DFG-Projekt

Beweissicheres elektronisches Laborbuch (BeLab)

Anforderungspapier

Anforderungspapier für die Anbindung von elektronischen Laborbüchern an das BeLab-Projekt

Projektpartner:

UNIKASSEL VERSITÄT provet

KIT Karlsruhe Institute of Technology

PTB

Ansprechpartner unter: www.belab-forschung.de

Version:1.1

Datum: 19. November 2010

gefördert durch

DFG Deutsche Forschungsgemeinschaft

Versionshistorie

Version 1.1:

- Überarbeitung der Funktionen basierend auf den Ergebnissen des am 03.05.2010 in Kassel durchgeführten BeLab-Workshops.
- Überarbeitung der Klassendefinitionen des Klassifizierungssystems.

19. November 2010

Inhalt

1 Zielbestimmung

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 typischerweise 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 sollen eLabs auf technischem Weg eine Sicherheit verliehen werden, welche mit der von herkömmlichen papiergebundenen Laborbüchern vergleichbar ist oder sogar darüber hinausgeht.

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).

Im Folgenden werden die Anforderungen für die Anbindung eines eLabs an das BeLab-System beschrieben.

2 Realisierung des BeLab-Systems

Das BeLab-System wird durch einen Web Service realisiert und kann dadurch auf entfernten Rechnern ausgeführt werden. Die Kommunikation zwischen den Rechnern erfolgt über eine sichere Verbindung, wie z. B. HTTPS.

Konkret wird das System als Web Service in der Programmiersprache Java implementiert. Der Service stellt dem Benutzer die benötigten Funktionen (siehe Kapitel 3.1) zur Verfügung. Auf BeLab-systeminterne Funktionen, wie zum Beispiel die Signatur-Funktion, hat der Benutzer keinen direkten Zugriff. Innerhalb des BeLab-Systems werden folgende Arbeitsschritte umgesetzt:

1. Authentifizierung/Autorisierung
2. Überprüfung von Eingangsdaten
    a. Überprüfung der Signatur
    b. Überprüfung der Datenvollständigkeit und -konsistenz

c. Überprüfung der LZA-Tauglichkeit

3. Generierung/Übernahme von Metadaten
4. Klassifizierung nach Sicherheit und LZA-Tauglichkeit
5. Signierung der Daten

Das Protokollieren des BeLab-Prozesses geschieht über alle hier aufgeführten Punkte hinweg (siehe dazu 5.2.).

Die Realisierung der beweiswerterhaltenden Langzeitarchivierung basiert auf den Vorgaben der technischen Richtlinie TR 03125. Diese beinhaltet die Module (siehe auch Abbildung 1): ArchiSafe-Modul, Krypto-Modul, ArchiSig-Modul und einen Langzeitspeicher.

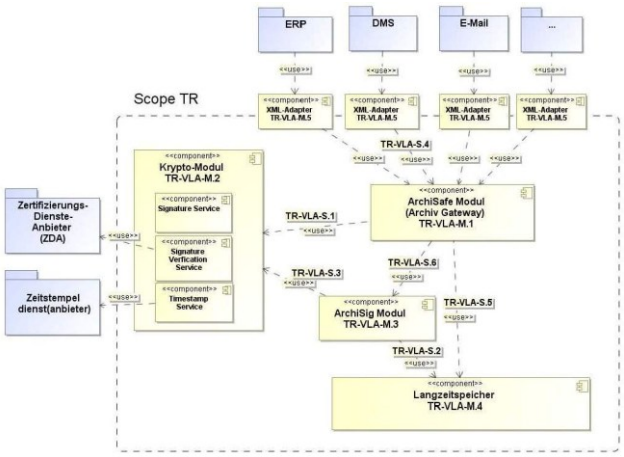

Abbildung 1: Schematischer Aufbau einer Referenzarchitektur[1]

3 Produktfunktionen

Im Folgenden werden die Funktionen des BeLab-Systems beschrieben. Unterschieden wird dabei nach externen Funktionen, die durch den Benutzer ausgeführt (Abschnitt 3.1) und internen Funktionen, die innerhalb das BeLab-Systems (Abschnitt 3.2) realisiert werden.

