



Bundesministerium
für Bildung
und Forschung

VDI|VDE|IT

Capgemini 

INFRASTRUKTURKOMPONENTEN UND BESCHAFFUNGSPROZESS IM DIGITALEN BILDUNGSRAUM

Vernetzungsinfrastruktur Digitale Bildung

Themenfeldkonferenz Bildung

14. September 2022



AGENDA

01 Begrüßung durch die Projektgruppe

02 Infrastrukturkomponenten

03 Beschaffungsprozess

04 Fragen



DIE VERNETZUNGSINFRASTRUKTUR DIGITALE BILDUNG



Die **Vernetzungsinfrastruktur Digitale Bildung** (ehem. Nationale Bildungsplattform) ist von der Konzeptualisierungsphase in die **Umsetzungsphase** übergegangen und soll durch **verschiedene Infrastrukturkomponenten als Anbieter und Betreiber** für Akteure des Digitalen Bildungsraums bereitstellen



Zum aktuellen Zeitpunkt wurden diese **Infrastrukturkomponenten des Digitalen Bildungsraums** definiert und werden momentan mithilfe des **dynamischen Beschaffungssystems für eine Beauftragung und Umsetzung vorbereitet**



Im heutigen Vortrag geben **Peter Hassenbach (BMBF), Cornelius Buchmann (Capgemini) und Maximilian Matting (PD)** einen Einblick in den aktuellen Stand **der fünf Infrastrukturkomponenten** sowie in den **Ablauf und die Durchführung des dynamischen Beschaffungssystems** zur Umsetzung der Komponenten



Peter Hassenbach (BMBF) – peter.hassenbach@bmbf.bund.de
Cornelius Buchmann (Capgemini) - cornelius.buchmann@capgemini.com
Maximilian Matting (PD) - maximilian.matting@pd-g.de



