Entries = OC_TN: führe Konstruktion von result gemäß Tabelle 23 durch; gib Ergebnis an aufrufenden Prozess zurück; terminiere diesen Prozessabschnitt. 	Tabelle 23: Umsetzung Attributwerte Teilnehmer	

Tabelle 17: Prozessabschnitt "Umsetzung Entry"

	D-DIT	Umsetzung in A-DIT
Attributtypen	AT_VoeD_visible	Umsetzung in Attribut PublicVisible > case: Wert des Ausgangsattributes in Val_VoeD_visible: Setze PublicVisible:=TRUE. > else: PublicVisible :=FALSE.
	AT_LastModified	Übertragen des Wertes in das Attribut LastModifiedSource
	AT_internal-Notification	Übertragen des Wertes in das Attribut vDKInternalNotification

Tabelle 18: Umsetzung Steuerattribute

	D-DIT	Umsetzung in A-DIT
Objektklasse	OC_CA (strukturell oder auxiliary)	strukturelle Objektklasse: organizational role Hilfsklassen : pkiCA, VDV-control
Attributtypen	commonName	Übername von Attribut und Wert Schwerer Fehler, wenn Attribut nicht vorhanden oder leer
	alle Attribute von pkiCA	Übername von Attribut und Wert Fehler, wenn nicht vorhanden
	Umsetzung Steuerattribute nach Tabelle 18.	
alle anderen Inhalte des Entries werden gelöscht		

Tabelle 19: Umsetzung Objektklassen und Attributtypen CA

	D-DIT	Umsetzung in A-DIT
Objektklasse	OC_CDP (strukturell oder auxiliary)	strukturelle Objektklasse: CrlDistributionPoint Hilfsklasse: VDV-control
Attributtypen	alle aus cRLDistributionPoint	Übername von Attribut und Wert Fehler, wenn nicht vorhanden
	Umsetzung Steuerattribute nach Tabelle 18.	
Alle anderen Inhalte des Entries werden gelöscht		

Tabelle 20: Umsetzung Objektklassen und Attributtypen CDP

	D-DIT-Entry	A-DIT-Entry	Umsetzung
Objektklasse	OC_person	strukturelle Objektklasse: VDV-Person Hilfsklasse: pkiUser, VDV-control	
Attributtypen	cn=	cn=	Übernahme Attributtyp und Wert, wenn vorhanden und einwertig
	AT_userCertificate	usercertificate	Umbenennung Attributtyp, Übernahme Wert,
	o=	o=	Übernahme Attributtyp und Wert , wenn vorhanden
	ou=	ou=	Übernahme Attributtyp und Wert , wenn vorhanden

	gn=	gn=	Übernahme Attributtyp und Wert , wenn vorhanden
	sn=	sn=	Übernahme Attributtyp und Wert , wenn vorhanden
	l= (locality)	l= (locality)	Übernahme Attributtyp und Wert , wenn vorhanden
	serialnumber=	serialnumber=	Übernahme Attributtyp und Wert , wenn vorhanden
	Umsetzung Steuerattribute nach Tabelle 18.		
alle anderen Inhalte des Entries werden gelöscht			

Tabelle 21: Umsetzung Objektklassen und Attributtypen Teilnehmer

Nr.	Funktionalität und Bedingungen	Verzweig.
1	Umsetzung DIT-DN für Win2k-Systeme	
1.1	<ul style="list-style-type: none"> ➤ case: Dir_constraint=Win2K und Objektklasse=OC_CA: Setze DIT-DN um gemäß Tabelle 24; gehe zu #2. 	Tabelle 24: Umsetzung DIT-DN CA-Entry
1.2	<ul style="list-style-type: none"> ➤ case: Dir_constraint=Win2K und Objektklasse=OC_CDP: Setze DIT-DN um gemäß Tabelle 25; gehe zu #2. 	Tabelle 25: Umsetzung DIT-DN CDP-Entry
2	Gebe veränderten Entry an aufrufenden Prozess zurück; Terminiere Prozessabschnitt	

Tabelle 22: Umsetzung Attributwerte CAs und CDPs

Nr.	Funktionalität und Bedingungen	Verzweig.
1	Konstruiere A-DIT-DN gemäß Tabelle 26 und schreibe Ergebnis als DIT-DN in result.	
2	Keine Attribut- und Wertumsetzung, wenn Entry zu löschen (nicht erforderlich)	
2.1	<ul style="list-style-type: none"> ➤ case: changetype=delete: gebe result zurück an aufrufenden Prozess (enthält nur DIT-DN und changetype); terminiere diesen Prozessabschnitt ➤ else: gehe zu #3. 	
3	E-Mail-Attribut: Setze Attribut mail in result auf im A-DIT-DN verwendeten Wert. (Konstruktion erfolgt im Rahmen von #1)	
4	Teste, ob cn im D-DIT-DN oder Entry vorhanden, ggf. umsetzen	
4.1	<ul style="list-style-type: none"> ➤ case: Attributtyp cn im D-DIT-DN nicht vorhanden und kein cn-Wert in result (aus Attributumsetzung) setze result := LEER, gebe an aufrufenden Prozess zurück 	
4.2	<ul style="list-style-type: none"> ➤ else: übernehme cn in passendes Attribut in result (existierender Wert wird dabei überschrieben). 	
5	Umsetzung der D-DIT-DN-Attribute und A-DIT-DN-Attribute in Entry Für jedes Attribut aus D-DIT-DN und A-DIT-DN:	

Nr.	Funktionalität und Bedingungen	Verzweig.
5.1	<ul style="list-style-type: none"> ➤ case: Attributtyp o und Attribut mit identischem Wert nicht in Entry: Schreibe Attributwert in passendes Attribut; setze dabei ggf. das Attribut auf "multivalued"; Gehe zu #5, nächstes Element. 	
5.2	<ul style="list-style-type: none"> ➤ case: Attributtyp ou und Attribut mit identischem Wert nicht in Entry: Schreibe Attributwert in passendes Attribut; setze dabei ggf. das Attribut auf "multivalued"; Gehe zu #5, nächstes Element. 	
5.3	<ul style="list-style-type: none"> ➤ case: Attributtyp gn und Attribut mit identischem Wert nicht in Entry: Schreibe Attributwert in passendes Attribut; setze dabei ggf. das Attribut auf "multivalued"; Gehe zu #5, nächstes Element. 	
5.4	<ul style="list-style-type: none"> ➤ case: Attributtyp sn und Attribut mit identischem Wert nicht in Entry: Schreibe Attributwert in passendes Attribut; setze dabei ggf. das Attribut auf "multivalued"; Gehe zu #5, nächstes Element. 	
5.5	<ul style="list-style-type: none"> ➤ case: Attributtyp l (locality) Attribut mit identischem Wert nicht in Entry: Schreibe Attributwert in passendes Attribut; setze dabei ggf. das Attribut auf "multivalued"; Gehe zu #5, nächstes Element. 	
5.6	<ul style="list-style-type: none"> ➤ case: Attributtyp serialnumber und Attribut mit identischem Wert nicht in Entry: Schreibe Attributwert in passendes Attribut; setze dabei ggf. das Attribut auf "multivalued"; Gehe zu #5, nächstes Element. 	
5.7	<ul style="list-style-type: none"> ➤ else: Gehe zu #5, nächstes Element. 	
6	Gebe result an aufrufenden Prozess zurück und terminiere diesen Prozessabschnitt.	

Tabelle 23: Umsetzung Attributwerte Teilnehmer

Nr.	Funktionalität und Bedingungen	Verzweig.
1	Umsetzung Objektklassen und Attributtypen CA	
1.1	<ul style="list-style-type: none"> ➤ case: DirConstraint=none gib Entry unverändert an aufrufenden Prozess zurück 	
1.2	<ul style="list-style-type: none"> ➤ case: DirConstraints=Win2K A-DIT-DN = CA_Subject_DN_root +D-DIT-CN Ersetze DIT-DN durch A-DIT-DN gib Ergebnis an aufrufenden Prozess zurück. 	

Tabelle 24: Umsetzung DIT-DN CA-Entry

Nr.	Funktionalität und Bedingungen	Verzweig.
1	Umsetzung Objektklassen und Attributtypen CA	
1.1	<ul style="list-style-type: none"> ➤ case: DirConstraint=none: gib Entry unverändert an aufrufenden Prozess zurück. 	
1.2	<ul style="list-style-type: none"> ➤ case: DirConstraints=Win2K: A-DIT-DN := CA_Subject_DN_root + D-DIT-CN des CDP + (CN="CDP"+D-DIT-DN des CDP) (String-Addition); Ersetze DIT-DN durch A-DIT-DN; gib Ergebnis an aufrufenden Prozess zurück. 	

Tabelle 25: Umsetzung DIT-DN CDP-Entry

Nr.	Funktionalität und Bedingungen	Verzweig.
1	Root-Ersetzung: Ersetze "EE_D-DIT-Naming-ROOT" durch "EE_A-DIT_Naming_ROOT" (Stringersetzung)	
2	Konstruktion c=de	
2.1	➤ case: kein c vorhanden oder Wert <>de: erzeuge Fehlereintrag; gehe zu #10.	
2.2	➤ else: A-DIT:="c=de"	
3	Konstruktion o	
3.1	➤ case: o im DIT-DN: nehme Wert und ergänze im A-DIT-DN; gehe zu #4.	
3.2	➤ case: ein o im Entry: nehme Wert und ergänze im A-DIT-DN; gehe zu #3.	
3.3	➤ else: erzeuge Fehlereintrag; gehe zu #10.	Abbruch (#10)
4	Konstruktion ou	
4.1	➤ case: ou in D-DIT-DN: nehme OU der Ordnung <i>rank_D-DIT-ou_for_A-DIT</i> und ergänze im A-DIT; gehe zu #5	
4.2	➤ case: ein ou im Entry: nehme Wert und ergänze im A-DIT-DN; gehe zu #5.	
4.3	➤ else: erzeuge Fehlereintrag; gehe zu #10.	
5	Konstruktion mail	
5.1	➤ case: AT_userEMail nicht LEER und Attribut einwertig und belegt: nehme Wert und ergänze als mail im A-DIT-DN; gehe zu #6.	
5.2	➤ case: AT_userEMail nicht LEER und Attribut mehrwertig oder leer: erzeuge Fehlermeldung; gehe zu #10	
5.3	➤ case: mail im D-DIT-DN: nehme Wert und ergänze als mail im A-DIT-DN; gehe zu #6.	
5.4	➤ case: email im D-DIT-DN: nehme Wert und ergänze als mail im A-DIT-DN; gehe zu #6.	
5.5	➤ case: rfc822 im D-DIT-DN: nehme Wert und ergänze als mail im A-DIT-DN; gehe zu #6.	
5.6	➤ case: emailaddress im D-DIT-DN: nehme Wert und ergänze als mail im A-DIT-DN; gehe zu #6.	
5.7	➤ case: singlevalued mail im D-DIT-Entry: nehme Wert und ergänze im A-DIT-DN; gehe zu #6.	
5.8	➤ case: singlevalued email im D-DIT-Entry: nehme Wert und ergänze im A-DIT-DN; gehe zu #6.	
5.9	➤ case: singlevalued rfc822 im D-DIT-Entry: nehme Wert und ergänze im A-DIT-DN; gehe zu #6.	

Nr.	Funktionalität und Bedingungen	Verzweig.
5.10	➤ case: singlevalued emailaddress im D-DIT-Entry: nehme Wert und ergänze im A-DIT-DN; gehe zu #6.	
5.11	➤ else: erzeuge Fehlermeldung; gehe zu #10	
6	Gebe Entry mit verändertem DIT-DN zurück; terminiere diesen Prozessabschnitt	
10	Gebe leeren Entry zurück; terminiere diesen Prozessabschnitt.	

Tabelle 26: Umsetzung DIT-DN Teilnehmer

D.3 Periodischer Rahmenprozess VDV

Der periodische Rahmenprozess beim VDV hat die Aufgabe, den Eingang von LDIF-Dateien festzustellen und diese an die Konsistenzprüfung zu übergeben.

Der Rahmenprozess des VDV wird nur in seinen allgemeinen Abläufen spezifiziert. Realisierungsdetails und eine differenzierte Berücksichtigung weiterer Fehlerfälle bleibt der Feinspezifikation bzw. Implementierung vorbehalten.

Die Fehlerbehandlung und das Monitoring erfolgen gemäß der Entwurfsentscheidungen. Der Betreiber des VDV muss dafür Sorge tragen, dass die entsprechenden Rollen durch Personal besetzt sind. Die Sicherheitsanforderungen müssen umgesetzt sein, d.h., dass der Teilprozess in einem Bereich konfiguriert und betrieben wird, auf den Unberechtigte keinen Zugriff haben.

