

INGEST

Version 2.0

16.11.2010

Dieses Dokument beschreibt den Ingest von digitalen Objekten in ein digitales Langzeitarchiv.

Zu Unterscheiden beim Ingest sind die Schnittstellen, über die der Dienstnehmer die zu archivierenden Daten an den LZA-Dienstleisters anliefern kann. Zur Verfügung stehen ein Hotfolder und eine OAI-PMH Schnittstelle.

Die Transferpakete, die über die Schnittstellen angeliefert werden, können dabei entweder ein gepacktes Paket mit mehreren digitalen Objekten sein, oder sie können als ein UOF konformes SIP angeliefert werden.

Im Folgenden wird das daraus resultierende Ingest-Konzept beschrieben.

STARTPUNKT

Auswahl der zu verwendenden Schnittstelle:

Schnittstelle Hotfolder → weiter mit H – Sammeln und Transfer

Schnittstelle OAI-PMH → weiter mit O – Aggregieren

SCHNITTSTELLE HOTFOLDER: H – SAMMELN UND TRANSFER

H.1 Einsammeln der zu archivierenden digitalen Objekte für ein Transferpaket

Der Dienstnehmer stellt die zu archivierenden digitalen Objekte sowie deren zugehörigen Checksummen zusammen. Optional kann eine Metadaten-Datei mitgeliefert werden, der ebenfalls eine zugehörige Checksumme mitgegeben wird. Das verwendete Checksummen-Verfahren muss vorher abgesprochen werden (MD5 oder SHA-1).

H.2 Packe Transferpaket

Der Dienstnehmer packt die zusammengetragenen Daten unter Berücksichtigung der Transferpaket-Definition in ein ZIP/TAR-Archiv.

H.3 Generiere TP-Checksumme

Der Dienstnehmer erzeugt aus dem generierten Transferpaket eine für die Absicherung der Übertragung genutzte Checksumme.

H.4 Übertrage TP und Checksumme

Der Dienstnehmer überträgt über eine gesicherte Verbindung das Transferpaket und die Checksummendatei an den LZA-Dienstleister.

H.5 Empfange TP und Checksumme in Hotfolder

Der LZA-Dienstleister empfängt das Transferpaket und die zugehörige Checksummendatei.

SCHNITTSTELLE OAI-PMH: O – AGGREGIEREN

O.1 Bereitstellung der zu archivierenden digitalen Objekte über eine OAI-PMH Schnittstelle

Der Dienstnehmer stellt die zu archivierenden digitalen Objekte über eine OAI-PMH Schnittstelle zur Verfügung. Dabei sind in den Metadaten sowohl die zugehörige Checksumme des digitalen Objekts als auch die URL zum Objekt enthalten (Pflichtangaben). Optional können deskriptive Metadaten mitgeliefert werden.

O.2 Harvesten

Die OAI-PMH Schnittstelle wird durch den LZA-Dienstleister geharvestet.

O.3 Lese Metadaten

Die Checksumme des Objekts und die optionalen deskriptiven Metadaten werden gelesen.

O.4 Schreibe Metadaten

Die zuvor ausgelesenen Metadaten werden in die Datenbank des Verwaltungssystems geschrieben.

O.5 Lade Datei

Das digitale Objekt wird vom LZA-Dienstleister bei der angegebenen URL abgerufen.

R – ROLLENPRÜFUNG

R.1 Prüfe Rollen

Anhand eines zuvor abgesprochenen Verfahrens mit dem Dienstnehmer findet eine Rollenprüfung der digitalen Objekte statt. Die folgenden Rollen sind möglich:

1. Rolle 1: Ablieferung aller Transferpakete erfolgt im Rahmen der LZA-Dienstleistungsvereinbarung
2. Rolle 2: Ablieferung erfolgt mit dem Ziel der Erfüllung der Pflichtabgabe
3. Rolle 3: Repräsentiert Rolle 1 und 2

Das Ergebnis der Prüfung wird in die Datenbank des Verwaltungssystems geschrieben.

