BILDUNGSRAUM.DIGITAL

Rahmenbedingungen für die Umsetzung der Nationalen Bildungsplattform

1 Intro

Im Digitalen Bildungsraum werden existierende digitale Bildungsangebote für Lernende und Lehrende aus allen Bildungsbereichen im Sinne einer Vernetzungsinfrastruktur erreichbar sein. Der Digitale Bildungsraum ermöglicht Bildung entsprechend als durchgängige Reise von der Schule über die Hochschule bis zur berufsbegleitenden Weiterbildung.

Ein Kernelement des Digitalen Bildungsraums ist die Nationale Bildungsplattform (NBP). Es handelt sich dabei um eine Vernetzungsinfrastruktur auf Basis von gemeinsamen Standards und Formaten. Es soll keine neue Lernumgebung geschaffen werden, sondern die Plattform soll als groß angelegtes Standardisierungs- und Infrastrukturprojekt individuellen Zugang zu den bereits existierenden Angeboten und Plattformen ermöglichen.

Lernende können ihre Daten im Kontext der Nationalen Bildungsplattform verwalten und über die Nutzung selbst entscheiden. So können auch Leistungsnachweise auf der Plattform digital und sicher hinterlegt werden. Zudem können die Nutzenden ihre Daten für Dritte freigeben, um individualisierte Lernangebote zu erhalten. Ein besonderes Augenmerk wird dabei auf Datenschutz und Datensouveränität gelegt.

2 Danksagung an die Auditoren

Wir danken den Auditor:innen, die durch ihre Kommentare und Rückmeldungen viele hilfreiche Ergänzungen beigetragen haben, um den Grundstein für die Architektur der Nationalen Bildungsplattform zu legen.

3 Lizenzierung

4 Änderungsverzeichnis

Datum	Version	Beschreibung	verändert durch
07.07.2022	2.1	Interne Links entfernt	PB

5 Technische Rahmenparameter

Die folgende Grafik skizziert die wesentlichen Komponenten der Basisinfrastruktur der Nationalen Bildungsplattform (NBP). Die Architektur schafft die Basis, um den Zweck der NBP als Innovationstreiber und Inkubator für eine digital vernetzte Bildungslandschaft effizient zu unterstützen. Das eigentliche Lernen findet weiter in bestehenden Anwendungen und Portalen statt, und nicht in der NBP selbst. Die NBP stellt lediglich die Basisinfrastruktur, um bestehende und neue digital gestützte Bildungsangebote und -plattformen von Akteuren aller Bildungsbereiche zu vernetzen. Die Eigenständigkeit und Vielfalt etablierter Bildungsanbieter und Plattformen der Länder wird somit nicht infrage gestellt. Die NBP Basisinfrastruktur beinhaltet die folgenden Module:

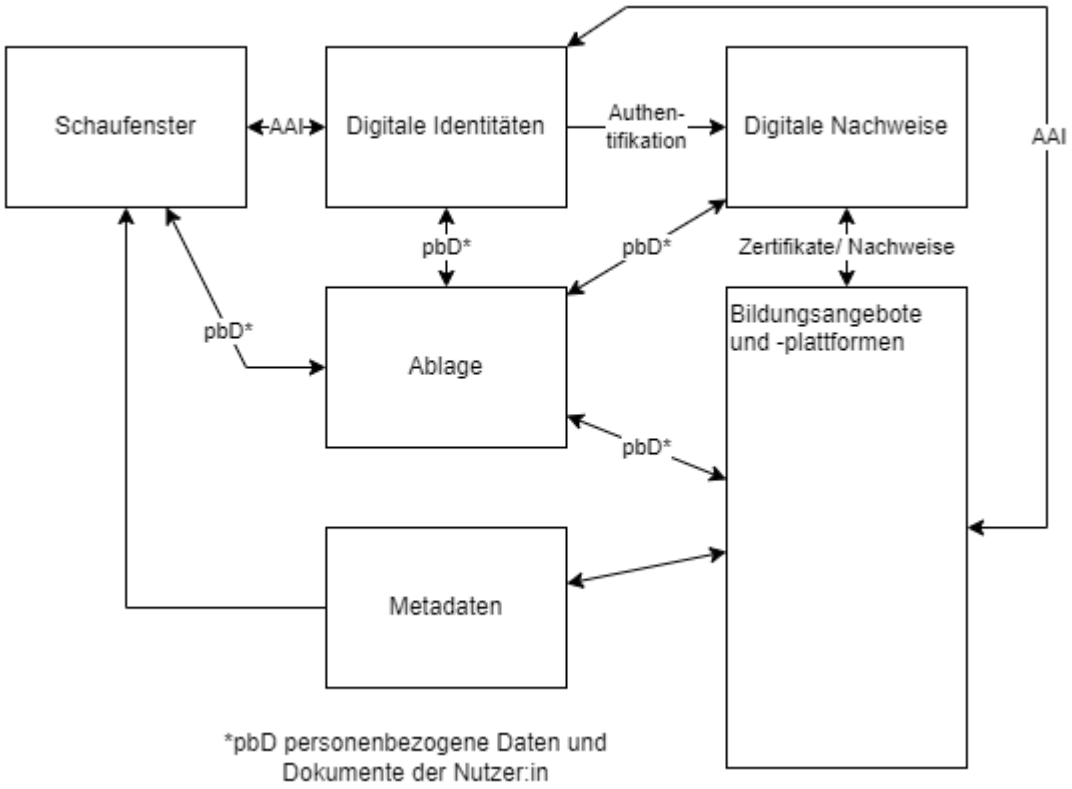


Abbildung 1 Basisinfrastruktur der NBP

Wie aus der Skizze ersichtlich besteht der Architekturkern für die NBP aus den Bereichen Identitätsmanagement (Digitale Identitäten), persönlicher Datenspeicher (Ablage), Bildungsmetadatenmanagement (Metadaten) und Zertifikate-Infrastruktur (Digitale Nachweise) in Verbindung mit einer für die Nutzenden sichtbaren Funktionalität (Schaufenster). Dies dient als Rahmen zur Anbindung von Konsolidierungspartner und Bildungseinrichtungen über die Bildungsinhalte und -angebote über alle Bildungsbereiche hinweg erschlossen und zugänglich gemacht werden.