D.3.1 Eingang von Dateien von den Domänen

Die Realisierung des kryptographisch gesicherten Zugangs der Domänen zum Ablagebereich des Dateieingangs wird nicht im Detail spezifiziert. Die Implementierung ist stark von den verwendeten Protokollen und Produkten abhängig. Unter der Annahme, dass SSH eingesetzt wird, sind folgende Anforderungen zu realisieren:

- Für jede Domäne existiert ein eigener Eingangsbereich.
- Jedem Eingangsbereich sind ein oder mehrere öffentliche Schlüssel zugeordnet. Nur solche Stellen, die sich korrekt authentisieren, erhalten Schreibrecht auf den jeweiligen Eingangsbereich.

-
- Die Verbindungsannahme einer Rufes erfolgt automatisch, wenn sich die rufende Stelle korrekt authentisiert.
 - Sofern eine erfolgreiche Übertragung einer LDIF-Datei im Rahmen dieses Prozessabschnitts festgestellt wird, könnten die nachfolgende Konsistenzprüfung direkt aufgerufen werden. Andernfalls ist der Rahmenprozess beim VDV zu implementieren.

D.3.2 Vorbedingungen

Es wird angenommen, dass für jeden Eingangsbereich in einer Datei die Parameter für die Konsistenzprüfung eingegangener Dateien abgelegt sind (Domain_Control_File). Auf dieses Konfigurations-File kann nur von der Administration des VDV, nicht aber von der Domäne zugegriffen werden.

Für den Rahmenprozess des VDV müssen folgende Vorbedingungen erfüllt sein:

- Zugriff auf die Eingangsbereiche der Domänen,
- Zugriff auf Zertifikate bzw. Schlüssel der Datenquellen zur Authentisierung der Datenquelle,
- Zugriff auf das eigene Schlüsselpaar für die Authentisierung des Eingangsbereichs des VDV,
- Zugriff auf die Konfigurationsdatei des Rahmenprozesses. Dies schließt ein, dass der Rahmenprozess die Zuordnung von Eingangsbereichen und den Domain_Control_Files kennt (z. B. aus der Konfigurationsdatei).

D.3.3 Invariante

Während der Rahmenprozess des VDV aktiv ist, gilt folgende Invariante:

- Der Rahmenprozess prüft ein mal je Minute, ob in den den Domänen zugeordneten Empfangsbereichen Dateien eingegangen sind.
- Wenn eine Datei gefunden wird, wird sie an die Konsistenzprüfung übergeben.

- Wenn Fehler auftreten, erfolgt eine Fehlermeldung an das Monitoring.

D.3.4 Aufruf des Rahmenprozesses

Der Prozess wird manuell oder beim Hochfahren des Systems automatisch gestartet.

D.3.5 Konfigurationsparameter des Rahmenprozesses VDV

Name	Format	Zweck	Default / Beispiel / Bemerkung
Area_of-incoming_files	festzulegen bei Implementierung	Verweis auf die Ablagebereiche, in denen die Domänen ihre LDIF-Dateien ablegen. Dabei ist die Domänentrennung und die Zuordnung der Domain_Control_Files abzubilden.	
Log- und Monitoring-parameter	wie erforderlich	legen fest, wie Meldungen an das Monitoring übertragen werden, z.B. eine E-Mail-Adresse, das Verzeichnis, in dem die Prozessspezifischen und die Gesamt-Log-Datei zu speichern sind, die Anzahl der Prozess-Log-Dateien und die Anzahl der Einträge im Gesamt-Log.	Implementierungsabhängig, die Parameter können vom Rahmenprozess und vom Teilprozess in der Domäne gemeinsam genutzt werden

Tabelle 27: Konfigurationsparameter des Rahmenprozesses beim VDV zur Steuerung des Teilprozesses beim VDV

D.3.6 Prozessabschnitt

Hinweise zur Implementierung:

- Die Spezifikation könnte so erweitert werden, dass LDIF-Dateien mit dem Umfang "CA" bevorzugt oder eine Verzögerung von "EE" Vollabgleichen auf lastarme Zeiten erfolgt. Hier wird aber angenommen, dass diese Lastverteilung durch Priorisierung eines Schedulers erfolgt. Die Steuerung kann dann im Rahmen der Konsistenzprüfung (unten) erfolgen.
- Es wird angenommen, dass die Dateien im Rahmen der Konsistenzprüfung in einen anderen Arbeitsbereich verlegt werden. Die Implementierung dieses Prozessabschnitts und der Konsistenzprüfung müssen sicherstellen, dass auch bei einem Systemabsturz ein korrektes Wiederaufsetzen möglich ist und einerseits keine Dateien ungeprüft in den VDV bzw. Austauschdienst

übernommen werden, andererseits aber auch keine Dateien für den Aktualisierungsprozess verloren gehen.

- Es wird angenommen, dass die Übergabe an die Konsistenzprüfung zeitnah erfolgt (wenige Minuten). Wenn dies nicht möglich ist, muss geprüft werden, ob in diesem Prozessabschnitt eine Priorisierung vorgenommen wird.
- Falls die Konsistenzprüfung nicht erfolgreich aufgerufen werden kann, sollte das Monitoring nicht mit Meldungen überflutet werden. Allerdings muss sichergestellt werden, dass in relativ kurzen Abständen eine Test erfolgt, ob der Prozess wieder erfolgreich zur Verfügung steht. Sofern dies nicht der Fall ist, sind regelmäßige Meldungen an das Monitoring erforderlich.

Nr.	Funktionalität und Bedingungen	Verzweigung
1	(Prozess wurde aufgerufen und alle Konfigurationsparameter sind gesetzt)	
2	Teste, ob in einem Eingangsbereich eine neue Datei abgelegt wurde.	
2.1	<ul style="list-style-type: none"> ➤ case: keine neue Dateien vorhanden weiter mit #1	weiter mit #1
3	(Neue Dateien vorhanden) für jede neue Datei mit Dateiname <ul style="list-style-type: none"> • stelle anhand des Eingangsbereichs das zugehörige Domain_Control_File fest • rufe auf "Prozessabschnitt Problemanalyse (Dateiname, Name des Domain_Control_File)" 	
3.1	<ul style="list-style-type: none"> ➤ case: Aufruf nicht erfolgreich melde schweren Fehler an Monitoring (qualifizierte Meldung mit Prozesskennung) schreibe qualifizierte Meldung in Übersichts-Log weiter bei #1	weiter bei #1
4	(für alle neuen Dateien wurde Prozessabschnitt "Konsistenzprüfung" aufgerufen) weiter bei #1	weiter bei #1

Tabelle 28: Prozessabschnitt "Dateieingang überwachen"

D.4 Teilprozess Verzeichnisdienst der Verwaltung

Der "Teilprozess Domäne" wird auf einem Server beim Verzeichnisdienst der Verwaltung ausgeführt. Er prüft zunächst die eingegangenen LDIF-Dateien auf Konsistenz. Von konsistenten LDIF-Dateien übergibt er eine Kopie an den Austauschdienst. Außerdem werden die konsistenten LDIF-Dateien priorisiert und zur Aktualisierung des Austausch-DIT abgearbeitet.

Nach der Überwachung des Dateieingangs werden die folgenden Prozessabschnitte im Rahmen des Aktualisierungsprozesses zum VDV durchgeführt:

- Konsistenzprüfungen,
- Upload und
- optional Löschung Inaktive Entries.

Die Fehlerbehandlung und das Monitoring erfolgen gemäß der Entwurfsentscheidungen. Die Domäne muss dafür Sorge tragen, dass die entsprechenden Rollen durch Personal besetzt sind. Die Sicherheitsanforderungen müssen umgesetzt sein, d.h., dass der Teilprozess in einem Bereich konfiguriert und betrieben wird, auf den Unberechtigte keinen Zugriff haben.

Hinweis: Die Prozessabschnitte außer der Dateiannahme werden identisch im Aktualisierungsprozess zur Domäne verwendet. Die dazu zusätzlich notwendigen Konfigurationsparameter und Verzweigungen sind bereits in dieser Spezifikation enthalten.

D.4.1 Vorbedingungen Teilprozess VDV

Für den Teilprozess Verzeichnisdienst der Verwaltung des VDV müssen folgende Vorbedingungen erfüllt sein:

- Der Teilprozess ist korrekt konfiguriert und kann seine Konfigurationsdatei lesen und schreiben.
- Zugriff auf die jeweilige LDIF-Datei.
- Die LDIF-Datei hält die Vorgaben des Verzeichnisdienstkonzepts an Aufbau und Inhalt ein.
- Bei Installation für den VDV: Zugriff auf die `Domain_Control_Files`.
- Für den Verzeichnisdienst der Verwaltung ist Schema-Konformität mit dem Austausch-DIT gegeben.
- Der Verzeichnisdienst der Verwaltung ist schreibend zugreifbar.

- Für die Uhr des Servers des Verzeichnisdienstes wird angenommen, dass sie auch nach Störfällen monoton steigend wiederhergestellt wird.
- Das Zielverzeichnis zur Ablage der LDIF-Dateien beim Austauschdienst ist schreibend zugreifbar.

D.4.2 Nachbedingungen Teilprozess VDV

Im Falle eines erfolgreichen Abschlusses aller Prozessabschnitte auf der Seite des VDV gelten folgenden Bedingungen:

- Die LDIF-Datei ist an den Austauschdienst übergeben.
- Alle Entries aus der LDIF-Datei wurden im Verzeichnisdienst der Verwaltung angelegt oder aktualisiert, sofern dies erforderlich war. Neuere Entries werden nicht mit älteren Informationen überschrieben. Für alle Entries im Verzeichnisdienst, die in der LDIF-Datei enthalten waren und die nicht gelöscht werden sollten, wurde der vDKActiveIndicator geeignet gesetzt.
- Es wurden Log-Einträge und bei Bedarf Meldungen an das Monitoring und Audit erzeugt.
- Im Falle eines Vollabgleichs wurde abschließend eine LDIF-Datei mit Löschbefehlen inaktiver Entries erzeugt. Diese Datei wird wieder an den normalen Ablauf übergeben.

D.4.3 Konfigurationsparameter im Domain Control File

Das Domain Control File enthält für einen Eingangsbereich die zulässigen Teilbäume des Austausch-DIT, die von der Domäne zu Aktualisierung angeliefert werden dürfen.

Hinweise zur Implementierung:

- Unabhängig von der jeweiligen Plattform müssen die DIT-DNs im Domain Control File Umlaute enthalten können!

Name	Format	Zweck	Default / Beispiel / Bemerkung
------	--------	-------	--------------------------------

Name	Format	Zweck	Default / Beispiel / Bemerkung
Version	String	Unterscheidung von Domain Control Files (DCF) des Verzeichnisdienstkonzept in verschiedenen Ausbaustufen. festgelegter Wert der Ausbaustufe 1: "DCF_VDV.01"	Version:DCF_VDV.01
Domain_Name	String	Kennzeichnung des Domain Control Files	Domain_Name:Bayern
permitted_subtrees	array of DIT-DNs	Liste aller zulässigen DIT-DNs für diese Domäne (Format nach Implementierungserfordernissen anpassbar)	permitted_subtrees: o=Bayern,c=DE; ou=Freistaat Bayern,o=PKI-1-Verwaltung,c=DE
VDV-HTTP-DomainCASite	String: HTTP-URL	gibt die Unterseite des HTTP-Dienstes für den VDV an, auf der die CA-Informationen der Domäne abgelegt werden.	für die Domäne Thüringen z. B. "VDV-HTTP-DomainCASite:Tueringen"
ggf. weitere Parameter		je nach Bedarf könnten hier auch weitere Informationen aufgenommen werden, z. B. ein Verweis auf den Authentisierungsschlüssel für die Datenquelle.	

Tabelle 29: Aufbau des Domain Control File beim VDV

D.4.4 Konfigurationsparameter für den Teilprozess beim VDV

Hinweise zur Implementierung:

- Unabhängig von der jeweiligen Plattform müssen DIT-DNs Umlaute enthalten können!
- Die Konfigurationsparameter, die mit "Local_" beginnen, werden nur vom Aktualisierungsprozess zur Domäne verwendet.