R.2 Exklusives Gateway

Abhängig von der Prüfung aus R.1:

Rolle 1 → weiter mit R.3

Rolle 2 → weiter mit R.4

Rolle 3 → weiter mit R.6

R.3 Verschiebe TP und Checksumme

Das Transferpaket wird zusammen mit der Checksummendatei in ein temporäres Arbeitsverzeichnis verschoben.

R.4 Verschiebe Transferpaket und evtl. Checksummendatei zum DNB-Import-Prozess

Das Transferpaket und evtl. die in diesem Falle als optional geltende Checksumme wird zum DNB Import-Prozess verschoben. Dieser Vorgang wird in der Datenbank des Verwaltungssystems protokolliert.

R.5 Terminierung

Nachdem das Transferpaket und evtl. die Checksummendatei an den DNB-Import-Prozess verschoben worden ist, endet der DP4lib-Workflow für das in der Rolle 2 abgelieferte Transferpaket.

R.6 Kopiere TP/Checksumme

Das Transferpaket (inkl. der Checksumme) wird für die weitere Bearbeitung kopiert.

R.7 Paralleles Gateway

Die vorher kopierten Transferpakete und Checksummendateien werden sowohl an den DP4lib-Workflow (R.3) als auch an den DNB-Import-Prozess (R.4) übergeben.

I – INTEGRITÄTSCHECK

I.1 Prüfe Existenz von Checksummendatei

In diesem Schritt wird überprüft, ob zum Transferpaket eine zugehörige Checksummendatei gefunden wird.

I.2 Wähle Prüfverfahren

Das Prüfverfahren, mit dem die mitgelieferte Checksumme verglichen wird, wird anhand der erkannten Dateiendung (md5 bzw. sha1) ausgewählt.

I.3 Exklusives Gateway

Im Fall, das das Prüfverfahren erkannt wurde, erfolgt die weitere Bearbeitung → weiter mit Schritt I.4. Sofern kein vereinbartes Verfahren erkannt worden ist, wird die Fehlerprotokollerstellung angestoßen → weiter mit F – Fehlerprotokoll.

I.4 Generiere Checksumme

In diesem Schritt wird eine Checksumme gemäß des festgestellten Prüfverfahrens für das Transferpaket vom LZA-Dienstleister generiert.

I.5 Vergleiche Checksumme

Die mitgelieferte Checksumme und die in Schritt I.4 generierte Checksumme werden miteinander verglichen. Das Ergebnis des Vergleichs und die Checksumme werden in der Datenbank des Verwaltungssystems protokolliert.

I.6 Exklusives Gateway

Bei identischen Checksummen → weiter mit E – Entpacken. Im Fehlerfall wird ein Fehlerprotokoll erstellt → weiter mit F – Fehlerprotokoll.

E – ENTPACKEN

E.1 Entpacke Transferpaket

Ein Transferpaket kann in einem ZIP- oder einem TAR-Format vorliegen. Für beide Dateiformate werden Funktionalitäten bereitgestellt, um das Transferpaket in diesem Schritt zu entpacken.

E.2 Exklusives Gateway

Handelt es sich bei dem Transferpaket um ein UOF konformes SIP → weiter mit G – Verarbeite SIP. Sofern das Transferpaket kein SIP ist → weiter mit I – Integritätscheck.

I – INTEGRITÄTSCHECK DER ZU ARCHIVIERENDEN OBJEKTE

Der Integritätscheck der einzelnen digitalen Objekte erfolgt in gleicher Weise wie auf Ebene der Transferpakete (siehe Abschnitt I).

T – TECHNISCHE METADATEN

T.1 Analysiere und extrahiere techn. Metadaten

Die technischen Metadaten für jedes zu archivierende digitale Objekt des Transferpakets werden generiert.

T.2 Exklusives Gateway

Können die technischen Metadaten mit Hilfe der vorhandenen Tools ordnungsgemäß generiert werden → weiter bei Schritt T.3. Tritt bei der Generierung der technischen Metadaten ein Fehler auf → weiter mit F – Fehlerprotokoll.