Digitale Nachweise

Die NBP wird eine Basisinfrastruktur für die Umsetzung von digitalen Nachweisen (verifiable claims oder VC) und der Signatur von Dokumenten bereitstellen. Grundlage hierfür ist eine PKI Infrastruktur mit einer zentralen Certification Authority (CA) für die Domäne Bildung. Die Registrierung (z.B. von Schulen, Hochschulen) erfolgt über dezentrale Registration Authorities (RAs).

Digitale Identität

Identitäten werden über verschiedene Anbieter (Identity Provider/ IdPs) angelegt und verwaltet, bzw. sind dort bereits vorhanden (z.B. Schulamt, Hochschule, Bildungsanbieter). Über eine NBP AAI (Authentication and Authorization Infrastructure) wird ein SSO Dienst (Single Sign On - beinhaltet auch den Single Sign Out) zur Verfügung gestellt. Damit ist der Login über die NBP auch bei anderen angebundenen Plattformen möglich.

Ablage

Nutzende können in ihrer Ablage Dokumente souverän ablegen und freigeben. Diese sind agnostisch in Bezug auf das Datenformat. Es können sowohl kleinteilige Lernaktivitäten und Lernstände (Microcredentials) als auch verifizierbare Nachweise, wie das Abiturzeugnis oder komplexere Dokumente abgelegt werden. Freigaben können einzeln oder dauerhaft erteilt werden, beispielsweise für verschiedene Services und Anwendungsfälle. Ein Übertragungslog hält dauerhaft für die Nutzenden nach, was an wen freigegeben und übertragen wurde. Über den Meta-Ablage-Connector können verschiedene Ablagen an die NBP angebunden werden. Durch diese Form der Ablage wird erreicht, dass nahezu keine persistente Speicherung nutzerbezogener Daten in der NBP stattfindet.

Metadaten und Datenräume

Im Metadatenspeicher werden Daten (z.B. Informationen über Studiengänge, Bildungseinheiten, Curricula) geordnet in abgestimmten Formaten abgelegt und in einem Datenraum zur Verfügung gestellt. Dies ermöglicht Funktionalitäten wie die Suche nach Lerninhalten oder Bildungseinrichtungen. Die Zulieferung erfolgt in der ersten Ausbaustufe hauptsächlich über sogenannte “Konsolidierungspartner”. Die durch diese Partner durchgeführte Konsolidierung umfasst dabei die Verarbeitung und Identifikation relevanter Daten (beispielsweise aussagekräftige Metadaten von Bildungsangeboten) als auch die Identifikation von problematischen Daten (fehlerhaft, irreführend, ...).

Schaufenster

Die Infrastruktur nutzt wie das CMS des Bundes die Plattform Liferay (oder gleichwertig), um als Schaufenster Lebenslagen, Zugang zur Suche und andere Funktionalitäten abzubilden. Das Schaufenster dienst auch als Informationsportal rund um die Dienste der NBP.

Berücksichtigung des künftigen Betriebs und Service Managements

Detaillierte ggf. zu berücksichtigende Aspekte des Betriebs- und des Service-Managements sowie Anforderungen an etwa zu berücksichtigende notwendige SLAs werden unter Berücksichtigung von Governance Rahmenbedingungen in den jeweiligen Ausschreibungen der Miniwettbewerbe bekanntgegeben.

Die Interoperabilität von Standards und offenen Schnittstellen, die sichere Ablage und Zugänglichkeit von persönlichen Nutzungsdaten, Artefakten und digitalen Nachweisen sowie eine eindeutige Identifizierung von Nutzerinnen und Nutzern auf adäquatem Vertrauensniveau wird durch eine sichere, offene, zukunftsfähige, flexible und herstellerneutrale Architektur gewährleistet. Zu den wesentlichen übergeordneten Architekturprinzipien der NBP zählen:

- Skalierbarkeit
- Nutzung etablierter Datenstandards
- Technische Integrierbarkeit durch standardisierte und dokumentierte Schnittstellen (APIs)
- Anpassbarkeit

- Sicherheit und Datenschutz in Entwicklung und Betrieb
- Wiederverwendbarkeit von Konzepten und Komponenten
- Datensouveränität der Nutzenden
- Datensparsamkeit
- Auffindbarkeit von Information
- Barrierefreiheit

Der skizzierte Architekturkern basiert auf der Auswertung und Begleitung von zahlreichen erfolgreichen, etablierten und innovativen Projekten und Architekturansätzen, insbesondere auch im Rahmen der vorgelagerten Begleitung der Ziel-3-Projekte der Förderbekanntmachung zur Entwicklung von Plattformprototypen. Jedes dieser Module hat einen eigenen thematischen und technischen Schwerpunkt, die in Architektursteckbriefen beschrieben und durch externe Gutachter der NBP evaluiert wurden. Die relevanten Steckbriefe sowie weitere Einzelheiten, Schnittstellen und Rahmenbedingungen werden den für den Bieterpool qualifizierten Unternehmen mit den Einzelausschreibungen in den jeweiligen Miniwettbewerben zur Verfügung gestellt.

5.1 Rahmenparameter der NBP Cloud-Infrastruktur

Die technische Umgebung der NBP für den Beta-Launch Ende 2023 wird durch das Projektbüro der NBP zur Verfügung gestellt und beinhaltet die Bereitstellung von drei Instanzen (Entwicklungs-, Testinstanz sowie Produktivbetrieb). Im Folgenden werden nur relevante Rahmenparameter der Cloud-Infrastruktur beschrieben. Weitere Details und Anforderungen werden in den Ausschreibungen der Miniwettbewerbe bzw. in den User Stories und Epics des Product Backlog spezifiziert.

Die technische Umgebung der NBP basiert weitestgehend auf Open-Source-Bestandteilen und schafft eine strukturierte, skalierbare und sichere Basis für eine Microservice Cloud-Computing Infrastruktur.

Alle zu erstellenden und verwendeten Dienste der NBP müssen hochskalierbar und innerhalb einer modernen Cloud-Native-Computing Infrastruktur ausführbar sein. Wenn immer möglich sollen etablierte und nachhaltig verfügbare Open-Source Lösungen und Technologien zum Einsatz kommen. Performance (und damit auch die nachhaltige Nutzung von Ressourcen) ist dabei von Anfang ein wichtiger Aspekt der NBP. Zur Vermeidung von Überlastzuständen (Lastenausgleich) wird ein hochverfügbarer und skalierbarer Loadbalancer für die Cloud-Umgebung zum Einsatz kommen.

Die spezifischen Leistungsmerkmale und Mengengrüste werden separat in der technischen Schnittstellenbeschreibung der einzelnen Miniwettbewerbe spezifiziert.