Name	Format	Zweck	Default / Beispiel / Bemerkung
Log- und Monitoring-parameter	wie erforderlich	legen fest, wie Meldungen an das Monitoring übertragen werden, z.B. eine E-Mail-Adresse, das Verzeichnis, in dem die Prozessspezifischen und die Gesamt-Log-Datei zu speichern sind, die Anzahl der Prozess-Log-Dateien und die Anzahl der Einträge im Gesamt-Log.	Implementierungsabhängig, die Parameter können vom Rahmenprozess und vom Teilprozess in der Domäne gemeinsam genutzt werden
DNS_Target_Dir	String (DNS-Name)	DNS-Name des Verzeichnisdienstes, in den die Daten geschrieben werden sollen	

Name	Format	Zweck	Default / Beispiel / Bemerkung
Port_Target_Dir	Zahl	Port des Verzeichnisdienstes, in den die Daten geschrieben werden sollen	
UserID_for_Upload	String	User-ID, mit der sich der Prozess am Target_Dir anmeldet	
Password_for_Upload		Passwort, mit dem sich der Prozess am Target_Dir anmeldet	
File_Location_AD	String	Datei-Verzeichnis, aus dem die Domänen LDIF-Dateien importieren	nur für VDV
update_delayHours_EE_warning	Zahl	Anzahl Stunden der Update Verzögerung. Wenn die Differenz zwischen dem Ende des upload-Prozesses für Teilnehmer-Entries und dem Zeitpunkt der Erzeugung der LDIF-Datei größer ist, erfolgt eine Warnung an das Monitoring	
update_delayHours_CA_warning	Zahl	für CA-Entries wie update_delayHours_EE_warning	
update_delayHours_EE_alarm	Zahl	für Teilnehmer-Entries wie update_delayHours_EE_warning, aber Fehler-Meldung	
update_delayHours_CA_alarm	Zahl	für CA-Entries wie update_delayHours_EE_warning, aber Fehler-Meldung	
Local_Directory-Flag	String: {TRUE, FALSE}	Kennzeichnet, ob der Prozess für den VDV oder ein lokales Directory ausgeführt wird	Default ist FALSE (für VDV)
Local_EE_A-DIT-DN-root	DIT-DN	Ziel-Teilbaum im A-DIT für Teilnehmer-Entries; substituiert die Namenswurzel "c=de"; nur bei Local_Directoy=TRUE	Local_EE_A-DIT-DN-root: "l=A-DIT,c=de" verlagert alle Entries des Austausch-DIT in einen eigenen Teilbaum
Local_Dir_Constraints		Kennzeichnung für Windows 2000 Ziel-Directories	
Local_CA_Subject_DN_root		Ziel-Teilbaum im A-DIT für CA-Entries (denkbar bei Windows 2000 Quellen), substituiert die Namenswurzel "o=PKI-1-Verwaltung, c=de"; nur bei Local_Directoy=TRUE	
audit_mail_address	String: E-Mail-Adresse	Dient zur Benachrichtigung der Rolle "Audit", wenn Log-Dateien gelöscht werden können.	
Archival_Period_Days	Zahl	Anzahl der Tage, nach denen archivierte Dateien gelöscht werden können	Default: 62 (2 Monate)
delete_subtree-entry-after-inactive-days	Zahl, 0 bedeutet "keine Löschung"	Anzahl der Tage, die ein Entry inaktiv sein muss, um nach einem Vollabgleich für den Subtree gelöscht zu werden	Default: 3; 0 bedeutet "keine Löschung auf Subtree"

Name	Format	Zweck	Default / Beispiel / Bemerkung
delete_ADIT-entry-after-inactive-days	Zahl, 0 bedeutet "keine Löschung"	Anzahl der Tage, die ein Entry aus dem gesamten Austausch-DIT inaktiv sein muss, um nach einem beliebigen Vollabgleich gelöscht zu werden	Default: 62; 0 bedeutet "keine Löschung auf gesamtem A-DIT"
delete_not_in_Subtree_on_percent	Zahl zwischen 0 und 100	Prozentzahl von inaktiven Entries im Subtree des aktuellen Vollabgleichs, ab der nicht mehr automatisch gelöscht werden soll	delete_not_in_Subtree_on_percent:10
delete_not_in_ADIT-on_number	Zahl	Anzahl von inaktiven Entries im Austausch-DIT, ab der nicht mehr automatisch gelöscht werden soll	delete_not_in_ADIT-on_number

Tabelle 30: Konfigurationsparameter für den Teilprozess beim VDV

D.4.5 Prozessabschnitte

D.4.5.1 Prozessabschnitt "Konsistenzprüfungen"

Der Prozessabschnitt prüft, ob der im Header der LDIF-Datei angegebene DIT-DN mit dem Namensraum übereinstimmt, der für den Eingangsbereich konfiguriert wurde.

Der Prozessabschnitt wird aufgerufen mit dem Namen des LDIF-Files und dem Namen des Domain_Control_File, das dem Eingangsbereich zugeordnet ist.

Hinweise zur Implementierung:

- Alle Variablen mit LF sind Werte aus der LDIF-Datei, alle Parameter mit DCF stammen aus dem Domain_Control_File.
- Um Performance-Problemen zu begegnen, wird dringend empfohlen, eine Art Scheduler zu implementieren mit folgender Funktionalität:
 - LDIF-Dateien mit dem Typ "CA" werden hoch priorisiert und möglichst sofort behandelt.
 - LDIF-Dateien mit dem Typ "EE" und Umfang "diff" erhalten eine mittlere Priorität.
 - LDIF-Dateien mit dem Typ "EE" und Umfang "full" erhalten eine niedrige Priorität.

-
- Es darf zu einem Zeitpunkt nur eine Datei eines Subtrees des Austausch-DIT bearbeitet werden, andernfalls können Probleme bei der Prozess-Synchronisation auftreten. Die Prüfung auf die Subtree-Eigenschaft muss berücksichtigen, dass "höhere" und "tiefere" Wurzelknoten verwendet werden können und im Laufe der Zeit durch Änderungen an der Konfiguration in den Domänen andere Zusammensetzungen von LDIF-Dateien ergeben können. Der Vergleich muss also anhand jeweiligen A-DIT ("EE_A-DIT-DN-root" bzw. "CA_Subject_DN_root") und nicht des Dateinamens erfolgen.
 - Wenn mehrere Dateien für den gleichen A-DIT mit unterschiedlichem Erstellungsdatum vorliegen, sollte die jüngste zuerst bearbeitet werden. Das stellt für CA-Entries sicher, dass auch beim Wiederaufsetzen die aktuellste verfügbare Sperrliste eingestellt wird. Ältere Updates werden im Rahmen der Aktualisierung der Entries erkannt.

Der Scheduler ist gegenwärtig in Schritt #10 vorgesehen. Er kann auch an andere Stellen verschoben oder ausgegliedert werden, bspw. indem eine Priorisierung von Prozessen mit Hilfe des Betriebssystems erfolgt. Der Scheduler sollte jedoch auch für den Aktualisierungsprozess zur Domäne enthalten sein.

- Das direkte Kopieren der konsistenten LDIF-Datei an den Austauschdienst scheint den einfachsten Übergabe-Mechanismus zu bieten. Im Rahmen der Implementierung sollten aber noch die möglichen Fehlerfälle analysiert und eine geeignete Strategie zur Behandlung festgelegt werden. Der Aufruf des Kontrollprozesses beim Austauschdienst mit dem Dateinamen dient dann nur noch dazu, auf der Seite des Austauschdienstes bei Bedarf die Dateien "aufzuräumen".
- **Sicherheit der Übertragung zum Austauschdienst:** Für die Übertragung der Dateien zwischen den beiden Diensten ist mindestens das Sicherheitsniveau zu realisieren, das auch für die Übertragung von den Domänen an den VDV gefordert ist. Die konkret zu realisierenden Sicherheitsmaßnahmen

hängen von der Verteilung der Dienste und den Bedingungen im Rechenzentrum ab.

Nr.	Funktionalität und Bedingungen	Verzweigung
1	(Aufruf mit LDIF_File, Domain_Control_File) Lese aus Konfigurationsdatei: • Local_Directory-Flag	
2	Lese: • LF_Version := LDIF_File.Version	
2.1	➤ case: LF_Version UNGLEICH "LDIF_for_VDV.01" unzulässige Version der LDIF-Datei Prozess beenden gemäß Fehlerbehandlung	schwerer Fehler
3	Lese • LF_Status := LDIF_File.Bearbeitungsstatus	
3.1	➤ case: LF_Status UNGLEICH "convtd" Status der LDIF-Datei stimmt nicht Prozess beenden gemäß Fehlerbehandlung	schwerer Fehler
4	(Verzweigung Ablauf VDV / Domäne) Überprüfe Local_Directory-Flag	
4.1	➤ case: Local_Directory-Flag = TRUE weiter bei #10 (ist Scheduler)	weiter #10
5	Lese: • DCF_Version := Domain_Control_File.Version	
5.1	➤ case: DCF_Version UNGLEICH "DCF_VDV.01" Fehler in Domain_Control_File Prozess beenden gemäß Fehlerbehandlung	schwerer Fehler
6	Lese • DCF_Domain:= Domain_Control_File.Domain_Name • LF_Domain := Domäne	
6.1	➤ case: DCF_Domain UNGLEICH LF_Domain Domänen-Name stimmt nicht überein Prozess beenden gemäß Fehlerbehandlung	schwerer Fehler
7	Lese • LF_Type := LDIF_File.Typkennzeichen	
7.1	➤ case: LF_type := "EE" dann: bestimme LF_A-DIT-subtree := EE_A-DIT-DN-root	
7.2	➤ case: LF_type := "CA" dann: bestimme LF_A-DIT-subtree := CA_Subject_DN_root	
7.3	➤ else: Entry-Typ fehlt oder wird nicht unterstützt Prozess beenden gemäß Fehlerbehandlung	schwerer Fehler
8	Lese • DCF_permitted_subtrees:= Domain_Control_File.permitted_subtrees	
8.1	➤ case: LF_A-DIT-subtree NICHT Subtree AUS Liste DCF_permitted_subtrees Unzulässiger Subtree für Austausch-DIT Prozess beenden gemäß Fehlerbehandlung	schwerer Fehler

Nr.	Funktionalität und Bedingungen	Verzweigung
9	(alle Konsistenzbedingungen sind erfüllt) Datei an Austauschdienst übergeben: <ul style="list-style-type: none"> • Kopiere LDIF_File in File_Location_AD • Schreibe Meldung in Log_File • Aufruf von "Dateiverwaltung Austauschdienst (Name des LDIF_File)" 	
9.1	<ul style="list-style-type: none"> ➤ case: kopieren oder Aufruf nicht erfolgreich melde schweren Fehler an Monitoring (qualifizierte Meldung mit Prozesskennung) schreibe qualifizierte Meldung in Übersichts-Log weiter bei nächsten Schritt 	weiter bei nächsten Schritt
10	(Schedule der Dateien organisieren) Organisiere Aufruf von Prozessabschnitt "Upload (LDIF_File)" gemäß Vorgaben für den Scheduler (siehe Hinweise zur Implementierung)	Prozessabschnitt "Upload"
10.1	<ul style="list-style-type: none"> ➤ case: Aufruf nicht erfolgreich melde schweren Fehler an Monitoring (qualifizierte Meldung mit Prozesskennung) Prozess beenden gemäß Fehlerbehandlung 	schwerer Fehler

Tabelle 31: Prozess-Schritte der Konsistenzprüfung beim VDV

D.4.5.2 Prozessabschnitt "Upload"

Der Prozessabschnitt "Upload" trägt die Änderungen aus einer LDIF-Datei in den Austausch-DIT des Verzeichnisdienstes ein (VDV oder lokaler Verzeichnisdienst).

Der Aufruf erfolgt mit Übergabe des Namens des LDIF-Files.

Bei der Aktualisierung werden folgende Regeln berücksichtigt.

- Es erfolgt für jeden Entry aus der LDIF-Datei eine Überprüfung, ob sie im Bereich der Namenswurzel aus dem Datei-Header liegt. Entries die diese Bedingung nicht erfüllen, werden ignoriert. Dies gilt bspw. auch, wenn die Namenswurzeln der Domäne im Austausch-DIT für Teilnehmer (o=) und CA-Entries (ou=) noch nicht angelegt wurden. Dadurch werden in Verbindung mit der ersten Konsistenz-Prüfung beim Dateieingang domänenübergreifende Angriffe gewehrt.
- ou-Knoten für Teilnehmer-Entries werden angelegt
- Für lokale Verzeichnisdienste von Domänen kann eine Namenswurzelersetzung vorgenommen werden.

