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
25.11.2022	2.2	Überarbeitung der Steckbriefe	Product Owner

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:

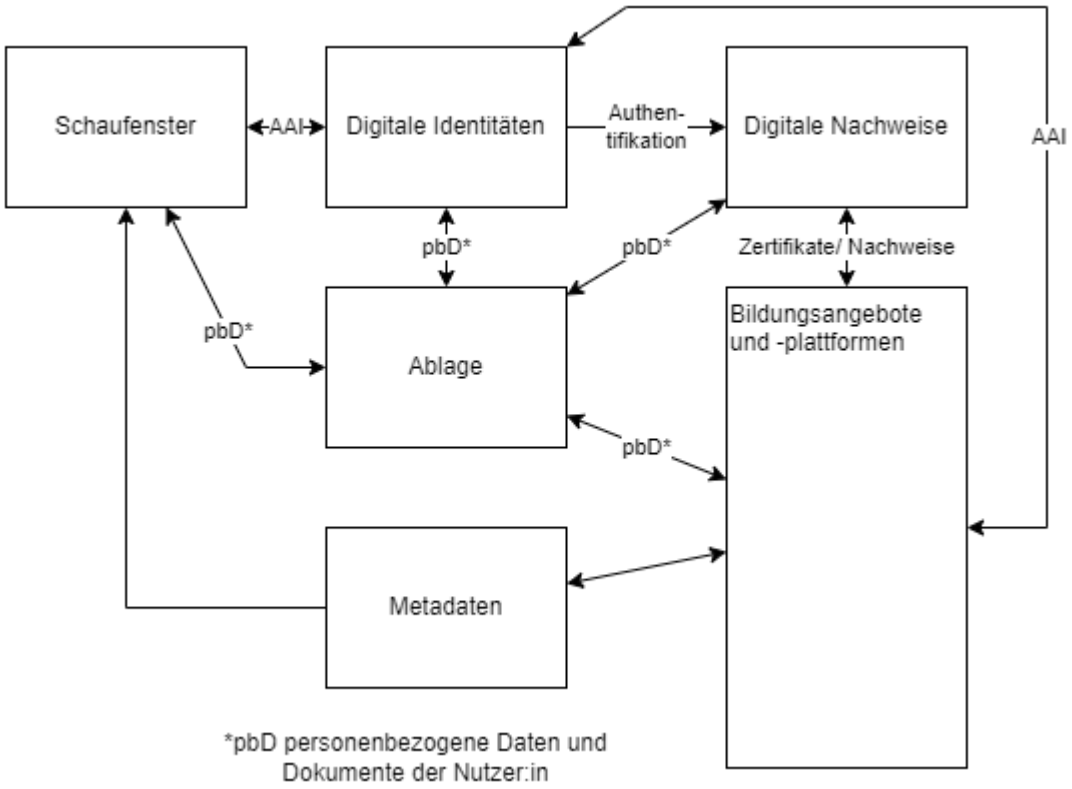


Abbildung 1 Basisinfrastruktur der NBP

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 Konsolidierungspartnern 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-App Dokumente souverän ablegen und an Service Provider und Nutzende freigeben. Die Ablage-App ist 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 an Service Provider und Nutzende 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. Das Gegenstück zur Ablage-App ist der Connector der direkt in der IT-Landschaft des Service Providers gehostet wird. Ablage-App und Connector kommunizieren Ende-zu-Ende verschlüsselt über ein zentral bereitgestelltes Backbone. 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.

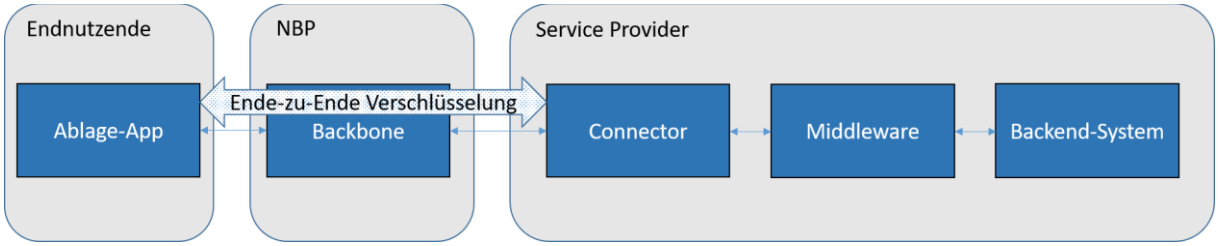
Die Schritte in einer CI/CD-Pipeline stellen verschiedene Untergruppen von Aufgaben dar, die in sogenannte Pipeline-Phasen eingeteilt werden. Zu diesen Phasen gehören üblicherweise:

- **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 ist die als Default bereitgestellte “NBP Ablage” 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. Das zentral von der NBP bereitgestellte und gehostete Backbone ermöglicht die bidirektionale Kommunikation zwischen Ablage-App-to-Connector, Connector-to-Connector und Ablage-App-to-Ablage-App.
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 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 • Bereitstellen einer API in Richtung der NBP • Darstellen aller notwendigen Funktionen, um Inhalte zwischen den Konnektoren auszutauschen

	• Darstellen aller notwendigen Funktionen, um Inhalte zwischen der NBP und den Konnektoren auszutauschen **Meta Ablage Connector (perspektivisch):** • Anbinden von unterschiedlichen Ablagesystemen, perspektivisch über eine einheitliche Schnittstelle. • Bereitstellen einer API in Richtung der Konnektoren • 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:** • **SDK**: Bereitstellung eines SDK um Komponenten, die an den Backbone andocken (zur Zeit App und Connector) nach Bedarf zu implementieren. Daneben sind MVP-App und MVP-Connector dann als Referenzimplementierungen verfügbar. • **Verifizierung (Konzept noch nicht vollständig ausgearbeitet)**: 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. o Eine Interoperabilität von Ablagen untereinander ist langfristig anzustreben. o 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)	Digitale Identitäten werden bereits über verschiedene Bildungsangebote per Identitätsanbieter (Identity Provider) angelegt und verwaltet (zum Beispiel beim Schulamt, in der Hochschule oder auf einzelnen Bildungsplattformen). Nutzende sollen einen einfachen Zugang zu den Inhalten der an die Digitale Vernetzungsinfrastruktur Bildung angeschlossenen Service Provider (SP bzw. Serviceanbieter) erhalten. Über die AAI (Authentication and Authorization Infrastructure) der Nationalen Bildungsplattform (NBP) als Vernetzungsinfrastruktur wird ein Single Sign-on-Dienst zur Verfügung gestellt. Damit ist der Login über die Vernetzungsinfrastruktur auch bei angeschlossenen Service Provider möglich. Bestehende Initiativen werden dabei berücksichtigt. Für Nutzende, die nicht über eine Digitale Identität aus den oben dargestellten AAIs verfügen, stellt die Vernetzungsinfrastruktur in Form eines Identity-Providers (IdP) eine Basisidentität zur Verfügung, um die NBP und die angeschlossenen Service Provider nutzen zu können. Der selbstbestimmte Umgang mit den eigenen Daten wird sichergestellt. Die Nutzenden sollen ihre Daten selbstsouverän ablegen und anderen Nutzenden und/oder Service Providern freigeben können. Hierbei bestimmt die sendende Person, wer zu welchem Zeitpunkt auf welche Daten zugreifen kann. Die angeschlossenen Dienste helfen, nicht nur datenschutzkonform, sondern auch sicher zu agieren.
Basisanforderungen	**Übersicht** Nutzende sollen einen einfachen Zugang zu den Inhalten der an die NBP angeschlossenen Service Provider (SP) erhalten. Die NBP bietet hierfür eine "Authentication and Authorization Infrastructure (AAI)". Mit dieser NBP AAI bekommen die Nutzenden abhängig von ihrem Profil, das 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 Nutzenden. Dieses Prinzip wird als Single Sign-on (SSO) bezeichnet (Single Log-out (SLO) gilt für die Zwecke dieser Ausschreibung als Bestandteil der SSO Funktionalität und wird deshalb 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 Nutzende, die nicht über eine digitale Identität aus den oben dargestellten AAIs verfügen, stellt die NBP in Form des NPB Identity-Providers (IdP) eine Basisidentität zur Verfügung. Über sogenannte "Self Service Funktionen" des NBP Identity-Managements (NBP IDM) können Nutzende 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 Nutzenden erfolgen. Weitere Attribute können über den Verwaltungsbereich eingestellt, gepflegt und gelöscht werden. Alle personenbezogenen Daten werden in die Ablage übertragen. Das Vertrauensniveau der Basisidentität wird an dem Vertrauensniveau der zugrundeliegenden Authentifikation ausgerichtet. Die aus den oben dargestellten AAIs stammenden digitalen Identitäten können auch mit der Basisidentität verbunden werden. Das ermöglicht es den Nutzenden auf Wunsch im späteren Verlauf auf die Nutzung unterschiedlicher digitaler Identitäten zu verzichten. Die Basisidentität 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. Um den Schutz von Minderjährigen zu wahren, aber auch die Verhinderung der Verbreitung von ggf. strafbewehrtem Material je nach Anwendungsfall zu gewähren sind eine sowohl gänzlich anonyme digitale Identität als auch eine digitale Identität mit niedrigem Vertrauensniveau ausgeschlossen. 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 Single-Sign-On (SSO) sollen möglichst wenig Metadaten (ggf. nur eine GUID) der Nutzenenden ausgetauscht werden. **NBP IDM** Das NBP IDM umfasst neben der Möglichkeit, eine digitale Identität für die Nutzung der NBP und der angeschlossenen Service Provider zu erzeugen, auch das Sicherstellen der Authentifikation dieser Identität. Die Authentifikation ist notwendig, um im weiteren Nutzungsverlauf auf die gesamte Funktionalität der NBP zugreifen zu können. Das Identitätsmanagement umfasst aus der Perspektive der Nutzenden unter anderem Funktionen wie das Einrichten, Verwalten und Löschen der digitalen Identität und weiterer Attribute, sowie die Verbindung mit der Ablage über Self-Service Funktionen. Um die Nutzung der Ablage in Kontext mit der digitalen Identität zu ermöglichen, erfolgt eine Anbindung des NBP-IDM an die Ablage über den Ablage-Connector. Für **den**