AGENDA

01 Begrüßung durch die Projektgruppe

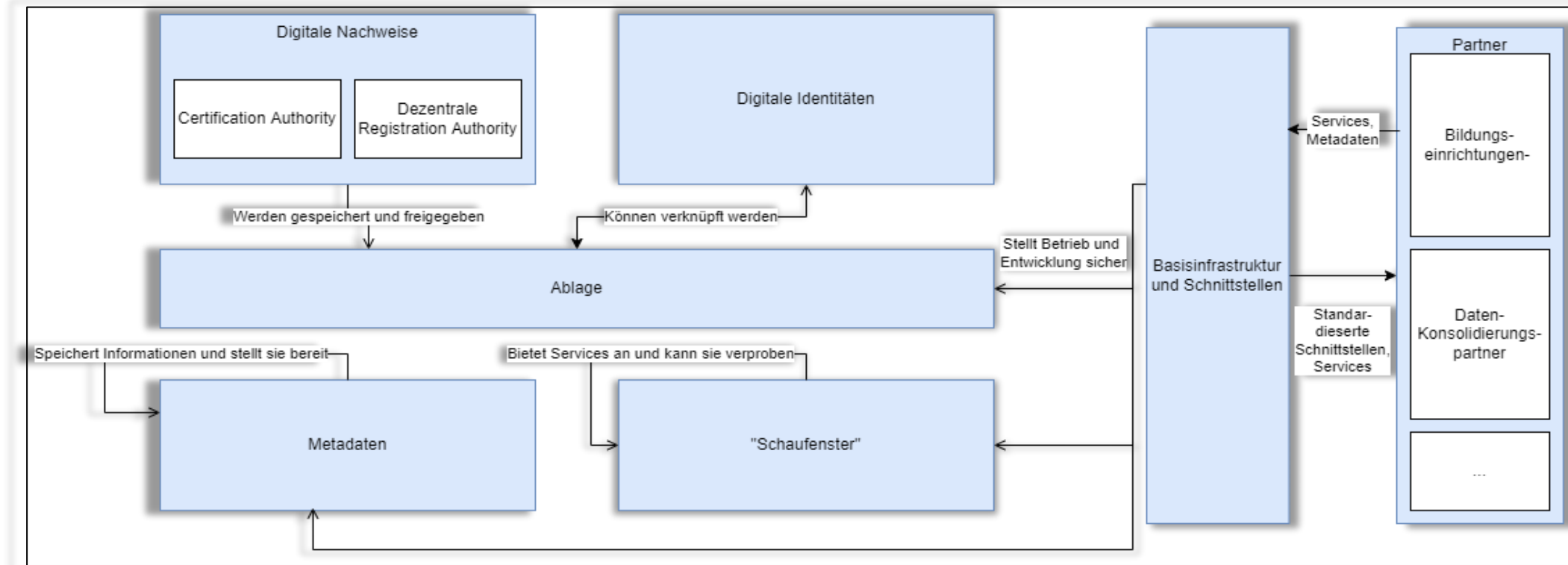
02 Infrastrukturkomponenten

03 Beschaffungsprozess

04 Fragen



ÜBERSICHT ÜBER INFRASTRUKTURKOMPONENTEN



Die Bereiche Identitätsmanagement (**Digitale Identitäten**), persönlicher Datenspeicher (**Ablage**), Bildungsmetadatenmanagement (**Datenraum**) und Certificate-Infrastruktur (**Digitale Nachweise**) bilden in Verbindung mit einem konfigurierbaren Schaufenster (**Schaufenster**) und programmierbaren Basisinfrastrukturrahmen (**Basisarchitektur**) den Architekturkern für die Vernetzungsinfrastruktur für digitale Bildung.

DIGITALE IDENTITÄTEN

Mit der digitalen Identität eines/-r Nutzer:in kann der/die Nutzer:in durch einmalige Authentifikation (nachfolgend als Single Sign-On oder SSO bezeichnet) an einem Browser prinzipiell alle an der Vernetzungsinfrastruktur Digitale Bildung angeschlossenen Service Provider (SP) während der jeweiligen Nutzungsperiode nutzen.

Kurzbeschreibung und Relevanz

- Die Vernetzungsinfrastruktur Digitale Bildung bildet eine "**Authentication and Authorization Infrastructure**" (AAI). Die Prüfung des Zugangs erfolgt durch dezentrale Identitätsanbieter (IdP) der jeweiligen Service Provider im Rahmen einer Föderation
- Die Freigabe zur Nutzung einzelner Angebote der jeweiligen Service Provider hängt von der **Qualität der einzelnen digitalen Identität** ab
- Metadaten der jeweiligen Nutzer:innen werden durch die Service Provider signiert und als sogenannte "**verifiable claims**" (**überprüfbare Behauptungen**) zur Verfügung gestellt

Basisanforderungen

- **IDM:** Management der Basisidentität der Vernetzungsinfrastruktur
 - Einrichten der Basisidentität über Self-Service Funktion
 - Ermöglichen der Nutzung der eID Funktion des neuen Personalausweise (nPA) über Nutzerkonto-Bund-Bridge (Siehe Digitale Nachweise)
 - Verzeichnis
 - Managementfunktionen
- **Identitätsanbieter:** Sicherstellen der Authentifikation der Basisidentität der Vernetzungsinfrastruktur
- **ID-Proxy:** Sicherstellen SSO Funktionalität über dezentrale Authentifikation der digitalen Identität im Rahmen der Föderation
- **Ablage:** siehe Ablage
- **CA:** Siehe Digitale Nachweise

Berührungspunkte und Abgrenzung

- Nutzendenindizierte Verknüpfung zu **OZG-Diensten** (z.B. Bafög), die über das Nutzerkonto angeschlossen werden

ABLAGE

Nutzende können in ihrer Ablage Dokumente souverän ablegen und freigeben. Diese sind agnostisch in Bezug auf das Datenformat. Es können sowohl kleinteilige Lernstände (Microcredentials) als auch verifizierbare Nachweise, wie das Abiturzeugnis oder komplexere Dokumente wie Bachelorarbeiten abgelegt werden.

Kurzbeschreibung und Relevanz

- Der/die Nutzer:in bestimmt, welche Partei zu welchem Zeitpunkt an die jeweiligen Daten kommt
- Der **Backbone/ Broker** sorgt dafür, dass die Datenkommunikation nur dann stattfindet, wenn dies auch wirklich von allen Parteien autorisiert wurde
- Die Anbindung an mögliche Backendsysteme soll über eine **Komponente (Connector)** erfolgen, **die eine API anbietet**, welche wiederum eine einfache Nutzung der Funktionalität und Anbindung ermöglicht
- Da der Connector in der **Sphäre des Service Providers (hier die Vernetzungsinfrastruktur)** betrieben wird, ist somit auch eine **echte Ende-zu-Ende Verschlüsselung** möglich