-
- Es werden nur Entries aktualisiert, deren lastModified neuer als das im Directory ist. Bei gleichem lastModified wird der Entry aktualisiert, wenn der Erzeugungszeitpunkt der LDIF-Datei nach lastModified liegt (wegen möglicher Prozess-Überschneidungen beim Erzeugen der LDIF-Datei).
 - Konsistent mit den Regeln für die Löschung von Entries darf der "changetype:delete" in LDIF-Dateien nur für Teilnehmer-Entries enthalten sein. Löschbefehle für CA- und CDP-Entries führen zu einem Fehler und werden ignoriert.
 - Es wird ein Zähler für die Zahl der aktualisierten Entries geführt. Dieser zählt alle erfolgreichen Löschungen und geänderten Entries mit Ausnahme der Entries, bei denen nur der ActiveIndicator geändert wurde.
 - Es wird ein Zähler für Fehler geführt. Dieser gibt aber die Zahl der Entries an, die nicht der Namenswurzel entsprachen, als CA- oder CDP-Entry gelöscht werden sollten, als CA- oder CDP-Entry oder unter einem nicht existierenden ou-Knoten angelegt werden sollten. Andere Fehler, z. B. das Löschen nicht existierender Entries, werden nicht gezählt.
 - Nach Abschluss eines Updates mit dem Typ "CA" wird der Prozess zur Aktualisierung der HTTP-Seiten für CA-Informationen angestoßen. (Hinweise zum Prozess finden sich im Haupt-Dokument, die Spezifikation ist zurückgestellt.)
 - Nach Abschluss eines Updates mit dem Typ "CA" wird der Prozess zur Aktualisierung des Veröffentlichungsdienst angestoßen. Dieser Prozess muss auch die Aktualisierung der dem Veröffentlichungsdienst zugeordneten HTTP-Seiten veranlassen, wenn die Aktualisierung durchgeführt wurde. (Hinweise zum Prozess finden sich im Haupt-Dokument, die Spezifikation ist zurückgestellt.)
 - Im Falle eines Vollabgleichs werden alle Entries, die in der LDIF-Datei enthalten sind, als "aktiv" gekennzeichnet. Teilnehmer-Entries, die längere Zeit nicht aktiv waren, werden anschließend automatisch gelöscht. Dabei kann die Zeitspanne anhand von zwei Parametern eingestellt werden: einmal

für die Entries aus dem Subtree der LDIF-Datei und zum andern für den gesamten Austausch-DIT.

Notationen:

- "LF_" leitet Variablen ein, die aus LDIF_File gelesen werden.
- LF_Entry ist der unter Bearbeitung befindliche Entry aus dem LDIF_File, Dir_Entry ist der für den gleichen DIT-DN schon existierende Entry aus dem Verzeichnisdienst. Soweit Attribute in der Variablen LF_Entry (z. B. realisierbar als Array of Strings) noch nicht existieren, werden sie automatisch angelegt, wenn sie erstmalig in der Prozessbeschreibung angesprochen werden.
- Attribute eines Entries werden aus der jeweiligen Entry-Variablen durch ".[Kürzel]" separiert. Entsprechend werden die Bestandteile aus einem Distinguished Name mit "DN.[Kürzel]" angesprochen. Da jedes Attribut im DIT-DN des Austausch-DIT nur einmal vorkommt, ist die Adressierung eindeutig. Achtung: durch die Namenswurzel-Ersetzung muss jeweils das erste Attribut des Typs im DN von unten verwendet werden.

Hinweise zur Implementierung:

- Jede LDIF-Datei kann nur einen "o-" Bereich des Austausch-DIT bearbeiten. Der o-Bereich muss bereits existieren (wird im Rahmen des Beitrittsverfahrens angelegt):
- Einige Operationen aus der "Konsistenzprüfung" werden zur Initialisierung von Upload wiederholt. Abhängig von der Organisation des Aufrufs könnten die Parameter aber auch übergeben werden.
- Schema-Fehler dürften nicht auftreten, da die Entries in den LDIF-Dateien durch den Teilprozess in der Domäne erzeugt werden. Möglich wäre allerdings Fehler, die durch zusätzliche Eingriffe entstehen. Es ist jedoch ausreichend, die Schema-Konformität bezüglich der Datenquelle implizit beim Anlegen oder Ändern von Entries zu prüfen. Wird ein Fehler festgestellt Wenn dennoch Schema-Fehler auftreten, wird im Falle neuer Entries der

eingestellt Entry wieder gelöscht. Im Falle von bereits bestehenden Entries wird der vorherige Zustand wiederhergestellt.

- Der Prozess verwendet eine Liste der existierenden ou-Knoten zu Optimierung: List_of_existing_ous im Format array of DIT-DNs. Diese Liste wird entsprechend dem Bedarf aufgefüllt.
- Sollte der Zugriff auf das Directory nicht möglich sein, führt dies bei allen entsprechende Operationen zu einem schweren Fehler gemäß Fehlerbehandlung.

Nr.	Funktionalität und Bedingungen	Verzweigung
1	Setzen von Prozess-Variablen <ul style="list-style-type: none"> • Setze Warning_Counter := 0 • Setze Error_Counter:= 0 • Setze NumberOfEntries := 0 • Setze NumberOfUpdatedEntries := 0 • Setze NumberOfActiveOnlyEntries := 0 • Setze List_of_existing_ous := LEER • AP-Server_StartTime := Systemzeit des Servers, auf dem der Teilprozess abläuft Initialisierungen aus Konfigurations-Datei <ul style="list-style-type: none"> • Lese Log- und Monitoringparameter • Lese Local_Directory-Flag • Lese Local_EE_A-DIT-DN-root • Local_Dir_Constraints • Local_CA_Subject_DN_root • Bestimme die Adresse von Dir_Server aus DNS_Target_Dir und Port_Target_Dir • Lese UserID_for_Upload • Lese Password_for_Upload Initialisierung aus Domain_Control_File <ul style="list-style-type: none"> • Lese VDV-HTTP-DomainCASite 	
1.1	<ul style="list-style-type: none"> ➤ case: Fehlerbehandlung (Tests auf Vollständigkeit) je nach Erfordernis der VDV und Domänen-Parameter ergänzen 	
2	(Dateioperationen und Initialisierungen) <ul style="list-style-type: none"> • Bilde Dateinamen für Log_File gemäß Regel • Erzeuge Start-Eintrag in Log_File Lese LF_Header aus LDIF_File <ul style="list-style-type: none"> • LF_Scope := LF_Header.Datenumfang • LF_Type := LF_Header.Typkennzeichen • LF_creationTime := LF_Header.Erzeugungszeit 	
2.1	<ul style="list-style-type: none"> ➤ case: LF_type := "EE" dann: bestimme LF_A-DIT-subtree := EE_A-DIT-DN-root 	
2.2	<ul style="list-style-type: none"> ➤ case: LF_type := "CA" dann: bestimme LF_A-DIT-subtree := CA_Subject_DN_root 	

Nr.	Funktionalität und Bedingungen	Verzweigung
3	(Überprüfe, ob Domänen-Wurzel im Austausch-DIT verfügbar, ggf. Substitution der Namenswurzel) <ul style="list-style-type: none"> • setze Test-DN := LF_A-DIT-subtree • Wenn Local_Directory-Flag=true und Local_EE_A-DIT-DN-root NICHT LEER dann: ersetzen in LF_Entry.dn den Anteil "c=de" durch Local_EE_A-DIT-DN-root • Streiche aus Test-DN alle unteren Namensbestandteile, bis nur noch ein "o=" enthalten ist. • Teste, ob Test-DN in Dir_Server existiert 	
3.1	<ul style="list-style-type: none"> ➤ case: Test-DN existiert nicht Prozess beenden gemäß Fehlerbehandlung 	schwerer Fehler
4	Positioniere in LDIF_File vor dem ersten "echten" Entry (überspringe restliche Header-Information)	
5	Lese nächsten Entry <ul style="list-style-type: none"> • LF_Entry := Entry aus LDIF_File 	
5.1	<ul style="list-style-type: none"> ➤ case: kein weitere Entry weiter bei #19 (Prozessabschluss) 	weiter bei #19
6	<ul style="list-style-type: none"> • inkrementiere NumberOfEntries • Teste, ob Namensbereich zulässig 	
6.1	<ul style="list-style-type: none"> ➤ case: LF_Entry.DN ist NICHT AUS LF_A-DIT-subtree Fehler gemäß Fehlerbehandlung inkrementiere Error_Counter Überspringe Entry Weiter mit nächsten Entry, #5 	weiter bei #5
7	(bei upload in Domäne: Namenswurzel ersetzen) <ul style="list-style-type: none"> • Wenn Local_Directory-Flag=true UND Local_EE_A-DIT-DN-root NICHT LEER dann: ersetzen in LF_Entry.dn den Anteil "c=de" durch Local_EE_A-DIT-DN-root 	
8	(setze ActiveIndicator; abfragen, ob Entry im Directory existiert, Operation abhängig von changetype) <ul style="list-style-type: none"> • setze LF_Entry.vDKActiveIndicator := LF_creationTime • Lese Dir_Entry für LF_Entry.dn aus Dir_Server 	
8.1	<ul style="list-style-type: none"> ➤ case: (Dir_Entry existiert) UND (LF_entry.changetype IST "add") weiter bei #15 	weiter bei #15
8.2	<ul style="list-style-type: none"> ➤ case: case: (Dir_Entry existiert) UND (LF_entry.changetype IST "delete") UND (LF_Type IST "EE") UND Dir_Entry.lastModifiedSource führe Löschung in Dir_Server für LF_Entry.DN aus inkrementiere NumberOfUpdatedEntries weiter bei #5 (nächster Entry) 	weiter bei #5
8.3	<ul style="list-style-type: none"> ➤ case: LF_entry.changetype IST "delete" UND LF_Type IST "CA" Fehler gemäß Fehlerbehandlung (keine automatische Löschung von CA oder CDP) inkrementiere Error_Counter Überspringe diesen Entry Weiter mit nächsten Entry, #5 	weiter bei #5
8.4	<ul style="list-style-type: none"> ➤ Else: (entspricht (Dir_Entry existiert nicht) UND (LF_entry.changetype IST "add")) Weiter mit nächstem Schritt 	weiter mit nächstem Schritt

Nr.	Funktionalität und Bedingungen	Verzweigung
9 9.1	(Dir_Entry existierte nicht: neuen Entry anlegen, ggf. auch ou-Knoten) • Teste, ob LF_Entry.DN.ou in List_of_existing_ous enthalten ist. ➤ case: LF_Entry.DN.ou IST IN List_of_existing_ous weiter bei #13	weiter bei #13
10 10.1 10.2 10.3	Teste, ob der Knoten zu LF_Entry.DN.ou im Austausch-DIT im Dir_Server existiert ➤ case: Knoten existiert weiter bei #13 ➤ case: Knoten existiert nicht und LF_Type IST "EE" weiter bei nächstem Schritt ➤ case: Knoten existiert nicht und LF_Type IST "CA" Fehler gemäß Fehlerbehandlung (keine automatisches Anlegen der Domänen-Wurzel für CA-Entries) inkrementiere Error_Counter Überspringe diesen Entry Weiter mit nächsten Entry, #5	weiter bei #13 weiter bei nächstem Schritt weiter mit , #5
11	(ou-Knoten existiert nicht) • lege Knoten zu LF_Entry.DN.ou im Austausch-DIT im Dir_Server an (Hinweis: berücksichtigen, dass die Namenswurzel-Ersetzung in LF_Entry.dn verwendet wird.)	
12	(ou Knoten wurde erzeugt oder existierte, war aber nicht in Liste) • erweitere List_of_existing_ous um LF_Entry.DN.ou	
13 13.1 13.2 13.3	(ou Knoten existiert und ist in Liste: erzeuge neuen Entry) • lege Knoten zu LF_Entry.DN mit LDAP-add im Austausch-DIT im Dir_Server an (alle Attribute aus LF_Entry verwenden) ➤ case: LDAP-modify war erfolgreich inkrementiere NumberOfUpdatedEntries weiter bei #5 (nächster Entry) ➤ case: LDAP-modify war wegen Schema-Fehler NICHT erfolgreich inkrementiere Error_Counter weiter mit nächsten Schritt ➤ else: weitere Fehlerbehandlung, falls notwendig, anschließend weiter bei #5 (nächster Entry)	weiter bei #5 weiter bei #5
14	(LDAP-Add erzeugte Schema-Fehler) • lösche Entry LF_Entry.dn in Dir_Server • anschließend weiter bei #5 (nächster Entry)	weiter bei #5
15 15.1 15.2	(LF_Entry.DN existiert bereits in Dir_Server; Beginn von "Entry ändern") Teste, ob Entry aus LDIF_File "jünger" als Entry in Directory ➤ case: LF_Entry.vDKLastModifiedSource > DIR_Entry.vDKLastModifiedSource: weiter bei #16 (aktualisiere Entry) ➤ case: LF_Entry.vDKLastModifiedSource = DIR_Entry.vDKLastModifiedSource UND LF_creationTime > DIR_Entry.vDKLastModifiedSource weiter bei #16 (aktualisiere Entry)	weiter bei #16 weiter bei #16