	Austausch mit anderen IdP und AAIs werden Standard-Authentifizierungsprotokolle (SAML2.0, OpenID Connect und OAuth2) genutzt. Hierfür müssen entsprechende Interfaces aufgebaut werden. **NBP AAI** Die NBP AAI bindet die an die NBP angeschlossenen Service Provider und die NBP zu einer AAI zusammen und bietet damit auch einen SSO (Single-Log-Out (SLO) immer inbegriffen) für die Nutzenden an. Zudem sorgt die NBP AAI für die Verbindung zu anderen AAIs wie beispielsweise der DFN-AAI des Deutschen Forschungsnetzes, für den Hochschulbereich in Deutschland, oder VIDIS als Vermittlungsdienst für das digitale Identitätsmanagement im Schulbereich. Nutzende sollen sich im Rahmen der NBP AAI immer an ihrem Heimatsystem anmelden und dann im Rahmen des SSO Zugang zur NBP und den angeschlossenen Service Providern bekommen. Hierfür nutzt die NBP-AAI SAML2.0, OpenID Connect und OAuth2 als Standard-Authentifizierungsprotokolle, die durch entsprechende Interfaces bereitgestellt werden. Aus Perspektive der Nutzenden sind in der NBP-AAI unter anderem Funktionen wie der Login im Heimatsystem, der Logout, die Verbindung zur Ablage und die Authentifikation der Identität über Self-Service Funktionen nutzbar. Für beide Komponenten, NBP-IDM und NBP-AAI werden für den Bereich Verwaltung und Administration bestehende Workflows angepasst oder neue Workflows entwickelt. Sowohl für die Umsetzung des NBP-IDM als auch der NBP-AAI soll Keycloak zum Einsatz kommen. Keycloak ist eine Open-Source-Lösung für Identity und Access Management, die auf die Absicherung moderner Anwendungen und Services ausgerichtet ist. Keycloak bietet anpassbare Benutzeroberflächen für die Anmeldung, Registrierung, Administration und Kontoverwaltung. Keycloak ermöglicht es, die anvertrauten digitalen Identitäten selbstständig zu verwalten oder sie von bestehenden Anbietern zu übernehmen. Keycloak ermöglicht außerdem eine einheitliche und sichere Kommunikationsschnittstelle zu Zielanwendungen und Social Logins, die auf verschiedenen Standard-Authentifizierungsprotokollen wie OpenID Connect, OAuth2 und SAML 2.0 basieren.
Zusatzanforderungen	**NBP-AAI:** • Umsetzung weiterer Protokolle, wie OAuth2.0 / OpenId Connect. • Weitere Anforderungen werden im späteren Verlauf weiter definiert.
MVP	• Authentifizierte Registrierung mit Bund-ID • Anbindung an Authentifikationsmechanismen auf Basis des nPA(neuer elektronischer Personalausweis)