3.1 Benutzerfunktionen

Die im Folgenden beschriebenen externen Funktionen stehen den Benutzern des BeLab-Systems zur Verfügung. Sie werden durch **/FExxxx/** gekennzeichnet. FE steht dabei für „Externe Funktion“.

[1] TR 03125 V1.0 Hauptdokument S. 56

3.1.1 Authentifizierung und Autorisierung

Um das BeLab-System nutzen zu können, muss der Benutzer registriert und angemeldet sein.

/FE0010/ *Anmelden:* Ein Benutzer kann sich mithilfe eines Zertifikats am BeLab-System anmelden.

/FE0020/ *Authentifizieren:* Durch das BeLab-System wird die Identität des Benutzer eindeutig überprüft.

/FE0030/ *Autorisieren:* Es erfolgt eine Überprüfung, ob die vom Benutzer gewünschte Funktion von diesem Benutzer ausgeführt werden darf.

/FE0040/ *Abmelden:* Der Benutzer wird vom System abgemeldet.

3.1.2 Datenverwaltung

Ist ein Benutzer am BeLab-System angemeldet, kann dieser mit entsprechenden Rechten (siehe Abschnitt 3.1.3) folgende Funktionen durchführen:

/FE0110/ *Daten importieren:* Der Benutzer kann Daten in das BeLab-System übertragen. Vor der Übertragung soll der Benutzer der Datei einen Datentyp zuordnen. Mögliche Datentypen sind: **/D040/**, **/D050/**, **/D060/** und **/D070/**. Als Rückgabewert erhält der Benutzer eine eindeutige ID (DatenID), die die Daten identifiziert. (Vorgesehen ist, dass der Benutzer den Import-Vorgang zu jeder Zeit der Dateneingabe selbst starten und dadurch die Datenauthentizität und -integrität gewährleisten kann.) Wird der Funktion zusätzlich eine DatenID übermittelt, oder sind im BeLab System Regeln für die Erkennung von Dubletten (z.B. eindeutige Messreihen-Nr. etc.) hinterlegt, so erfolgt eine Versionierung des archivierten Datensatzes.

/FE0120/ *Daten exportieren:* Mit entsprechenden Rechten kann der Benutzer Daten aus dem BeLab-System exportieren. Dazu muss vom Benutzer die DatenID angegeben werden. Wird der Funktion zusätzlich der Parameter „Version“ übermittelt, so wird exakt diese angeforderte Version des Datensatzes, anstelle der aktuellen Version, exportiert.

/FE0130/ *Daten stornieren:* Das Stornieren von Daten kann der Benutzer anhand der DatenID veranlassen. Stornierte Daten (oder modifizierte) Daten bleiben jedoch unabhängig von ihrer Stornierungs-Kennzeichnung im Archiv gespeichert und können vom Administrator ausgelesen werden. Eine Stornierung ist bei mehreren vorliegenden Versionen nur insgesamt für die gesamte DatenID möglich.

Eine Löschung der Daten wird explizit nicht unterstützt, um eine nachträgliche Manipulation von Forschungsdaten zu verhindern.

/FE0140/ *Daten suchen:* Das Archiv kann vom Benutzer durchsucht werden. Dazu muss der Benutzer gewünschte Suchkriterien angeben. Als Rückgabewert erhält der Benutzer eine Liste von DatenIDs. Die zugehörigen Daten können über Funktion **/FE0120/** gelesen werden.

3.1.3 Administration

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 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). Die Administratoren können folgende Funktionen durchführen:

/FE0210/ *Benutzer anlegen:* Definition eines Benutzers, der auf das BeLab-System zugreifen darf.

/FE0220/ *Benutzerrolle definieren:* Definition der Benutzerrechte:

- Schreibzugriff (Funktion **/FE0110/**)
- Lesezugriff (Funktion **/FE0120/**)
- Stornieren (Funktion **/FE0130/**)
- Suchen (Funktion **/FE0140/**)

Benutzerrechte können zusätzlich auf Projekt- oder ContainerID Ebene vergeben werden.

/FE0230/ *Benutzer löschen:* Der ausgewählte Benutzer wird aus der Benutzerverwaltung gelöscht. (Der Administrator kann nicht gelöscht werden.)

/FE0240/ *Zertifikat ändern:* Dem Benutzer wird vom Administrator ein anderes Benutzer-Zertifikat für dessen Authentifizierung zugeordnet.