Nr.	Funktionalität und Bedingungen	Verzweigung
15.3	<ul style="list-style-type: none"> ➤ case: LF_Entry.vDKLastModifiedSource < DIR_Entry.vDKLastModifiedSource UND scope IST "full": (älterer Entry, nur ActiveIndicator setzen) weiter mit #18 	weiter mit #18
15.4	<ul style="list-style-type: none"> ➤ else: LF_Entry.vDKLastModifiedSource < DIR_Entry.vDKLastModifiedSource: (älterer Entry im Diff.-Abgleich, überspringen) weiter bei #5 (nächster Entry) 	weiter bei #5
16	<p>(Entry ist zu aktualisieren)</p> <ul style="list-style-type: none"> • Generiere einen LDAP-modify Befehl durch Vergleich von LF_Entry und Dir_Entry so, dass nach der Modifikation genau die Attribute aus LF_Entry im Directory gespeichert sind. (Hinweis: auch bei multivalued-Attributen dürfen nach der Operation nur die neuen im Entry stehen, die in LF_Entry enthalten sind. Die Modify-Operation muss modular durchgeführt werden) • Führe LDAP-modify durch 	
16.1	<ul style="list-style-type: none"> ➤ case: LDAP-modify war erfolgreich inkrementiere NumberOfUpdatedEntries weiter bei #5 (nächster Entry) 	weiter bei #5
16.2	<ul style="list-style-type: none"> ➤ case: LDAP-modify war wegen Schema-Fehler NICHT erfolgreich inkrementiere Error_Counter weiter mit nächsten Schritt 	
16.3	<ul style="list-style-type: none"> ➤ else: weitere Fehlerbehandlung, falls notwendig, anschließend weiter bei #5 (nächster Entry) 	weiter bei #5
17	<p>(Änderung wg. Schema-Fehler rückgängig machen)</p> <ul style="list-style-type: none"> • Generiere einen LDAP-modify Befehl durch Vergleich von LF_Entry und Dir_Entry so, dass nach der Modifikation genau die Attribute aus Dir_Entry im Directory gespeichert sind. (Hinweis: ggf. erst aktuellen Stand im Directory feststellen, da Zustand wg. Schema-Fehler nicht konsistent mit LF_Entry. Auch bei multivalued-Attributen dürfen nach der Operation nur die neuen im Entry stehen, die in Dir_Entry enthalten sind.) • Führe LDAP-modify durch • anschließend weiter bei #5 (nächster Entry) 	
18	<p>(Update des ActiveIndicator bei Vollabgleich, nur nötig, falls der Entry nicht bereits mit jüngerem Datum aktualisiert wurde)</p> <p>Teste, ob Update erforderlich</p>	weiter bei #5
18.1	<ul style="list-style-type: none"> ➤ case: Dir_Entry.vDKLastModifiedSource < LF_Entry.vDKActiveIndicator: * Generiere einen LDAP-modify Befehl so, dass Entry im Dir_Server nur verändert wird das Attribut vDKActiveIndicator := LF_Entry.vDKActiveIndicator Alle anderen Attribute bleiben erhalten * Führe LDAP-modify durch * inkrementiere NumberOfActiveOnlyEntries anschließend weiter bei #5 (nächster Entry) 	
18.2	<ul style="list-style-type: none"> ➤ else: weiter bei #5 (nächster Entry) 	weiter bei #5

Nr.	Funktionalität und Bedingungen	Verzweigung
19	(Abschluss des Prozesses nach Bearbeitung aller Entries) Auswertung und Warnungen bei kritischer Laufzeit des gesamten Aktualisierungsprozesses <ul style="list-style-type: none"> • Bestimme process-duration := SystemTime des Servers - AP-Server_StartTime • Schreibe SystemTime und process-duration in Log 	
19.1	<ul style="list-style-type: none"> ➤ case: LF_Type IST "EE" UND (SystemTime > LF_creationTime + update_delayHours_EE_alarm) direkte Meldung an Monitoring mit qualifizierter Ursache Fehlerbehandlung für "Fehler" und Eintrag in Übersicht-Log weiter bei #20 	weiter #20
19.2	<ul style="list-style-type: none"> ➤ case: LF_Type IST "EE" UND (SystemTime > LF_creationTime + update_delayHours_EE_warning) Fehlerbehandlung für "Warnung" und Eintrag in Übersicht-Log weiter bei #20 	weiter #20
19.3	<ul style="list-style-type: none"> ➤ case: LF_Type IST "CA" UND (SystemTime > LF_creationTime + update_delayHours_CA_alarm) direkte Meldung an Monitoring mit qualifizierter Ursache Fehlerbehandlung für "Fehler" und Eintrag in Übersicht-Log weiter bei #20 	weiter #20
19.4	<ul style="list-style-type: none"> ➤ case: LF_Type IST "CA" UND (SystemTime > LF_creationTime + update_delayHours_CA_warning) Fehlerbehandlung für "Warnung" und Eintrag in Übersicht-Log weiter bei #20 	weiter #20
20	Log und Meldungen abschließen <ul style="list-style-type: none"> • Erstelle zusammenfassende Meldung gemäss "Fehlerbehandlung" und "Monitoring" (unter Berücksichtigung von NumberOfEntries, NumberOfUpdatedEntries, NumberOfActiveOnlyEntries, Warning_Counter und Error_Counter, process-duration) • Schreibe zusammenfassende Meldung in Log_File • schreibe zusammenfassende Meldung in Übersichts-Log • Schliesse offene Dateien 	
20.1	<ul style="list-style-type: none"> ➤ case: Eine Aktion nicht erfolgreich <ul style="list-style-type: none"> * melde schweren Fehler an Monitoring * Schreibe Fehler-Meldung in Log_File * schreibe Fehler-Meldung in Übersichts-Log weiter mit nächstem Schritt 	weiter mit nächstem Schritt
21	(Aktualisierungsprozess für Veröffentlichungsdienst aufrufen, Übergabe aller ggf. erforderlichen Parameter) <ul style="list-style-type: none"> • rufe auf "Aktualisierung VöD (LF_Scope, LF_Type, LF_creationTime, LF_A-DIT-subtree, VDV-HTTP-DomainCASite) 	
21.1	<ul style="list-style-type: none"> ➤ case: Aufruf nicht erfolgreich <ul style="list-style-type: none"> * melde schweren Fehler an Monitoring * Schreibe Fehler-Meldung in Log_File * schreibe Fehler-Meldung in Übersichts-Log weiter mit nächstem Schritt 	weiter mit nächstem Schritt
22	Aktualisierungsprozess für HTTP-Seite aufrufen, wenn CA	
22.1	<ul style="list-style-type: none"> ➤ case: LF_Type IST NICHT "CA": weiter mit #24 	weiter mit #24

Nr.	Funktionalität und Bedingungen	Verzweigung
23	(war CA-Update, HTTP aktualisieren) rufe auf "Aktualisierung VDV-HTTP-Seiten (LF_creationTime, LF_A-DIT-subtree, VDV-HTTP-DomainCASite)	
23.1	<ul style="list-style-type: none"> ➤ case: Aufruf nicht erfolgreich * melde schweren Fehler an Monitoring * Schreibe Fehler-Meldung in Log_File * schreibe Fehler-Meldung in Übersichts-Log weiter mit nächstem Schritt	weiter mit nächstem Schritt
24	(Verzweigung für besondere Aktionen bei "Vollabgleich") <ul style="list-style-type: none"> • verlege LDIF_File in Archiv • verlege zugehöriges Log-File ins Log Archive • Teste LF_Scope 	
24.1	<ul style="list-style-type: none"> ➤ case: LF_Scope ist "diff": beende Prozess regulär 	Beende Prozess
25	(scope ist "full": Vollabgleich) <ul style="list-style-type: none"> • falls im LDIF-Datei-Archiv Dateien vorhanden sind, die älter als Archival_Period_Days Tage sind: lösche diese Dateien • falls im Log-Archiv Dateien vorhanden sind, die älter als Archival_Period_Days Tage sind, generiere E-Mail an audit_mail_address mit Anzahl dieser Dateien, verbrauchtem Speicherplatz und verfügbarem Speicherplatz. 	
25.1	<ul style="list-style-type: none"> ➤ case: Eine der Aktionen nicht erfolgreich * direkte Fehler-Meldung (mit qualifizierter Ursache) an das Monitoring * schreibe Fehler-Meldung in Übersichts-Log 	
26	(Löschung von inaktiven Entries nach Vollabgleich nur für Typ EE)	
26.1	<ul style="list-style-type: none"> ➤ case: LF_Type IST "CA": beende Prozess regulär 	beende Prozess regulär
27	fahre fort mit Prozessabschnitt "Vorbereitung Löschung Inaktive Entries"	nächster Prozessabschnitt

Tabelle 32: Prozess-Schritte für den Upload von Entries

D.4.5.3 Prozessabschnitt "Löschung Inaktive Entries"

Der Prozessabschnitt dient zur Identifikation inaktiver Entries. Es sucht dazu Entries aus dem Austausch-DIT, deren ActiveIndicator längere Zeit nicht aktualisiert wurde. Auf der Basis des Suchergebnisses erzeugt er eine LDIF-Datei im Format des Verzeichnisdienstkonzepts und stößt den Aktualisierungsprozess mit dieser neuen Datei an.

Sofern die Obergrenzen für automatische Löschungen überschritten wurden, wird eine Meldung an das Monitoring erzeugt und die LDIF-Datei wird nicht in das Archiv verlegt.

Hinweise zur Implementierung:

- Dem Prozess stehen alle Parameter aus dem Prozessabschnitt "update" zur Verfügung. Andernfalls müssen sie entsprechend gebildet werden.
- Im Rahmen der Implementierung sollte geprüft werden, ob für CA- und CDP-Entries eine Warnung erzeugt werden soll, wenn sie eine bestimmte Zeit inaktiv sind.
- Im Rahmen der Implementierung sollte außerdem ein Mechanismus realisiert werden, mit dem ou-Entries im Austausch-DIT gelöscht werden, wenn sie keine nachgeordneten Teilnehmer-Entries mehr haben.

Nr.	Funktionalität und Bedingungen	Verzweigung
1	<p>Setzen globaler Variablen</p> <ul style="list-style-type: none"> • Setze Warning_Counter := 0 • Setze Error_Counter:= 0 • Setze NumberOfDeletedEntries := 0 • AP-Server_StartTime := Systemzeit des Servers, auf dem der Teilprozess abläuft <p>Lese aus Konfigurationsdatei</p> <ul style="list-style-type: none"> • delete_subtree-entry-after-inactive-days • delete_ADIT-entry-after-inactive-days • delete_not_in_Subtree_on_percent • delete_not_in_ADIT-on_number <p>LDIF-Datei vorbereiten: Bilde Dateinamen für Working_File gemäß Regel mit</p> <ul style="list-style-type: none"> • alle Werte aus Name von LDIF_File außer: • Datenumfang ist "diff" • Status ist "genDeIS" <p>Bilde Dateinamen für Log_File gemäß Regel</p> <ul style="list-style-type: none"> • Erzeuge Start-Eintrag in Log_File 	
1.1	<ul style="list-style-type: none"> ➤ case: Fehler in der Dateivorbereitung Prozess beenden gemäß Fehlerbehandlung mit schwerem Fehler 	schwerem Fehler
2	Erzeuge Start-Eintrag in Übersichts-Log	
2.1	<ul style="list-style-type: none"> ➤ case: delete_subtree-entry-after-inactive-days IST 0 weiter bei #8 	weiter bei #8
3	<p>Konstruktion des 1. Suchfilters (auf dem Subtree für den Vollabgleich):</p> <ul style="list-style-type: none"> • setze DN_SelectedSubTree := LF_A-DIT-subtree • Wenn Local_Directory-Flag=true UND Local_EE_A-DIT-DN-root NICHT LEER DANN: dann: ersetzen in DN_SelectedSubTree den Anteil "c=de" durch Local_EE_A-DIT-DN-root • Searchfilter := alle Entries aus DN_SelectedSubTree mit (ENTHÄLT objectclass="vDKPerson" UND (vDKActiveIndicator < (LF_creationTime - delete_subtree-entry-after-inactive-days))) 	
3.1	<ul style="list-style-type: none"> ➤ case: delete_ADIT-entry-after-inactive-days IST 0 weiter mit #8 	