T.3 Schreibe techn. Metadaten

Die generierten technischen Metadaten werden in einem XML-Objekt zwischengespeichert.

T.4 Speichere Kernset von techn. Metadaten in Verwaltungsdatenbank

Aus den erzeugten Metadaten werden vorher festgelegte Elemente extrahiert und in der Datenbank des Verwaltungssystems abgelegt.

D – DESKRIPTIVE METADATEN

Die folgenden beiden Schritte treffen nur auf die Ablieferung über einen Hotfolder zu.

D.1 Extrahiere deskriptive Metadaten

Die Anlieferung deskriptiver Metadaten ist optional. Wenn sie mitgeliefert werden, dann müssen sie zur weiteren Verarbeitung in dem Metadatenformat DC-Simple vorliegen.

Sollten entsprechende deskriptive Metadaten mitgeliefert werden, dann werden sie im Folgenden Schritt extrahiert.

D.2 Speichere deskriptive Metadaten in Verwaltungsdatenbank

Die zuvor extrahierten deskriptiven Metadaten werden in der Datenbank des Verwaltungssystems gespeichert.

K – KLASSIFIZIEREN

K.1 Lese Modulname

Das verwendete Analyse-Modul zur Generierung der Metadaten aus Schritt T.1 wird aus der Datenbank des Verwaltungssystems gelesen.

K.2 Exklusives Gateway

Wurde kein zum Dateiformat passendes Analyse-Modul im Schritt T.1 gefunden → weiter mit Schritt K.10.
Anderenfalls – also bei der Verwendung eines passenden Analyse-Moduls → weiter mit Schritt K.3.

K.3 Lese Dokumentenbeschränkung

Hier werden aus der Datenbank des Verwaltungssystems die Informationen bzgl. möglich vorhandener Dokumentenbeschränkungen gelesen. Diese wurden im Zuge der Metadatengenerierung ermittelt, sofern das eingesetzte Tool und das zum Dateiformat passende Analyse-Modul diese Fähigkeit besitzt.

K.4 Exklusives Gateway

Wenn Dokumentenbeschränkungen vorhanden sind → weiter mit Schritt K.10. Anderenfalls → weiter mit Schritt K.5.

K.5 Formatspezifische Metadaten

In diesem Schritt wird geprüft, ob dateiformatspezifische Metadaten generiert werden konnten.

K.6 Exklusives Gateway

Wenn keine dateiformatspezifischen Metadaten generiert werden konnten → weiter mit Schritt K.11.
Anderenfalls → weiter mit Schritt K.7.

K.7 Lese ob wohlgeformt und valide

Hier werden Informationen aus der Datenbank des Verwaltungssystems entnommen, ob Wohlgeformtheit und Dateiformatvalidität für das Dokument erfolgreich geprüft worden sind oder nicht.

K.8 Exklusives Gateway

Wenn Formatvalidität vorliegt → weiter mit Schritt K.9. Anderenfalls → weiter mit Schritt K.12.

K.9 Weise Ingest-Level 3 zu

Dieser Schritt weist dem digitalen Objekt den Ingest-Level 3 zu und schreibt das Ergebnis in die Datenbank des Verwaltungssystems.

K.10 Weise Ingest-Level 0 zu

Dieser Schritt weist dem digitalen Objekt den Ingest-Level 0 zu und schreibt das Ergebnis in die Datenbank des Verwaltungssystems.

K.11 Weise Ingest-Level 1 zu

Dieser Schritt weist dem digitalen Objekt den Ingest-Level 1 zu und schreibt das Ergebnis in die Datenbank des Verwaltungssystems.

K.12 Weise Ingest-Level 2 zu

Dieser Schritt weist dem digitalen Objekt den Ingest-Level 2 zu und schreibt das Ergebnis in die Datenbank des Verwaltungssystems.