Bei der Nutzung von Datenbanken ist eine gemeinsame Nutzung durch Dienste zu vermeiden. Basierend auf der modularen Architektur der NBP soll jeder Dienst sein eigenes Dataset verwalten, um versteckte Abhängigkeiten zwischen Diensten und eine unbeabsichtigte Kopplung von Diensten zu vermeiden.

Bei der Entwicklung der NBP hat Sicherheit einen sehr hohen Stellenwert. Dies ist in gleicher Weise zu beachten für die Cloud-Umgebung, die zu erstellende Software und angeschlossenen Angebote. Die NBP kooperiert mit dem Bundesamtes für Sicherheit in der Informationstechnik (BSI) um hier begleitend entsprechende Vorgaben zu definieren..

5.2 Entwicklungsumgebung

Der Auftragnehmer ist verpflichtet, die vorgenannten Komponenten entsprechend den vertraglichen Vereinbarungen der einzelnen Miniwettbewerbe zu erstellen, deren Betriebsbereitschaft herbeizuführen und das Projektbüro bei deren Inbetriebnahme zu unterstützen. Dazu hat das

Entwicklerteam die einzelnen von ihm zu liefernden oder zu erstellenden Komponenten sowie die durch das Projektbüro des Auftraggebers beizustellenden Komponenten anderer agiler Entwicklerteams zu integrieren, zu customizen, zu testen und weiterzuentwickeln sowie bei deren Inbetriebnahme zu unterstützen. Agile Frameworks für die Softwareentwicklung (wie Scrum, Kanban oder Extreme Programming - XP) bilden hierbei die Grundlage für gängige Softwareentwicklungsprozesse wie DevOps und CI/CD (Continuous Integration/Continuous Delivery). Im CI/CD-Prozess soll ein möglichst hoher Automatisierungsgrad erreicht werden, so dass die Entwicklungsumgebung ein homogenes System bildet, dass die Entwicklung beschleunigt und das Testen automatisiert.

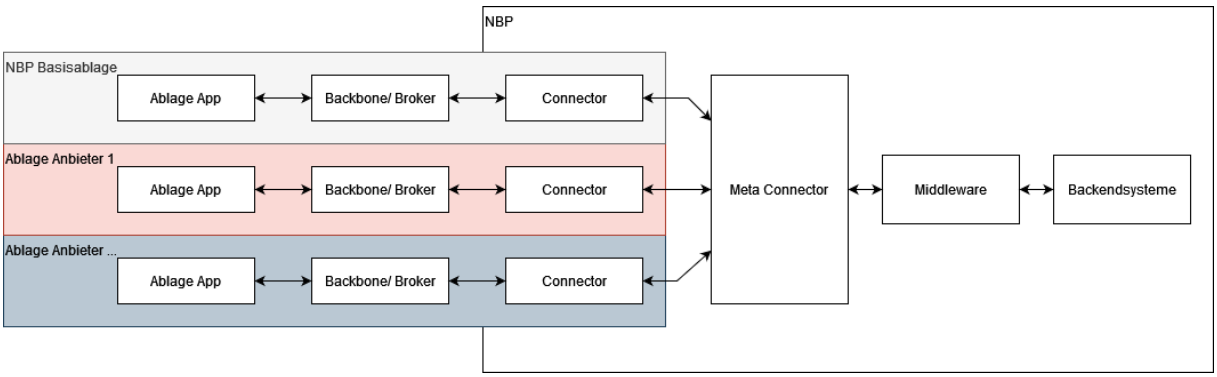
Die Schritte in einer CI/CD-Pipeline stellen verschiedene Untergruppen von Aufgaben dar, die in sogenannte Pipeline-Phasen eingeteilt werden. Zu diesen Phasen gehören üblicherweise:

- **Build**: Die Phase, in der die Anwendung kompiliert wird.
- **Test**: Die Phase, in der der Code getestet wird. Hier lassen sich durch Automatisierung sowohl der Zeit- als auch der Arbeitsaufwand verringern.
- **Release**: Die Phase, in der die Anwendung ins Repository gestellt wird.
- **Bereitstellung**: In dieser Phase wird der Code in der Produktionsumgebung bereitgestellt.
- **Validierung und Compliance**: Welche Schritte zur Validierung eines Builds notwendig sind, bestimmen die Anforderungen des jeweiligen Miniwettbewerbs.

Bei der Programmierung sollten die Clean-Code-Richtlinien beachtet werden, die das Ändern, Lesen, Erweitern und Warten von Softwarecode erleichtern. Der Source-Code muss gut dokumentiert und technischen Zusammenhänge und Schnittstellen in einer separaten Dokumentation beschrieben werden. Der Source Code muss über Git verwaltet werden. Ein entsprechendes Repository wird vom Projektbüro des Auftraggebers zur Verfügung gestellt.

6 Ablage

Diagramm



Steckbrief

Kurzbeschreibung (inkl. Wert für die NBP)	Die Nutzer:in (Sender:in) soll ihre Daten nutzer:innenselbstsouverän ablegen und anderen Nutzer:innen und/oder Service Providern (SP) (zusammen Empfänger:in) freigeben können. Hierbei bestimmt die Sender:in, wer zu welchem Zeitpunkt an die welche Daten kommt. Die Sender:in kann die Daten selbständig distribuieren und/oder einer Empfänger:in die Freigabe erteilen, bestimmte Daten zu einem bestimmten Zeitpunkt selbständig aus der Ablage abzufragen. Da die NBP selbst, wie in den Grundlagen festgelegt, keine Daten von Nutzer:innen persistent speichert und zwischen der Nutzer:in und der NBP eine sichere Verbindung zur Datenkommunikation aufgebaut werden soll, ist eine Technologie sinnvoll, die den Kontakt und die Kommunikation zwischen der Komponente der Nutzer:in (Ablage App) und der NBP verwaltet und regelt. Der Backbone-Broker sorgt dafür, dass die Datenkommunikation nur dann stattfindet, wenn dies auch wirklich von allen Beteiligten freigegeben wurde. In der Abbildung sind die Ablage-spezifischen und die übergreifend in der NBP verorteten Komponenten der Ablage dargestellt. Beispielhaft sind die als Default bereitgestellte “NBP Ablage” und zwei weitere Ablagen anderer Anbieter mit den jeweils Ablage-spezifisch bereitgestellten (Ablage App und Broker) bzw. konfigurierten (Connector) Komponenten eingezeichnet. Die Anbindung an mögliche Backendsysteme soll über eine Komponente (Connector) erfolgen, die eine API anbietet, die wiederum eine einfache Nutzung der Funktionalität und Anbindung ermöglicht. Da der Connector in der Sphäre des Service Providers (hier die NBP) betrieben wird, ist somit auch eine echte Ende-zu-Ende Verschlüsselung möglich. Es ist davon auszugehen, dass Nutzer:innen perspektivsich nicht nur eine spezifische Ablage, sondern unterschiedliche Ablagen von verschiedenen Herstellern nutzen werden. Ggf. werden sogar unterschiedliche Ablagen pro Nutzer:in eingesetzt. Der Meta Ablage Connector soll in der Lage sein,