Nr.	Funktionalität und Bedingungen	Verzweigung
4	(Abfrage der Entries:) <ul style="list-style-type: none"> • Schreibe Suchfilter in Log_File • LDAP-Search in Domain_Dir_Server mit SearchFilter 	
5	Teste Suchergebnis	
5.1	<ul style="list-style-type: none"> ➤ case: Suchergebnis war LEER (kein Entry gefunden: der Prozesslauf kann abgeschlossen werden. weiter bei #8 	weiter bei #8
5.2	<ul style="list-style-type: none"> ➤ case: ist nicht LEER, aber enthielt neben Entries auch Fehlermeldungen: <ul style="list-style-type: none"> * setze Error_Counter auf Anzahl der Fehler; * schreibe Log-Eintrag * weiter mit nächstem Schritt 	weiter mit nächstem Schritt
6	Schreibe Suchergebnis in Working_File (Optional: DN's der Entries wären ausreichend. Ergänzung von "changetype:delete" würde weitgehende Konformität mit VDK-LDIF-Anforderungen ergeben)	
6.1	<ul style="list-style-type: none"> ➤ case: (Verhältnis von Anzahl von Entries im Subtree / Anzahl Entries im working_File) > delete_not_in_Subtree_on_percent Meldung an Monitoring über zu viele zu löschende Entries im Subtree mit Angabe des Namens von Working_File weiter bei #8 	weiter bei #8
7	Für jeden Entry aus Working_File <ul style="list-style-type: none"> • LDAP-delete Entry.DN • inkrementiere NumberOfDeletedEntries Nach Bearbeitung aller Entries: <ul style="list-style-type: none"> • verlege LDIF_File in Archiv 	
8	2. LDIF-Datei vorbereiten: Bilde Dateinamen für Working_File gemäß Regel mit <ul style="list-style-type: none"> • alle Werte aus Name von LDIF_File außer: • Datenumfang ist "diff" • Status ist "genDeIA" Bilde Dateinamen für Log_File gemäß Regel <ul style="list-style-type: none"> • Erzeuge Start-Eintrag in Log_File 	
8.1	<ul style="list-style-type: none"> ➤ case: Fehler in der Dateivorbereitung Prozess beenden gemäß Fehlerbehandlung mit schwerem Fehler 	schwerer Fehler
8.2	<ul style="list-style-type: none"> ➤ case: delete_ADIT-entry-after-inactive-days IST 0 weiter mit #14 	weiter mit #14

Nr.	Funktionalität und Bedingungen	Verzweigung
9	Konstruktion des 2. Suchfilters (auf dem gesamten A-DIT für den Vollabgleich): <ul style="list-style-type: none"> • Wenn Local_Directory-Flag=true UND Local_EE_A-DIT-DN-root NICHT LEER DANN: setze DN_ADIT := Local_EE_A-DIT-DN-root SONST setze DN_ADIT := "c=de" Searchfilter := Searchfilter ODER alle Entries aus DN_ADIT mit (ENTHÄLT objectclass="vDKPerson" UND (vDKActiveIndicator < (LF_creationTime - delete_ADIT-entry-after-inactive-days)))	
10	(Abfrage der Entries:) <ul style="list-style-type: none"> • Schreibe Suchfilter in Log_File • LDAP-Search in Domain_Dir_Server mit SearchFilter 	
11	Teste Suchergebnis	
11.1	<ul style="list-style-type: none"> ➤ case: Suchergebnis war LEER (kein Entry gefunden: der Prozesslauf kann abgeschlossen werden. weiter bei #14 	weiter bei #14
11.2	<ul style="list-style-type: none"> ➤ case: ist nicht LEER, aber enthielt neben Entries auch Fehlermeldungen: <ul style="list-style-type: none"> * erhöhe Error_Counter um Anzahl; * schreibe Log-Eintrag * weiter mit nächstem Schritt 	weiter mit nächstem Schritt
12	Schreibe Suchergebnis in Working_File (Optional: DN's der Entries wären ausreichend. Ergänzung von "changetype:delete" würde weitgehende Konformität mit VDK-LDIF-Anforderungen ergeben)	
12.1	<ul style="list-style-type: none"> ➤ case: (Anzahl der Entries im working_File) > delete_not_in_ADIT-on_number: Meldung an Monitoring über zu viele zu löschende Entries im Austausch-DIT mit Angabe des Namens von Working_File weiter bei #14 	weiter bei #14
13	Für jeden Entry aus Working_File <ul style="list-style-type: none"> • LDAP-delete Entry.DN • inkrementiere NumberOfDeletedEntries Nach Bearbeitung aller Entries: <ul style="list-style-type: none"> • verlege LDIF_File in Archiv 	
14	Log und Meldungen abschließen <ul style="list-style-type: none"> • Bestimme process-duration := SystemTime des Servers - AP-Server_StartTime • Erstelle zusammenfassende Meldung gemäss "Fehlerbehandlung" und "Monitoring" (unter Berücksichtigung von NumberOfDeletedEntries, Warning_Counter und Error_Counter, SystemTime, process-duration) • Schreibe zusammenfassende Meldung in Log_File • schreibe zusammenfassende Meldung in Übersichts-Log • Schliesse offene Dateien • verlege beide zugehörigen Log-Files ins Log Archive 	
15	Beende Prozess regulär	

Tabelle 33: Prozess-Schritte für die Identifikation und Löschung inaktiver Entries

Anhang E: Spezifikation "Aktualisierungsprozess Austauschdienst"

In diesem Anhang wird der Aktualisierungsprozess des Austauschdienstes spezifiziert. Der Austauschdienst muss je Entry-Gruppe, die von einer Domäne angeliefert wird, die aktuellste Generation von LDIF-Dateien bereitstellen.

Jede **Entry-Gruppe** ist gekennzeichnet durch den Anfang des Dateinamens der LDIF-Dateien, in denen Aktualisierungsinformationen zu dieser Entry-Gruppe geliefert werden. Die relevanten Namensbestandteile der LDIF-Dateien sind "[Domänen-Kennzeichen]-[TypKennzeichen]-[VD-Kennzeichen]-[Teilbaum]".

Eine **Generation von LDIF-Dateien** einer Entry-Gruppe besteht aus dem einem Vollabgleich und allen darauf folgenden Differenz-Abgleichen bis zum nächsten Vollabgleich (letztere Datei ist nicht mehr Bestandteil).

Der Aktualisierungsprozess des Austauschdienstes hat in der Ausbaustufe 1 die folgenden Aufgaben:

- Er übernimmt die beim Verzeichnisdienst der Verwaltung eingegangenen LDIF-Dateien. Diese sind bereits der Konsistenzprüfung bezüglich der Urheberschaft und Zulässigkeit des Teilbaums unterzogen.
- Er stellt die LDIF-Datei für den Aktualisierungsprozess zur Domäne zur Verfügung.
- Er archiviert LDIF-Dateien, wenn eine neue Generation begonnen wird.
- Er löscht alte Generationen aus dem Archiv, wenn mehr als 2 Generationen dort abgelegt sind.

Der Aktualisierungsprozess zum Austauschdienst besteht konzeptionell nur aus einem Teilprozess mit einem Prozessabschnitt, der die Dateiverwaltung übernimmt.

Hinweise zur Implementierung:

- Nach der vorliegende Spezifikation kopiert bereits der Teilprozess VDV aus dem Aktualisierungsprozess zum VDV jede relevante LDIF-Datei in das richtige Datei-Verzeichnis (File_Location_AD).
- Der Prozessabschnitt: "Dateiverwaltung Austauschdienst" wird mit dem Namen jeder neuen LDIF-Datei aufgerufen.
- Sofern eine Domäne die Gruppierung von Entries ändert oder ausscheidet, muss die letzte Generation von LDIF-Dateien aus dem Abrufverzeichnis von Hand gelöscht werden.

E.1 Teilprozess Austauschdienst

Die Fehlerbehandlung und das Monitoring erfolgen gemäß der Entwurfsentscheidungen. Der Betreiber des Austauschdienstes muss dafür Sorge tragen, dass die entsprechenden Rollen durch Personal besetzt sind. Die Sicherheitsanforderungen müssen umgesetzt sein, d.h. insbesondere, dass der Teilprozess in einem Bereich konfiguriert und betrieben wird, auf den Unberechtigte keinen Zugriff haben.

E.1.1 Vorbedingungen Teilprozess Austauschdienst

Folgende Vorbedingungen und Annahmen müssen erfüllt sein, damit der Aktualisierungsprozess für den Austauschdienst der Verwaltung auf der Seite der Domäne erfolgreich durchgeführt werden kann:

- Der Teilprozess ist korrekt konfiguriert und kann seine Konfigurationsdatei lesen und schreiben.
- Der Teilprozess kann auf sein Übersichts-Log schreibend zugreifen.
- Zugriff auf die jeweilige LDIF-Datei.
- Das Dateiarchiv ist lesend und schreibend zugreifbar.

E.1.2 Nachbedingungen Teilprozess Austauschdienst

Im Falle eines erfolgreichen Abschlusses des Teilprozesses zum Austauschdienst gelten folgenden Bedingungen:

- Der Aktualisierungsprozess zur Domäne hat sofortigen Zugriff auf jede neue LDIF-Datei.
- Bei Eintreffen einer neuen LDIF-Datei vom Umfang "voll" werden alle vorherigen Generationen mit dem entsprechendem Dateinamen archiviert.
- Im LDIF-Datei-Archiv sind nicht mehr als 2 Generationen einer Entry-Gruppe abgelegt, es sei denn der jeweilige Vollabgleich ist jünger als eine Mindestanzahl von Tagen.

E.1.3 Konfigurationsparameter

Name	Format	Zweck	Anmerkung / Default / Beispiel
minimum_Days_of_archival	Zahl	bestimmt, wie lange eine Dateigeneration mindestens archiviert werden muss, bevor sie automatisch gelöscht werden darf.	
File_Location_LF_Archive	String	Verzeichnis, in dem LDIF-Files archiviert werden.	
Log- und Monitoringparameter (Liste ist im Rahmen der Implementierung zu ergänzen)	wie erforderlich	legen fest, wie Meldungen an das Monitoring übertragen werden, z.B. eine E-Mail-Adresse, das Verzeichnis, in dem die Prozessspezifischen und die Übersichts-Log-Datei zu speichern sind, die Anzahl der aufzubewahrenden Prozess-Log-Dateien und die Anzahl der Einträge im Übersichts-Log.	Implementierungsabhängig, die Parameter können vom Rahmenprozess und vom Teilprozess in der Domäne gemeinsam genutzt werden

Tabelle 34: Konfigurationsparameter des Teilprozesses Austauschdienst

E.1.4 Aufruf des Teilprozesses

Der Prozessabschnitt wird aufgerufen mit

"Dateiverwaltung Austauschdienst (LDIF-File-Name)".

E.1.5 Prozessabschnitte

E.1.5.1 Prozessabschnitt "Dateiverwaltung Austauschdienst"

Der Prozessabschnitt dient dazu, bei Neueingang von LDIF-Dateien bei Bedarf alte Generationen auszulagern. Sofern danach im Archiv danach überflüssige Dateien gespeichert sind, werden diese gelöscht.

Hinweise zur Implementierung:

- Dateien können aus dem Austauschdienst von den Domänen zu beliebigen Zeitpunkten abgerufen werden. Deshalb kann es Überschneidungen zwischen dem Abruf und dem Versuch geben, eine Datei ins Archiv zu verlegen. Diese Überschneidungen sind aber nur in einer Übergangsperiode relevant, da der Aktualisierungsprozess zur Domäne immer nur Dateien der neuesten Generation abrufen.
- Der Prozess benutzt ein Open_Actions_File, in dem alle offenen Aktionen vermerkt werden. Bei jedem Aufruf wird versucht, die Aktionen aus dem Open_Actions_File abzuarbeiten. Können Aktionen beispielsweise wegen Überschneidungen beim Dateizugriff nicht ausgeführt werden, bleiben sie bis zum nächsten Aufruf erhalten.
- Wenn nicht anders angegeben, finden die Tests und Operationen im Abrufverzeichnis des Austauschdienstes statt. (Das Abrufverzeichnis ist das Dateiverzeichnis, aus dem die Domänen mit dem Aktualisierungsprozess zur Domäne die LDIF-Dateien abrufen.)

