DFG-Projekt

# Beweissicheres elektronisches Laborbuch (BeLab)

## Schnittstellenpapier

Konzept für die Realisierung eines Prototyps zur
beweiswerterhaltenden Langzeitarchivierung von elektronischen Laborbüchern

**Projektpartner:**

UNIKASSEL VERSITÄT provet

KIT Karlsruhe Institute of Technology

PTB

Ansprechpartner unter: www.belab-forschung.de

*Version: 1.2*

*Datum: 22. Juli 2011*

**gefördert durch**

DFG Deutsche Forschungsgemeinschaft

# Versionshistorie

**Version 1.2:**

- Überarbeitung des Kapitels 4 basierend auf den Ergebnissen des am 25.01.2011 in Braunschweig durchgeführten BeLab-Workshops.
- Aufnahme weiterer Anforderungen in den Entwurf der Architektur des BeLab-Systems.
- Zuordnung der externen und internen Funktionsbeschreibungen der BeLab-Schnittstelle zur Architekturbeschreibung des BeLab-Systems.
- Einheitliche Darstellung der Anforderungen an ein Archivsystem.
- Gesonderte Darstellung des Klassifizierungssystems.

22. Juli 2011

**Version 1.1:**

- Überarbeitung der grafischen Darstellung der Komponenten des BeLab-Systems und des internen Verarbeitungsprozesses.

21. Februar 2011

# Inhalt

# 1 Einleitung / Zielsetzung

Das elektronische Laborbuch (eLab) dient einer einheitlichen Verwaltung von Forschungsdaten und Forschungsergebnissen. Im eLab sollen alle für das Forschungsprojekt notwendigen Fakten und Daten, wie z. B. Planung, Durchführung, Messdaten oder Auswertung von Experimenten, dokumentiert werden.

Neben der eindeutigen und nachvollziehbaren Dokumentation ist nach den Regeln der guten wissenschaftlichen Praxis die Archivierung der Forschungsdaten von mindestens zehn Jahren vorzusehen. Im Zulassungsbereich sind weitaus längere Zeiträume zu berücksichtigen. Dabei ist darauf zu achten, dass die Daten lesbar und auch langfristig interpretierbar gesichert werden. Daneben ist die Datenauthentizität und Datenintegrität sicherzustellen.

Im Rahmen des BeLab-Projekts soll eLabs auf technischem Weg eine Sicherheit verliehen werden, welche mit der von herkömmlichen papiergebundenen Laborbüchern vergleichbar ist oder sogar darüber hinaus geht.

Zur Sicherstellung der Datenintegrität sollte eine Signierung der Daten möglichst früh erfolgen. Diese Signierung muss dann in das eLab übernommen werden können. Gleiches gilt für sonstige Daten, welche aus anderen IT-Diensten übernommen werden (z. B. Datenimporte aus anderen Anwendungen oder Messgeräten, welche aber nicht automatisiert erfolgen).

**Dieses Papier ist eine Zusammenstellung der bis zum Veröffentlichungsdatum erzielten Ergebnisse und bildet die Grundlage für weitere Entwicklungen sowie die Ausgestaltung eines Prototyps.**

# 2 Grundlagen

Die nachfolgenden Abschnitte erläutern die für die Realisierung der Schnittstellen des BeLab-Systems erforderlichen Grundlagen. Diese umfassen IT-Sicherheitsanforderungen und -maßnahmen, Spezifikationen der über die Schnittstelle verarbeiteten Daten, sowie rechtliche Aspekte in Bezug auf die Verarbeitung und nachhaltige Gewährleistung der IT-Sicherheitsanforderungen bzw. Erhaltung des Beweiswertes der Daten.

## 2.1 Gewährleistung der Datenauthentizität/-integrität

Elektronische Dokumente gelten bei dem Gesetzgeber und Gerichten grundsätzlich als flüchtig und leicht manipulierbar.[1] Dies gilt auch für Metadaten, wie beispielsweise die in der Regel von der Systemzeit abhängigen Dateizeitstempel, welche vom Anwender manipuliert werden könnten. Mithin kann es schwierig sein zu beweisen, dass einem ein elektronisches Dokument zu einer bestimmten Zeit vorlag, wer das Dokument erstellt hat und dass es inhaltlich nicht mehr verändert worden ist. Zur Sicherung der Daten, zur Beweiswerterhaltung und späteren Verwertung in einem Antrags- oder Gerichtsverfahren können verschiedene Dokumentations- und Sicherungsmaßnahmen eingesetzt werden.
Nachträgliche Veränderungen der eingegebenen Daten jeder Art (auch zur Fehlerkorrektur) werden durch diese Sicherungsmaßnahmen dokumentiert. Diese umfassen beispielsweise in Bezug auf die Verarbeitung der Daten im BeLab-System:

- Logging inkl. Audit
- Schnittstellenaktivitäten inkl. Audit
- Nachvollziehbarkeit

Neben den Anforderungen an das BeLab-System müssen für eine ganzheitliche Gewährleistung der Datenauthentizität und -integrität auch bereits in den an das BeLab-System angebundenen eLabs Sicherheitsmaßnahmen realisiert werden. Diese bilden die Basis für die Datenauthentizität und -integrität der Eingabedaten des BeLab-Systems. Beispiele für geeignete Sicherheitsmaßnahmen bilden:

- Mandantenfähigkeit inkl. Rechtekonzept
- Sicherheitskonzept des eLabs

Weiter ist zu beachten, dass sowohl die Integrität als auch die Authentizität digitaler Daten durch elektronische Signaturen nach dem Signaturgesetz (SigG) gesichert werden. Abgestuft

[1] Vgl. nur Erwägungsgründe der RL 1999/93/EG (Signaturrichtlinie) und Einleitung der Begründung zum Justizkommunikationsgesetz BT- Drs 15/4067, S. 24 ff.
[2] Siehe https://www.pki.dfn.de/, Stand 21.1.2011.
[3] Vgl. http://www.selma-project.de/index.html, Stand 21.1.2011.

werden muss hier nach dem Grad der Signatur (einfach, fortgeschritten, qualifiziert) und der Einbindung des Verfahrens in die Datenerhebung. Entscheidend kommt es darauf an, wann und wodurch die Integrität einmal erhobener Daten sichergestellt wird. Veränderungen sollen dokumentiert und Verfälschungen nachgewiesen werden. Insbesondere der Zeitpunkt der Verarbeitung der Daten kann durch die Verwendung von elektronischen Zeitstempeln gesichert werden. Der Gesetzgeber hat diesem Umstand mit der Einführung des qualifizierten elektronischen Zeitstempels Rechnung getragen. Dieser ist nach § 2 Nr. 14 SigG die elektronische Bescheinigung eines Zertifizierungsdiensteanbieters darüber, dass ihm bestimmte elektronische Daten zu einem definierten Zeitpunkt vorgelegen haben.

### 2.1.1 Qualifizierte und fortgeschrittene Signaturen

Zur Sicherstellung der Datenauthentizität und -integrität können fortgeschrittene oder qualifizierte elektronische Signaturen nach dem Signaturgesetz (SigG) verwendet werden. Zu beachten ist jedoch, dass nach den Vorstellungen des Gesetzgebers und den Bestimmungen der relevanten Gesetze (z. B. BGB, ZPO, VwGO, VwVfG; siehe auch Abschnitt 3.2) nur die qualifizierte Signatur die eigenhändige Unterschrift ersetzen kann. Auch wenn die fortgeschrittene Signatur zur Beweissicherung oft ausreichen wird, etwa dort wo es nur auf die Integrität der erhobenen Rohdaten ankommt, sollte die qualifizierte Signatur immer eingesetzt werden können. Entsprechend muss das eLab die Möglichkeit bieten qualifizierte Signaturen zu verwenden und mit der dafür notwendigen Infrastruktur zu kommunizieren.

Wichtig ist, dass die Voraussetzungen einer typischen Forschungsumgebung mit berücksichtigt werden. So stellt der DFN-Verein[2] eine Infrastruktur für den Einsatz von fortgeschrittenen Signaturen und Zeitstempeln bereit, die sich aus kryptographischer Sicht nicht von einer qualifizierten Signatur unterscheiden. Daher ist von der Software kein Unterschied in der Behandlung notwendig. Zur Klassifizierung der Sicherheit siehe Abschnitt 3.3.

### 2.1.2 Frühzeitige Gewährleistung der Datenintegrität

Insbesondere zur Gewährleistung der Datenintegrität sollte möglichst früh eine Signierung der Daten erfolgen. Diese Signierung muss dann in das eLab übernommen werden können. Gleiches gilt für sonstige Daten, welche aus anderen IT-Diensten übernommen werden

Durch die Verwendung von Messgeräten, die bereits über eine Signaturkomponente verfügen, ist es möglich die Daten über den gesamten wissenschaftlichen Forschungsprozess (von der Datenerhebung bis zur Archivierung) mit elektronischen Signaturen zu sichern.

[2] Siehe https://www.pki.dfn.de/, Stand 21.1.2011.

Messgeräte, welche bereits Roh- oder Primärdaten elektronisch signieren, tragen dazu bei die Datenintegrität der im eLab aufgezeichneten Forschungsdaten sicherzustellen. Nach Möglichkeiten sollen diese Daten vollständig inklusive elektronischer Signatur übernommen werden. So kann der Forscher z. B. Vorwürfe der Manipulation seiner Messungen entkräften. Produkte wie SELMA[3] oder zum Smart Metering[4] ermöglichen es den Hashwert der digital erzeugten Forschungsdaten zu sichern und zu verschlüsseln um spätere Manipulationen nachweisen und damit verhindern zu können. Ein Beispiel bildet der im folgenden Abschnitt skizzierte Anwendungsfall.

### 2.1.3 Anwendungsbeispiel: Signierende Kameras

Im Rahmen des BeLab-Projekts wurden digitalen Industriekameras der Firma Kappa optronics GmbH getestet. Verwendet wurde hierbei das Modell DX-40S. Die Kamera wird entweder über ein CameraLink- oder Gigabit-Ethernet-Interface direkt mit dem Computer verbunden. Für das CameraLink-Interface wird ein PCI- oder alternativ ein PCMCIA-Steckplatz benötigt. Im Trigger-Modus[5] der für die Verwendung erforderlichen Software der Firma Kappa lassen sich mit der Kamera signierte Bilder in einem Intervall von zwei Sekunden erzeugen. Dazu besitzt die Kamera ein internes Signaturverfahren, das einen Signatur-Chip umfasst. Dieser enthält ein Zertifikat, mit dessen Hilfe der über das Bild berechnete Hashwert asymmetrisch verschlüsselt wird (elektronische Signatur). Verwendet wird für die asymmetrische Verschlüsselung ein 1024 Bit RSA-Signaturverfahren. Für die Berechnung des Hashwertes wird ein SHA-512 Algorithmus eingesetzt. Das Austauschen des Signatur-Chips bzw. Veränderungen am Verschlüsselungsverfahren oder dem verwendeten Schlüssel sind nur durch eine physikalische Manipulation nach Öffnung der Kamera möglich. Über eine Versiegelung der Kamera können daher Manipulationen nachgewiesen werden. Nach Herstellerangaben werden Manipulation durch die Verwendung ein geschlossenen Security Controller Chips mit Schlüsselverwaltung verhindert.

Die zu der Kamera DX40-S zugehörige Software bietet die Möglichkeit einen zusätzlichen Text an die Kamera zu senden und mit zu signieren[6]. Dazu kann ein benutzerdefinierter Text in ein hierfür vorgesehenes Textfeld eingegeben werden. Bei der Erzeugung des Bildes wird der angegebene Text mit in die sog. raw-Datei (Rohdaten der Bilderfassung) aufgenommen. Zusätzlich besteht die Möglichkeit das aktuelle Datum und die Uhrzeit automatisiert in den Text zu übernehmen. Die so in die raw-Datei aufgenommen Daten werden bei der elektronischen Signierung des Bildes durch die Kamera berücksichtigt, d. h. ein nachträglich

[3] Vgl. http://www.selma-project.de/index.html, Stand 21.1.2011.

[4] Vgl. http://en.wikipedia.org/wiki/Smart_meter, Stand 21.1.2011.

[5] Über den Trigger-Modus kann ein Zeitpunkt (Zeitdauer) angegeben werden, ab dem Bilder aufgezeichnet werden sollen.