/FE0250/ *eLab-System registrieren:* Dem eLab, das an das Belab-System angebunden werden soll, wird eine eindeutige ID (SystemID) zugewiesen. Nur für dieses System registrierte Benutzer mit entsprechenden Rechten können auf das Datenarchiv zugreifen.

/FE0260/ *Abhängigkeiten/Prüfungen konfigurieren:* Eingangsdaten werden vom BeLab-System auf Ihre Konsistenz und Vollständigkeit überprüft. Die Struktur von Daten und deren Konsistenz kann individuell für das angebundene eLab (SystemID) und darin enthaltenen Projekten (ContainerID) anhand von Container-Strukturen vorgegeben werden (siehe auch Abschnitt 5.6).

3.2 Interne Funktionen des BeLab-Systems

Die in den folgenden Abschnitten beschriebenen internen Funktionen können durch den Benutzer nicht direkt aufgerufen werden. Sie werden durch das BeLab-System realisiert und ausgeführt. Gekennzeichnet sind die Funktionen durch **/FIxxxx/**. FI steht dabei für „interne Funktion“.

3.2.1 Datenprüfung

/FI0310/ *Metadatencontainer anlegen:* Werden durch den Benutzer Daten in das BeLab-System übertragen (Funktion **/FE0110/**) erzeugt das BeLab-System einen Metadatencontainer, in dem alle Metadaten und Ereignisse protokolliert werden. Zur Überprüfung der Vollständigkeit (Funktion **/FI0340/**) wird des Weiteren ein Datentypcontainer angelegt, der die Struktur der empfangen Daten definiert. Es folgt Funktion **/FI0320/**.

/FI0320/ *Signatur überprüfen:* Sind die Daten signiert, wird vom BeLab-System die Signatur geprüft, um die Integrität und Authentizität zu gewährleisten. Hierbei wird zusätzlich die Gültigkeit des zugehörigen Zertifikats über Online Certificate Status Protocol (OCSP) überprüft. Allgemein sind folgende Ergebnisse möglich:

- Keine Signatur
- Ungültige Signatur (Art der Signatur)
- Gültige Signatur (Art der Signatur)

Ist die Signatur ungültig, werden die Daten abgelehnt. Das BeLab-System lehnt ungültig signierte Daten grundsätzlich ab. Sollen die Daten dennoch eingelagert werden, so muss die ungültige Signatur vorher vom Benutzer entfernt werden. Dem Benutzer wird eine entsprechende Information gesendet (Funktion **/FI0390/**). Bei gültiger Signatur oder wenn keine Signatur vorhanden ist, folgt Funktion **/FI0330/**. Zusätzlich wird das Ergebnis der Signaturprüfung in den Metadaten des BeLab Systems vermerkt.

/FI0330/ *Dateiformat überprüfen:* Das BeLab-System prüft, ob das Format der übergebenen Datei für die Langzeitarchivierung geeignet ist.

Geeignete Datenformate werden im Abschnitt 5.5 genannt.

Entspricht das Dateiformat nicht den hier angegeben, wird ein entsprechender Hinweis gesendet (Funktion **/FI0390/**). Folgende Ergebnisse sind möglich:

- Dateiformat nicht geeignet
- Dateiformat geeignet

- Dateiformat empfohlen

In allen Fällen folgt Funktion **/FI0340/**.

/FI0340/ *Vollständigkeit überprüfen:* Wurden mehrere Dateien übertragen (Funktion **/FE0110/)** wird im Anschluss der Überprüfung aller Dateien eine Vollständigkeitsprüfung (soweit möglich) durchgeführt. Folgende Ergebnisse sind möglich:

- Vollständigkeit nicht überprüfbar
- Daten nicht vollständig
- Daten vollständig

Sind die Daten nicht vollständig, wird durch das BeLab-System vom Benutzer eine Bestätigung zur Archivierung eingefordert (Funktion **/FI0380/**). Bei fehlender Überprüfbarkeit wird eine entsprechende Nachricht an den Benutzer gesendet und eine Bestätigung zur Archivierung eingefordert (Funktion **/FI0390/**). Nach erfolgter Bestätigung oder nachdem die Vollständigkeit festgestellt wurde folgt Funktion **/FI0350/**.