	unterschiedliche Connectoren der jeweiligen Ablagen über deren APIs anzusprechen. Über einen einheitlichen Funktionsumfang über alle Connectoren ist die Komponente die eigentliche Schnittstelle zur NBP.
Basisanforderungen	**Ablage App:** • Die Architektur der Ablage App ist grundsätzlich agnostisch hinsichtlich der Art der abzulegenden Daten. Spezielle Dateiformate werden aber was ihre Anzeige und Möglichkeiten der Weiterverarbeitung angeht besonders unterstützt. • Es gibt keine Möglichkeit eines Rückschlusses von der Ablage App auf das Endgerät der Sender:in und Empfänger:in. Die Ablage App darf nicht in Verbindung mit einer Identifikationsnummer (beispielsweise die Mobilfunknummer, IMEI o.ä.) des Endgeräts der Sender:in oder Empfänger:in betrieben werden. • Die Ende zu Ende verschlüsselte Übermittlung der Daten zwischen Sender:in (Ablage App, Connector) und Empfänger:in (Ablage App, Connector) erfolgt über den Backbone/ Broker (beinhaltet auch Push-Kommunikation). • Eine initiale Übermittlung von Daten wird, durch das Eingehen einer Beziehung zwischen Sender:in und Empfänger:in, wird erst dann möglich, wenn sowohl Sender:in als auch Empfänger:in hierfür eine Freigabe erteilt haben. Wird diese Freigabe entzogen kann die Kommunikation, auch temporär, unterbrochen werden. Die ausgetauschten Daten bleiben dabei auf beiden Seiten erhalten. • Die Ablage App muss der Sender:in die Möglichkeit verschaffen, bestimmte Daten einer/m hierfür freigegebenen Empfänger:in zur Verfügung zu stellen, ohne dabei bei jedem Zugriff der Empfänger:in eine Freigabe erteilen zu müssen. • Der Zugriff auf die Daten kann durch Sender:in eingeschränkt werden (Kriterien wäre beispielsweise: Service Provider-Typ, Attributs-Typ, Attributs-Set / Typ des VC/ Datentyp, Uhrzeit/ Datum/ Dauer/ Anzahl der Zugriffe, ...). • Es soll möglich sein, die Daten auf mehreren Ablage Apps auf unterschiedlichen Endgeräten synchron zu halten. • Ein verschlüsseltes Backup der Daten der Ablage App soll möglich sein. **Backbone/ Broker:** • Schaffen einer Beziehung (1:1 Verbindung) zwischen Ablage App und Connector und oder Ablage App und Ablage App durch hierfür notwendigen Freigaben der Beteiligten. Dabei ist kein Rückschluss auf die Endgeräte möglich. • Technische Distribution der Daten zwischen Sender:in und Empfänger:in. • Anbindung an einen Zeitstempelserver. Versehen der technischen Nachrichten mit entsprechenden Zeitstempeln.

	• Tools für die Administration des Backbones und der angeschlossenen Ablage Apps und Connectoren. **Connector:** • Die Ende zu Ende verschlüsselte Übermittlung der Daten zwischen Sender:in (Ablage App, Connector) und Empfänger:in (Ablage App, Connector) erfolgt über den Backbone/ Broker (beinhaltet auch Push-Kommunikation). • Bereitstellen einer API für die Anbindung von Backendsystemen **Meta Ablage Connector:** • Anbinden von unterschiedlichen Ablagesystemen, perspektivisch über eine einheitliche Schnittstelle. • Darstellen aller notwendigen Funktionen, um Inhalte zwischen den Konnektoren auszutauschen • Darstellen aller notwendigen Funktionen, um Inhalte zwischen der NBP und den Konnektoren auszutauschen • Bereitstellen einer API in Richtung der Konnektoren • Bereitstellen einer API in Richtung der NBP • Festhalten der Beziehung eines/r Nutzer:in zu unterschiedlichen Ablagen (keinen Rückschluss auf den/die Nutzer:in)
Zusatzanforderungen	**Ablage App:** • Keine **Backbone/ Broker:** • Keine **Connector:** • Keine **Daten der Nutzer:in müssen bei der Nutzer:in verbleiben**. • Im Falle technischer Notwendigkeiten bei der Benutzer:innen bezogene Daten gespeichert werden müssen (gesetzliche Rahmenparameter → DSGVO), soll der/die Nutzer:in in der Lage sein, über jede Art der Datendistribution an einen Serviceprovider (SP) eine Übersicht zu bekommen und von dort auch Grundrechte der DSGVO wahrzunehmen (Auskunft, Löschung). • Falls der SP Daten über den/die Nutzer:in erzeugt, die über die Lebensdauer einer Session hinaus gespeichert werden, sollen diese Daten an den/die Nutzer:in übermittelt werden. • Die NBP nutzt keine Cloudspeicher für die *Ablage* personenbezogener Daten, um Angriffsvektoren zu minimieren.
MVP	Siehe Basisanforderungen
Nicht funktionale Anforderungen/ Kennzahlen	**Ablage App:** • Die Ablage ist eine ausführbare Applikation, die ohne weitere Applikationen lauffähig ist. • Die Ablage muss auf unterschiedlichen Betriebssystemen lauffähig sein:

	○ iOS ○ Android ○ Windows ○ Linux ○ MacOS Soweit keine Sicherheitsaspekte bzw. keine im Bezug auf die Verbreitung der jeweiligen Betriebssystemversion unangemessenen Aufwände entstehen, ist geplant, Betriebssystemversionen der letzten 5 Jahre zu unterstützen. **Backbone/ Broker:** • Lösung muss Container-fähig sein **Connector:** • Lösung muss Container-fähig sein **Komponentenübergreifend:** • In der Kommunikation zwischen Nutzer:in bzw. deren Ablage mit Service Providern sehen die Nutzenden häufig nur einen QR-Code, dem sie vertrauen müssen. Hier müssen durch entsprechende Vorgaben für die Service Provider Man-in-the-Middle-Angriffe wirksam verhindert werden – eine Möglichkeit, hier mehr Sicherheit zu schaffen, wäre es z.B. bei der erstmaligen Freigabe von VCs an einen Service Provider einen AAI-Login zu triggern. Damit ließe sich sicherstellen, dass es sich tatsächlich um einen SP innerhalb der NBP-AAI handelt.
Lösungsansätze/ Fertige Lösungen	• Lösungsansätze: ○ eduwallet https://github.com/digitalcredentials/learner-credential-wallet/blob/main/readme.md ○ Learner-Credential-Wallet-Specification-May-2021.pdf (mit.edu) → nicht Payload agnostisch • Fertige Lösungen bzw. Lösungen die ggf. erweitert werden können: ○ BIRD - enmeshed (open source/ MIT Licence)
Berührungspunkte und Abgrenzung	• Die Ablage berührt unterschiedliche Projekte, Initiativen und Vorhaben ○ Global ▪ Entwicklung von Data Wallets allgemein/ Open Wallet Standard ▪ Apple/ Google mit der Implementierung ISO/IEC 18013-5:2021 (https://www.iso.org/standard/69084.html) ○ EU ▪ Toolbox ▪ Europass ▪ SDG ○ DE

	▪ ID-Wallet und andere Schaufenster Digitale Identität Projekte, aka BKAmt App, aka Lissi ▪ Es erfolgt keine direkte Anbindung der Ablage an OZG-Services. Verbindung zu OZG Services erfolgt über die (mögliche) Anbindung von OZG-Services an die NBP. ○ Eine Interoperabilität von Ablagen untereinander ist langfristig anzustreben. ○ Eine Berücksichtigung von Ansätzen mit DLT und oder SSI findet nicht statt (siehe Grundsätze). Es findet weiterhin ein offenes Technologiemonitoring statt.
Offene Punkte	Keine

7 Digitale Identitäten

Kurzbeschreibung (inkl. Wert für die NBP)	Nutzer:innen sollen einen einfachen Zugang zu den Inhalten der an die NBP angeschlossenen Serviceprovider (SP) erhalten. Die NBP bildet hierfür eine "Authentication and Authorization Infrastructure (AAI)". Mit dieser AAI bekommt der/die Nutzer:in abhängig von ihrem Profil, dass in der Ablage gespeichert ist, und ihrer authentifizierten Identität, abhängig davon wie die Authentifikation durch die jeweiligen SPs erfolgt ist, Zugang zu dem jeweiligen Angebot. Der Vorteil dieser AAI liegt in der für die Nutzungsperiode einmaligen Identifikation der Nutzer:in. Dieses Prinzip wird als Single Sign On (SSO) bezeichnet (Single Logout – SLO – wird als Bestandteil der SSO Funktionalität betrachtet und nicht gesondert erwähnt). Die Prüfung des Zugangs im Rahmen des SSO durch die AAI erfolgt durch dezentrale Identity Provider (IdP), die entweder direkt an die NBP AAI oder über andere an die NBP AAI angeschlossene AAIs wie beispielsweise die DFN AAI oder VIDIS angeschlossen sind. Hierfür muss die NBP AAI in den anzuschließenden AAI registriert werden. Für Nutzer:innen, die nicht über eine digitale Identität aus den oben dargestellten AAIs verfügen, stellt die NBP in Form des NPB Identity-Providers (IdP) eine Basis Identität zur Verfügung. Über sogenannte „Self Service Funktionen" des NBP Identity-Managements (IDM) kann die Nutzer:in die Basisidentität anlegen, verwalten und wieder löschen. Zudem soll über eine weitere "Self Service Funktion" mittels der Nutzung der Online-Ausweisfunktionen des Personalausweises eine direkte Authentifikation der Nutzerin erfolgen. Weitere Attribute können über den Verwaltungsbereich eingestellt, gepflegt und gelöscht werden. Alle personenbezogenen Daten werden in die Ablage übertragen. Das Vertrauensniveau der Basis Identität wird an dem Vertrauensniveau der zugrundeliegenden Authentifikation ausgerichtet. Die aus den oben dargestellten AAIs digitalen Identitäten können auch mit der Basis Identität verbunden werden. Damit kann im späteren Verlauf auf Wunsch auf die Nutzung unterschiedlicher digitaler Identitäten verzichtet werden. Die Basis Identität bleibt auch nach Entfall (z.B. nach Abschluss einer Ausbildung) der verbundenen digitalen Identität erhalten. Die Freigabe zur Nutzung einzelner Angebote durch die jeweiligen Service Provider hängt von der Qualität der Authentifikation der einzelnen digitalen Identität ab, da der Schutz von Minderjährigen, aber auch die Verhinderung der Verbreitung von ggf. strafrechtlich bewährten Material je nach Anwendungsfall eine sowohl gänzlich anonyme digitale Identität als auch eine mit niedrigem Vertrauensniveau ausschließt. Um die Datensouveränität der Nutzenden zu gewährleisten, müssen die eigentlichen personenbezogenen Metadaten einer digitalen Identität über

	die Ablage zur Verfügung gestellt werden. Im Rahmen der Kommunikation bezüglich SSO sollen möglichst wenig Metadaten (ggf. nur eine GUID) der Nutzer:innen ausgetauscht werden.
Basisanforderungen	**IDM NBP:** Management der Basisidentität der NBP • Einrichten, Verwalten und Löschen der Basisidentität sowie Einstellen, Pflegen und Löschen von weiteren Attributen über Self-Service Funktionen. • Authentifikation der Nutzer:in mittels der Online-Ausweisfunktionen des Personalausweises und des Nutzerkontos Bund. • Managementfunktionen für den Betrieb des IDMs **IdP NBP:** Sicherstellen der Authentifikation der Basisidentität der NBP **NBP-AAI:** Sicherstellen SSO Funktionalität über dezentrale Authentifikation der digitalen Identität im Rahmen der Föderation **Ablage:** Siehe Ablage
Zusatzanforderungen	**NBP-AAI:** • Umsetzung weiterer Protokolle, wie OAuth2.0 / OpenId Connect. • Weitere Anforderungen werden im späteren Verlauf weiter definiert.
MVP	Siehe Basisanforderungen
Nicht funktionale Anforderungen/ Kennzahlen	Werden im späteren Verlauf definiert.
Lösungsansätze/ Fertige Lösungen	Als Beispiel dient hier die DFN AAI mit der sich gerade in Entwicklung befindlichen edu-ID. Die Umsetzung könnte mit gängigen Open Source Lösungen (Shibboleth, Keycloak, etc.) realisiert werden. Eine zusätzliche Abstimmung mit VIDIS hat das Ziel, Synergien in Technologie, Governance und Betrieb zu heben.
Berührungspunkte und Abgrenzung	Ablage: Eine für die Authentifizierung bei der NBP genutzte Identität muss auch mit der Ablage verknüpfbar sein