[6] Unterschieden werden die Signatur des Bildes, die im Sinne der elektronischen Signatur erzeugt wird, und ein Signatur-Text.

verändertes Datum (Uhrzeit) kann anhand der Prüfung der elektronischen Signatur nachgewiesen werden.
Die Kamera der Firma Kappa eröffnet die Möglichkeit eine elektronische Signierung der Rohdaten vor der Übertragung zum Computer durchzuführen und bietet damit einen höheren Beweiswert nach den Anforderungen des BeLab-Systems. Interessant ist die Möglichkeit des Einfügens eines Datums (Uhrzeit), welches mit signiert wird. Vergleichbar ist diese Möglichkeit mit einem Eintrag in einem Laborbuch, der durch den Autor mit seiner Unterschrift bestätigt wird.

### 2.1.4 Elektronische Zeitstempel

Elektronische Zeitstempel spielen an mehreren Stellen eine besondere Rolle:

- beim Experiment selbst
- bei der Überprüfung der Authentizität
- bei Änderungen an den Daten (korrigieren oder gar stornieren)
- bei der Übernahme signierter Daten in das BeLab-System (OCSP-Request), genauer: Der Zeitpunkt an dem die Signatur im TR 03125-spezifischen Modul überprüft wird (TSP gemäß RFC 3161).
- bei der Langzeitarchivierung insb. bei der Übersignatur (erneute elektronische Signatur zur Erneuerung)

Zeitstempel sind die authentische und unverfälschbare Verknüpfung von Daten mit einer Zeitaussage. Dazu wird der aus einem Dokument ermittelte „Hashwert“ mit der Zeit beim Stempelvorgang verbunden. Ein qualifizierter Zeitstempel im Sinne des Signaturgesetzes ist eine mit einer elektronischen Signatur versehene elektronische Bescheinigung einer Zertifizierungsstelle. Diese bestätigt, dass bestimmte elektronische Daten zum entsprechenden Zeitpunkt vorgelegen haben. Dazu wird der Hashwert einer Datei an den Zertifizierungsdiensteanbieter übermittelt, von diesem in einer gesicherten Umgebung mit der gesetzlichen Zeit verbunden und an den Dokumenteninhaber zurückgesandt. Zeitstempel dienen dazu, den unveränderten Zustand eines elektronischen Dokumentes von einem bestimmten Zeitpunkt an nachzuweisen.
Die Verwendung eines qualifizierten Zeitstempels nach § 9 Signaturgesetz (SigG) ist für die Zwecke der Langzeitarchivierung bzw. der Übersignatur von qualifizierten elektronischen Signaturen notwendig (vgl. § 17 Signaturverordnung (SigV)). Bei der Übersignierung soll mit dem qualifizierten elektronischen Zeitstempel nachgewiesen werden, dass das Zertifikat der ursprünglichen qualifizierten elektronischen Signatur zum Zeitpunkt der erneuten Signierung nicht schon durch Zeitablauf oder Widerruf ungültig war. Juristische Simulationsstudien haben gezeigt, dass qualifizierten elektronischen Zeitstempeln dabei besonderes Vertrauen entgegengebracht worden ist.

Für die genannten Zwecke bietet der qualifizierte elektronische Zeitstempel daher ein besonderes Maß an Vertrauen und Sicherheit. Aber auch elektronische Zeitstempel, welche durch eine sonstige vertrauenswürdige dritte Stelle ausgestellt wurden, eignen sich für die Zwecke der Beweiswerterhaltung. Aus Kosten- und Praktikabilitätsgründen sind sie in Einzelfällen ggf. sogar vorzugswürdig. Denn für die Beweiskraft von qualifizierten Zeitstempeln existieren im deutschen Recht keine gesonderten Regelungen, so dass die beweisrechtlichen Vorschriften für elektronische Dokumente anzuwenden sind. Für eine höhere Beweisgeeignetheit des qualifizierten Zeitstempels als sonstige elektronische Dokumente spricht, dass die Verknüpfung und Bescheinigung durch einen akkreditierten Dritten erfolgt. Es besteht eine Parallele zur Mitunterzeichnung einer Urkunde durch einen Dritten zur Bezeugung des Vorgangs. Je vertrauenswürdiger der Zeuge, desto eher ist seiner Aussage zu glauben. Diese glaubwürdige „Bescheinigung“ ist wiederum ein elektronisches Dokument, welches auch mit einer qualifizierten elektronischen Signatur versehen wurde, weswegen die besonderen Beweisverwertungsregeln des Urkundenbeweises gelten (vgl. § 371a ZPO; siehe auch Abschnitt 3.3).

Ein Zeitstempel von einem Anbieter, welcher vergleichbaren Anforderungen genügt wie denen von einem qualifizierten Zeitstempelanbieter kann aber ebenso in den Prozess als Beweismittel eingeführt werden und muss als ebenso beweiskräftig gelten soweit der Anbieter des Zeitstempels sonst als vertrauenswürdig gilt.

## 2.2 Daten innerhalb des eLabs

Die nachfolgenden Abschnitte beschreiben unterschiedliche Arten von Daten, die über vom eLab an die Schnittstelle des BeLab-Systems übermittelt werden.

### 2.2.1 Labormetadaten

Alle Informationen, die das Experiment beschreiben, werden hier dokumentiert.

Neben der Beschreibung und der Dokumentation von wichtigen Parametern (z. B. Umgebungstemperatur, Messgeräteinstellungen, Mengeneinheiten von verwendeten Chemikalien etc.) gehören auch andere aussagefähige Daten (z. B. Fotos vom Versuchsaufbau) dazu. Insbesondere ist auch die Messapparatur inklusive des Messdatenhandlings genau zu erfassen.

### 2.2.2 Messdaten

Während dem Ablauf eines Experiments bzw. über den Forschungsprozess hinweg entstehen insb. in naturwissenschaftlichen Fachbereichen Messdaten. Eine grobe Klassifizierung dieser Messdaten wird in den folgenden Abschnitten vorgenommen.

#### 2.2.2.1 Allgemeine Messdaten

Messdaten, die bei der Durchführung des Versuchs anfallen, werden dokumentiert.

Zu diesen Daten gehören sowohl automatisch von der Messapparatur erfasste als auch manuell erfasste Daten. Die Dateneingabe erfolgt unmittelbar während oder nach dem Versuch.

#### 2.2.2.2 Rohdaten / interpretierte Daten / Primärdaten

Bei den Messdaten ist zwischen Rohdaten und interpretierten Daten zu unterscheiden. Rohdaten werden nicht in jedem Fall aufgenommen. Der Wissenschaftler hat darüber zu entscheiden, ob er die Rohdaten und oder die interpretierten Daten aufnimmt. Diese Entscheidung muss der Wissenschaftler gegenüber der Forschungs-Community verantworten.

### 2.2.3 Auswertung

Während der Auswertung von Ergebnissen werden innerhalb des Forschnungsprozesses unterschiedliche Daten verarbeitet. Die hierbei entstehenden Daten müssen ebenfalls dokumentiert werden. Dies kann automatisch durch die verwendete Software oder manuell erfolgen. Im Falle einer automatisierten Auswertung ist auch der Auswertungsprozess ansich bzw. die verwendete Software (beispielsweise durch die Archivierung des zugehörigen Source-Codes) zu dokumentieren. Auch Konfigurations- und Verarbeitungsparameter (z. B. Hardware, Betriebssystem, Version), bzw. die Umgebung in der die Auswertung erfolgt, sollten festgehalten werden.

### 2.2.4 Dateiformate

Das DOMEA-Organisationskonzept 2.1[7] und die Standards und Architekturen für E-Government-Anwendungen (SAGA)[8] empfehlen, ebenso wie die von der Europäischen Kommission geförderte Anforderungsspezifikation für die elektronische Schriftgutverwaltung für die langfristige Ablage von elektronischem Schriftgut nur wenige und einheitliche Datenformate zu benutzen. Dazu gehören die in den folgenden Abschnitten aufgeführten Formate.

#### 2.2.4.1 Text (ASCII)

ASCII (American Standard Code for Information Interchange) steht für einen Zeichensatz und für ein Textformat. Ein ASCII-Text beschreibt ein Dokument, das nur aus Zeichen des ASCII-Zeichensatzes besteht, also keine Layout-Informationen beinhaltet und eignet sich somit besonders für einfache Textinformationen und Metadaten. Der ASCII-Code wurde

[7] Vgl. http://www.opentext.de/3/global/sol-products/sol-pro-docmgmt-collaboration/pro-domea-overview.htm, Stand 21.1.2011.

[8] Vgl. http://www.cio.bund.de/DE/Standards/SAGA/saga_node.html, Stand 21.1.2011.

1972 von der International Organisation für Standardisation als ISO 64632 spezifiziert und bietet aus heutiger Sicht die besten Voraussetzungen für eine andauernde Verkehrsfähigkeit. Dieses Dateiformat kann man für einfache und unformatierte Texte (Textdateien) verwenden.

#### 2.2.4.2 PDF/A

PDF/A-134 ist ein als ISO-Norm verabschiedeter Standard zur Verwendung von PDF 1.4 für die Langzeitarchivierung elektronischer Dokumente. Es wird als ISO 19005-1:2005 veröffentlicht.
Die Norm spezifiziert zwei Konformitätsebenen:

- PDF/A-1a - Level A conformance: sowohl eindeutige visuelle Reproduzierbarkeit als auch Abbildbarkeit von Text nach Unicode und inhaltliche Strukturierung des Dokuments.
- PDF/A-1b - Level B conformance: eindeutige visuelle Reproduzierbarkeit.

PDF/A wird auch in der von der Europäischen Kommission geförderten Richtlinie für die elektronische Schriftgutverwaltung als Format für die Archivierung empfohlen.
Es wird für sämtliche zeichenorientierten Dokumente verwendet.

#### 2.2.4.3 ODF

Das Open Document Format (ODF) wurde von OASIS als XML-basiertes Dokumentenformat für Texte, Tabellenkalkulationen, Präsentationen und andere Office-Dokumente standardisiert. Inhalt der Dokumente und Informationen über ihr Layout sind voneinander getrennt und können dadurch unabhängig verarbeitet werden. Es kann zum Austausch von komplexen Dokumenten eingesetzt werden, die zur Weiterbearbeitung vorgesehen sind. Im November 2006 erfolgte die Veröffentlichung von OpenDocument v1.0 unter dem Namen ISO/IEC 26300:2006 als Standard. Das OpenDocument Format wird u. a. durch das plattformunabhängige, lizenzfreie und offene Office-Paket von OpenOffice.org unterstützt. Es wird für sämtliche zeichenorientierten Dokumente verwendet.

#### 2.2.4.4 TIFF

Das „Tagged Image File Format“ (TIFF) erlaubt das Speichern von Grafikinformationen ohne Informationsverlust und ist nach ISO 12639 für die medienunabhängige Bildverarbeitung standardisiert worden. Die Kodierung des Formats erlaubt es, mehrere Darstellungen (z. B. Thumbnails) oder Versionen einer Grafik oder auch Textinformation als Metadaten in einer Datei abzulegen. Der Einsatz von TIFF ist vor allem immer dann angezeigt, wenn die grafischen Informationen eines Dokuments von maßgeblicher Bedeutung für die Aussagekraft sind. Unterstützt wird TIFF durch alle gängigen Grafik- und

Präsentationsprogramme. TIFF kann zum Einsatz kommen, wenn die Fähigkeit des Formats benötigt wird, mehrseitige Dokumente darzustellen. Für eingescannte Textdokumente (Graustufen- oder S/W-Grafiken) ist TIFF besonders geeignet. Es wird für Abbildungen (Non Coded Information, bspw. Rasterbilder) verwendet.

#### 2.2.4.5 JPEG

Das JPEG-Format (Joint Photographic Experts Group) steht für ein Kompressionsverfahren und ein Grafikformat und ist eines der am häufigsten im Internet verwendeten Grafikformate. Der JPEG-Standard wurde als ISO / IEC 10918-1 im Jahr 1992 veröffentlicht. Da die Definition der Struktur von JPEG-Dateien viele Freiheiten erlaubt, wurde mit dem „JPEG File Interchange Format“ (JFIF) ein Standard definiert, der den Austausch von JPEG-komprimierten Bilddaten organisiert. JFIF baut auf den JPEG-Standard auf und ist plattformunabhängig. Die Verwendung des JPEG-Formates als Alternative zu TIFF kann angezeigt sein, wenn ein Kompromiss zwischen Bildqualität und Dateigröße gefunden werden muss.