	• Mechanismen zur Datensparsamkeit (z.B. Workflow zum Löschen von Nutzerkonten)
Nicht funktionale Anforderungen/ Kennzahlen	• Die gesamte Entwicklung (IDM & AAI) erfolgt auf Grundlage von Open-Source-Java-Anwendungen. • Die gesamte Entwicklung muss Container-fähig sein • Die Umsetzung der NBP AAI und NBP IDM ist mit dem Open Source Produkt Keycloak zu realisieren.
Lösungsansätze/ Fertige Lösungen	Als Beispiel dienen hier die an die NBP anzubindenden AAIs: • DFN AAI (setzt Shibboleth ein) mit der sich gerade in Entwicklung befindlichen edu-ID • VIDIS AAI (setzt Keycloak ein)
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 und der Austausch der digitalen Nachweise bzw. Artefakte wird immer wichtiger. Zu den Nachweisen zählen beispielsweise Lernstände oder Bildungs- oder Kompetenznachweise von Nutzenden. Die Nachweise enthalten Aussagen über eine Person, eine Organisation oder Sache. Solche Aussagen können z.B. Noten, Namen und andere Inhalte umfassen. Das Nutzungsspektrum der Nachweise im Bereich Bildung ist breit gefächert über verschiedene Bildungsinstitutionen und -sektoren hinweg. Die enthaltenen Daten müssen durch eine autorisierte Institution bestätigt und gegen Veränderung geschützt werden. Ein wichtiger Aspekt bei der Vernetzung und Nutzung dieser Nachweise ist daher deren Integrität und Authentizität. Um diese sicherstellen zu können, werden die Nachweise und deren Daten digital signiert. Digitale Signaturen sind durch das Ausstellen digitaler Zertifikate abgesichert und überprüfbar. Ein bewährter Standard zum Ausstellen und Verwalten digitaler Zertifikate ist die Verwendung einer Public Key Infrastructure (PKI). Innerhalb der PKI sorgen Certification Authorities (Zertifikatsstellen, CAs) dafür, dass vertrauenswürdige Zertifikate ausgestellt werden. Über Registration Authorities (Registrierungsstellen, RAs) wird gewährleistet, dass nur eindeutig identifizierte und autorisierte Institutionen Berechtigung zum Ausstellen der Zertifikate erhalten. Die NBP wird aufgrund der besonderen Bedeutung von digitalen Nachweisen Kernkomponenten für die Umsetzung bereitstellen. Basis bilden hierbei bereits erprobte Standards und Technologien, sowie Open-Source-Lösungen analog zu bereits existierenden Systemen (beispielsweise DFN-PKI). Die bereitgestellten Technologien sollen unabhängig vom Typ der Nachweise und deren Daten (Schulzeugnisse, Berufsausbildungszeugnisse, Studienleistungen, berufliche Qualifikationen oder jeweilige Teilleistungen, Visa für Studierende, etc.) sein. Die digitalen Nachweise in der NBP sollen nachhaltig umgesetzt werden in Hinblick auf Technologie, offene Standards, Vendor Lock-in, Transparenz der Codebasis, aber auch bezüglich Lizenzmodellen (Investitionen und Kosten), um hier für eine breite Akzeptanz zu sorgen.

	Die individuellen Workflows auf Seite der Bildungsinstitutionen und die Präsentation der Zeugnisse werden hier nicht spezifiziert. Innerhalb der NBP gibt es für die Komponente "Digitale Nachweise" folgende Teilkomponenten: • Certificate Authority (CA) mit Certificate Revocation List • Registration Authority (RA) • Bildungsinstitutionsverzeichnis • Schlüsselgenerierung • Nachweissignatur • Nachweisanpassungen • Nachweiszustellung • [Inforegister/Bildungsnachweisregister (enthält Metadaten und Mappings der Curricula etc.) > out of Scope] • Certificate Gateway (Anbindung nationaler CAs, Verifizierung von Zertifikaten/Nachweisen auf europäischer/globaler Ebene) • Überprüfungskomponente Im Rahmen der Corona-Warn App wurde mittels erprobter Technologien (PKI, X.509) eine Anwendung erstellt, um VCs (COVID Zertifikate) schnell und sicher auszustellen, zurückzuziehen und zu verifizieren, denen in allen Mitgliedsländern der EU, der Schweiz und Norwegen vertraut wird.

Basisanforderungen	*Certificate Authority (CA):*
	
	Grundlage für einen sicheren Umgang mit Nachweisen ist eine Struktur, der alle Beteiligten vertrauen können. Dabei bilden sogenannte Zertifikatsstellen (Certificate Authorities, CAs) den zentralen "Vertrauensanker" (trust anchor). CAs stellen digitale Zertifikate aus und bestätigen, dass digitale Unterschriften von einer vertrauenswürdigen Stelle kommen.
	