/FI0350/ *Metadaten übernehmen:* Metadaten, die in der übergebenen Datei oder im zugehörigen Datencontainer vorhanden sind, werden in den Metadatencontainer übernommen. Weitere Metadaten werden ggf. durch das BeLab-System angefügt.

/FI0360/ *Daten signieren:* Die Daten werden vom BeLab-System signiert. Es ist vorgesehen, dass mehrere Instanzen elektronischer Signaturen sequentiell verwendet werden können. So können sowohl bereits signierte Dateien mit einer weiteren Signatur versehen werden als auch mehrere Benutzer eine Datei signieren. Auch sollen parallel verschiedene Signaturtechniken verwendet werden können.

/FI0370/ *Parallel signieren:* Eingangsdaten können außerhalb und innerhalb des BeLab-Systems mehrfach signiert werden. Dies umfasst insbesondere die Signatur der Daten durch unterschiedliche Benutzer z.B. im Rahmen des abgebildeten Forschungsprozesses.

/FI0380/ *Bestätigung anfordern:* Das BeLab-System fordert vom Benutzer eine Signatur des Vorgangs für das Fortfahren der Archivierung ein.

/FI0390/ *Information senden:* Dem Benutzer werden durch das BeLab-System entsprechende Informationen gesendet, die den Status der Datenverarbeitung widerspiegeln.

3.2.2 Klassifizierung

Auf der Grundlage der Ergebnisse der Funktionen **/FI0320/**, **/FI0330/**, **/FI0340/** und der durch das BeLab-System verwendeten Signatur (**/FI0360/**) wird durch das BeLab-System eine Bewertung durchgeführt.

/FI0410/ *Datenformat bewerten:* In Bezug auf die Langzeitarchivierung wird die Datei klassifiziert. Die Klassifizierung wird in Kapitel 5.5 näher beschrieben.

/FI0420/ *Beweissicherheit bewerten:* Über dem gesamten Einlagerungsprozess wurden die (nicht) verwendeten Signaturen dokumentiert. Abschließend erfolgt eine Klassifizierung durch das BeLab-System. Die Klassifizierung der Beweissicherheit wird in Kapitel 5.5 näher beschrieben.

/FI0430/ *Konvertierungen des BeLab-Systems bewerten:* Durch evtl. vorgenommene Konvertierungen des BeLab-Systems ist evtl. eine Minderung der Datenqualität verursacht worden. Die Bewertung soll dies wiedergeben.

/FI0440/ *Datenvollständigkeit bewerten:* Zu bewerten ist, ob die Vollständigkeit überprüft werden konnte und ob eine Vollständigkeit vorlag. Weitere Informationen siehe Kapitel 5.6.

3.2.3 Pflege der Metadaten

Grundlage für die Pflege der Metadaten bildet der Metadaten-Standard Dublin-Core. Metadaten, die auf diesen Standard nicht abgebildet werden können, werden über einen erweiterten Metadatencontainer aufgenommen.

/FI0510/ *Metadatencontainer anlegen:* Im Metadatencontainer werden für jede übergebene Datei alle im Rahmen des BeLab-Prozesses verarbeiteten Metadaten gesammelt. (Siehe auch Funktion **/FI0310/**.)

/FI0520/ *Metadatencontainer erweitern:* Enthält eine übergebene Datei mehr als im Metadatencontainer vorgesehene Metadaten, wird der Metadatencontainer entsprechend erweitert.

/FI0530/ *Metadaten auslesen:* Metadaten, die mit der übergebenen Datei vorhanden sind, werden vom BeLab-System ausgelesen.

/FI0540/ *Metadatum übernehmen:* Ein Metadatum wird durch das BeLab-System in den entsprechenden Metadatencontainer eingetragen.

4 Produktdaten

In den folgenden Abschnitten werden die Daten beschrieben, die im BeLab-System Verwendung finden. Unterschieden werden Daten, die zur Administration des Systems benötigt (Abschnitt 4.1) und Daten, die während des wissenschaftlichen Forschungsprozesses entstehen und so im Laborbuch verwaltet werden (Abschnitte 4.2 und 4.3).

4.1 System-interne Daten

Das BeLab System verwendet die in diesem Abschnitt genannten Parameter für die interne Verarbeitung der übermittelten Daten.

/D010/ *Benutzerdaten:* Alle Daten, die zur Authentifizierung des Benutzers genutzt werden.