#### 2.2.4.6 PNG

PNG (Portable Network Graphics) wurde von der späteren „PNG Development Group“ als Alternative zum GIF-Format entwickelt und eignet sich wegen der Möglichkeit der verlustfreien Kompression und inkrementellen Anzeige der Grafiken vor allem für Anwendungen im Internet. Die PNG-Spezifikation ist offengelegt und wurde als ISO / IEC 15948 im Jahr 2003 zum internationalen Standard erhoben. Das PNG-Format wird von den meisten Bildverarbeitungsprogrammen standardmäßig unterstützt. So genannte Kalibrierungs-Datenblöcke erlauben die Kalibrierung der Darstellung damit z. B. der Ausdruck eines Bildes genauso aussieht, wie es der Autor an seinem Bildschirm gesehen hat. Es wird für Abbildungen (Non Coded Information, bspw. Rasterbilder) verwendet.

#### 2.2.4.7 AnIML und GAML

Die Analytical Information Markup Language (AnIML) ist eine Standardisierung des E13.15 Sub-Komitee der American Society for Testing and Materials (ASTM). AnIML ist ein Standard, der ein XML-basiertes, universelles Dateiformat für die Dokumentation, den Austausch und die Verwaltung von Labordaten beschreibt. Es eignet sich für viele verschiedene analytische Messtechniken.

AnIML besteht aus einem generischen Datencontainer, der die Speicherung von beliebigen analytischen Daten ermöglicht. Dieser Datencontainer enthält mehrdimensionale Daten, Name-Wert-Paare und Hierarchien. Um die sich kontinuierlich ändernden Anforderungen in der Messtechnik zu erfüllen, unterstützt AnIML ein Erweiterungs-Konzept, das den

Herstellern oder Endverbrauchern ermöglicht, zusätzliche Daten zu spezifizieren, die für eine bestimmte Messtechnik gespeichert werden sollen.
Die Generalized Analytical Markup Language (GAML) ist ebenfalls ein XML-basiertes Format, das speziell für die Speicherung und Archivierung von Daten aus einem breiten Spektrum von analytischen Messgeräten entworfen wurde. Ziel der GAML-Entwicklung ist der Schutz des geistigen Eigentums in wissenschaftlichen Organisationen. Das Design von GAML ist flexibel genug, um viele verschiedene Arten von Daten aufzunehmen. Die Verwendung des GAML-XML-Schemas ist lizenzfrei.

# 3 Rechtliche Aspekte

Das BeLab-Projekt berührt in Zielsetzung und Ausgestaltung unterschiedliche Rechtsgebiete. Zuvorderst steht die Beweiswerterhaltung wissenschaftlicher Forschungsergebnisse im Kontext digitaler Datenerzeugung, -auswertung und -haltung. Es geht um die „gerichtsfeste“ Aufbereitung und Aufbewahrung wissenschaftlicher Daten für den Eventualfall der gerichtlichen Auseinandersetzung. Im Zuge dessen werden etablierte Techniken und Konzepte (z. B. elektronische Signaturen und Zeitstempel nach dem Signaturgesetz) für elektronische Daten überprüft und auf deren Anwendbarkeit bewertet. Dies zieht die Fragestellung nach anderen und neuen Sicherheits- und Archivierungstechniken nach sich, welche ihrerseits wieder rechtlich überprüft werden müssen. Schließlich werden durch die verwendeten Technologien weitere Rechte und Pflichten der Nutzer und Verwender eines eLab berührt, deren Einsatz daher rechtskonform ausgestaltet werden muss.

## 3.1 Chancen: Einsatz und Verwendungsmöglichkeiten

Durch den Einsatz der BeLab-Schnittstelle ergibt sich eine Reihe von Vorteilen (Chancen) im rechtlichen Kontext. Denn die beweissichere Erhebung und die langfristige Verfügbarkeit von Forschungsprimärdaten und Forschungsmetadaten als Beweismittel ist für verschiedene potentielle Streitgebiete relevant. Die Beweisbarkeit wissenschaftlicher Ergebnisse ist Grundlage für die Verwirklichung der Ziele guter wissenschaftlicher Praxis (GWP) und der guten Laborpraxis (GLP), wie sie in verschiedenen technischen Richtlinien, Normen und den Bestimmungen von Forschungseinrichtungen (z. B. Max-Planck-Gesellschaft - MPG)[9] und Fördermittelgebern (z. B. Deutsche Forschungsgemeinschaft - DFG)[10] zum Ausdruck kommen.[11] Gleichzeitig können durch die Beweisbarkeit wissenschaftlicher Ergebnisse Fälschungs- und Plagiatsvorwürfe entkräftet und strafrechtlich relevante Falle des „Wissenschaftsbetrugs“ aufgedeckt werden. Auch geht es um die Einhaltung von Formvorschriften bei Zulassungs- und Kontrollverfahren sowie um den Streit um Urheberechte und Patente. Daneben ist die Verwirklichung von Aufbewahrungspflichten (auch im Sinne von Compliance) erforderlich, welche sich aus Bestimmungen der GWP, der GLP, der Produkt- und Materialprüfung und von Zulassungs- und Kontrollverfahren ergeben können.

---

[9] Vgl. Max-Planck-Gesellschaft: Regeln zur Sicherung guter wissenschaftlicher Praxis, Max-Planck-Gesellschaft, 2000, http://www.mpip-mainz.mpg.de/~pleiner/ombuds/regeln.pdf, Stand 21.1.2011.

[10] Vgl. Deutsche Forschungsgemeinschaft: Sicherung guter wissenschaftlicher Praxis – Safeguarding Good Scientific Practice – Denkschrift, WILEY-VCH, 1998, http://www.dfg.de/download/pdf/dfg_im_profil/reden_stellungnahmen/download/empfehlung_wiss_praxis_0198.pdf, Stand 21.1.2011.

[11] Vgl. zu den verschiedenen Kodizes zur GWP die Zusammenfassung bei Hartmann, K. / Fuchs, T, WissR 2003, 204(205f.).

## 3.2 Ausgangspunkt: Prozessrecht und das „gerichtsfeste“ Laborbuch

Zur Verwirklichung der Ziele muss eine Überlegung zum Prozessrecht angestellt werden. Denn es geht um die Beweiswerthaltung von Forschungsdaten für den Eventualfall der gerichtlichen Auseinandersetzung.[12] Von entscheidender Bedeutung ist daher die Bewertung von Forschungsdokumentationen und elektronischen Labordaten im Prozessrecht. Ausgangspunkt für die Überlegungen seien die Regeln der Zivilprozessordnung (ZPO).

Auf die Vorschriften der ZPO zur Beweisaufnahme und Beweisverwertung wird auch in den Verfahren- und Prozessordnungen anderer Gerichtsbarkeiten Bezug genommen. Sie gelten aufgrund von Verweisungen entsprechend.[13] Dies gilt ohne Einschränkungen auch für die Regelungen zum Beweiswert von elektronischen Dokumenten nach § 371a ZPO; so nach § 98 VwGO für die Verfahren vor den Verwaltungsgerichten,[14] nach § 118 Absatz 1 SGG für die Verfahren vor den Sozialgerichten,[15] nach § 58 ArbGG in Verbindung mit § 46 Absatz 2 ArbGG für Verfahren vor den Arbeitsgerichten,[16] nach § 99 Absatz 1 PatG[17] sowie nach § 82 Absatz 1 S.1 MarkenG[18] sowie nach § 18 Absatz 2 GebrMG sowie nach § 23 Absatz. 2 GeschmMG und nach § 36 SortSchG[19] in Verfahren vor dem Bundespatentgericht. Dagegen sind für Verfahren vor den Finanzgerichten nach § 82 FGO die Vorschriften (siehe §§ 371a, 415 - 444 ZPO), die den Urkundenbeweis regeln, ausdrücklich nicht in Bezug genommen. Auch in den Strafverfahren nach der StPO gelten keine Beweisverwertungsreglungen hinsichtlich Urkunden bzw. elektronischen Dokumenten. Elektronische Dokumente werden im Strafverfahren wahlweise als Urkunden oder sonstige Beweismittel angesehen. Da die StPO jedoch keine Beweisverwertungsregeln hinsichtlich der Art des Beweises kennt, erübrigt sich eine Abgrenzung. Elektronische Dokumente inkl. elektronischer Zeitstempel unterliegen im Strafprozess der freien Beweiswürdigung des Gerichts.

Zusammenfassend lässt sich festhalten, dass abgesehen von Verfahren vor den Strafgerichten und den Finanzgerichten, die Regelungen der ZPO zur Beweisverwertung für Urkunden und von elektronischen Dokumenten uneingeschränkt für die wichtigsten öffentlichen Gerichtsbarkeiten und Verfahren.

---

[12] Damit sei hier auch jede Art von außergerichtlichen Streitverfahren bezeichnet, bei denen es auf die Entscheidung eines unabhängigen Dritten auf Grundlage von Tatsachen ankommen kann: z. B. Mediations- und Schlichtungsverfahren, Widerspruchsverfahren, Universitäre Prüfungs- und Ehrenrausschüsse.

[13] Dazu und zur Verweisungstechnik allgemein: Rudisile, Schoch/Schmidt-Aßmann/Pietzner, VwGO, 20. Ergl. 2010, § 98 Rn. 2ff.

[14] *Garloff*, BeckOK VwGO, Stand 01.10.2010, Edition 15, § 98 Rn. 5.

[15] *Keller*, Meyer-Ladewig/Keller/Leitherer, Sozialgerichtsgesetz, 9. Aufl. 2008, § 118 Rn. 9ff.

[16] *Koch*, Erfurter Kommentar zum Arbeitsrecht, 11. Aufl. 2011, ArbGG § 58 Rn. 1.

[17] Mes, Patentgesetz Gebrauchsmustergesetz, 2. Aufl. 2005, PatG § 99 Rn. 2; Schäfers, Benkard, 10. Aufl. 2006, PatG § 88 Rn. 2.

[18] Ingerl/Rohnke, Markengesetz, 3. Aufl. 2010, § 82 Rn. 1ff. und § 74 Rn. 1.

[19] Wobei das GebrMG, das GeschmMG und das SortSchG jeweils ihrerseits nur auf das PatG verweisen.

## 3.3 Beweissicherheit durch Signaturen und Zeitstempel

Herkömmliche Laborbücher aus Papier könnten als Urkunden im Sinne der §§ 415ff. ZPO Eingang in das Verfahren finden. Urkunden unterliegen besonderen Beweisverwertungsregeln und gelten deswegen bereits als das stärkste und sicherste Beweismittel im Prozessrecht. Elektronische Dokumente aller Art sind dagegen nach § 371 Absatz 1 S.2 ZPO Objekte des Augenscheins und unterliegen der freien Beweiswürdigung des Gerichts. Nur über die Ausnahmereglung des § 371a Absatz 1 ZPO gelten für elektronischen Dokumenten, welche mit einer qualifizierten elektronischen Signatur nach dem SigG ausgestatte sind, die Regeln für Urkunden.

Im Rahmen der BeLab-Anwendung wird dieser Nachteil elektronischer Dokumente adressiert und versucht über zwei Ansätze auszuräumen:

### 3.3.1 Qualifizierte elektronische Signaturen und Zeitstempel

BeLab wird es ermöglichen, dass der Anwender seine Daten mit seiner eigenen qualifizierten elektronischen Signatur versehen kann. Mit der qualifizierten elektronischen Signatur lässt sich die Authentizität und die Integrität eines elektronischen Dokuments nachweisen. Es lässt sich feststellen wer das Dokument erstellt hat und dass es nicht mehr verändert wurde. Über § 371a ZPO genießen solcherart signierte elektronische Dokumente eine Privilegierung und für sie gelten die Beweisregeln für Urkunden entsprechend.

BeLab wird es auch ermöglichen, dass der Anwender seine Daten mit einem qualifizierten elektronischen Zeitstempel versehen kann. Dieser Zeitstempel muss vom Anwender von einem Zertifizierungsdiensteanbieters nach Wahl dessen Wahl bezogen werden. Der Anwender trägt die Kosten dafür. Mit dem qualifizierten elektronischem Zeitstempel, der in der Regel einen qualifizierte elektronische Signatur beinhaltet, kann nachgewiesen werden, dass ein elektronisches Dokument in unveränderten Form ab einem bestimmten Zeitpunkt vorgelegen hat.