Nr.	Funktionalität und Bedingungen	Verzweigung
1	Aufruf durch "Dateiverwaltung Austauschdienst (LDIF-File-Name)"	
2	<ul style="list-style-type: none"> • schreibe Meldung zu Aufruf mit LDIF-File-Name in Übersichts-Log • teste, ob LDIF-File-Name ein Vollabgleich 	
2.1	<ul style="list-style-type: none"> ➤ case: LDIF-File-Name ENTHÄLT NICHT "voll" weiter bei #5 	weiter bei #5

Nr.	Funktionalität und Bedingungen	Verzweigung
3	(LDIF-File-Name ist Vollabgleich) <ul style="list-style-type: none"> • Bestimme alle Dateien vorheriger Generationen von LDIF-File-Name im Abrufverzeichnis • Erzeuge im Open_Actions_File für alle identifizierten Verlege-Aktionen in das File_Location_LF_Archive 	
4	Teste, ob Open_Actions_File leer <ul style="list-style-type: none"> ➤ case: Open_Actions_File ist LEER weiter bei #5 	weiter bei #5
5	Für alle offenen Aktionen aus Open_Actions_File <ul style="list-style-type: none"> • führe Aktion aus Nach letzter Aktion: weiter bei #6	
5.2	<ul style="list-style-type: none"> ➤ case: Aktion erfolgreich: <ul style="list-style-type: none"> * schreibe Meldung ins Übersichts-Log * lösche Aktion in Open_Actions_File * weiter bei #5 mit nächster Aktion 	weiter bei #5
5.1	<ul style="list-style-type: none"> ➤ case: Zugriffsfehler auf LDIF-Dateien beim Versuch, zu verlegen (ist in Benutzung): weiter bei #5 mit nächster Aktion 	schwerer Fehler
5.2	<ul style="list-style-type: none"> ➤ case: Zugriffsfehler auf Zielverzeichnis beim Kopieren: <ul style="list-style-type: none"> * Meldung über schweren Fehler an Monitoring * schreibe Meldung ins Übersichts-Log * beende Prozess regulär 	terminiere
6	Teste, ob unter folgenden Bedingungen LDIF-Dateien aus dem File_Location_LF_Archive gelöscht werden müssen: <ul style="list-style-type: none"> • Es sind nach der Löschung mindestens 2 Generationen der Entry-Gruppe im Archiv verfügbar und • Für das im Dateinamen enthaltene Erzeugungsdatum ist gilt Erzeugungsdatum < SystemTime - minimum_Days_of_archival 	
6.1	<ul style="list-style-type: none"> ➤ case: Nach den genannten Bedingungen sind Dateien im Archiv überflüssig: <ul style="list-style-type: none"> * lösche alle als überflüssig identifizierten Dateien in File_Location_LF_Archive * schreibe Meldung ins Übersichts-Log * weiter mit 7 	* weiter mit 7
7	Schreibe Meldung über Prozess-Abschluss in Übersichts-Log beende Prozess regulär	

Tabelle 35: Prozess-Schritte des Prozessabschnitts "Dateiverwaltung Austauschdienst"

Anhang F: Spezifikation "Aktualisierungsprozess Domäne"

Der Aktualisierungsprozess zur Domäne besteht aus zwei Teilprozessen:

- Der Teilprozess im Bereich der Domäne baut die Verbindung zum Austauschdienst auf, stellt fest, welche neuen LDIF-Dateien dort abgelegt wurden und kopiert sie in ein lokales Verzeichnis. Die kopierten Dateien dienen zur Aktualisierung des Austausch-DIT im lokalen Verzeichnisdienst. Abgearbeitete Dateien werden lokal verwaltet. Hier muss nur der erste Prozessabschnitt "Abruf von LDIF-Dateien" durch den "Rahmenprozess Domäne" spezifiziert werden. Für die weiteren Schritte wird der "Teilprozess Verzeichnisdienst der Verwaltung" eingesetzt, der bereits über die notwendigen Konfigurationsmöglichkeiten verfügt (vgl. Anhang D.4).
- Ein Teilprozess im Bereich des Austauschdienstes nimmt die Verbindungsanfragen der Domänen an und räumt das Leserecht auf den Abrufbereich ein.

F.1 Abrufender Rahmenprozess Domäne

Die Domäne kann über die Namensregeln für LDIF-Dateien konfigurieren, für welche Gruppen von Entries aus dem Austausch-DIT sie die Aktualisierungsinformationen "abonnieren" will. Der Rahmenprozess Domäne prüft in periodischen Abständen, ob für die abonnierten Gruppen neue LDIF-Dateien zur Verfügung stehen und kopiert diese in den Bereich der Domäne.

Die Fehlerbehandlung und das Monitoring erfolgen gemäß der Entwurfsentscheidungen. Der Betreiber des Austauschdienstes muss dafür Sorge tragen, dass die entsprechenden Rollen durch Personal besetzt sind. Die Sicherheitsanforderungen müssen umgesetzt sein, d.h. insbesondere, dass der Teilprozess in einem Bereich konfiguriert und betrieben wird, auf den Unberechtigte keinen Zugriff haben.

F.1.1 Vorbedingungen abrufender Rahmenprozess Domäne

Für den Rahmenprozess müssen folgende Vorbedingungen erfüllt sein:

- Der Teilprozess ist korrekt konfiguriert und hat Zugriff auf die Konfigurationsdatei für den Rahmenprozess
- Zugriff auf die Systemzeit des Servers, auf dem der Rahmenprozess läuft (SystemTime)
- Zugriff auf PSE und Passwort zur Authentisierung der Verbindung zum Austauschdienst
- schreibender Zugriff auf das Verzeichnis, in das die abzurufenden LDIF-Dateien kopiert werden sollen,

F.1.2 Invariante

Während der abrufende Rahmenprozess der Domäne aktiv ist, gilt folgende Invariante:

- Der Rahmenprozess wird alle "restartAfterMinutes" gestartet.
- nach einem erfolgreichen Ablauf sind alle LDIF-Dateien der neuesten Generation aller "abonnierten" Gruppen von Entries lokal verfügbar.
- Für alle neuen LDIF-Dateien wurde der upload der Informationen in das lokale Verzeichnis angestoßen.
- Falls Fehler auftraten, wurde das Monitoring informiert.

F.1.3 Konfigurationsparameter abrufender Rahmenprozess Domäne

Abhängig davon, ob im Rahmen der Implementierung Prozess-Schritte aus dem "Teilprozess VDV" in den "abrufenden Rahmenprozesses Domäne" verlegt werden, sind die Parameter der folgenden Tabelle um Parameter aus der Tabelle "Konfigurationsparameter für den Teilprozess beim VDV" zu ergänzen.

Name	Format	Zweck	Anmerkung / Default / Beispiel
restartAfterMinutes	numerisch	legt die Periode fest, nach der der nächste automatische Start des Aktualisierungsprozesses in der Domäne mit "diff" durchgeführt wird	restartAfterMinutes=30 führt zu einem Prozess-Lauf je halber Stunde. Der Wert darf für den Abruf vom Typ CA nicht größer als 30 sein, um die geforderte Servicequalität sicherzustellen.
DNS_AD	String (DNS-Name)	DNS-Name des Verzeichnisdienstes, aus dem die Daten abgefragt werden sollen	
Port_AD	Zahl	Port des Verzeichnisdienstes, aus dem die Daten abgefragt werden sollen	
File_Location_AD	String	gibt das Datei-Verzeichnis an, in dem auf dem Austauschdienst die LDIF-Dateien zum Abruf bereitgestellt werden	
PSE-Location	String	Stelle, an der die PSE zur Sicherung der SSH Verbindung in der Domäne abgelegt ist	
PasswordConnection PSE	zu klären	Passwort zur Verwendung der PSE aus PSE-Location Implementierungshinweis: möglicherweise sollte das Passwort separat abgelegt werden können, um den Zugriff besser begrenzen zu können.	
Proc_Name_D-Preprocessing	String: {LEER [voller Prozedur-name]}	Name der Prozedur, die das domänenspezifische Preprocessing durchführt (Interface zu spezifizieren)	
subscribed_Groups_of_Entries	Array of Strings, VDK-LDIF-Dateinamen	enthält die Liste der LDIF-Dateinamen mit Wildcards, die vom Austauschdienst abgerufen werden sollen	
imported_files_of_Groups_current_Generation	Array of Array of Strings	enthält je konfigurierter Gruppe aus subscribed_Groups_of_Entries die Liste der in der aktuellen Generation importierten LDIF-Dateien	
incoming_file_location	String	Verzeichnis, in das die vom Austauschdienst abgerufenen LDIF-Dateien kopiert werden sollen	

Name	Format	Zweck	Anmerkung / Default / Beispiel
Log- und Monitoringparameter (Liste ist im Rahmen der Implementierung zu ergänzen)	wie erforderlich	legen fest, wie Meldungen an das Monitoring übertragen werden, z.B. eine E-Mail-Adresse, das Verzeichnis, in dem die Prozessspezifischen und die Übersichts-Log-Datei zu speichern sind, die Anzahl der aufzubewahrenden Prozess-Log-Dateien und die Anzahl der Einträge im Übersichts-Log.	Implementierungsabhängig, die Parameter können vom Rahmenprozess und vom Teilprozess in der Domäne gemeinsam genutzt werden

Tabelle 36: Konfigurationsparameter des "abrufenden Rahmenprozesses Domäne"

F.1.4 Aufruf des Rahmenprozesses

Der Rahmenprozess wird automatisch beim Systemstart oder durch manuellen Aufruf gestartet.

F.1.5 Prozessabschnitte

An dieser Stelle wird nur der Prozessabschnitt "Abruf von LDIF-Dateien" spezifiziert.

Abgerufene Dateien werden zur eingeschränkten Konsistenzprüfung und zum upload an die gleichen Prozessabschnitte übergeben, die zu diesem Zweck für die Aktualisierung des Verzeichnisdienstes der Verwaltung spezifiziert wurden.

F.1.5.1 Prozessabschnitt "Abruf von LDIF-Dateien"

Der Prozessabschnitt dient dem Abruf der LDIF-Dateien vom Austauschdienst.

Hinweise zur Implementierung:

- Es wird vorgeschlagen, zur Sicherung der Verbindung SSH (mindestens Version 2) mit fest konfigurierten Schlüsseln einzusetzen. Ein äquivalentes Verfahren ist möglich, muss aber in der Spezifikation entsprechend nachgepflegt werden.
- Der Prozessabschnitt fragt vom Austauschdienst zunächst die Dateinamen der aktuell verfügbaren Dateien der abonnierten Gruppen (subscribed_Groups_of_Entries) ab. Anhand der Liste der bereits importierten LDIF-

Dateien (`imported_files_of_Groups_current_Generation`) bestimmt er, welche neuen Dateien vom Austauschdienst auf die lokale Plattform kopiert werden müssen. Dazu werden für jede Gruppe folgende Regel angewandt:

- Wenn im Austauschdienst keine neuere Generation vorliegt, als die lokal verfügbare, werden die Differenzabgleiche importiert, die lokal noch nicht verfügbar sind.
- Wenn eine neuere Generation vorliegt (Kennzeichen "voll"), als die, die lokal verfügbar ist, werden nur dieser Vollabgleich und alle nachfolgenden Differenzen importiert.

Im Rahmen der Implementierung kann eine abweichende Struktur oder Strategie zur Behandlung der `subscribed_Groups_of_Entries` und der `imported_files_of_Groups_current_Generation` realisiert werden.

- Es ist ausreichend, die Auswahl der Dateien anhand der Dateinamen durchzuführen. In vielen Fällen können Wildcards angewandt werden, wenn die Plattformen dies unterstützen.
- Durch die Verlagerung von Dateien im Austauschdienst kann es vorkommen, dass eine Datei als zu importieren identifiziert wurde, sie aber für das Kopieren nicht mehr zur Verfügung steht. Dies kann nur der Fall sein, wenn zwischenzeitlich ein neuer Vollabgleich auf dem Austauschdienst abgelegt wurde. Dieser wird dann ersatzweise importiert.
- 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. Die Schnittstelle zum Aufruf ist im Rahmen der Implementierung zu spezifizieren.
- Der eigentliche upload in das lokale Verzeichnis wird durch den Aufruf des Prozessabschnitts Konsistenzprüfungen angestoßen (Anhang D.4.5.1). Dort werden allerdings nur die `LDIF_File-Version` und der `LDIF_File-Bearbeitungsstatus` geprüft. Anschließend sollte auch im lokalen Aktualisierungsprozess der Scheduler zum Tragen kommen.