8 Digitale Nachweise

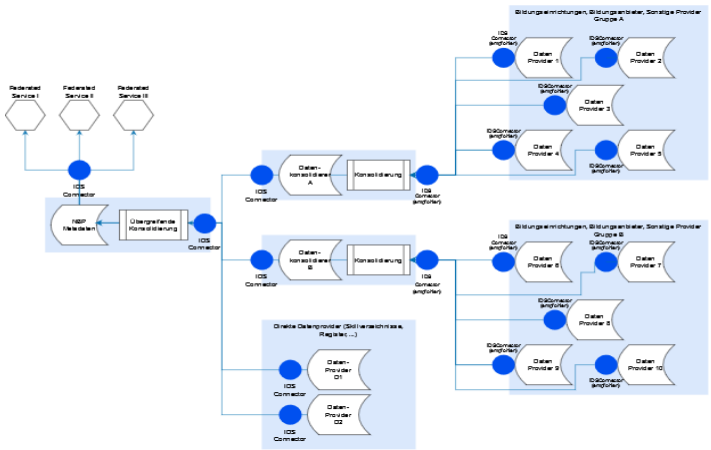
Kurzbeschreibung (inkl. Wert für die NBP)	Digitale Nachweise finden sich in der Domäne Bildung an vielen Stellen. Die NBP wird aufgrund der besonderen Bedeutung von digitalen Nachweisen, Kernkomponenten für die Umsetzung bereitstellen. Hierbei soll auf Basis bereits erprobter Standards und Technologien analog zu bereits existierenden Systemen (beispielsweise DFN-PKI) die besonderen Bedingungen der Domäne Bildung (siehe Grundlagen) einbezogen werden. Die individuellen Workflows auf Seite der Bildungsinstitutionen und die Präsentation der Zeugnisse werden hier nicht spezifiziert. Eine besondere Rolle bekommt die dezentrale "Registration Authority", die nicht nur die Identität einer Organisation oder Person authentifiziert, sondern auch qualitativ bewertet, welche Art von Organisation und oder Person vorliegt und welche Art von digitalen Nachweisen damit jeweils herausgegeben werden darf.
Basisanforderungen	**Certificate Authority (CA):** • Root CA • Herausgebende CA (Public Keys und ggf. weitere Informationen wie Typ der Bildungseinrichtung etc.) • CRL - Certificate Revocation List mit einer Erweiterung um zurückgezogene "Verifiable Claims" • Authentifikation der Nutzer:in mittels der Online-Ausweisfunktionen des Personalausweises und des Nutzerkontos Bund. • Signatur Service für Organisationen und/oder Personen, die keine Möglichkeit haben, auf ihrer lokalen Infrastruktur ein Signatur Modul oder eine Signatur App zu nutzen. Signiert "Verifiable Claims" und/oder Dokumente • Private Key Vault als Speicher für relevante Informationen • Verwaltungssoftware für die CA **Registration Authority (RA):** • Software für die Umsetzung einer RA • Authentifikation der Nutzer:in mittels der Online-Ausweisfunktionen des Personalausweises und des Nutzerkontos Bund. • Verwaltungssoftware für die RA **Signatur Modul/ Signatur App:** • Generieren Schlüssel/Kommunikation mit RA • Signieren von Dokumenten und/oder VC • Zurückziehen von Signaturen/ Kommunikation mit CA • Verwalten von durchgeführten Signaturvorgängen • API (nicht Mobile) damit weitere Komponenten (beispielsweise Verwaltungssysteme) die Funktionen nutzen können

	Modul für angepasste VC: • Entgegennahme eines bereits erstellten VC und der Anpassungswünsche → Verifiable Presentation • Ansprechen des API Signaturmoduls um die Signatur des VC umzusetzen • Bereitstellen der neuen angepassten VC • Verwaltungssoftware für angepasste VC
Zusatzanforderungen	Keine
MVP	Siehe Basisanforderungen
Nicht funktionale Anforderungen/ Kennzahlen	**Signatur Modul/ Signatur App:** • Hinsichtlich der Struktur von VC müssen die aktuell gängigen Standards berücksichtigt werden (beispielsweise XBildung, ESCO, Europass). Weitere werden im späteren Verlauf definiert.
Lösungsansätze/ Fertige Lösungen	Die DFN PKI dient als mögliches Anschauungsobjekt.
Berührungspunkte und Abgrenzung	**Relevante Projekte:** • Europass • DiBiHo • OpenBadges • SSI Projekte • EU Toolbox inkl Use Case • XBildung Keine Berücksichtigung von Ansätzen, die DLT oder SSI enthalten. Berücksichtigen von SSI Funktionen wie "Verifiable Presentation". Der Unterschied zur aktuellen DFN PKI wäre eine zentrale CA, die von allen Beteiligten genutzt wird. Damit entstehen keine n-stufigen Zertifikatsketten. Lokale CA würden nur aus repräsentativen Gründen genutzt, hätten aber keine Bedeutung. Gleiches gilt für Themen wie Revocation. Alle Vorgänge werden sowohl lokal als auch zentral vorgehalten mit der Vorgabe, dass die zentralen Daten, die zu nutzenden Daten sind. Die/der Nutzer:in speichert ihre VC in ihrer Ablage. Die aktuell in Entwicklung befindlichen Standards des BSI zu dem Thema werden berücksichtigt.
Offene Punkte	Keine