### 3.3.2 Lückenlose Datenhaltung und fortgeschrittene Signaturen

BeLab wird die Beweiswerterhaltung elektronischer Dokumente weiter durch die Verwendung von fortgeschrittenen Signaturen und der in der Archivierung immanenten lückenlosen Datenhaltung steigern:

BeLab wird es ermöglichen, dass Anwender ihre Daten mit einer fortgeschrittenen elektronischen Signatur versehen können. Durch deren Verwendung wird zwar nicht der Anwendungsbereich des § 371a ZPO eröffnet, jedoch lässt sich im Rahmen der freien Beweiswürdigung die Entscheidung des Gerichts durch äußere Tatsachen lenken. Fortgeschrittenen Signaturen, welche von einem vertrauenswürdigen Anbieter (z. B. DFN-

PKI) stammen, ermöglichen der Nachweis, wer ein signiertes Dokument unterzeichnet hat und das es nicht mehr verändert wurde.
BeLab wird es auch ermöglichen, dass die Daten des Anwenders durch einen sonstigen elektronischen Zeitstempel (z. B. des DFN-Dienstes) gesichert werden können. Auch damit ließe sich der Beweis darüber führen, dass bestimmte Daten unverändert ab einem bestimmten Zeitpunkt vorlagen.
Daneben wird BeLab eine lückenlose Datenhaltung der Forschungsdokumentationen ermöglichen. Das Löschen von Daten wird nur unter eingeschränkten Vorrausetzungen möglich sein. Daten können in der Regel. nur storniert werden. Wird storniert, wird der Vorgang protokolliert und später Nachweisbar sein, ob etwas storniert wurde. So soll das Verschwinden und Schönigen von Messreihen verhindert werden. Der Anwender kann beweisen, dass er seine Ergebnisse lückenlos protokolliert und seine Ergebnisse nicht im Nachhinein verfälscht hat.

## 3.4 Risiken und rechtliche Rahmenbedingungen

Schließlich werden durch die verwendeten Techniken weitere Rechte und Pflichten der Nutzer und Verwender eines eLab berührt, deren Einsatz daher rechtskonform ausgestaltet werden muss.
Zu Fragen ist besonders nach der rechtkonformen Ausgestaltung des Angebots im Bezug auf das Recht der Informationellen Selbstbestimmung und bzw. des Datenschutzrechts. Betroffene Person ist hier vor allen der Forscher / Verwender. Die in einem eLab aufgezeichneten Daten könnten Personenbezug haben oder über eine Profilbildung der Nutzung Rückschlüsse über die Arbeitstätigkeit erlauben, wodurch sich auch ein Personenbezug herstellen ließe. Noch größere Relevanz erlangt dies im Kontext von offensichtlich personenbezogenen Daten von Patienten, Probanden und menschlichen Forschungsobjekten. Hier muss sichergestellt werden, dass die in den Datenschutzgesetzen des Bundes und der Länder verankerten Prinzipen der Datensparsamkeit, Anonymisierung und Pseudonymisierung umgesetzt werden. Dies ist bereits Aufgabe des vorgeschalteten eLabs. Entsprechendes gilt für Fragen der IT-Sicherheit und das Recht auf Integrität informationstechnischer Systeme. Verhindert werden muss ein Angriff auf gespeicherte Forschungsprimärdaten um Diebstahl, Sachbeschädigung, Terrorismus, Spionage, Wirtschaftskrieg, Werks- und Betriebsspionage und Fälle des unlauteren Wettbewerbs zu verhindern.
Festzustellen bleibt das sich ein eLab und die BeLab Schnittstelle im Umfeld von verfassungsrechtlichen und einfachgesetzlichen Rahmenbedingungen bewegt und entsprechende Ge- und Verbote einhalten muss. Berührte Grundrechte können sein

- Freiheit der Wissenschaft, Art. 5 Abs. 3 GG,
- Eigentumsgarantie in Bezug auf Forschungsdaten, Art. 14. Abs.1 GG,
- Recht auf informationelle Selbstbestimmung, Art. 2 Abs.1; 1 Abs.1 GG,
- Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 Abs.1; 1 Abs.1 GG.

Im einfachgesetzlichen Rahmen geht es um

- Bereichsspezifisches Datenschutzrecht,
- Allgemeines Datenschutzrecht,
- Zulassungs- und Kontrollverfahren,
- (besondere)Verwaltungsverfahren,
- Subventionen und staatliche Förderung,
- Privatwirtschaftliche Förderung,
- Arbeitnehmerschutz,
- Urheberrecht,
- Patentrecht,
- Zivilprozess, Strafprozess, Verwaltungsgerichtsverfahren,
- Umsetzung (technischer) Normen und Standards (DIN, ISO etc.).

# 4 Die BeLab-Schnittstelle

Neben der Darstellung der Anforderungen an das zu entwerfende System und anzubindener Systeme, werden in diesen Abschnitt sowohl die eModule des BeLab-Systems beschrieben, als auch die Schnittstellen zu externen Systemen, wie Archiv- und eLab-Systemen. Des Weiteren erfolgt die Definition der Konzepte für: Klassifizierung, Metadaten und Sicherheit.

## 4.1 Anforderungen an die Realisierung des BeLab-Systems

In Abschnitt 4.3 werden in Anlehnung an die TR 03125 die Anforderungen an die Realisierung der Ausgabeschnittstelle des BeLab-Systems zur Anbindung von Archivsystemen spezifiziert. Zusätzlich werden an das BeLab-System durch die angebundenen Laborbücher sowie die Beweiswerterhaltung und Langzeitarchivierung Anforderungen gestellt. Die Anforderungen an das BeLab-System können wie folgt zusammengefasst werden:

a) Anbindung von eLabs an das BeLab-System.
b) Gewährleistung der Anforderungen zur Beweiswerterhaltung sowie Langzeitarchivierung bei der Verarbeitung von Daten im BeLab-System.
c) Anbindung des BeLab-System an Archivsysteme, z. B. über einen XML-Adapter zur Referenzarchitektur der TR 03125.
d) Berücksichtigung der Schnittstelle TR-VLA-S.4 zwischen dem XML-Adapter und dem ArchiSafe-Modul bei der Implementierung des XML-Adapters als Modul für die Ausgabeschnittstelle des BeLab-Systems.

Für die Umsetzung von a) sind intensive Arbeiten des BeLab-Projekts zusammen mit Entwicklern von eLabs erforderlich. Hierfür wurden unterschiedliche eLabs analysiert. An der Entwicklung des Prototyps für das BeLab-System sind beispielsweise die Entwickler der Projekte DataFinder[20] und OpenEnventory[21] sowie weitere externe Partner beteiligt.

Die Umsetzung der Anforderungen in b) erfordert die Berücksichtigung der in Abschnitt 3 vorgegebenen rechtlichen Aspekte. Zusätzlich werden bestehende Rahmenrichtlinien und Empfehlungen für die Langzeitarchivierung z. B. basierend auf dem nestor Handbuch[22] in der Implementierung des BeLab-Systems umgesetzt.

Um die in c) gestellten Anforderungen zu adressieren, ist es empfehlenswert, sich an dem entsprechenden Abschnitt TR-VLA-M.5 in der TR 03125 zu orientieren. Da die TR 03125, wie in 4.3.1 erläutert, aktuell noch überarbeitet wird, sind für die Realisierung eines

[20] Vgl. http://www.dlr.de/sc/datafinder, Stand: 21.1.2011.

[21] Vgl. http://www.open-enventory.de, Stand: 21.1.2011.

[22] Vgl. Neuroth, H.; et al. (Hrsg.): nestor Handbuch - Eine kleine Enzyklopädie der digitalen Langzeitarchivierung - Version 2.3, Niedersächsische Staats- und Universitätsbibliothek Göttingen, 2010, http://nestor.sub.uni-goettingen.de/handbuch/nestor-handbuch_23.pdf, Stand: 21.1.2011.

entsprechenden XML-Adapters intensive Arbeiten des BeLab-Projekts erforderlich. Eine Referenzimplementierung hierfür existiert derzeit nicht.

Die durch d) implizierten Anforderungen sind im Rahmen der TR 03125 (ArchiSafe Interface, TR-VLA-S.4) definiert. Der XML-Adapter eröffnet zu diesem Zweck einen sicheren Kommunikationskanal mit dem ArchiSafe-Modul und versendet eine Archivanfrage. Diese Anfrage enthält eine Aufgabenbeschreibung[23] und optional das zu archivierende Objekt in Form eines XAIP-Dokumentes (XML Archive Information Package)[24].

Da das BeLab-System gemäß der Anforderungen aus a) und b) die beweiswerterhaltende Archivierung von Daten unterschiedlicher eLabs in verschiedene Archivsysteme unterstützen soll, ist sowohl für die Eingabe- als auch die Ausgabeschnittstelle des BeLab-Systems eine generische Schnittstelle erforderlich. Die Anbindung der eLabs und Archivsysteme erfolgt in Form von unterschiedlichen Moduln dieser generischen Schnittstellen (z. B. als XML-Adapter gemäß Referenzarchitektur der TR 03125).

## 4.2 Architektur des Belab-Systems

Abbildung 2 zeigt die Komponenten des BeLab-Systems. In den folgenden Abschnitten werden der konkrete Aufbau und die Funktion der einzelnen Komponenten erläutert. Ausgehend von dem Import der beweissicher zu archivierenden Daten aus eLabs zeigt die Abbildung den Verlauf von deren Verarbeitung bis hin zur Langzeitarchivierung. Die Komponenten adressieren somit die im vorherigen Abschnitt gestellten Anforderungen durch die Anbindung von eLabs sowie der Anbindung des BeLab-Systems an Archivsysteme.

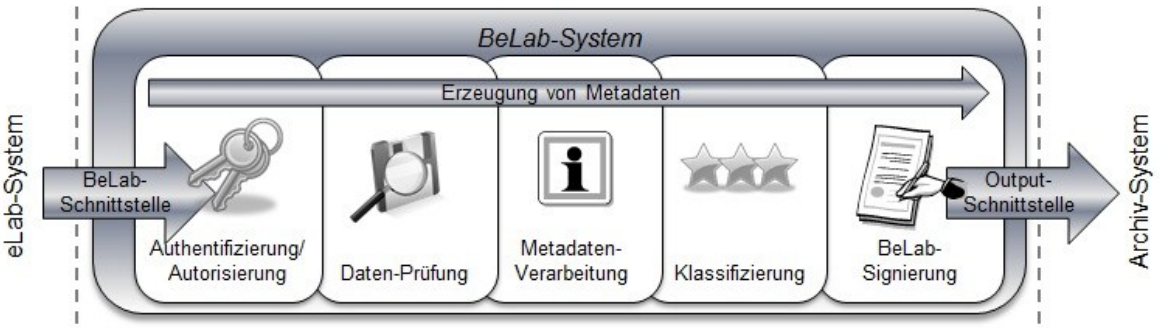


**Abbildung 2: Komponenten des BeLab-Systems**

### 4.2.1 Anbindung elektronischer Laborbücher (eLab-Schnittstelle)

An das BeLab-System lassen sich unterschiedliche eLabs anbinden. Die eLabs übermitteln hierfür z. B. zu archivierende Labor-, Mess- oder Forschungsdaten an die BeLab-Schnittstelle. Die Daten müssen hierfür vom eLab entsprechend aufbereitet werden. Im

[23] Siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_S4.pdf?__blob=publicationFile, Stand 21.1.2011.

[24] Siehe Anhang TR-VELS-F in https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_F.pdf?__blob=publicationFile, Stand: 21.1.2011.

Idealfall handelt es sich bereits um XML-Daten. Die BeLab-Schnittstelle akzeptiert jedoch zusätzlich Dateien in unterschiedlichen Formaten. Siehe dazu auch Abschnitt 4.5.

### 4.2.2 BeLab-Schnittstelle

Die BeLab-Schnittstelle ist als Web Service realisiert, der von den angebundenen eLabs verwendet wird. Über SOAP und REST Nachrichten können die Laborbücher zu archivierende Daten an das BeLab-System übermitteln. Eine detaillierte Beschreibung der zur Verfügung gestellten externen Funktionen ist im Anforderungspapier [BeA10] für die Anbindung externer Laborbücher enthalten. Dies umfasst auch die anschließende Suche nach archivierten Daten bzw. das Auslesen von Informationen und die Prüfung von Signaturen.