- BenutzerID (eindeutig)
- Zertifikat

/D020/ *Systemdaten:* Alle Daten, die zur Identifikation des eLabs dienen.

- SystemID (eindeutig)

/D030/ *Containerdaten:* Container werden im BeLab-System in unterschiedlichen Zusammenhängen verwendet, um Daten zu bündeln.

- ContainerID (eindeutig)
- ProjektID (eindeutig)

4.2 Anwendungsdaten

Anwendungsdaten können dem BeLab System sowohl in strukturierter als auch in unstrukturierter Form übermittelt werden. Unstrukturierte Daten können beispielsweise von Messgeräten in Form von Dateien geliefert werden. Strukturierte Daten können aus Datenbanken in das BeLab System archiviert werden. Durch die Verwendung von Archiven (z.B. TAR) können unstrukturierte Daten darüber hinaus kontextbezogen in einer strukturierten Form übergeben werden.**/D040/** *Labormetadaten:* Alle Informationen, die das Experiment beschreiben. Neben der verbalen Beschreibung und der Dokumentation von wichtigen Parametern (z. B. Umgebungstemperatur) gehören auch andere aussagefähige Daten (z. B. Fotos vom Versuchsaufbau) dazu. Insbesondere ist auch die Messapparatur inklusive des Messdatenhandlings genau zu erfassen.

- Bilder des Versuchsaufbaus
- Verwendete Messgeräte
- Durchführende Experimenteure
- Statusberichte / Anzeigen von Messgeräten

/D050/ *Messdaten:* Messdaten, die bei der Durchführung des Versuchs anfallen, werden hier dokumentiert. Zu diesen Daten gehören sowohl automatisch von der Messapparatur als auch manuell erfasste Daten. Die Dateneingabe erfolgt unmittelbar während oder nach dem Versuch.

- Daten von Messgeräten

/D060/ *Rohdaten, Interpretierte Daten, Primärdaten:* Bei den Messdaten ist zwischen Rohdaten und interpretierten Daten zu unterscheiden. Rohdaten werden keineswegs immer aufgenommen. Der Wissenschaftler hat darüber zu entscheiden, ob er die Rohdaten und oder die interpretierten Daten aufnimmt. Dies muss der Wissenschaftler gegenüber der Forschungs-Community verantworten. BeLab übernimmt keine Einteilung oder inhaltliche Prüfung der eingegeben Daten.

4.3 Auswertungsmittel

Um die archivierten Daten zu einem späteren Zeitpunkt interpretieren zu können, sind u.U. zusätzliche Werkzeuge erforderlich. Diese sollten als Kontextinformationen zur Archivierung beschrieben werden.

/D070/ *Auswertung:* Hier ist die Beschreibung der Auswertemechanismen zu hinterlegen. Wird Software für die Auswertung benutzt, so ist eine Beschreibung des Gesamtsystems aus Hardware, Betriebssystem, systemnaher Software sowie der Software selbst zu hinterlegen. Ist die Software selbst entwickelt worden, so sollte der Sourcecode hinterlegt werden.

- Theoretischer Ansatz
- Quellenangaben
- Sourcecode

5 Qualitätsbestimmungen

5.1 Zeitstempel

Zeitstempel spielen an mehreren Stellen eine besondere Rolle:

- Beim Experiment selbst
- Beim Authentizitätsprozess
- 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 Änderungen an den Daten (Korrigieren oder gar Stornieren)
- Bei der Übersignatur
- Bei der Langzeitarchivierung

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) bietet sich zum Zwecke der Langzeitarchivierung bzw. der Übersignatur von qualifizierten elektronischen Signaturen an. Bei der Übersignierung soll mit dem qualifizierten 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 Zeitstempeln dabei besonderes Vertrauen entgegengebracht worden ist.

Für andere Zwecke reicht ein elektronischer Zeitstempel durch eine sonstige vertrauenswürdige dritte Stelle. 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 allenfalls, dass die Verknüpfung und Bescheinigung durch einen Dritten erfolgt. Es besteht eine Parallele zur Mitunterzeichnung einer Urkunde durch einen Dritten zur Bezeugung des Vorgangs. Ein Zeitstempel von einem Anbieter, welcher vergleichbaren Anforderungen genügt wie denen von einem qualifizierten Zeitstempelanbieter kann daher als ebenso beweiskräftig gelten soweit der Anbieter des Zeitstempels sonst als vertrauenswürdig gilt.