K.13 Prüfe Klassifizierung gegen Ingest-Policy

Hier erfolgt ein Schritt zur Qualitätsbestimmung. Dazu wird eine Überprüfung des in der Klassifizierung ermittelten Ingest-Levels gegen die mit dem Dienstnehmer vereinbarte Ingest-Policy durchgeführt.

Die Prüfung erfolgt für jedes einzelne Objekt. Sobald ein Objekt die zutreffenden Policy-Kriterien nicht erfüllt, verstößt das gesamte Transferpaket gegen die Policy.

K.14 Exklusives Gateway

Sofern ein digitales Objekt aus dem Transferpaket nicht der vereinbarten Ingest-Policy entspricht, tritt der Fehlerfall ein → weiter mit F – Fehlerprotokoll. Sollten alle digitalen Objekte den Vereinbarungen entsprechen → weiter mit C – SIP-Paket

C – SIP-PAKET

C.1 Erstelle interne URN

Es wird eine interne URN erstellt und in der Datenbank des Verwaltungssystems gespeichert.

C.2 Erstelle METS-Datei

Die technischen Metadaten, die interne URN sowie die mitgelieferten deskriptiven Metadaten werden in eine METS-Datei geschrieben.

C.3 Generiere SIP

In diesem Schritt werden die digitalen Objekte des Transferpakets und die METS-Datei zu einem, SIP verpackt.

C.4 Übertrage SIP an das Storage-System

Das vollständige SIP wird über eine gesicherte Verbindung an das Storage-System übertragen.

G – VERARBEITE SIP

G.1 Auslesen der METS-Datei

Hier werden sowohl die zuvor vereinbarten deskriptive Metadaten als auch dem Kernset entsprechenden technischen Metadaten aus der METS-Datei gelesen und in die Datenbank des Verwaltungssystems übernommen.

G.2 Exklusives Gateway

Konnten die notwendigen METS-Daten erfolgreich ausgelesen werden → weiter mit Schritt G.3. Andernfalls → weiter mit F – Fehlerprotokoll.

G.3 Vergeben der internen URN

Zur internen Verwaltung ist die Vergabe einer internen URN zwingend erforderlich. Diese interne URN wird in diesem Schritt vergeben und sowohl in die METS-Datei als auch in die Datenbank des Verwaltungssystems geschrieben.

G.4 Packe SIP

In diesem Schritt wird das SIP wieder gepackt.

G.5 Übertrage SIP an das Storage-System

Das vollständige SIP wird über eine gesicherte Verbindung an das Storage-System übertragen.

V – VERFAHREN IM STORAGE-SYSTEM

V.1 Empfange SIP

Das Storage-System empfängt das SIP.

V.2 Überprüfe SIP

Im Storage-System findet eine Überprüfung des generierten SIP auf Integrität und UOF-Kompatibilität statt.

V.3 Exklusives Gateway

Sofern die Überprüfung erfolgreich war → weiter mit Schritt V.4. Andernfalls → weiter mit Schritt V.7.

V.4 Archiviere SIP

In diesem Schritt wird die eigentliche Archivierung durch das Storage-System durchgeführt.

V.5 Sende Archivierungsbestätigung

Das Storage-System bestätigt, dass das SIP fehlerfrei angenommen wurde und archiviert worden ist.

V.6 Terminierung

Die Aufgaben im Storage-System sind abgeschlossen.

V.7 Lösche SIP

Das abgelehnte SIP wird vom LZA-Dienstleister gelöscht.

V.8 Sende Fehlerprotokoll

Das Storage-System meldet einen Archivierungsfehler an den LZA-Dienstleister.

V.9 Fehlerverfahren

Das Fehlerverfahren ist für das Storage-System mit einer Fehlermeldung abgeschlossen.

M – RÜCKMELDUNG**M.1 Empfange Antwort vom Storage-System**

Die Empfangsbestätigung vom Storage-System wird vom LZA-Dienstleister angenommen und in der Datenbank des Verwaltungssystems gespeichert.