Daten können entweder direkt als XML-Strukturen in den Anfragen an die BeLab-Schnittstelle (SOAP / REST) oder als Datei (SOAP Attachment) übermittelt werden. Die BeLab-Schnittstelle erfordert zusätzlich, dass in den Anfragen ein sog. BeLab-Container angegeben wird. Dieser Container umfasst beispielsweise eine eindeutige ID des eLab (SystemID) und ermöglicht eine Strukturierung der vom eLab abgelegten Daten (ProjektID, ContainerID). Nach erfolgreicher Archivierung liefert die BeLab-Schnittstelle dem Benutzer eine Antwort zurück, die eine eindeutige ID der eingelagerten Daten im Archiv beinhaltet.

#### 4.2.2.1 Daten importieren

Der Benutzer kann Daten an die BeLab-Schnittstelle übergeben. Vor der Übertragung werden die Daten durch den Benutzer einem Datentyp zugeordnet, um eine Strukturierung der Daten zu erzielen. Die Verantwortung der Richtigkeit liegt beim Benutzer. Jedem übertragenen Datum wird vom System eine eindeutige DatenID zugewiesen. Dadurch wird ein späteres Auslesen des Datums ermöglicht. Der Import-Vorgang kann zu jeder Zeit durch den Benutzer gestartet werden.

Aus Performancegründen kann es von Vorteil sein nicht alle Daten an das BeLab-System übertragen zu müssen. Des Weiteren dies auch aus Gründen der Vertraulichkeit der Daten gewünscht sein. In diesem Fall ist der Import des zu den Daten gehörigen Hashwertes vorgesehen. Anstelle der Daten wird also der Hashwert durch das BeLab-System beweiswerterhaltend archiviert. Die Archivierung der Daten übernimmt der Benutzer des Systems.

#### 4.2.2.2 Daten exportieren

Daten, die durch den Benutzer an die BeLab-Schnittstelle zur Archivierung übergeben wurden, können aus dem Archiv exportiert werden. Dazu muss vom Benutzer die entsprechende DatenID angegeben werden. Exportiert werden benutzerabhängig nur die zu den Projektdaten gespeicherten Metadaten oder der gesamte Datenumfang.

#### 4.2.2.3 Daten stornieren

Daten können aus dem Archiv nicht gelöscht werden, um eine nachträgliche Manipulation der Forschungsdaten zu verhindern. Stattdessen kann ein Benutzer Daten als storniert kennzeichnen. Dazu ist vom Benutzer die entsprechende DatenID anzugeben. Entsprechende Zugriffe auf das BeLab-System werden protokolliert.

Aufgrund existierender Vorgaben bzgl. einer Archivierungsfrist von Daten, wie beispielsweise die Forderung der DFG Forschungsdaten für mind. 10 Jahre vorzuhalten, kann beim Datenimport eine Archivierungsdauer angegeben werden. Innerhalb dieser Frist ist das Stornieren der Daten nicht möglich.

#### 4.2.2.4 Daten suchen/Management der DatenIDs

Das Archiv kann vom Benutzer durchsucht werden. Dazu muss der Benutzer gewünschte Suchkriterien angeben. Als Rückgabewert erhält der Benutzer eine Liste von DatenIDs.

#### 4.2.2.5 Administration

Die administrativen Tätigkeiten werden protokolliert. Während der Installation des BeLab-Systems werden Administratoren festgelegt, denen die alleinige Verantwortung für die Pflege des Systems zugewiesen wird. Bei allen schreibenden administrativen Tätigkeiten (Schreibzugriff, Stornieren) kann bei besonders sensiblen Fällen ein Vier-Augen-Prinzip realisiert werden. Entsprechende Tätigkeiten können somit nur ausgeführt werden, wenn zwei Administratoren in die Veränderung einwilligen (z. B. durch die Verwendung eines geteilten Schlüssels oder Passworts).

Neben den Administrationen werden Benutzer und Systeme verwaltet, die auf die BeLab-Schnittstelle zugreifen dürfen. Dabei werden die Benutzer den Systemen zugeordnet, so dass durch den Benutzer kein Zugriff auf Daten erfolgen kann (Mandantenfähigkeit), für die er keine Berechtigung besitzt.

Des Weiteren werden in der BeLab-Schnittstelle verschieden Zugriffsrechte verwaltet. Diese sind:

- Schreibzugriff
- Lesezugriff
- Stornieren
- Suchen

Die Zugriffsrechte werden durch die Administratoren der eLabs im BeLab-System gepflegt.

### 4.2.3 Erzeugung von Metadaten

Während der gesamten Verarbeitung der vom eLab übermittelten Daten werden zusätzliche Metadaten erzeugt. Hierfür wird für jede Anfrage an die BeLab-Schnittstelle ein Metadaten-Container erzeugt, der anschließend gefüllt und an das Archivsystem übermittelt wird. Im

Metadaten-Container werden beispielsweise die Ausgabe bzw. der Status der Verarbeitung durch die Komponenten des BeLab-Systems gespeichert. Der Metadaten-Container kann somit auch als zusätzliche Protokollierung (Logfile) der BeLab-Verarbeitung, die den archivierten Daten direkt zugeordnet ist, angesehen werden. Als Basis für den Container werden Dublin Core Metadaten sowie eine zugehörige RDF Struktur verwendet. Details hierzu können dem Metadaten-Konzept in Abschnitt 4.5 entnommen werden.

### 4.2.4 Authentifizierung und Autorisierung

Die Web Services des BeLab-Systems werden unter Verwendung von HTTPS realisiert, um neben der Vertraulichkeit, Integrität und Verbindlichkeit der übermittelten Daten auch die Authentizität des Absenders (eLab) und des BeLab-Systems (als Empfänger) gleichermaßen zu gewährleisten. Für die Übermittlung von Anfragen an die BeLab-Schnittstelle, müssen die angebundenen eLabs hierfür Client-Zertifikate (nach X.509) verwenden. Anhand dieser Client-Zertifikate erfolgt die Authentifizierung des eLabs, angebundenen Geräten bzw. Ressourcen des Labors sowie insbesondere von Benutzern bzw. natürlichen Personen, die das eLab verwenden. Im BeLab-System werden Wurzelzertifikate für die Überprüfung der Authentizität der Zertifikate (z. B. der DFN-PKI[25]) hinterlegt. Anhand der eindeutigen ID des Zertifikats (distinguished name) erfolgt eine anschließende Autorisierung, die beispielsweise den Zugriff bestimmter Benutzer für einzelne System-, Projekt- oder ContainerIDs erlauben oder verweigern kann. Das BeLab-System beinhaltet hierfür eine entsprechende Benutzerverwaltung, deren Administration in einzelnen Bereichen auch an die Betreiber des eLabs delegiert werden kann.

### 4.2.5 Datenprüfung

Das BeLab-System kann eine Konsistenzprüfung der von den eLabs übermittelten Daten durchführen (z. B. Gewährleistung fortlaufender Zeitstempel oder Sequenznummern, Verarbeitung von Bildern nur mit zugehörigen Messdaten). Diese Validierung der Eingabedaten kann von den Betreibern der eLabs für die jeweilige System-, Projekt- oder ContainerID angepasst werden. Durch die Prüfung der Konsistenz kann eine fehlerhafte Archivierung von Daten zusätzlich vermieden werden. Vorrangig ermöglicht die Daten-Prüfung allerdings die Abbildung von Forschungsprozessen auf die Verarbeitung der Daten im BeLab-System. So kann beispielsweise gewährleistet werden, dass zu einem Experiment bzw. Projekt, gemäß den Vorgaben der Wissenschaftler, in jedem Fall alle erforderlichen Daten (Versuchsaufbau, Messwerte) hinterlegt werden[26]. Eine vollständige inhaltliche

[25] Siehe https://www.pki.dfn.de/, Stand 21.1.2011.

[26] Vgl. Abschnitt 2.2.

Prüfung der einzelnen Daten ist hierbei aufgrund der individuellen Prozesse und damit verbundenen Daten in unterschiedlichen Forschungsbereichen nicht möglich.
Im Rahmen der Datenprüfung können auch die eingehenden Datenformate geprüft werden. Beispielsweise können Formate, die für die Langzeitarchivierung nicht geeignet sind abgelehnt werden. Handelt es sich hierbei um Datenformate die bereits eine elektronische Signatur der Daten beinhalten, kann diese Signatur für die Konsistenzprüfung (Integrität und Authentizität der übermittelten Daten) verwendet werden.
Werden während der Konsistenz-, Format- oder Signaturprüfung von der Komponente Fehler ermittelt, so wird die weitere Verarbeitung im BeLab-System abgebrochen und dem Benutzer bzw. dem eLab eine Fehlermeldung zurückgeliefert. Durch eine Bestätigung des Benutzers kann der Archivierungsprozess fortgesetzt werden. Die fehlerhafte Prüfung sowie die manuelle Bestätigung für die Fortsetzung des Archivierungsprozesses werden protokolliert. Sie werden gemeinsam mit den Ergebnissen von erfolgreich durchgeführten Prüfungen im Metadaten-Container vermerkt und somit für eine spätere Verwendung archiviert.

#### 4.2.5.1 Überprüfung der Signatur

Wurde eine Datei übertragen, die bereits mit einer Signatur versehen ist, wird diese durch die BeLab-Schnittstelle unter Zuhilfenahme des Kryptomoduls (TR-03125-VLA-M.2, siehe Abschnitt 4.3.1) überprüft. Ist die Signatur nicht gültig, wird die Datei abgewiesen und nicht eingelagert. Das Einreichen von Dateien, die nicht signiert sind, ist möglich. In diesem Fall kann jedoch nur eine geringe Beweiskraft gewährleistet werden, welche sich in der niedrigeren Klassifizierung widerspiegelt (siehe dazu Abschnitt 4.4).

#### 4.2.5.2 Signieren von Daten

Alle Daten, d. h. bereits signierte Daten oder nicht signierte Daten, die an die BeLab-Schnittstelle übertagen wurden, werden (über-)signiert. Parallel können mehrere Signierungstechniken eingesetzt werden.

#### 4.2.5.3 Überprüfung des Datenformats

Das BeLab-System prüft, ob das Format der übergebenen Datei für die Langzeitarchivierung geeignet ist. Als geeignet werden folgende Formate eingestuft:

- ASCII etc.
- PDF/A
- TIFF nach ISO
- ODF
- PDF, TIFF (bedingt geeignet)

Entspricht das Dateiformat nicht den hier angegeben, wird ein entsprechender Hinweis gesendet. Die Archivierung der Datei ist auch bei einem ungeeigneten Datenformat möglich. In diesem Fall wird jedoch seitens der BeLab-Schnittstelle keine Aussage über eine langfristige Interpretierbarkeit der Daten getroffen und dies entsprechend in der Klassifizierung (vgl. Abschnitt 4.4) vermerkt.

#### 4.2.5.4 Konsistenzchecks

Wurden mehrere Dateien übertragen wird im Anschluss der Überprüfung aller Dateien eine Vollständigkeitsprüfung (soweit möglich) durchgeführt. Möglich ist z. B. das Überprüfen von Sequenznummern einer Reihe von eingereichten Bildern. Um Daten auf ihre Vollständigkeit und Konsistenz überprüfen zu können, muss durch den Administrator des zugehörigen eLabs eine Datenstruktur definiert werden. Nach diesem Schema erfolgt anschließend die Datenüberprüfung.

Nur bei einer positiven Datenüberprüfung erfolgt eine direkte Archivierung der Daten. Bei einer negativen Überprüfung bedarf es der Bestätigung des Benutzers zur weiteren Verarbeitung. Ist die Vollständigkeit nicht überprüfbar, erfolgt ein entsprechender Hinweis an den Benutzer. Nach dessen Bestätigung können die Daten auch in ungeprüfter Form archiviert werden. Die Fortsetzung der Archivierung trotz fehlerhafter Datenüberprüfung wird in den Metadaten archiviert (Log) protokolliert und gemeinsam mit den Daten archiviert.

### 4.2.6 Metadaten-Verarbeitung

Bereits in den übermittelten Daten vorhandene Metadaten (Zeitstempel, Namen und Bezeichnungen, Kameraparameter usw.) werden in der Komponente für die Metadaten-Verarbeitung in den von der BeLab-Schnittstelle angelegten Metadaten-Container übernommen. Zusätzliche Erweiterungen für die Metadaten-Verarbeitung können durch die eLab Betreiber implementiert werden. Diese Erweiterungen erlauben die Ableitung weiterer Metadaten aus den übermittelten Daten. Die Metadaten ermöglichen z. B. eine spätere Suche nach den archivierten Daten.