Nr.	Funktionalität und Bedingungen	Verzweigung
1	lese alle Konfigurationsparameter aus Konfigurationsdatei	
1.1	➤ case: Zugriff nicht erfolgreich oder Parameter nicht gesetzt: * Eintrag in Übersichts-Log * Prozess beenden gemäß Fehlerbehandlung (mit qualifizierter Meldung über die Ursache)	schwerer Fehler
2	Baue SSH Verbindung zum Austauschdienst auf unter Verwendung von <ul style="list-style-type: none"> • DNS_AD • Port_AD • File_Location_AD • PSE-Location • PasswordConnectionPSE 	
2.1	➤ case: case: Verbindungsaufbau gescheitert: * Eintrag in Übersichts-Log * Prozess beenden gemäß Fehlerbehandlung (mit qualifizierter Meldung über die Ursache)	schwerer Fehler
3	(Verbindung zum Austauschdienst aufgebaut) <ul style="list-style-type: none"> • frage die Dateinamen aller aktuell verfügbarer Dateien ab • erstelle List_of_new_files (wie unter Hinweise zur Implementierung beschrieben) 	
3.1	➤ case: List_of_new_files ist LEER * Eintrag in Übersichts-Log * Beende Prozessabschnitt regulär	terminiere
4	(Liste war nicht leer) Für alle Files aus List_of_new_files <ul style="list-style-type: none"> • kopiere Datei von Austauschdienst nach lokalem Server auf incoming_file_location 	
4.1	➤ case: erfolgreich * Eintrag in Übersichts-Log * weiter mit #4 (nächstes File)	weiter mit #4
4.2	➤ case: nicht erfolgreich, weil Verbindung zusammengebrochen oder andere Zugriffsprobleme auf Austauschdienst * Prozess beenden gemäß Fehlerbehandlung (mit qualifizierter Meldung über die Ursache)	schwerer Fehler
4.3	➤ case: nicht erfolgreich, weil File nicht mehr auf Austauschdienst verfügbar UND neuerer Vollabgleich dieser Gruppe verfügbar * aktualisiere List_of_new_files * Eintrag in Übersichts-Log * weiter mit #4 (geändertes File)	weiter mit #4
4.4	➤ case: nicht erfolgreich, weil File nicht mehr auf Austauschdienst verfügbar UND KEIN neuerer Vollabgleich dieser Gruppe verfügbar * Eintrag in Übersichts-Log * Meldung schwerer Fehler an Monitoring * weiter mit #4 (nächstes File)	weiter mit #4
5	Teste, ob lokales Preprocessing notwendig	
5.1	➤ case: Proc_Name_D-Preprocessing IST LEER weiter bei #7	weiter bei #7

Nr.	Funktionalität und Bedingungen	Verzweigung
6	(Proc_Name_D-Preprocessing war nicht LLER) Für alle Files aus List_of_new_files • Aufruf von Proc_Name_D-Preprocessing (File_Name, ...) Nach letztem File: weiter mit #7	
6.1	➤ case: erfolgreich, * Eintrag in Übersichts-Log * weiter mit #6 (nächstes File)	weiter bei #6
6.2	➤ case: nicht erfolgreich oder Fehler * Eintrag in Übersichts-Log * weiter bei #6 mit nächsten File oder schwerer Fehler	weiter bei #6 mit nächsten File oder schwerer Fehler
7	(Für alle Files Preprocessing beendet) Für alle Files aus List_of_new_files • Aufruf von "Prozessabschnitt Konsistenzprüfungen (LDIF_File, "LEER")" Nach letztem File: weiter mit #8	
7.1	➤ case: erfolgreich, * Eintrag in Übersichts-Log * weiter mit #7 (nächstes File)	weiter bei #7
7.2	➤ case: nicht erfolgreich oder Fehler * Eintrag in Übersichts-Log * Prozess beenden gemäß Fehlerbehandlung (mit qualifizierter Meldung über die Ursache)	schwerer Fehler
8	Beende Prozessabschnitt regulär	

Tabelle 37: Prozess-Schritte zum Abruf von LDIF-Dateien

F.2 Annahme von Verbindungen der Domänen

Die Realisierung des kryptographisch gesicherten Zugangs der Domänen zum Abrufbereich für LDIF-Dateien wird nicht im Detail spezifiziert. Die Implementierung ist stark von den verwendeten Protokollen und Produkten abhängig. Unter der Annahme, dass SSH eingesetzt wird, sind folgende Anforderungen zu realisieren:

- Es existiert ein gemeinsamer Abrufbereich. für alle Domänen.
- Diesem Abrufbereich sind alle zulässigen öffentlichen Schlüssel zugeordnet. Nur solche Stellen, die sich korrekt authentisieren, erhalten Leserecht auf den Abrufbereich.
- Die Verbindungsannahme eine Rufes erfolgt auf der Seite des Austauschdienstes automatisch, wenn sich die rufende Stelle korrekt authentisiert.

Anhang G: Fragebogen-Antworten der Domänen

Zu Beginn des Projektes wurde an die beteiligten Domänen ein Fragebogen verschickt, um Informationen über den aktuellen Status zu sammeln und diese als Grundlage für das Design des VDKs zu verwenden. Die folgenden Tabellen stellen die für das VDK besonders relevanten Ergebnisse zusammen.

Domäne	DIT-DN	Subject-DN
PCA	cn=pca-1-verwaltung, o=pki-1verwaltung, c=de	identisch
IVBB	cn=pca-1-verwaltung, o=pki-1-verwaltung, c=de	Identisch
	cn=ca ivy deutsche telecom ag, o=bund, c=de	identisch
Sachsen-Anhalt	noch keine Namensfestlegungen	
Testa	cn=ca testa deutschland, ou=testa deutschland, o=pki-1-verwaltung, c=de	identisch
Bayern	CN=CA-1-BYBN, CN=AIA, CN=Public Key Services, CN=Services, CN=Configuration, DC=PKI1, DC=Bayern, DC=de	CN=CA-1-BYBN, ou=Freistaat Bayern, o=pki-1-verwaltung, c=de
	CN=MFCA-1-BYBN, CN=AIA, CN=Public Key Services, CN=Services, CN=Configuration, DC=PKI1, DC=Bayern, DC=de	CN=MFCA-1-BYBN, ou=Freistaat Bayern o=pki-1-verwaltung, c=de
	zwei weitere geplante CAs noch ohne genauen Namen, Struktur vermutlich ähnlich	
Rheinland-Pfalz	c=de,o=rlp-Trust,cn=rlp-Trust CA	identisch (Ermittelt durch Abfrage des Zertifikats aus dem IVBB-Verzeichnis)
Freie Hansestadt Hamburg	c=de, o=PKI-1-Verwaltung, cn=???	
	c=de, o=Hamburg, cn=???	

Tabelle 38: Übersicht CA-Namen der Domänen (Fragebogen 3.2.1)

Domäne	CDP im Directory verwendet?	CDP-DIT-DN
PCA	nein (CDP im Zertifikat verweist auf Sperrliste im CA-Entry)	-
IVBB	nein (da keine Angaben)	-
Sachsen-Anhalt	nein (da keine Angaben)	-
Testa	nein	-
Bayern	ja	Windows2000-Standard (s.u.)
Rheinland-Pfalz	nein (da keine Angaben)	

Freie Hansestadt Hamburg	nein (da keine Angaben)	
---------------------------------	-------------------------	--

Tabelle 39: Übersicht CDP-Verwendung der Domänen (Fragebogen 5.1.1)

Domäne	Mehrere Teilnehmer mit selber E-Mail-Adresse?
PCA	ja (analog zu IVBB)
IVBB	ja
Sachsen-Anhalt	nein
Testa	nein
Bayern	nein
Rheinland-Pfalz	nein
Freie Hansestadt Hamburg	nein

Tabelle 40: Verwendung von einer E-Mail-Adresse für mehrere TN (Fragebogen 5.1.2)

Domäne	mehrere E-Mail-Adressen im Entry?
PCA	nein
IVBB	nein
Sachsen-Anhalt	nein
Testa	ja
Bayern	ja
Rheinland-Pfalz	nein
Freie Hansestadt Hamburg	nein

Tabelle 41: Eine oder mehrere der E-Mail-Adressen pro Entry (Fragebogen 5.1.2)

Domäne	Kennzeichen für veränderte Entries	Name des Attributs	Veränderung außerhalb PKI-Prozesse	Bemerkung
PCA	Änderungsflag	ivbbLastDelivery Collective	(wie IVBB)	Annahme: über Anpassungen IVBB zu realisieren
IVBB	Änderungsflag	ivbbLastDelivery Collective	zeitgesteuerte Datenlieferung ohne Änderungen am Datenbestand, >1x/Tag	prinzipiell besteht die Anpassungsmöglichkeit auf "lastModified" [Telefonat Lüers, 4.2. 2002]
Sachsen Anhalt	Datum und Uhrzeit	lastModified	Import von externen DIR	
TESTA (Thüringen)	Datum und Uhrzeit	lastModified	nein	
Bayern	Datum und Uhrzeit	automatisch durch ADS	ADS-Prozesse	Annahme: es gibt ein geeignetes Attribut "xxxModified". Es besteht Klärungsbedarf, welches auszuwählen ist
Rheinland-Pfalz	k.A.		nein	
Freie Hansestadt Hamburg	Datum und Uhrzeit	whenChanged	nein	

Tabelle 42: Kennzeichen veränderter Entries in den Verzeichnisdiensten der Domänen (Fragebogen 6.1.4)

Domäne	VDV-Attribut / Wert	VöD-Attribut / Wert	Bemerkung
PCA	(bisher nicht unterstützt)	publicVisible	
IVBB	(bisher nicht unterstützt)	publicVisible (Werte: nein; 0-4; leer)	
Sachsen Anhalt	(bisher nicht unterstützt)	(bisher nicht unterstützt)	
Thüringen	(bisher nicht unterstützt)	publicVisible (ja, nein)	
Bayern	employeeTyp "3" = nur im Behördenbereich (auch außer-bayerisch)	employeeTyp "9" = im Internet	
Rheinland-Pfalz	(bisher nicht unterstützt)	(bisher nicht unterstützt)	
Freie Hansestadt Hamburg	(bisher nicht unterstützt)	(bisher nicht unterstützt)	

Tabelle43: Attribut-Typen und Werte für die Steuerung von Replikation (Fragebogen 7.1.1, 7.1.2)

Domäne	heute mehrere Zertifikate im Entry?	zukünftig geplant/möglich?
IVBB	nein	ja
Bayern	ja	ja

Sachsen-Anhalt	offen	ja
Testa	nein	ja
PCA	ja	ja
Rheinland-Pfalz	ja	ja
Freie Hansestadt Hamburg	ja	ja

Tabelle44: Zertifikate je Entry (Fragebogen 7.1.4)

Domäne	Löschinformation verfügbar
PCA	ja, über Log-Files
IVBB	ja, über Log-Files
Sachsen Anhalt	ja, erhält vor dem Löschen ein delete-Flag
TESTA (Thüringen)	
Bayern	unbekannt
Rheinland-Pfalz	nein
Freie Hansestadt Hamburg	unbekannt

Tabelle 45: Verfügbarkeit domänenseitiger Löschinformationen für Entries (Fragebogen 8.1.1)

Domäne	regelmäßig	spätestens erzeugt (Policy)	zusätzlich	Delay Veröff. VD Dom.	max Delay Veröff. (Policy).	max Bearb. Revoc. gesamt	Gü.-Dauer	Bemerkung
PCA	7 T	7 T	sof.	Stunden	gl. Tag		9 T	
IVBB	1/T	1/T	sof.	0	gl. Tag		1T	
Sachsen Anhalt								offen
Thüringen	1/T	1/T	sof.	sof	1T	1T	1T	
Bayern	1/T	1/T	nein	1T	unverzögl.	1T	1T	Die Angaben beziehen sich auf die CA für Teilnehmer (MFCA1). Die CA 1 (nur CA-Zertifikate) muss nach Policy nur alle 28 Tage eine neue CRL ausstellen
Rheinland-Pfalz	nein		nein					
Freie Hansestadt Hamburg	1/T	1/T	1T	1T	1T	1T	7T	

Tabelle 46: Praxis und Policy-Aspekte der Domänen für die lokale Bereitstellung von Sperrlisten (Fragebogen 8.1.3)

Domäne	Abruf-Policy	Bemerkung
PCA	k.A.	
IVBB	bei Auslaufen der Sperrliste, beim Anmelden des Clients	
Sachsen Anhalt		
Thüringen	bei Auslaufen	
Bayern	bei Auslaufen	
Rheinland-Pfalz	k.A.	
Freie Hansestadt Hamburg	bei Auslaufen	

Tabelle 47: Policy der Domänen für den Abruf von Sperrlisten durch Clients (Fragebogen 8.1.3 / 8.1.4)

Domäne	Push gefordert	Pull gefordert	Push möglich	Pull möglich	Bemerkung
PCA		X		X	(entsprechend IVBB)
IVBB		X		X	Netzanbindung zum IVBB nur lesend möglich (DAP, FTP nicht zugelassen). Auf Nachfrage: Aus Sicht des IVBB ist push prinzipiell möglich, wenn das Sicherheitskonzept des IVBB angepasst wird [Telefonat Lüers, 4.2. 2002] Nach Rücksprache mit Herr. Dr. Fuhrberg, BSI, ist eine restriktive Öffnung für eine SSH-Verbindung für Push kein Problem.
Sachsen Anhalt	X				
Thüringen	X				Domäne Herr des Verfahrens
Bayern	X				Firewallkonzept und DMZ-Konzept
Rheinland-Pfalz		X	X		Auf Nachfrage: Aus Sicht von RLP ist push prinzipiell möglich [Gespräch mit Hr. Boffo am 10.4. 2002].
Freie Hansestadt Hamburg	X				

Tabelle 48: Präferenzen Push- / Pull-Konzept für Transfer zum Verzeichnisdienst der Verwaltung bzw. Austauschdienst (Fragebogen 8.1.2)