	An die CA stellen wir folgende Anforderungen:
	• *Fachliche:*
	  ○ *Zertifikate*
	  ▪ Zur Ausstellung von Zertifikaten wird eine für alle Systeme erreichbare CA benötigt.
	  ▪ Zertifikate können von der ausstellenden oder ggf. einer übergeordneten Institution widerrufen werden (Certificate Revocation).
	  ▪ Zertifikate können von jedem überprüft werden. Widerrufene Zertifikate gelten als ungültig.
	  ▪ Es muss die Möglichkeit geben, dass ein Zertifikat ungültig gesetzt oder an eine übergeordnete Instanz übertragen wird, ohne dass die Nachweise ungültig werden (Institution darf keine neuen Zeugnisse signieren)
	  ▪ Wenn Schlüssel nicht mehr vorhanden sind, muss es die Möglichkeit geben, Schlüssel zu widerrufen

	▪ Für den Aufbau einer CA-Struktur soll kein Vertrauensdiensteanbieter eingebunden werden, um einen Vendor-Lock-In zu vermeiden. ▪ Die CA soll über eine Verwaltungsoberfläche administriert werden können. o ~~*Nachweise*~~ ▪ ~~Nachweise können von der ausstellenden oder ggf. einer übergeordneten Institution widerrufen werden.~~ ▪ ~~Nachweise können von jedem überprüft werden. Widerrufene Nachweise gelten als ungültig.~~ o *Beide* ▪ Es muss die Möglichkeit geben, einen Widerruf ausgehend von einem Schulverwaltungssystem (bspw. per Schnittstelle) durchzuführen ▪ Es muss die Möglichkeit geben, einen Widerruf per Webanwendung durchzuführen ▪ Eine übergeordnete Institution muss die Möglichkeit haben, Zertifikate und Nachweise einer Institution zu widerrufen, die nicht mehr existiert • *Technische:* o Zertifikate ▪ Mögliche Umsetzungsvarianten: Zentrale Root-CA, die direkt angesprochen wird oder Hierarchie mit Root-CA und ggf. mehreren Ebenen an ausstellenden CAs ▪ Herausgebende CAs können Public Keys und ggf. weitere Informationen wie Typ der Bildungseinrichtung etc. bereitstellen ▪ Widerrufene Zertifikate sind über eine zentrale Liste (Certificate Revocation List, CRL) abrufbar. Der Abruf kann über ein Self-Service-Portal (Webanwendung) oder per API erfolgen. ▪ Das genutzte Root-Zertifikat soll in die deutschlandweite / EU-weite Trusted-List aufgenommen werden ▪ Die Zertifikatsinhaber sollen einen Private-Key-Vault als Speicher für relevante Informationen erhalten ▪ Zertifikate müssen alle n Jahre technisch erneuerbar sein, ohne dass die Nutzenden etwas tun müssen oder dies mitbekommen *Nachweis-Revokationsservice* Im Fehlerfall müssen Nachweisaussteller (Bildungseinrichtungen oder übergeordnete Institutionen) die Möglichkeit haben, Nachweise zu widerrufen. • *Fachliche:*

	○ Nachweise können von der ausstellenden oder ggf. einer übergeordneten Institution widerrufen werden. ○ Nachweise können von jedem überprüft werden. Widerrufene Nachweise gelten als ungültig. ○ Es muss die Möglichkeit geben, einen Widerruf ausgehend von einem Schulverwaltungssystem (bspw. per Schnittstelle) durchzuführen ○ Es muss die Möglichkeit geben, einen Widerruf per Webanwendung durchzuführen ○ Eine übergeordnete Institution muss die Möglichkeit haben, Nachweise einer Institution zu widerrufen, die nicht mehr existiert • *Technische:* ○ ▪ ▪ Widerrufene Nachweise sind über eine zentrale Liste abrufbar. Der Abruf kann über ein Self-Service-Portal (Webanwendung) oder per API erfolgen. ▪ ***Wie werden Nachweise unterzeichnet?*** ▪ ***Ein Zertifikat pro Zeichnung → CRL funktioniert automatisch auch für Widerruf von Nachweisen*** ▪ ***Ein Zertifikat pro Bildungseinrichtung/Zeichner → Separate Liste für widerrufene Nachweise*** *Registration Authority (RA):* Bevor unterschreibende Stellen ein Zertifikat erhalten, mit dem ihre Unterschrift bestätigt wird, muss sichergestellt werden, dass sie zur Unterschrift berechtigt sind. Dafür müssen sie sich gegenüber einer sogenannten Registrierungsstelle (Registration Authority, RA) zunächst authentifizieren. Die RA prüft im Anschluss, ob die unterschreibende Stelle die von ihr gewünschten Nachweise unterzeichnen darf. Falls ja, wird die CA darüber in Kenntnis gesetzt und diese stellt ein Zertifikat an die unterschreibende Stelle aus. An die RA stellen wir folgende Anforderungen: • *Fachliche:* ○ *Authentifizierung/Autorisierung* ▪ Die RAs werden dezentral betrieben, beispielsweise auf Landes- oder Kommunenebene. ▪ Die RAs "wissen", für welche Art von Nachweisen sie Zertifikate beantragen können. ▪ Die RAs authentifizieren Organisationen und Personen. Im Anschluss werden diese autorisiert, um bestimmte Nachweise auszustellen und die