Basisanforderungen

- **Ablage App:**
 - Abwicklung Kommunikation mit Backbone/ Broker: Erzeugen von Ende zu Ende verschlüsselter Kommunikation.
 - Die Architektur der Ablage ist so ausgelegt, dass es keine Möglichkeit eines Rückschlusses von der Ablage auf das Device des/der Nutzer(s):in und damit auf den/die Nutzer:in herbeigeführt werden kann
 - Unterstützung von DSGVO-Funktionen für Nutzer:innen und Service Provider (Auskunftsrecht, Recht auf Vergessenwerden)
- **Backbone/ Broker:**
 - Schaffen einer Beziehung zwischen Ablage und Connector
 - Schaffen einer Beziehung zwischen Ablage und Ablage
- **Connector:**
 - Abwicklung Kommunikation mit Backbone/ Broker: Erzeugen Ende-zu-Ende verschlüsselter Kommunikation
 - Bereitstellen einer API für die Anbindung von Backendsystemen

Berührungspunkte und Abgrenzung

- Die Ablage basiert auf bestehenden Arbeiten in den Bereichen **Verschlüsselung, dezentrale Identitäten und Open Wallet** Spezifikationen
- Es werden keine Distributed-Ledger-Technologien verwendet
- Berücksichtigung von der **Entwicklung von Data Wallets allgemein / Open Wallet Standards**
- Projekte aus Schaufenster Sichere Digitale Identitäten (BMWK) u.a.
- **OZG** Kontext

DATENRAUM

Im Datenraum werden Daten (z.B. Informationen über Studiengänge, Bildungseinheiten, Curricula) geordnet in abgestimmten Formaten abgelegt und über möglichst standardisierte Formate maschinenlesbar zur Verfügung gestellt. Dies ermöglicht Funktionalitäten wie die durch mächtige Filterfunktionen ergänzte Suche nach Lerninhalten oder Bildungseinrichtungen.

Kurzbeschreibung und Relevanz

- Metadaten Speicher dienen zur **Speicherung von nicht personenspezifischen und nicht transaktionsspezifischen Daten** wie Moduldaten aus Studiengängen, Studiengänge, Weiterbildungen und Abschlüsse oder Curricula
- Sie bilden die Grundlage für einen Datenraum Bildung. Vorzugsweise soll auf **existierende Standards** zurückgegriffen werden
- Lerninhalte selbst sind nicht Teil der hier zu betrachtenden Informationen
- Durch **Metadaten** können verschiedenste föderierte Dienste (z.B. mit **nutzendenzustimmung-personalisierter Suchfunktionen**, „Lernpfadfinder“, Buddy-Finder – ggf. auch in Kombination) angeboten werden und weitere Innovationen entstehen

Basisanforderungen

- **Metadaten** werden in die Vernetzungsinfrastruktur eingespeist, verarbeitet und vorgehalten, um in **Verbindung** mit anderen Werkzeugen wie der **Ablage** leistungsfähige, **gezielte Suchen** (beispielsweise nach Lerninhalten oder Bildungseinrichtungen) zu ermöglichen, Lernooptionen aufzuzeigen und Zugänge zu schaffen
- Die Metadaten werden möglichst **von den Anbietern von Bildungsangeboten selbst zur Verfügung gestellt und gepflegt**
- Die Vernetzungsinfrastruktur stellt diesen als **Service Assistenzsysteme und Redaktionstools zur Verfügung**, um Metadaten automatisiert vorzubefüllen, **Qualitätssicherung durch die Urheber zu ermöglichen** und die Daten in geeigneten Formaten wegzuschreiben. Wo immer möglich, wird angeboten, die Prozesse teilweise oder ganz zu automatisieren.
- Wo nachgefragt, werden hierzu mit Zustimmung der Urheber Konsolidierungspartner eingesetzt

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)
 -

DIGITALE NACHWEISE

Die Vernetzungsinfrastruktur Digitale Bildung 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, perspektivisch förderierbaren *Certification Authority* (CA) für die Domäne Bildung.