Metadaten

Kurzbeschreibung (inkl. Wert für die NBP)	Metadatenspeicher dienen zur Speicherung von nicht personenspezifischen und nicht transaktionsspezifischen Daten. Im Kontext der NBP lassen sich diese in folgende grobe Rubriken einteilen: 1. Informationen (Metadaten) über Inhalte von Bildungsangeboten und Medien (Learning Opportunities) 2. Moduldaten aus Studiengängen 3. Studiengänge 4. Weiterbildungen und Abschlüsse 5. Statistische und Analyse-Daten 6. Verzeichnisse von Bildungsinstitutionen und deren Struktur 7. Kompetenzen und Skills 8. Lernorte 9. Curricula Sie bilden die Grundlage für einen **Datenraum Bildung**. Vorzugsweise soll auf existierende Standards zurückgegriffen werden. Werden neue Standards oder Erweiterungen und Anpassungen bestehender Standards als notwendig erachtet, haben diese in geeigneten Gremien und so global wie möglich zu erfolgen. Lerninhalte selbst sind nicht Teil der hier zu betrachtenden Rubriken. Sollte es sich als notwendig erweisen, dass die NBP selbst Inhalte ausliefert (OER Daten oder CDN Strukturen um Anbieter zu entlasten), so wird dies in einem dedizierten Projekt erfolgen. Durch die Metadaten können verschiedenste förderierte Dienste (z.B. Empfehlungsfunktionen, Suchfunktionen) mit hoher Effizienz angeboten werden und weitere Innovationen entstehen. Im weiteren Verlauf werden die Aktivitäten im Kontext der Registermodernisierung mit den Aktivitäten der NBP abgestimmt. Bei nachfolgenden Umsetzungen im Rahmen der Registermodernisierung werden die jeweiligen Daten überführt.
Basisanforderungen	• Metadaten werden von der NBP verarbeitet, um Suche (beispielsweise nach Lerninhalten oder Bildungseinrichtungen) zu ermöglichen. • Die Metadaten werden von Konsolidierungspartnern in den unterschiedlichsten Formaten des Marktes erfasst und von dort an die NBP in abgestimmten Formaten gepusht. • Die NBP stellt als Service Redaktionstools zur Verfügung, um Metadaten anpassbar zu machen (z.B. die Korrektur von Rechtschreibfehlern oder geringfügigen Änderungen in Beschreibungen oder Zuordnungen). • Inwieweit einer dieser Konsolidierungspartner im Rahmen der NBP selbst betrieben wird, muss noch abhängig vom Bedarf abgestimmt werden.

	• Durch die Verwendung von Connectoren in Anlehnung an https://internationaldataspaces.org/ werden die Daten mit Nutzungs-Policies versehen. Dieses Pattern ist zumindest für die direkt an den NBP-Metadatenspeicher angebundenen Daten-Provider - z.B. die Datenkonsolidierungspartner - vorgesehen. By Default sind die Daten gemäß Open Data Lizenz zu lizensieren (z.B. Public Domain Dedication and License - PDDL, Open Database License - ODC ODbL). • Existierende Vorarbeiten (auch domänenspezifisch) werden, wo immer möglich, berücksichtigt.
Zusatzanforderungen	Bisher keine
MVP	Siehe Basisanforderungen
Nicht funktionale Anforderungen/ Kennzahlen	Die Anforderungen für die Basisinfrastruktur (z.B. Skalierbarkeit, DevOP-Fähigkeit) sind für die Artefakte der NBP Metadaten zu berücksichtigen.
Lösungsansätze/ Fertige Lösungen	• **Architektur zur datenagnostischen Speicherung von Metadaten** Die Datenbank ist so strukturiert, dass beliebige Key/Value-Paare einschließlich ihrer hierarchischen Struktur gespeichert werden können. Diese Grundstruktur ist damit insbesondere sehr effizient in der Speicherung von Daten in XML- oder JSON-Form. Es wird damit eine hohe Datenagnostik unter Beibehaltung von semantischen Informationen quasi beliebiger Daten unabhängig von Ihrer Ontologie ermöglicht. • **Federated Services zum Zugriff / zur Nutzung der Metadaten** Über Services (z.B. eine Suchfunktion nach Skills oder Bildungsangeboten) wird auf die Metadaten zugegriffen. Der Service muss Basis-Informationen zur Struktur der relevanten Daten besitzen, z.B. die kennzeichnenden oberen Key/Value Strukturen der relevanten Datenrubrik (z.B. Skill-Verzeichnisse) und die Keys für die interessierenden Daten kennen, um auf die semantisch richtigen Daten/Datenstrukturen im datenagnostischen Meta-Repository zugreifen zu können. D.h. die Daten nutzenden Services sind im Gegensatz zu den Datenstrukturen des Repositories nicht agnostisch, sondern spezifisch auf die Ontologie und Semantik der Datenstrukturen angepasst. Zur Förderung innovativer Nutzungsszenarien der Metadaten ist es erwünscht, dass Services aus der breiten Community heraus entstehen. Die Umsetzung kann dann im Einklang mit den Paradigmen der NBP erfolgen.

	• **Architektur zur Umsetzung der Datenkonsolidierung und Standardisierung durch Datenkonsolidierungspartner und von Datennutzungs-Policies** Sowohl die direkten Daten-Provider Schnittstellen, als auch die Schnittstellen zu den Daten-konsumierenden förderierten Services sind an IDS angelehnte Connectoren (siehe https://internationaldataspaces.org/) gekapselt, um die Nutzungs-Policies für die Daten im jeweiligen Datenfluss zur Verfügung zu stellen. Insbesondere für die Informationen zu Bildungsinstitutionen ist geplant, Konsolidierungspartner (z.B. Kursnet, hoch&weit) einzusetzen. Aufgabe der Konsolidierungspartner ist einerseits die Zulieferung der Daten in einem standardisierten Format (z.B. XHochschule für Hochschulen) und andererseits auch eine Gewährleistung von Mindeststandards. Diese Schritte erfolgen im Ablauf "Datenkonsolidierung". Die Datenkonsolidierung seitens der NBP dient z.B. dazu, redundante Daten der Konsolidierungspartner herauszufiltern und ggf. noch redaktionelle Anpassungen im geringeren Umfang durchzuführen (z.B. Bereinigung typografischer Fehler). Bei Daten, die nicht über Konsolidierungspartner laufen (z.B. Skill Verzeichnisse) erfolgt auch eine inhaltliche Prüfung auf Problemfälle und eine ggf. notwendige Anpassung an obligatorische Standards. Es ist geplant, sukzessive Adaptoren in der NBP zu verwenden, um ggf. verbreitete Formate in den bevorzugten Standard umwandeln zu können. Die Zusammenhänge von den Datenprovidern bis zu den förderierten Services sind in der folgenden Grafik dargestellt. 
Berührungspunkte und Abgrenzung	Metadaten enthalten keine personenspezifischen Daten ausgenommen ggf. Quellen/Urheberrechtsinformationen unter Berücksichtigung von DSGVO Vorgaben • Datenstrategie und Datenlabor des BMBF gem. Strategie des Bundes