	dafür notwendigen Zertifikate von der CA zu erhalten. ▪ Antragsteller können sich mittels der Online-Ausweisfunktionen des Personalausweises und des Nutzerkontos Bund authentifizieren lassen ▪ Eine Offline-Validierung soll möglich sein (RA Struktur auf Device, zentrale Stelle, Pflege durch Länder) ▪ Die Registrierung und die Autorisierung von Institutionen sollen im Rahmen eines Batchbetriebs (per API) möglich sein. o *Anbindung Bildungsinstitutionsverzeichnis* ▪ Autorisierte Bildungseinrichtungen werden automatisch im Bildungsinstitutionsverzeichnis eingetragen • *Technische:* o *Authentifizierung/Autorisierung* ▪ Die RAs sollen über eine Verwaltungsoberfläche administriert werden können. ▪ Die RAs sollen an ein Identitätsmanagement angebunden sein ▪ Es soll ein Logging erfolgen, wer zugegriffen und wer Zeugnisse ausgestellt hat *Bildungsinstitutionsverzeichnis* Das Bildungsinstitutionsverzeichnis soll eine zentrale Stelle sein, bei der Institutionen, die zur Ausstellung von bestimmten Nachweisen berechtigt sind, gelistet werden. Auf diese Weise existiert ein Einstiegspunkt für die Verifizierung der Nachweissignaturen. An das Bildungsinstitutionsverzeichnis stellen wir folgende Anforderungen: • *Fachliche:* o Das Bildungsinstitutionsverzeichnis enthält eine Liste aller teilnehmenden autorisierten Bildungseinrichtungen mitsamt deren Typ und dem Typ der Nachweise, die die Einrichtung ausstellen darf. o Das Bildungsinstitutionsverzeichnis soll an zentraler Stelle gehalten werden o Berechtigte Personen sollen die Möglichkeit erhalten, Einträge über eine Webanwendung manuell vorzunehmen oder bestehende zu ändern. o Es soll nur die Verwendung von allgemeinen Institutionsdaten erfolgen, es sollen keine personenbezogenen Daten in einem Bildungsinstitutionsverzeichnis vorgehalten werden o Die für ein Bildungsinstitutionsverzeichnis benötigten Daten sollen sich an der „Liste aktiver Schulen in Deutschland“ orientieren: https://xschule.digital/web/ListeAktiverSchulen_DE

	○ Das Bildungsinstitutionsverzeichnis soll über eine Administrationsoberfläche verwaltbar sein, um Einträge manuell hinzuzufügen, zu editieren oder zu entfernen. ○ *Optional: Das Bildungsinstitutionsverzeichnis muss eine Authentifizierung gegenüber Verwaltungen durchführen. Dies ist notwendig, wenn eine Einrichtung sich nicht zuerst bei einer Verwaltung mit RA authentifiziert, sondern im Bildungsinstitutionsverzeichnis direkt eintragen lässt.* • *Technische:* ○ Zentraler/dezentrale Bildungsmanagementsysteme sollen via API angebunden werden ○ Das Bildungsinstitutionsverzeichnis soll per Web-Service (API) die Informationen zu den Institutionen der Länder automatisiert abfragen können. ○ Die Registrierung und die Autorisierung von Institutionen sollen im Rahmen eines Batchbetriebs (per API) möglich sein. ○ Das Bildungsinstitutionsverzeichnis soll über eine Webanwendung ○ Das Bildungsinstitutionsverzeichnis muss an ein Identitätsmanagement angebunden sein, um nur berechtigten Personen Zugriff auf das Register zu gewähren. *Nachweissignatur* Um zu gewährleisten, dass Bildungsverwaltungssysteme einheitliche Standards für die Nachweissignatur verwenden und die Signatur unabhängig vom Verwaltungssystem getätigt werden kann, wird eine gesonderte Softwarekomponente benötigt. An die Nachweissignatur stellen wir folgende Anforderungen: • *Fachliche:* ○ Zum Signieren der Nachweise wird ein remote Modul bereitgestellt, das an Bildungssysteme (z.B. Schulverwaltungssysteme) angebunden/von diesen aufgerufen werden kann. ○ Das Modul soll einen Nachweis in Präsentationsform (PDF) und entsprechende strukturierte Daten in einem Eingangsformat (JSON nach XSchule-Vorbild) entgegennehmen. ○ Das Modul konvertiert die strukturierten Daten in ein Ausgabeformat ○ ***Momentan angedachte Formate:*** ▪ ELM ▪ ELMO ▪ W3C VC ▪ Open Badges ▪ XHochschule und XSchule, darüber XBildung