M.2 Exklusives Gateway

Ist die Aufnahme des SIPs erfolgreich → weiter mit P – Ingestprotokoll. Ist die Aufnahme fehlgeschlagen → weiter mit Schritt M.3.

M.3 Überprüfe Fehlerprotokoll

Bei Sendung eines Fehlerprotokolls durch das Storage-System wird versucht den Grund zu analysieren.

M.4 Exklusives Gateway

Ist eine Fehlerkorrektur seitens des LZA-Dienstleister möglich → weiter bei Schritt M.5. Ist keine Fehlerkorrektur möglich → weiter mit F – Fehlerprotokoll.

M.5 Exklusives Gateway

Handelte es sich bei dem Transferpaket um ein UOF konformes SIP → weiter mit G – Verarbeite SIP. War das Transferpaket kein SIP → weiter bei Schritt C.2.

P – INGESTPROTOKOLL

P.1 Erstelle Ingestprotokoll

Aus den in der Datenbank des Verwaltungssystems gesammelten Daten über die Verarbeitung des Transferpaketes, wird ein Protokoll erstellt.

P.2 Sende Ingestprotokoll

Das zusammengestellte Protokoll wird entweder aktiv an den Dienstnehmer gesendet oder dem Dienstnehmer über ein Web-Service bereitgestellt.

P.3 Empfange Ingestprotokoll

Der Dienstnehmer empfängt das Ingestprotokoll oder holt sich die Informationen aktiv ab.

P.4 Überprüfe Ingestprotokoll

Das Ingestprotokoll muss innerhalb eines zuvor festgelegten Zeitraums vom Dienstnehmer überprüft werden.

A – ABNAHME

A.1 Exklusives Gateway

Hier muss vom Dienstnehmer eine Entscheidung getroffen werden, ob der Ingest aus seiner Sicht erfolgreich stattgefunden hat. Wenn „Ja“ → weiter mit Schritt A.2, wenn „Nein“ → weiter mit Schritt A.8.

A.2 Sende Abnahmebestätigung

Im Falle der Zufriedenheit seitens des Dienstnehmers, wird vom Dienstnehmer eine Abnahmebestätigung an den LZA-Dienstleister geschickt.

A.3 Terminierung

Die Übernahme wurde auf Seiten des Dienstnehmers erfolgreich beendet.

A.4 Bedingungsereignis

Die Geschäftsregeln schreiben vor, dass der LZA-Dienstleister den Übernahmeprozess erst beenden kann, wenn vom Dienstnehmer hierüber eine Benachrichtigung erfolgt. Die Benachrichtigung kann eine Annahmebestätigung oder einer Ablehnung sein.

A.5 Warte auf Abnahme

Der Geschäftsprozess der Abnahme des Transferpaketes muss vom Dienstnehmer bestätigt werden, vorher wird der Geschäftsgang nicht innerhalb des LZA-Dienstleisters als abgeschlossen vermerkt.

A.6 Exklusives Gateway

Abhängig von der Benachrichtigung des Dienstnehmers kann der Dienstleister nun die Übernahme beenden → weiter mit Schritt A.7 oder im Ablehnungsfall ein Eskalationsverfahren einleiten → weiter mit Schritt A.10.

A.7 Terminierung

Die Übernahme wird erfolgreich beendet und entsprechend in der Datenbank des Verwaltungssystems vermerkt.

A.8 Sende Abnahmeverweigerung

Sofern Unstimmigkeiten aus dem Ingestprotokoll entstanden sind, wird eine Abnahmeverweigerung vom Dienstnehmer an den LZA-Dienstleister geschickt.

A.9 Fehlerverfahren

Die Übernahme wurde von Seiten des Dienstnehmers abgelehnt. Ein Eskalationsverfahren wird notwendig.

A.10 Lösche SIP

Da generell die Aufnahme ins Storage-System vorgenommen worden ist, aber die Abnahme des Transferpaketes vom Dienstnehmer letztendlich verweigert wurde, muss in diesem Schritt das bereits archivierte Transferpaket wieder aus dem Archiv entfernt werden. Dieser Schritt wird in der Datenbank des Verwaltungssystems protokolliert.