Kurzbeschreibung und Relevanz

- **Digitale Nachweise** finden sich in der Domäne **Bildung an vielen Stellen**
- Die **Vernetzungsinfrastruktur Digitale Bildung** 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 dargestellt werden

Basisanforderungen

- **Certificate Authority (CA)**
 - Etablierung einer Root CA
 - Herausgebende CA für Public Keys, ggf. Typ der Bildungseinrichtung
 - Certificate Revocation List für „verifiable claims“
 - Nutzerkonto BUND-Bridge
- **Registration Authority (RA)**
 - Software Artefakte für die Umsetzung einer RA
 - Nutzerkonto BUND-Bridge
- **Bildungseinrichtungsregister**
 - Zentrales Register der Institutionen zur Nachweisausstellung
- **Signatur Modul**
 - Generieren von Schlüsseln
 - Signieren von Dokumenten und/ oder verifiable claims
 - Verwalten und Zurückziehen von Signaturen

Berührungspunkte und Abgrenzung

- **Relevante Projekte:**
 - Europass
 - OZG Bildungsjourney
 - DiBiHo
 - OpenBadges, inkl V3
 - SSI Projekte
 - EU Toolbox inkl Use Case Diplom
 - Xbildung
- **Unterschied zur DFN-PKI:**
 - In der Vernetzungsinfrastruktur Digitale Bildung würden alle Beteiligten eine zentrale CA nutzen, wodurch keine n-stufigen Zertifikatsketten entstehen

SCHAUFENSTER

Die Vernetzungsinfrastruktur nutzt wie das CMS des Bundes die Plattform Liferay (oder gleichwertig), um als Schaufenster Lebens-lagen, Zugang zur Suche und andere Funktionalitäten abzubilden und für Nutzungen Open Source zugänglich zu machen. Zusätzliche Funktionalitäten können so beispielhaft umgesetzt, gezeigt und mit Nutzendenfeedback versehen werden und später final implementiert werden.

Kurzbeschreibung und Relevanz

- Das Schaufenster verfügt über einen direkten von dem/der Nutzer:in freigegebenen **Zugang zur persönlichen Ablage** des/der Nutzer(s):in
- Ein **Lebenslagenmanager** kann mit diesen Informationen, den/die Nutzer:in kontextbezogen zu angeschlossenen Angeboten der Service Provider leiten sowie dem/der Nutzer:in je nach Lebenslage Tipps geben und weitere Schritte aufzeigen

Basisanforderungen

- Das Schaufenster soll die Möglichkeit bieten, unterschiedlichste Funktionen und Services so miteinander zu verbinden, dass für den/die Nutzer:in ein **nahtloser Gebrauch des Schaufensters entsteht** und damit ein durchgängig adressierbares, über die Vernetzungsinfrastruktur erreichbares Nutzungsspektrum.
- 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

Berührungspunkte und Abgrenzung

- Wird auf Basis der **Basisinfrastruktur** betrieben und im wesentlichen zu Anschauungszwecken zur Verfügung gestellt
- Nutzt weitere Komponenten wie die **Vernetzungsinfrastruktur AAI, Ablage, Metadaten** und weitere technische Komponenten, die, solange sie Open Source sind, weiter verwendet werden können



AGENDA

01 Begrüßung durch die Projektgruppe

02 Infrastrukturkomponenten

03 Beschaffungsprozess

04 Fragen



BESCHAFFUNGSPROZESS: DYNAMISCHES BESCHAFFUNGSSYSTEM (DBS)

Für den Aufbau der Vernetzungsinfrastruktur Digitale Bildung wurde ein Dynamisches Beschaffungssystem (DBS) eingerichtet. Ein Dynamisches Beschaffungssystem ist ein zeitlich befristetes, ausschließlich elektronisches Verfahren zur Beschaffung marktüblicher Leistungen, bei denen die allgemein auf dem Markt verfügbaren Merkmale den Anforderungen des öffentlichen Auftraggebers genügen

Teilnahmephase (Stufe 1)

- Unternehmen werden nach zuvor festgelegten Eignungskriterien zunächst zur Abgabe einer Bewerbung für einen Lieferantenpool aufgefordert
- Die Anzahl der teilnahmeberechtigten Unternehmen am DBS ist nicht begrenzt
- Das DBS steht allen interessierten Unternehmen, welche die Eignungskriterien erfüllen, während der gesamten Laufzeit des Systems offen
- So können auch nach der initialen Bewerbungsphase jederzeit weitere interessierte Unternehmen in den Bieterpool des DBS aufgenommen werden. Ebenso können sich zunächst abgelehnte Interessenten bei Änderung und Verbesserung der Eignungskriterien erneut bewerben