	• GAIA-X Datenraum in der Domäne Bildung • Mundo • WirLernenOnline • Kursnet / Now • Europass • OpenSkillNetwork • OZG (Institutionsregister) Der Einsatz von sogenannten Crawlern wird nicht erwogen. Hintergrund dieser Entscheidung sind unterschiedliche Aspekte: • Nicht alle Inhalte sind durch Crawler erreichbar. • Vor Aufnahme in Datenräume ist Bewertung des Inhalts notwendig → Hier könnte Crawler höchstes als Vorstufe unterstützend wirken (siehe erster Punkt). • Schlechte bis keine Metadaten - Im weiteren Verlauf ggf. durch eine KI gestützte Vorgehensweise zu lösen. Trotzdem wird es am Ende immer noch eine manuelle Qualitätssicherung geben müssen.
Offene Punkte	• Default Open Data Lizenzmodell (PDDL, ODC-ODbL, ...) • Die Verwendung / Konformität mit GAIA-X Datenräumen • Die tatsächliche Umsetzbarkeit der IDS Connectoren für die NBP-Metadaten

10 Schaufenster

Kurzbeschreibung (inkl. Wert für die NBP)	Durch die NBP besteht neben den durch die NBP selbst bereitgestellten Komponenten auch die Möglichkeit, Angebote zu nutzen, die durch die angeschlossenen Service Provider bereitgestellt werden. Die nahtlose Nutzung erfolgt durch den Anschluss dieser Service Provider an die NBP AAI. In diesem Rahmen erfüllt das Schaufenster der NBP die Funktion einer Art Leitstelle, die zum einen die Angebote darstellt, die prinzipiell nutzbar und zum andern kontextbezogen darstellt, welche Angebote für die Nutzer:innen geeignet sind. Dabei ist dies kein exklusiver Zugang, sondern eine mögliche Nutzung der darunterliegenden Daten- und Serviceschicht. Über eine Workbench werden dem/der Nutzer:in die möglichen Funktionen des Schaufensters dargestellt. Das Schaufenster verfügt über einen direkten von dem/der Nutzer:in freigegebenen **Zugang zur persönlichen Ablage** des/der Nutzer(s):in. Damit können beispielsweise Statusdaten zu Nutzer:innen betreffenden Vorgängen und Bildungsnachweisen in einem Dashboard dargestellt werden. Ein **Lernpfadfinder** kann mit diesen Informationen, den/die Nutzer:in kontextbezogen zu angeschlossenen Angeboten der Service Provider leiten sowie je nach Lebenslage Tipps geben und weitere Schritte aufzeigen. Weitere Funktionen wie beispielsweise bildungsinstitutionen- und bildungssektorenübergreifende Kollaborationsräume werden über die Workbench nutzbar gemacht. Ein weiterer Bestandteil des Schaufensters ist die Möglichkeit, neue Services und Technologien - auch der Basisinfrastruktur - durch eine breite Nutzer:innenbasis testen zu lassen. Damit können am lebenden Objekt objektiv Erfahrungen für zukünftige Nutzer:innenszenarien für alle Stakeholder gesammelt werden. Zudem können bereits bestehende Services auf Basis der Nutzer:innen-Rückmeldung verbessert werden.

Basisanforderungen	• Folgende Funktionen und Services sollen von Beginn an im Schaufenster der NBP verfügbar sein:
	  ○ Lernpfadfinder: Begleiten den/die Nutzer:in im Übergang zwischen Bildungsinstitution und oder Bildungssektoren. Aufzeigen von Lösungsansätzen und weiteren Schritten in unterschiedlichen Lebenslagen, wie beispielsweise der Entscheidung für den nächsten Schritt in der persönlichen Bildungsreise.
	  ○ Dashboard: Darstellung aller aktuellen Vorgänge auf persönlichen Bildungsreise und deren Status. Die Inhalte entstammen der Ablage (personenbezogene Daten).
	  ○ Personalisierte Suche von Inhalten und Services.
	  ○ Buddy Finder: Service zum Auffinden von weiteren Nutzer:innen, wo eine Kontaktaufnahme kontextbezogen (beispielsweise für den Austausch zu einem bestimmten

	Thema oder zum gemeinsamen Lernen) Sinn ergeben könnte. o Kollaborationswerkzeuge, in denen sich Nutzer:innen unabhängig von bestehenden Service Providern und damit bildungsinstitutionen- und bildungssektorenübergreifend zu Themen zusammenfinden und austauschen können o Eine tiefere Integration von einzelnen Services angeschlossener Service Provider (beispielsweise die geförderten Ziel-1 und Ziel-2 Projekte), deren Nutzbarkeit dadurch gesteigert wird. Dies soll aus der Perspektive der Nutzer;in so erfolgen, dass ein nahtloses Nutzer;innenerlebnis entsteht. • Für eine einfache und schnelle Umsetzung von Workflows des Schaufensters soll eine anzuschließende BPMN Engine genutzt werden. • Über eine Service Architektur soll das Schaufenster einfach und schnell durch neue Funktionen und Services erweitert werden können. Neue Services sollen so implementiert werden, dass die eigentliche Funktionalität über eine API angesprochen wird. • Basierend auf den Daten der Ablage und der jeweiligen IdP können Funktionen und Services des Schaufensters gesperrt werden. Dies dient zum Schutz der jeweiligen Nutzer:innen im Kontakt untereinander.
Zusatzanforderungen	Werden im späteren Verlauf definiert
MVP	Siehe Basisanforderungen.
Nicht funktionale Anforderungen/ Kennzahlen	Werden im späteren Verlauf definiert.
Lösungsansätze/ Fertige Lösungen	Als Plattform-Lösung hat sich Liferay (mindestens in der Version 7.3) (Open Source LGPL) im Rahmen eines fertigen Prototypen (BIRD) als sehr praktikabel erwiesen.
Berührungspunkte und Abgrenzung	• Wird auf Basis der Basisinfrastruktur betrieben. • Nutzt weitere Komponenten wie die NBP AAI, NBP Ablage, Metadaten und weitere.
Offene Punkte	• Welche weiteren Funktionalitäten und Services werden aufgenommen? • Abgrenzung zu bestehenden Funktionalitäten und Services von angeschlossenen Service Providern. Zielsetzung ist hier komplementär zu kooperieren, um eine Marktverzerrung in Richtung bereits bestehender Services zu verhindern.