### 4.2.7 Klassifizierung

Insbesondere basierend auf den in Abschnitt 4.2.5 durchgeführten Überprüfungen der vom eLab übermittelten Daten wird in dieser Komponente eine Klassifizierung des Beweiswerts sowie der Eignung der Daten für die Langzeitarchivierung vorgenommen. Das BeLab-Projekt definiert unterschiedliche Klassen für den Beweiswert (z. B. unsignierte, signierte Daten, fortgeschrittene oder qualifizierte Signaturen, Konsistenz des Forschungsprozesses) und die Langzeitarchivierung (geeignete Formate wie PDF/A oder TIFF nach ISO). Siehe auch Abschnitt 4.4. Die Klassifizierung der Daten ermöglicht eine qualitative Bewertung der durch

das BeLab-System in Bezug auf die übermittelten Daten gewährleisteten Anforderungen im Hinblick auf die langfristige Beweiswerterhaltung.

### 4.2.8 BeLab-Signierung

Von den eLabs übermittelte Daten, im Rahmen des BeLab-Systems erzeugte Metadaten sowie vorrangig die durch die im vorherigen Abschnitt beschriebene Komponente ermittelte Klassifizierung werden mit einer elektronischen Signatur durch das BeLab-System bestätigt. Diese Signatur gewährleistet bei nachfolgenden Prüfungen der Daten im Archiv die korrekte Verarbeitung durch das BeLab-System, sowie die Integrität der erzeugten Metadaten. Sie erfüllt mindestens die Anforderungen der fortgeschrittenen elektronischen Signatur und stammt von einem vertrauenswürdigen Anbieter (z. B. DFN-PKI).

### 4.2.9 Anbindung externer Archivsysteme

Für die Anbindung von Archivsystemen realisiert das BeLab-System eine generische Schnittstelle, die für verschiedene Archivsysteme benutzt werden kann. Als Beispiel für ein Archivsystem kann das ArchiSafe Projekt, wie im Abschnitt 4.3.1 beschrieben, dienen. In diesem Beispiel implementiert diese Schnittstelle ein XML-Adapter gemäß den Vorgaben der TR 03125 (TR-VLA-M.5). Um diese XML-Adapter zu implementieren wird im Sinne dieser Richtlinie ein Archivdatenobjekt erstellt, d. h. ein für die langfristige Ablage in einem elektronischen Archivsystem bestimmtes elektronisches Dokument. Dieses Archivdatenobjekt ist ein selbst-beschreibendes XML-Dokument, das gegen ein gültiges und autorisiertes XML-Schema geprüft werden kann (wie beispielsweise XAIP). Ein solches Archivdatenobjekt enthält sämtliche Inhaltsdaten (Primärinformationen) und Metainformationen, die für eine rechts- und revisionssichere Rekonstruktion von Geschäfts- oder Verwaltungsvorgängen bis zum Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfristen erforderlich sind.

## 4.3 Anforderungen an das Archivsystem

Im Abschnitt 4.1 wurden bereits Anforderungen an das BeLab-System in Bezug auf die Anbindung an die nachgelagerten Archivsysteme definiert. In diesem Abschnitt werden darüber hinaus relevante Vorgaben und Empfehlungen für geeignete Archivsysteme erläutert.

### 4.3.1 Die TR 03125

Ausgangspunkt für die Implementierung der Ausgabeschnittstelle des BeLab-Systems zu angebundenen Archivsystemen bildet die technische Richtlinie 03125[27] des BSI. Die TR

[27] Siehe BSI Technische Richtlinie 03125: Vertrauenswürdige elektronische Langzeitspeicherung (VELS), vgl. https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html, Stand 21.01.2011.

03125 wird momentan überarbeitet. Sie wird Anfang 2011 neu veröffentlicht als: BSI Technische Richtlinie 03125: Beweiswerterhaltung kryptographisch signierter Dokumente (BSI 03125: TR-ESOR).

Teilnehmer des BeLab-Projekts sind in diese Überarbeitung involviert und übernehmen die resultierenden Veränderungen in die vorliegende Spezifikation für die Schnittstelle des BeLab-Systems zur Anbindung von externen Archivsystemen. Das BSI hat darüber hinaus in Gesprächen angedeutet, das Projekt BeLab dahingehend fördern zu wollen, dass eine IT-Architektur gemäß des „Scope TR“[28] zur Verfügung gestellt wird.

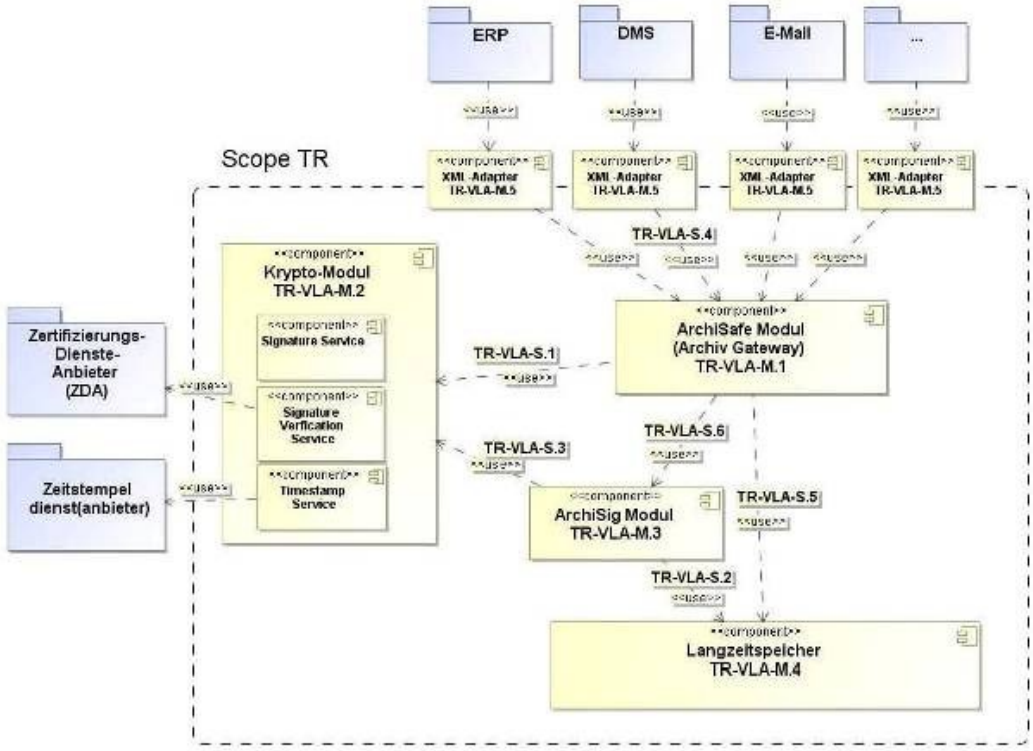


**Abbildung 1: Schematischer Aufbau einer Referenzarchitektur[29]**

Die XML-Adapter sind anwendungsspezifische oder anwendungstypspezifische Datenkonverter, welche die Daten und Dokumente aus den jeweiligen Datenformaten der vorgelagerten Anwendungen in das einheitliche, XML basierte Datenformat des elektronischen Archivs überführen. Über die XML-Adapter wird auch die standardisierte Kommunikation mit dem zentralen *Archiv-Gateway,* dem ArchiSafe-Modul, geführt. Der XML-Adapter übernimmt dabei die Rolle eines standardisierten Konnektors.

Der XML-Adapter soll, je nach Gesamtarchitektur des Archivs und Bedarf, mandantenfähig sein. Er muss in der Lage sein, alle Funktionen des ArchiSafe-Moduls, an das er

[28] Siehe Abbildung 1.

[29] Siehe TR 03125 V1.0 Hauptdokument S. 56.

angeschlossen ist, korrekt zu nutzen und eine sichere und zuverlässige Kommunikation in beide Richtungen (Anwendung und Archiv) korrekt abzubilden.

### 4.3.2 Meta-Datenbank

Das eingesetzte Archivsystem sollte über die Möglichkeit zum Führen einer Meta-Datenbank verfügen. Diese ermöglicht das Auffinden archivierter Objekte anhand von bekannten Attributen (bzw. Metadaten). Ein mögliches Szenario, könnte der Verlust der nach der Archivierung zurückgelieferten Objekt-Identifikation sein. Hier könnte mittels der archivierten Metadaten eine nachträgliche Ermittlung der Identifikation erfolgen. Innerhalb des XAIP-Objektes (vgl. Abschnitt 4.2.9) wird ein Bereich zur Aufnahme von spezifischen Metadaten vorgehalten. Diese werden durch einen Adapter mandantenspezifisch der Meta-Datenbank übergeben.

### 4.3.3 ArchiSig

Zweck des ArchiSig-Moduls ist der rechtskonforme Erhalt der Authentizität, Integrität und damit des beweisrechtlichen Werts vor allem elektronisch signierter Archivdatenobjekte durch zusätzliche kryptographische Sicherungsmittel. Das ArchiSig-Modul implementiert für diesen Zweck eine kryptographische Lösung, die insbesondere sicherstellt, dass das durch §17 Signaturverordnung (SigV) normierte Verfahren zur Aufrechterhaltung der Sicherheit und Vertrauenswürdigkeit elektronischer Signaturen durch eine erneute Signatur zuverlässig und wirtschaftlich, d. h. auch für große Datenmengen, erfüllt werden kann. Die erneute elektronische Signatur muss die Daten und frühere Signaturen einschließen und mit sicherheitsgeeigneten kryptographischen Algorithmen und Parametern erzeugt werden. Für die erneute elektronische Signatur ist zumindest ein qualifizierter Zeitstempel notwendig, der eine qualifizierte elektronische Signatur trägt. Das Erneuerungsverfahren kann automatisiert und so eingerichtet werden, dass viele Dokumente gemeinsam elektronisch neu signiert werden.

## 4.4 Klassifizierungssystem

Durch die Klassifizierung der Daten anhand der Datenformate, erhobenen Metadaten und verwendeten Signatur erhält der Nutzer einen Hinweis auf den Grad des Beweiswerts und mögliche Risiken bei der Langzeitarchivierung der Daten.
Bzgl. des Beweiswerts sind folgende Klassen vorgesehen:

**/Klasse B1/** *Keine*: Es ist keine oder nur eine einfache elektronische Signatur vorhanden.

**/Klasse B2/** *Fortgeschritten*: Die Daten werden vom BeLab-Nutzer mit einer fortgeschrittenen elektronischen Signatur versehen; es besteht die Möglichkeit der Authentifizierung und Integritätsprüfung. Die Sicherung wird mit einem

elektronisch signierten Zeitstempel, der vom BeLab-Anbieter zur Verfügung gestellt wird, dokumentiert.

**/Klasse B3/** *Qualifiziert:* Die Daten werden vom BeLab-Nutzer mit einer qualifizierten elektronischen Signatur versehen; es besteht die Möglichkeit der Authentifizierung und Integritätsprüfung. Die Sicherung wird mit einem elektronisch signierten Zeitstempel, der vom BeLab-Anbieter zur Verfügung gestellt wird, dokumentiert.

**/Klasse B4/** *Qualifiziert+*: Wie **/Klasse B3/**, jedoch wird die Sicherung mit einem qualifizierten elektronisch signierten Zeitstempel von einem Zeitstempeldienst nach Wahl des BeLab-Nutzers dokumentiert.

**/Klasse B5/** *Akkreditiert*: Die Daten werden vom BeLab-Nutzer mit einer qualifizierten elektronischen Signatur eines akkreditierten Zertifikatdiensteanbieters versehen; es besteht die Möglichkeit der Authentifizierung und Integritätsprüfung. Die Sicherung wird mit einem elektronisch signierten Zeitstempel, der vom BeLab-Anbieter zur Verfügung gestellt wird, dokumentiert.

**/Klasse B6/** *Akkreditiert+*: Wie **/Klasse B5/**, jedoch wird die Sicherung mit einem qualifizierten elektronisch signierten Zeitstempeldienst nach Wahl des BeLab-Nutzers dokumentiert.

Zusätzlich zu den **Klassen B1** bis **B6** kann eine Sicherung der Datenintegrität in folgende Klassen eingestuft werden:

**/Klasse S1/** *ungesicherte Datenerzeugung*: Bei der Datenerzeugung (z. B. den Messungen, der Übertragung an Auswertungsgeräte und Programme, der Übertragung der Daten in das eLab) wird keine besondere Sicherung der Datenintegrität durch automatisierte Verschlüsselung / Signierung am Messgerät sichergestellt.