Angebotsphase (Stufe 2)

- Entsteht auf Seiten des Auftraggebers ein konkreter Beschaffungsbedarf, wird die gesuchte Leistung per Einzelvergabe durch Aufforderung zur Angebotsabgabe in sogenannten Einzelabrufen/Miniwettbewerben jeweils bei allen zum betreffenden Zeitpunkt für den Bieterpool qualifizierten Unternehmen angefragt
- Nach Abgabe der Angebote wird das wirtschaftlichste Angebot schließlich anhand zuvor definierter Zuschlagskriterien ermittelt und der Zuschlag erteilt
- Die Angebotsphase wird wiederholt, sobald neue Bedarfe während der Laufzeit des DBS auf Seiten des Auftraggebers entstehen

Da das Verfahren für potenzielle Teilnehmende während der gesamten Laufzeit frei zugänglich ist, bietet ein DBS das größtmögliche Spektrum an potenziellen Auftragnehmern, darunter KMU. Das erhöht die Flexibilität sowie die Modularität, Anknüpfung und Vernetzbarkeit der Nationalen Bildungsplattform an bestehende Lösungen.

EIN LEITFADEN ALS INSTRUMENT ZUR PRÜFUNG DER PASSFÄHIGKEIT EINES DBS FÜR GEPLANTE AUSSCHREIBUNGEN WURDE ENTWICKELT

✔ Erfüllt ✘ Nicht erfüllt ? Unklar / n.a.
⚡ KO-Kriterium




Dimension	Kriterium	Einschätzung
Marktüblichkeit der Leistung	⚡ Auftraggeber-Anforderungen durch auf dem Markt verfügbare Leistungen erfüllbar	
	⚡ Keine konzeptionellen oder kreativ-schöpferischen Lösungen enthalten	
Häufigkeit des Bedarfs	⚡ Wiederkehrender Bedarf an der Leistung gegeben	
	Unterschiedliche Lieferanten fachlich und technisch akzeptabel Keine Pfadabhängigkeiten bestimmter Anbieter zu erwarten	
Leistungsgegenstand	⚡ Darstellbarkeit aller Leistungen zum Zeitpunkt der Auftragsbekanntmachung gegeben	
	Aufwand eines DBS durch Ausschreibungsvolumen gerechtfertigt	

Dimension	Kriterium	Einschätzung
Marktsicht	Hohes Innovationspotenzial und Veränderungstempo im Markt vorhanden	
	Ausreichende Teilnehmerzahl und Akzeptanz durch den Markt gegeben	
Auftraggeber-Aufwand	⚡ Fortlaufende Eignungsprüfungen innerhalb der Frist zu bewältigen	
	Bewertungszeit für Angebote innerhalb der Frist zu bewältigen	
	Vergabedokumentation der Einzelbeauftragungen zu bewältigen	
DL-Steuerung	Kaufmännisches Controlling der zu erbringenden Leistungen etabliert	
	Fachliche Steuerung und Qualitätssicherung vorbereitet	
	Onboarding / Offboarding der Auftragnehmer gewährleistet	

Zielstellung des DBS-Leitfadens

1. Analyse der DBS-Passfähigkeit zur Leistung
2. Bereitstellung einer einheitlichen Entscheidungshilfe
3. Erhöhung der Transparenz in der Verfahrenswahl

Aufbau des DBS-Leitfadens

-  Abbildung in 6 Dimensionen und 15 Kriterien mit Blick auf Markt, Auftraggeber und Leistungsgegenstand
-  5 KO-Kriterien von besonderer Bedeutung für die Passfähigkeit
-  Identifizierung von Handlungsbedarfen zur weiteren Prüfung und ggfs. Nachschärfung des DBS-Ansatzes



AGENDA

01 Begrüßung durch die Projektgruppe

02 Infrastrukturkomponenten

03 Beschaffungsprozess

04 Fragen





Bundesministerium
für Bildung
und Forschung

VDI|VDE|IT

Capgemini 

**VIELEN DANK FÜR DIE
AUFMERKSAMKEIT!
ZEIT FÜR IHRE FRAGEN!**