	○ Das Modul soll die Präsentationsform mit den strukturierten Daten zu einem kombinierten Nachweis verbinden. ○ Das Modul soll den kombinierten Nachweis mit einer vorher konfigurierten/bereitgestellten und durch ein Zertifikat abgesicherten Signatur unterschreiben. ○ Offen: ▪ ***Welche anderen Eingangsformate neben XSchule unterstützen wir/welches soll verwendet werden?*** ▪ ***Sollen die strukturierten Daten vor der Kombination mit der Präsentationsform ebenfalls signiert werden?*** ▪ ***Wie wird mehrfaches Signieren abgebildet?*** ○ Organisationen und/oder Personen, die keine Möglichkeit haben, die Nachweissignatur per API aufzurufen, können über einen zentralen Signatur-Service (Webanwendung) Nachweise signieren ○ Andere Komponenten können den Signatur-Service per API aufrufen • *Technische:* ○ Als PDF-Standard soll PDF 3A verwendet werden. ○ Die Signatur basiert auf BSI-Standards für die elektronische Signatur (Advanced electronic Signature, AeS) → ***AeS und keine QeS*** *Schlüsselgenerierung/ -übertragung* Zur Signatur von digitalen Nachweisen müssen Schlüsselpaare (bestehend aus Public Key und Private Key) erzeugt werden. • Der Public Key muss verfügbar gemacht werden, sodass eine CA ein entsprechendes Zertifikat ausstellen und den Key somit legitimieren kann. • Der Private Key muss der Teilkomponente Nachweissignatur verfügbar gemacht werden, damit sie mit ihm Nachweise digital signieren kann. • Es soll die Möglichkeit geboten werden, Schlüsselpaare zentral (lokale Signatur) zu erstellen. *Nachweiszustellung* Nachdem Nachweise ausgestellt und signiert wurden, müssen sie auf sicherem Weg dem Antragsteller/der Antragstellerin zugänglich gemacht werden. Dies kann auf unterschiedlichen Wegen erfolgen. An die Nachweiszustellung stellen wir folgende Anforderungen: • *Fachliche:*

	- Nachweise sollen den Nachweisinhaber*innen/Anstragsteller:innen auf sicherem Weg zugestellt werden. - Nachweise sollen in ein Servicekonto zugestellt werden können. - Nachweise sollen in der Komponente Ablage verfügbar sein. *Technische:* - Bildungsnachweise müssen per API an die Ablage angebunden sein. *Überprüfungskomponente* Nachweisempfänger:innen müssen in der Lage sein, einen erhaltenen Nachweis auf Echtheit und Gültigkeit zu prüfen. Hierfür nimmt eine öffentlich erreichbare Überprüfungskomponente Nachweise entgegen und gibt der/dem Überprüfenden Auskunft, ob der Nachweis selbst und das zur Unterzeichnung des Nachweises verwendete Zertifikat gültig sind. Als Echtheit definieren wir, dass es sich um einen legitimen Nachweis handelt, der von einer autorisierten und authentisierten Bildungseinrichtung ausgestellt wurde, welche zur Ausstellung dieser Nachweisart berechtigt ist. Als Gültigkeit definieren wir, dass die digitale Unterschrift, die für den Nachweis verwendet wurde, durch ein valides, nicht zurückgezogenes Zertifikat abgesichert ist und dass der Nachweis selbst nicht widerrufen wurde. An die Überprüfungskomponente stellen wir folgende Anforderungen: *Fachliche:* - Nutzer:innen sollen über eine Webanwendung in der Lage sein, Nachweise zur Überprüfung hochzuladen. - Die Webanwendung soll die Echtheit und Gültigkeit des Nachweises prüfen und dem/der Nutzer*in das Ergebnis der Prüfung anzeigen. - Nutzer:innen sollen die Möglichkeit erhalten, Massendaten zur Überprüfung zu senden *Technische:* - Bildungsinstitutionsverzeichnis, Certificate Authority und Nachweisrevokationsservice sollen per API angebunden sein. - Hochgeladene Nachweise sollen nicht persisitert werden. - Es soll die Signatur der kombinierten Form (Präsentation+ strukturierte Daten) für die Überprüfung herangezogen werden
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