5.2 Logging-Mechanismus

Die BeLab-Schnittstelle unterstützt grundsätzlich die Sicherung von Protokolldateien der eLabs. In diesen automatisch geführten Protokollen werden alle oder bestimmte Aktionen oder Prozesse in einem eLab aufgezeichnet. Welche Daten „geloggt“ werden liegt im Ermessen des eLab Entwicklers (z.B. Log On und Log Off von Nutzern, Protokoll welcher Nutzer auf welche Projektdaten wann zugegriffen hat.). Der eLab Entwickler / Anbieter (z.B. Arbeitgeber) sollte beim Umfang der Aufzeichnungen dabei aber auf Einhaltung der jeweiligen datenschutzrechtlichen Bestimmungen achten. Insbesondere sollte der Nutzer (bzw. Arbeitnehmer) über Art und Umfang der Aufzeichnungen aufgeklärt werden.

Zur Sicherung der Systemintegrität protokolliert BeLab alle Benutzerfunktionen (siehe 3.1: Authentifizierung und Autorisierung; Datenverwaltung). Auch Systemfunktionen (siehe 3.2: Datenprüfung, Klassifizierung, Pflege der Metadaten) werden protokolliert. Aufgezeichnet wird welcher Nutzer welche Funktion zu einem bestimmten Systemzeitpunkt aufruft und welche Dateien er dabei anlegt bzw. verändert. Auf diese Weise soll die Manipulation von Daten verhindert bzw. Manipulationsversuche leichter aufgeklärt werden. Durch die Angaben zu 3.1.1 „Authentifizierung und Autorisierung“ sind Rückschlüsse auf den Nutzer möglich. Es handelt sich um personenbezogene Daten. Zum Zwecke der Datensparsamkeit nicht protokolliert wird deswegen, welche Dateien nur gelesen werden. Dadurch soll die Möglichkeit der Profilbildung über einen Nutzer verhindert werden.

Für die von der BeLab-Schnittstelle gespeicherten Dateien (inkl. Protokolldateien) übernimmt der BeLab-Anbieter die administrative Verantwortung. Es wird die vertragliche Verpflichtung übernommen, die geltenden datenschutzrechtlichen Bestimmungen in ihrer jeweils geltenden Fassung einzuhalten.
Der Anbieter verpflichtet sich auch, über alle ihm im Rahmen der Vorbereitung, Durchführung und Erfüllung dieses Vertrages zur Kenntnis gelangten vertraulichen Vorgänge, insbesondere Geschäfts- oder Betriebsgeheimnisse des Benutzers strengstes Stillschweigen zu bewahren und diese weder weiterzugeben noch auf sonstige Art zu verwerten. Der Benutzer wird berechtigt, von dem Anbieter jederzeit den Nachweis einer vertragsgemäßen und ausreichenden Datensicherung zu verlangen und bleibt in jedem Fall Alleinberechtigter an den Daten und kann daher jederzeit, die Herausgabe oder Löschung einzelner oder sämtlicher Daten verlangen, ohne dass ein Zurückbehaltungsrecht des Anbieters besteht.

5.3 Fortgeschrittene, qualifizierte 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 (BGB, ZPO, VwGO, VwVfG) 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 haben 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 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 5.5.

5.4 Messgeräte mit Signaturkomponente

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 Signaturen zu sichern.

Messgeräte, welche bereits Rohdaten oder Primärdaten elektronisch signieren tragen dazu bei die Datenintegrität der im eLab aufgezeichneten Forschungsdaten sicherzustellen. Nach Möglichkeiten sollen diese Daten inkl. Signatur gesamt übernommen werden. So kann der Forscher z.B. Vorwürfe der Manipulation seiner Messungen entkräften.

5.5 Klassifizierung der Beweiswerterhaltung und Langzeitarchivierung

Durch die Klassifizierung der Daten anhand der Datenformate, erhobenen Metadaten und verwendeten Signatur erhält der Nutzer einen Hinweis auf den Grad der Beweissicherheit und mögliche Risiken bei der Langzeitarchivierung der Daten.

Bzgl. der Beweissicherheit 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 elektronischen 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 elektronischen Zeitstempel, der vom BeLab-Anbieter zur Verfügung gestellt wird, dokumentiert.