**/Klasse S2/** *gesicherte Datenerzeugung*. Die Sicherung der Datenintegrität wird durch die automatische Übernahme der erzeugten Daten vom Messgerät zum eLab, einer Prüfung der Datenkonsistenz innerhalb des Forschungsprozesses und der Signierung (Verschlüsselung durch elektronische Signaturverfahren) dieser Daten belegt.

Die Bewertung der Tauglichkeit zur Langzeitarchivierung basiert auf dem Datenformat der übergebenen Datei. Strukturierte Daten, wie z. B. Datenbanken (oder Archive), sollten vor der Archivierung aufgetrennt werden, so dass ihre einzelnen enthaltenen Datensätze (bzw.

Dateien) während der Archivierung klassifiziert werden können. Folgende Klassen sind vorgesehen:

**/Klasse L1/** *Ungeeignet*: Eine in dem Datenformat übergebene Datei kann evtl. nach einigen Jahren nicht mehr interpretiert werden. Beispiele: proprietäre und/oder nicht weit verbreitete Datenformate.

**/Klasse L2/** *Geeignet:* Eine in dem Datenformat übergebene Datei kann wahrscheinlich nach einigen Jahren noch interpretiert werden. Beispiele: PDF, TIFF, DOC, DOCX, XLS, XLSX sowie Archive im ZIP Format, die diese Formate enthalten.

**/Klasse L3/** *Empfohlen*: Für das gewählte Datenformat kann angenommen werden, dass sie auf lange Zeit interpretierbar bleiben. Beispiele: ASCII, XML, PDF/A, PDF/E, PDF/UA bzw. PDF/X, TIFF nach ISO; SVG; ODF sowie Archive im TAR Format, die diese Formate enthalten.

Eine detaillierte Begründung für die Eignung von den jeweiligen Dateiformaten für die Langzeitarchivierung wird im nestor Handbuch beschrieben[30].
Eine Klassifizierung besteht aus der Zusammensetzung der Klassen **B**, **S** und **L**.

**Beispiel:** Eine Sicherung wird vom BeLab-Nutzer mit einer qualifizierten elektronischen Signatur versehen. Zur Dokumentation des Sicherungszeitpunkts wird der Zeitstempel des BeLab-Anbieters benutzt. Die Daten wurden nicht automatisch bzw. ohne Sicherung von den Messgeräten händisch ins eLab übertragen. Das Datenformat PDF/A wird verwendet. Die Sicherung erfüllt damit Vorrausetzungen der Klassen **B3**, **S1** und **L3**; d. h. die Eigenschaft zur Beweiswerterhaltung wird als *qualifiziert* eingestuft. Die Datenerzeugung ist *ungesichert.* Die Sicherung ist zur Langzeitarchivierung *geeignet*.

## 4.5 Metadatenkonzept

Mithilfe von Metadaten können zusätzlich Kontextinformationen zu Daten hinterlegt werden. So werden beispielsweise deskriptive Metadaten (beschreibende Metadaten) genutzt, um das Auffinden von Ressourcen zu ermöglichen. Während strukturelle Metadaten (Strukturdaten) Informationen zu Eigenschaften der Datei (wie Dateiname, Format, Größe, Prüfsumme etc.) liefern, dienen administrative Metadaten als Informationsquelle für Herkunft, Archivierung und Technik. Des Weiteren existieren Metadaten, die speziellen Anforderungen angepasst wurden, wie z. B. Metadaten zur Rechteverwaltung.

[30] Ludwig, J.: Formate - Auswahlkriterien. In Neuroth, H., Oßwald, A., Scheffel, R., Strathmann, S. & Jehn, M. (Hrsg.), *Nestor Handbuch – Eine kleine Enzyklopädie der digitalen Langzeitarchivierung* (Version 2.3) (Kap.7.3), siehe http://nestor.sub.uni-goettingen.de/handbuch/ - Stand vom 23.01.2011.

In der Regel werden in einem Forschungsprozess eine Vielzahl von Daten (Dateien) unterschiedlichster Formate erzeugt, die teilweise in Beziehung stehen. Daher ist es von Vorteil, wenn mehrere Dateien zusammengefasst und deren Beziehung zueinander beschrieben werden kann. Da die Forschungsdaten einem (Langzeit-)Archiv übergeben werden sollen, sind administrative Metadaten und Metadaten, die für die Langzeitarchivierung benötigt werden, unerlässlich.
Für die Strukturierung von Metadaten wurden eine Reihe von Standards definiert. Die in BeLab verwendet werden, sollen im Folgenden dargestellt werden:

- Dublin Core: Der Dublin Core Standard ist von allgemeinerer Natur. Mit ihm lassen sich Dokumente (Ressourcen) jeglicher Art beschreiben. Dazu werden 15 Kernelemente, wie creator, title und subject, definiert. Der Standard wird domain-übergreifend von Museen, Bibliotheken, Archiven, Regierungsbehörden und der Wirtschaft verwendet. Ein Mapping von umfangreichen Formaten zu Dublin Core ist möglich.
- METS: Mit dem METS Standard, basierend auf dem Projekt Making of America II (MOA2), wurde ein Konzept für ein XML-Dokument entworfen, das mithilfe von Metadaten die Verwaltung und den Austausch von digitalen Objekten ermöglichen sollte. Ein METS-Dokument besteht dabei aus sieben Hauptabschnitten, denen die Metadaten (deskriptive, strukturelle und administrative Metadaten) zugeordnet werden. Des Weiteren dienen zwei Abschnitte als Container für die digitalen Objekte selbst und als Strukturbeschreibung des digitalen Objekts.
- LMER: LMER ist ein Standard für Langzeitarchivierungsmetadaten und dient als Ergänzung zu existierenden Standards für bibliographische Metadaten. Er ist größtenteils auf Angaben, die automatisiert generiert werden können, beschränkt und beinhaltet Kernelemente, die für alle Dateikategorien (Dateiformat) gültig sind.
- UOF: Im Rahmen des Projekts kopal wurde ein Format definiert, mit dem digitale Objekte und die dazugehörigen Metadaten zusammen archiviert und zwischen Archivsystemen ausgetauscht werden können. Das Format basiert auf den Standards METS und LMER und wird als METS-Profile-Universelles-Objektformat (UOF) bezeichnet. Ein Objekt nach UOF kann beliebig viele Dateien in einer frei definierbaren Ordnerstruktur enthalten. Pflicht ist lediglich eine auf der Wurzelebene befindlichen Datei mit der Bezeichnung „mets.xml“. Diese muss eine nach dem METS-Schema gültige XML-Datei darstellen. Teile der METS-Struktur werden durch Elemente des LMER-Standards ersetzt, wobei Elemente, die bereits durch METS-Elemente beschrieben wurden, weggelassen werden.

Die während eines Forschungsprozesses anfallenden (Labor-)metadaten sind vom Forschungsprozess und dem jeweiligen Forschungsgebiet abhängig. Jedoch lassen sich allgemein gültige Metadaten, wie z. B. Projektkennzeichnung, Forscher, Datum etc., definieren. Für diesen Fall eignet sich der Dublin Core Standard, der durch die Kernelemente eine gute Basis bildet. Um dem Forscher die größtmögliche Freiheit hinsichtlich der Angabe von deskriptiven Metadaten zu ermöglichen, ist es sinnvoll die Auswahl nicht durch einen Standard zu beschränken, sondern mehrere Formate zuzulassen.
Ein Metadaten-Standard bzw. die Definition eines Archivformats, das die genannten Forderungen erfüllt, bildet das o. g. universelle Objektformat (UOF). Bis zu 5000 Dateien können in einer beliebigen Verzeichnisstruktur in einem UOF zusammengefasst werden. Als Paketformate können ZIP oder TAR verwendet werden. Metadaten zum Archivobjekt werden innerhalb der mets.xml-Datei angegeben. Die im UOF verwendeten Abschnitte sind: METS Header, Descriptive Metadata, Administrative Metadata, File Section und Structural Map. Wobei sich der Abschnitt Administrative Metadata in die Unterabschnitte Technical Metadata und Digital Provenance Metadata unterteilt. Optional können auch weitere Abschnitte, die über den METS Standard definiert wurden, verwendet werden. Die administrative Metadaten werden durch den Standard LMER 1.2 in einem modularen Aufbau beschrieben, wobei nur Elemente des Standards und nicht die Struktur selbst verwendet werden. Zum Einsatz kommen die XML-Schemata: lmer-object.xsd, lmer-file.xsd und lmer-process.xsd.
Aus den o. g. Gründen ist es für das BeLab-Metadatenformat sinnvoll auf dieser Datenstruktur aufzubauen. Dadurch ist zum einen eine flexible Verwendung von Metadaten möglich, basiert jedoch auf existierenden Standards (METS und LMER). Des Weiteren kann ein im Projekt kopal entwickelter Konverter (kolipri) für die Dateiformatierung genutzt werden. Durch ihn werden von Nutzer ausgewählte Dateien zu einem UOF-Elemente verknüpft und eine mets.xml automatisch generiert. Metadaten, die auf der Basis der Dateiinformationen zur Verfügung stehen, werden automatisiert extrahiert und in die mets.xml übernommen. Im Anschluss können weitere Metadaten durch den Anwender oder während der Verarbeitung im BeLab-System hinzugefügt werden.

## 4.6 Sicherheitskonzept

Dargestellt wird eine Abgrenzung der Verantwortungsbereiche, die auf die Kooperation mehrerer eigenständiger Systeme (dem BeLab-System sowie angebundene eLabs und Archivsysteme) zurückzuführen ist. Neben den grundlegend geltenden Sicherheitskriterien werden Maßnahmen beschrieben, die im Rahmen des BeLab-Systems realisiert werden.

### 4.6.1 Verantwortungsbereich

Grundlage für die Betrachtung des Sicherheitsaspektes bildet die physikalische Trennung von eLab-, BeLab- und Archivsystem. Die Verantwortung für ein hinreichend entwickeltes Sicherheitskonzept für das verwendete eLab- und Archivsystem liegt in der Verantwortung der jeweiligen Entwickler und Anwender der Systeme.

Unabhängig davon trägt allein der Wissenschaftler, der die Daten im eLab bereitstellt, die inhaltliche Verantwortung für deren Sicherheit. Dies bedeutet insbesondere, dass er selbständig geeignete Maßnahmen vorsehen muss, um die Vertraulichkeit von Daten zu gewährleisten. Für weiterführende Informationen zum Thema IT-Sicherheitsrichtlinien sei auf das IT-Sicherheitsmanagement nach ISO 27001 und den IT-Grundschutz des BSI[31] verwiesen.

Allgemein werden im Rahmen des Sicherheitskonzepts für das BeLab-System folgende grundlegenden Kriterien an die Übertragung und Verarbeitung von Daten betrachtet:

- Integrität: Die Integrität der Daten ist gewährleistet, wenn nachgewiesen kann, dass die Daten vollständig und unverfälscht vorliegen. D. h. Manipulationen oder ungewollte Veränderungen, z. B. durch Übertragungs- oder Hardwarefehler, müssen nachweisbar sein.
- Vertraulichkeit: Der Zugriff auf Daten durch unberechtigte Personen muss verhindert werden. Dazu gehören das unberechtigte Einsehen, Weiterleiten oder Veröffentlichen der Daten.
- Verfügbarkeit: Zu jeder Zeit muss ein Zugriff auf das System gewährleistet sein. Die Zugriffszeit muss dabei in einem vertretbaren Rahmen liegen. Außerdem darf das System keine Schwachstellen bieten, deren Ausnutzung den ordnungsgemäßen Betrieb mindern.
- Verbindlichkeit/Authentizität: Die Identität eines Erstellers eines Datums muss eindeutig nachweisbar und unveränderbar sein.

Generell liegt die Verantwortung für die gesicherte Nutzung des BeLab-Systems beim Anwender, da im Rahmen der prototypischen Implementierung des Systems keine Gewährleistung gegenüber möglichen Manipulationen übernommen werden kann. Maßnahmen, die zur Sicherung der oben genannten Kriterien innerhalb des BeLab-Projekts vorgenommen wurden, werden in den folgenden Abschnitten dargelegt.

[31] Siehe hierzu https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html, Stand: 21.1.2011.

### 4.6.2 Sicherheitsmaßnahmen

In die Betrachtung des Sicherheitskonzepts fallen die Datenübertragung zum BeLab-System, die interne Verarbeitung der Daten im BeLab-System und das externe Umfeld des Systems.