Datenraum

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 könnten 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)	Das Schaufenster der NBP fungiert als eine Art Leitstelle, die Nutzer:innen auf Basis eines individuellen Such-, Kompetenz- und Bedürfnisprofils den Zugang zu angeschlossenen Service-Providern ermöglicht. Die nahtlose Nutzung erfolgt durch den Anschluss dieser Service Provider an die NBP AAI. Dabei ist dies kein exklusiver Zugang, sondern eine mögliche Nutzung der darunterliegenden Daten- und Serviceschicht. Ein Dashboard dient als User Interface zur Darstellung der Schaufenster-Funktionalitäten. Die ersten Schritte der User Journey sind die Bereitstellung einer Suchfunktion als Ausgangspunkt der Interaktion sowie die Registrierung als Übergangspunkt von anonymen zu registrierten Nutzer:innen. Mithilfe der Registrierung können beispielsweise Suchanfragen gespeichert und personalisiert werden sowie 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 und entsprechend des individuellen Kompetenz- und Bedürfnisprofils Empfehlungen zu passenden Bildungsangeboten geben. Weitere Funktionen, die über das Schaufenster für registrierte Nutzer:innen zur Verfügung stehen, sind Kollaborationstools sowie ein Service-/Analysebereich zur Auswertung von Nutzendendaten und Wartung bzw. Optimierung des laufenden Plattformbetriebs. 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	Die Umsetzung der Funktionalitäten und Komponenten des Schaufensters erfolgt nutzendenzentriert, wobei ein besonderer Schwerpunkt auf der formativen Evaluation von Teilergebnissen mit Nutzenden liegen wird. Folgende Funktionen und Services sollen von Beginn an im Schaufenster der NBP verfügbar sein: *Suchfunktion* samt dazugehöriger Features, die sowohl für anonyme als auch für registrierte Nutzende den Einstiegspunkt der User Journey darstellt • *Anonyme und registrierte Nutzende*: Suchabfragen mit Überblicks-Dashboard bzw. Trefferliste, Filterfunktionen, Definition von Suchkriterien, Login- / Registrierungs-Bereich • *Angemeldete Nutzende:* Speicherung von Suchabfragen, kompetenzbasierter Matching-Algorithmus, Suchhistorie / Vergleich von Suchabfragen, Notizen-Funktion für Priorisierungen oder zusätzliche Erläuterungen

	Gestaltung des *User Interface* für mobile Endgeräte und Desktop-Systeme mit *Registrierungsvorgang* • *User Interface für anonyme und registrierte Nutzende*: Info-Bereich mit allgemeiner Einführung und Infografiken bzw. inhaltlichen Kategorien, FAQ, News/Aktuelles/Ankündigungen, Service-Bereich, Impressum, Navigationskonzept der Website • *User Interface für registrierte Nutzende*: Bildungsreise-Dashboard mit Suchhistorie, Skillset-Darstellung und Schnittstellenanbindung, Registrierungsvorgang und Anmeldung Komponenten/Funktionalitäten zur *Optimierung* der *User Experience* für registrierte Nutzende • *Lernpfadfinder / Buddy Finder* als Teil der Suchfunktion und auf Basis des Matching-Algorithmus (z.B. basierend auf Skills, Interessen, Zielen) und unter Berücksichtigung der Lernstände sowie Lernfortschritte. Die Entscheidung über nächste passende Schritte der persönlichen Bildungsreise soll unterstützt werden. • *Kollaborationswerkzeuge* als Service-Provider-unabhängige Funktion mit dem Ziel des Zusammenfindens und Austauschs, auch über Bildungsinstitutionen oder Bildungsebenen hinweg. • *Service-Bereich / Analysefunktionen* (Authoring) – Tracking und Auswertung von User Daten bzw. User Statistiken, Support- und Service-Bereich (z.B. Ticket-System, Kontaktformular) 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	Bisher keine.
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. Darüber hinaus wird das Informationsportal mithilfe des GSB realisiert.
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.