A.11 Fehlerverfahren

Nach Ablehnung der Übernahme durch den Dienstnehmer wird ein Eskalationsverfahren eingeleitet.

B – INGESTBERICHT

B.1 Zeit-Ereignis

In vorher vereinbarten Abständen wird ein Ingestbericht bereitgestellt.

B.2 Erstelle Ingestbericht

Ein menschen-lesbarer Bericht über einen bestimmten, vorher festgelegten Zeitraum wird erstellt.

B.3 Sende Ingestbericht

Der Ingestbericht wird an den Dienstnehmer gesendet bzw. wird dem Dienstnehmer aktiv über einen Web-Service angeboten.

B.4 Empfange Ingestbericht

Der Dienstnehmer empfängt den Ingestbericht.

F – FEHLERPROTOKOLL

F.1 Lösche TP

Das Transferpaket wird gelöscht.

F.2 Erstelle Fehlerprotokoll

Der LZA-Dienstleister erstellt ein Fehlerprotokoll für das betroffene Transferpaket.

F.3 Sende Fehlerprotokoll

Der LZA-Dienstleister sendet ein Fehlerprotokoll an den Dienstnehmer.

F.4 Empfange Fehlerprotokoll

Das Fehlerprotokoll wird auf Seiten des Dienstnehmers empfangen und ausgewertet. Das betroffene Transferpaket kann vom Dienstnehmer korrigiert und erneut in den Ingest-Prozess eingebracht werden.

F.5 Fehlerverfahren

Bei der Übertragung ist ein Fehler aufgetaucht. Ein Eskalationsverfahren wird notwendig.

ANHANG

GLOSSAR

Checksummendatei	Die Checksummendatei erhält den gleichen Namen wie das Transferpaket (inklusive Dateieindung) ergänzt um die zusätzliche Dateieindung „.md5“ oder „.sha1“.
Exklusives Gateway	Ein exklusives Gateway stellt eine Weggabelung dar. Nur ein Weg kann weiter verfolgt werden.
Ingest-Policy	Für die grundsätzliche Absprache der Ingest-Policy stellt der LZA-Dienstleister im Vorfeld der individuellen Vertragsverhandlungen eine Muster-Policy zur Verfügung, die auf den bisherigen Erfahrungen des Dienstleisters in Bezug auf die einzuspielenden Dateiformate des Dienstnehmers aufbaut. Diese Policy wird mit dem Dienstnehmer abgestimmt und als Standardpolicy in der Datenbank des Verwaltungssystems abgelegt.
Ingestprotokoll	Das Ingestprotokoll ist ein maschinen-lesbares Protokoll über den Ingest der Transferpakete. Im Ingestprotokoll sind die folgenden Informationen enthalten: Transferpaketname, interne URN, Ergebnis der Rollenprüfung, festgestelltes Ingest-Level, Archivierungsbestätigung des Storage-Systems, Ingest-Zeitpunkt
Interne URN	Es wird jeweils eine interne URN je Transferpaket zugewiesen. Alle digitalen Objekte aus dem Transferpaket sind dann im Folgenden über diese URN auffindbar.
Kernset technischer Metadaten	Das Kernset besteht aus ausgewählte Elemente technischer Metadaten, die aus dem Output von JHOVE gewonnen werden. Folgende Elemente fallen darunter: <ul style="list-style-type: none"> • verwendetes JHOVE-Modul • Dokumentenbeschränkungen (PDF)
OAI-PMH	Das auf XML und REST basierende OAI Protocol for Metadata Harvesting (OAI-PMH) wurde 2000 entwickelt. Das Verfahren ist für den Austausch und die Synchronisation von Metadaten zwischen Data- und Service-Provider konzipiert.
Paralleles Gateway	Ein paralleles Gateway symbolisiert eine Weggabelung, von der aus mehrere Wege beschrritten werden.