#### 4.6.2.1 Datenübertragung

Die Übertragung der Daten zum BeLab-System erfolgt über HTTPS. Hierbei werden neben Server-Zertifikaten zur Gewährleistung der Authentizität des BeLab-Systems gegenüber dem eLab zusätzlich Client-Zertifikate verwendet, die eine eindeutige Authentifizierung jedes angeschlossenen eLab Systems gegenüber dem BeLab-System erlauben (zusammen mit dem Server-Zertifikat des BeLab-Systems wird eine gegenseitige Authentifizierung ermöglicht). Die Zertifikate können von dem Administrator des BeLab-Systems für das eLab registriert werden. Durch die Verwendung von HTTPS inkl. Client-Zertifikaten, ist die Integrität, die Verbindlichkeit (sowie Authentizität) und die Vertraulichkeit der Daten während der Datenübertragung gewährleistet.

#### 4.6.2.2 BeLab-System intern

##### 4.6.2.2.1 Reproduzierbarkeit der Klassifizierung

Die Integrität der im Rahmen des BeLab-Systems erfolgten Klassifizierung wird durch eine (erneute) Signatur gewährleistet. Um Manipulationsmöglichkeiten an der vom BeLab-System ausgeführten Klassifizierung weitestgehend auszuschließen, erfolgt nach der Signierung eine erneute Klassifizierung. Das Ergebnis wird mit der zuvor durchgeführten Klassifizierung verglichen. Nur bei einer Übereinstimmung der Ergebnisse wird eine positive Meldung an den Benutzer ausgegeben.

##### 4.6.2.2.2 Art der Signatur

Die Signierung der Klassifizierung wird durch den BeLab-Anbieter vorgenommen. Dieser verwendet dazu wenigstens eine fortgeschrittene elektronische Signatur von einem vertrauenswürdigen Anbieter (z. B. DFN-PKI).

##### 4.6.2.2.3 Verfügbarkeit des BeLab-Systems

Das System wird in dem Maße abgesichert, dass evtl. (interne) Systemfehler nicht zu einem Systemabbruch, sondern zu einem kontrollierten Abbruch des Prozesses führen.

##### 4.6.2.2.4 Container des BeLab-Systems

Das BeLab-System soll als Java-basierter Web Service realisiert werden. Als Applikationsserver wird der Tomcat Server der Apache Software Foundation eingesetzt. Das System selbst nutzt AXIS2 zur Realisierung des Web Service. An dieser Stelle sei erneut

darauf hingewiesen, dass dieses Sicherheitskonzept nicht die Absicherung der verwendeten Systeme (Tomcat, AXIS2) umfasst.

#### 4.6.2.3 BeLab-System extern

##### 4.6.2.3.1 Administration

Das BeLab-System sieht die Definition eines Administrators vor. Nur durch ihn können Funktionen des BeLab-Systems manipuliert werden. Die Administration des Servers liegt in der Verantwortung des Systembetreibers.

##### 4.6.2.3.2 Verfügbarkeit des externen Systems:

Die Verfügbarkeit eingesetzter, externer Systeme, wie eLab- oder Archivsystem, liegt in der Verantwortung des Betreibers des entsprechend genutzten Systems.

##### 4.6.2.3.3 eLab und Archivsystem

Das Sicherheitskonzept umfasst keine Sicherung des eLab- und des Archivsystems. Entsprechende Sicherheitsmaßnahmen sind nach den Vorgaben der eingesetzten System einzuhalten.

# 5 Schlussbetrachtung / Summary

Die BeLab-Schnittstelle sorgt im Zusammenspiel mit der Verwendung eines entsprechenden eLabs für die medienbruchfreie Datenhaltung von wissenschaftlichen Prozessen und Dokumentationen in digitaler Form. Daten werden im modernen Forschungs- und Laborbetrieb digital erzeugt, erhoben, ausgewertet und archiviert. Eine Übertragung von Zwischenergebnissen in ein klassisches Laborbuch aus Papier ist damit im Rahmen des für das BeLab-System betrachteten Prozesses nicht mehr erforderlich. Eine nachträgliche Sicherung der digitalen Daten in analoger Form (etwa durch Ausdruck) zum Zwecke der Beweiswerterhaltung oder Langzeitarchivierung wird ebenfalls entbehrlich. Denn unter Ausnutzung der bereits bestehenden rechtlichen Rahmenbedingungen im Form des Rechts der elektronischen Signaturen und der Möglichkeit elektronische Dokumente in das Gerichtsverfahren einzubringen, lässt sich der Beweiswert der digital gehalten Forschungsdokumentationen wenigstens an den von Laborbüchern aus Papier angleichen, wenn nicht sogar verbessern. Gleichzeitig wird auf geprüfte Konzepte zur Langzeitarchivierung zurückgegriffen, um auch Archivierungspflichten hinsichtlich der Daten zu genügen.

# 6 Literatur und Quellen


| | |
|---|---|
| ArbGG | Arbeitsgerichtsgesetz (ArbGG) in der Fassung der Bekanntmachung vom 2. Juli 1979 (BGBl. I S. 853, 1036), das zuletzt durch Artikel 9 Absatz 5 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2449) geändert worden ist. |
| BeckOK VwGO | Posser, H. / Wolff, H. A., Beck'scher Online Kommentar VwGO, Stand 01.10.2010, Edition 15, C.H. Beck - München 2010, siehe http://beck-online.beck.de/Default.aspx?typ=reference&y=400&w=BeckOK&name=VwR - Stand 24.01.2011. |
| Benkhard, G. (Begr.) | Patentgesetz Gebrauchsmustergesetz, 10. Auflage, C.H. Beck - München 2006. |
| BeA10 | Projektgruppe Beweissicheres elektronisches Laborbuch (BeLab): Anforderungspapier V1.1 vom 19.11.2010, abzurufen unter: http://www.belab-forschung.de/belab/fileadmin/templates/mm_dam_fe/Anforderungspapier_V1.1_19.11.10.pdf |
| DFG | Deutsche Forschungsgemeinschaft: Sicherung guter wissenschaftlicher Praxis – Safeguarding Good Scientific Practice – Denkschrift, WILEY-VCH, 1998, siehe http://www.dfg.de/download/pdf/dfg_im_profil/reden_stellungnahmen/download/empfehlung_wiss_praxis_0198.pdf - Stand vom 23.01.2011. |
| FGO | Finanzgerichtsordnung (FGO) in der Fassung der Bekanntmachung vom 28. März 2001 (BGBl. I S. 442, 2262; 2002 I S. 679), die zuletzt durch Artikel 6 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2449) geändert worden ist. |
| GebrMV | Gebrauchsmusterverordnung (GebrMV) vom 11. Mai 2004 (BGBl. I S. 890), die zuletzt durch Artikel 3 der Verordnung vom 26. September 2006 (BGBl. I S. 2159) geändert worden ist. |
| GeschmMV | Geschmacksmusterverordnung (GeschmMV) vom 11. Mai 2004 (BGBl. I S. 884), die zuletzt durch Artikel 2 der Verordnung vom 6. Dezember 2010 (BGBl. I S. 1763) geändert worden ist. |
| GG | Grundgesetz (GG) für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch das Gesetz vom 21. Juli 2010 (BGBl. I S. 944) geändert worden ist. |
| Hartmann, K. / Fuchs, T | Standards guter wissenschaftlicher Praxis und wissenschaftliches Fehlverhalten vor dem Hintergrund der Wissenschaftsfreiheit, Wissenschaftsrecht 2003, S. 204 - 222. |
| Ingerl, R. / Rohnke, C. | Markengesetz, 3. Auflage, C.H. Beck - München 2010. |
| JKomG | Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG) vom 22.März 2005 (BGBl. I S. 837) . |

| | |
|---|---|
| Ludwig, J. | Formate - Auswahlkriterien. In Neuroth, H., Oßwald, A., Scheffel, R., Strathmann, S. & Jehn, M. (Hrsg.), *Nestor Handbuch – Eine kleine Enzyklopädie der digitalen Langzeitarchivierung* (Version 2.3) (Kap.7.3), siehe http://nestor.sub.uni-goettingen.de/handbuch/ - Stand vom 23.01.2011. |
| MarkenG | Markengesetz (MarkenG) vom 25. Oktober 1994 (BGBl. I S. 3082; 1995 I S. 156; 1996 I S. 682), das zuletzt durch Artikel 17 des Gesetzes vom 22. Dezember 2010 (BGBl. I S. 2248) geändert worden ist" |
| Mes, P. | Patentgesetz Gebrauchsmustergesetz, 2. Auflage, C.H. Beck - München 2005. |
| Meyer-Ladewig, J. / Keller, W, / Leitherer, S. | Sozialgerichtsgesetz - Kommentar, 9. Auflage, C.H. Beck - München 2008. |
| MPG | Max-Planck-Gesellschaft: Regeln zur Sicherung guter wissenschaftlicher Praxis, Max-Planck-Gesellschaft, 2000, siehe http://www.mpip-mainz .mpg.de/~pleiner/ombuds/regeln.pdf - Stand vom 23.01.2011. |
| Müller-Glöge, R. / Preis, U. (Hrsg.) | Erfurter Kommentar zum Arbeitsrecht, 11. Auflage, C.H. Beck - München 2011. |
| Neuroth, H.; et al. (Hrsg.) | nestor Handbuch - Eine kleine Enzyklopädie der digitalen Langzeitarchivierung - Version 2.3, Niedersächsische Staats- und Universitätsbibliothek Göttingen, 2010, siehe http://nestor.sub.uni-goettingen.de/handbuch/nestor-handbuch_23.pdf - Stand 23.01.2011. |
| PatG | Patentgesetz in der Fassung der Bekanntmachung vom 16. Dezember 1980 (BGBl. 1981 I S. 1), das zuletzt durch Artikel 1 des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2521) geändert worden ist. |
| RegE JKomG | Regierungsentwurf zum Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (BT- Drs 15/4067). |
| Schoch, F. / Schmidt-Aßmann, E. / Pietzner, R. | Verwaltungsgerichtsordnung - Kommentar, 20. Ergänzungslieferung, C.H.Beck - München, 2010. |
| SGG | Sozialgerichtsgesetz (SGG) in der Fassung der Bekanntmachung vom 23. September 1975 (BGBl. I S. 2535), das zuletzt durch Artikel 2 des Gesetzes vom 22. Dezember 2010 (BGBl. I S. 2262) geändert worden ist. |
| SigG | Signaturgesetz (SigG) vom 16. Mai 2001 (BGBl. I S. 876), das zuletzt durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091) geändert worden ist. |
| Signaturrichtlinie | Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Amtsblatt Nr. L 013 vom 19/01/2000, S. 12 bis 20 |

| | |
|---|---|
| SigV | Signaturverordnung (SigV) vom 16. November 2001 (BGBl. I S. 3074), die zuletzt durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542) geändert worden ist. |
| SortSchG | Sortenschutzgesetz (SortSchG) in der Fassung der Bekanntmachung vom 19. Dezember 1997 (BGBl. I S. 3164), das zuletzt durch Artikel 13 des Gesetzes vom 9. Dezember 2010 (BGBl. I S. 1934) geändert worden ist. |
| StPO | Strafprozeßordnung (StPO) in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 des Gesetzes vom 22. Dezember 2010 (BGBl. I S. 2300) geändert worden ist. |
| TR 03125 | Bundesamtes für Sicherheit in der Informationstechnik (2009). Technische Richtlinie 03125 - *Vertrauenswürdige elektronische Langzeitspeicherung*, siehe https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html - Stand vom 23.01.2011. |
| UrhG | Urheberrechtsgesetz (UrhG) vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 83 des Gesetzes vom 17. Dezember 2008 (BGBl. I S. 2586) geändert worden ist. |
| VwGO | Verwaltungsgerichtsordnung (VwGO) in der Fassung der Bekanntmachung vom 19. März 1991 (BGBl. I S. 686), die zuletzt durch Artikel 9 des Gesetzes vom 22. Dezember 2010 (BGBl. I S. 2248) geändert worden ist. |
| VwVfG | Verwaltungsverfahrensgesetz (VwVfG) in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), das zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2827) geändert worden ist. |
| ZPO | Zivilprozessordnung (ZPO) in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), die zuletzt durch Artikel 3 des Gesetzes vom 24. September 2009 (BGBl. I S. 3145) geändert worden ist. |