/Klasse B4/ *Qualifiziert*+: Wie **/Klasse B3/**, jedoch wird die Sicherung mit einem qualifizierten elektronischen 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 elektronischen Zeitstempel, der vom BeLab-Anbieter zur Verfügung gestellt wird, dokumentiert.

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

Zusätzlich zu den **Klassen B1** bis **B6** kann einer 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 digitale Signaturverfahren) dieser Daten belegt.

Zu beachten ist, dass Klassifizierung und Signierung aufeinander rekurrieren. Die Klassifizierung wird aufgrund der Signatur mitbestimmt und auch mit verschlüsselt.

Die Bewertung der LZA-Tauglichkeit 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. Unbekannte Datenformate werden ebenfalls der Klasse L1 zugeordnet.

/Klasse L2/ *Geeignet:* Eine in dem Datenformat übergebene Datei kann wahrscheinlich nach einigen Jahren noch interpretiert werden. Beispiele: PDF, TIFF, DOC, DOCX, XLS, XLSX usw. 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 etc.; PDF/A; PDF/E; PDF/UA bzw. PDF/X; TIFF nach ISO; SVG; ODF usw. sowie Archive im TAR Format, die diese Formate enthalten.

Eine Liste von Dateiformaten der Klasse L1 wird im Zwischenbericht zum BeLab-Projekt aufgeführt. Eine detaillierte Begründung für die Eignung von den jeweiligen Dateiformaten für die Langzeitarchivierung wird im NESTOR Handbuch beschrieben.

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 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*.

5.6 Überprüfung der Datenkonsistenz

Die Zuweisung der im vorherigen Abschnitt genannten Klassen für die Sicherung der Datenintegrität (S1 und S2) basiert im BeLab-System auf einer automatisierten Prüfung der vom eLab übermittelten Daten. Ziel ist die Sicherung der Integrität und, soweit überprüfbar, der Vollständigkeit der Daten über den gesamten Forschungsprozess und der Verarbeitung im BeLab-System hinweg. Im BeLab-System können hierfür entsprechende Validierungsprozesse definiert werden. Die Validierung bezieht sich dabei immer auf einen zusammenhängenden an das BeLab-System zur Archivierung übermittelten Container. Folgende Validierungen werden unterstützt:

- Vorgabe einer festen Metadaten-Struktur (z.B. im Rahmen eines Projekts erforderliche Angaben und Pflichtfelder, unterstützt durch den Dublin-Core Standard)
- Validierung von Metadaten (Datenformate z.B. für Datums- und Zeitangaben)
- Konsistenz der übermittelten Meta- und Rohdaten (z.B. Verifikation übermittelter digitaler Signaturen z.B. von Messgeräten, Überprüfung auf fortlaufende Bild-Sequenznummern, Datums- und Zeitangaben, festen Messparametern usw.)
- Konsistenz des Forschungsprozesses (z.B. Prüfung von Abhängigkeiten der Daten untereinander im übermittelten Container, beispielsweise keine Einlagerung eines Bildes ohne zugehörige Messdaten, keine Messdaten ohne Messprotokoll usw.)

Alle Überprüfungen sind optional und können für einzelne angebundene elektronische Laborbücher (SystemID) oder auch für einzelne darin unterschiedene Projekte (ProjektID) frei

definiert werden. Die Definition der der Validierungsprozesse kann eigenständig durch die Betreiber des eLabs erfolgen.

6 Glossar

/BeLab-System/ Das BeLab-System (Beweissicheres elektronisches Laborbuch) bildet die Schnittstelle zwischen einem elektronischem Laborbuch (eLab) und einem Archivierungssystem (hier: ArchiSafe).

/Benutzer/ Ein Benutzer des BeLab-Systems kann sowohl eine Person als auch ein Messgerät sein. Somit ist es auch möglich Daten direkt vom Messgerät an das BeLab-System weiterzuleiten.

/eLab/ Abkürzung für elektronisches Laborbuch

/LZA/ Abkürzung für Langzeitarchivierung

/Zertifikat/ Ein digitales Zertifikat nach dem X.509 Standard, welches entweder für die Erstellung oder Überprüfung einer digitalen Signatur (gemäß SigG) oder für die beidseitige Authentifizierung von Benutzern bzw. Clients und Servern verwendet wird.