Rollenprüfung

Hotfolder: Jede Institution erhält auf dem Hotfolder einen eigenen Ordner. Ausgehend von einem übergeordneten Verzeichnis für eine Institution, werden drei Unterverzeichnisse angelegt. Jedes Unterverzeichnis wird durch eine spezielle Rollen-ID, gemäß den existierenden Rollen gekennzeichnet.

Anhand der Verzeichnisse, in denen das Transferpaket vom Dienstnehmer eingespielt worden ist, wird die Zuweisung der Rollen durchgeführt.

OAI-PMH: Die Rollenprüfung für die OAI-PMH Schnittstelle muss noch durch DP4lib definiert werden.

SIP

Submission Information Package (siehe OAIS-Terminologie:
<http://public.ccsds.org/publications/archive/650x0b1.pdf>)

UOF

Universelles Objektformat gemäß Spezifikation:
http://www.kopal.langzeitarchivierung.de/downloads/kopal_Universelles_Objektformat.pdf

BASISELEMENTE UND AUFBAU DES INGESTPROTOKOLLS

```

Ingestbericht = {Transferpaket};

Transferpaket = Paketname, Integrität, {digitales_Objekt},
Paket_archiviert;

Paketname = *, ".zip" | *, ".tar";

Integrität = true | false;

digitales_Objekt = Dateiname, Integrität, Ingest-Level;

Dateiname = *, ".pdf" | *, ".html" | *, ".xml" | *, ".txt" | *. ... ;

Ingest-Level = „0“ | „1“ | „2“ | „3“;

Paket_archiviert = true | false;

```

Erläuterung zur Notation (EBNF)

=	Definition
;	Ende der Definition
{Element}	Wiederholung (mind. 1x) von Element
,	Sequenz (logisches UND)
	Alternative
*	beliebiges nichtleeres Literal (nicht EBNF)
...	usw. (nicht EBNF)
true	das Literal für wahr
false	das Literal für falsch

Bsp. Paketname = *, ".zip" | *, ".tar";

bedeutet: Das Element „Paketname“ besteht aus einer beliebigen Folge von Literalen gefolgt von der Zeichenkette „.zip“ oder „.tar“.

Das Element „Integrität“ gibt entweder für das Transferpaket oder für ein einzelnes Dateiojekt darüber Auskunft, ob die Checksummenprüfung erfolgreich durchgeführt wurde (true) oder nicht (false).

Weiteres zu EBNF: http://de.wikipedia.org/wiki/Erweiterte_Backus-Naur-Form

Basiselemente und Aufbau des Fehlerprotokolls in EBNF-Notation:

```

Fehlerprotokoll = Transferpaket;

Transferpaket = Paketname, Validität, {digitales_Objekt};

Paketname = *, ".zip" | *, ".tar";

Validität = true | false;

digitales_Objekt = Dateiname, Validität, „ermitteltes“, Ingest-Level,
„gefordertes“ Ingest-Level;

Dateiname = *, ".pdf" | *, ".html" | *, ".xml" | *, ".txt" | *. ... ;

```

Ingest-Level = „0“ | „1“ | „2“ | „3“;

BEISPIEL EINES INGESTPROTOKOLLS IN XML-NOTATION

(1 Transferpaket bestehend aus 2 digitalen Objekten)

```
<ingestbericht>
  <transferpaket>
    <paketname>Ablf-ID-20100716_001.zip</paketname>
    <integrität>true</integrität>
    <digitales_objekt>
      <dateiname>abstract.html</dateiname>
      <integrität>true</integrität>
      <ingest-level>2</ingest-level>
    </digitales_objekt>
    <digitales_objekt>
      <dateiname>LZA-dissertation.pdf</dateiname>
      <integrität>true</integrität>
      <ingest-level>3</ingest-level>
    </digitales_objekt>
    <paket-archiviert>true</paket-archiviert>
  </transferpaket>
</ingestbericht>
```