1.DSGVO und Datenschutz

Vorwort

Der vorliegende Bericht ist Teil des Pakets DSGVO UND DATENSCHUTZ des Projekts Synapse . Er befasst sich mit der Problematik des Zugangs zu digitalen Bildungsressourcen bei gleichzeitiger Gewährleistung der Einhaltung der rechtlichen Anforderungen in Bezug auf den Schutz personenbezogener Daten und die Verwaltung von Urheberrechten. Ziel ist es, die mit dem Projekt verbundenen rechtlichen und technischen Risiken zu identifizieren und spezifische Empfehlungen zur Absicherung zukünftiger Phasen zu formulieren.

Der erste Teil des Berichts ist dem Umgang mit personenbezogenen Daten gewidmet. Er analysiert den anwendbaren Rechtsrahmen, wobei die Verpflichtungen der DSGVO und die Besonderheiten des Bundesdatenschutzgesetzes (BDSG) hervorgehoben werden. Die Untersuchung der Datenströme ermöglicht es, die zwischen den Plattformen ausgetauschten Informationen zu identifizieren, insbesondere die Identifikations-, Bildungs- und Verhaltensdaten der Nutzer. Die Rollen und Verantwortlichkeiten der beteiligten Akteure werden geklärt, wobei zwischen für die Verarbeitung Verantwortlichen, Mitverantwortlichen und Auftragsverarbeitern unterschieden wird. Es werden spezifische Empfehlungen zur Sicherung dieser Verarbeitungen ausgesprochen, darunter die Einrichtung von Verträgen über Unterauftragnehmer und Mitverantwortung, die Verschlüsselung der Datenströme, die Minimierung der gesammelten Informationen sowie die Durchführung einer Datenschutz-Folgenabschätzung (DSFA). Besondere Aufmerksamkeit wird minderjährigen Nutzern gewidmet, indem für bestimmte Verarbeitungen eine doppelte Zustimmung (Schüler und Eltern) vorgeschrieben wird.

Der zweite Teil des Berichts befasst sich mit der Nutzung von digitalem Content. Er untersucht den rechtlichen Status von urheberrechtlich geschützten Bildungsinhalten und die Bedingungen, unter denen sie von den Verlegern zur Verfügung gestellt werden. Die durch den Digital Services Act (DSA) und die DAMUN-Richtlinie vorgeschriebene Regulierung wird ebenfalls behandelt, wobei die Verantwortung der Plattformen für die Moderation von Inhalten und die Verhinderung von Urheberrechtsverletzungen hervorgehoben wird. Zu den

ermittelten Risiken gehören unter anderem der unerlaubte Zugriff auf lizenzierte Inhalte, grenzüberschreitende Streitigkeiten über Verbreitungsrechte und die Nichteinhaltung der Nutzungsbedingungen durch die Endnutzer. Um diesen Problemen zu begegnen, empfiehlt der Bericht die Formalisierung von Lizenzverträgen mit den Verlagen, die Integration von Systemen zur Verwaltung digitaler Rechte (DRM), die Rückverfolgbarkeit der Nutzung über die Blockchain sowie die Sensibilisierung der Nutzer für die Regeln des geistigen Eigentums. Schließlich werden regelmäßige Audits empfohlen, um die Einhaltung der Vorschriften zu gewährleisten und die Transparenz bei der Nutzung digitaler Ressourcen sicherzustellen.

Anhand dieser Analysen und Empfehlungen legt dieser Bericht die Grundlagen für einen sicheren und rechtlich robusten Rahmen für die Entwicklung des Projekts, der pädagogische Innovation und die Einhaltung der rechtlichen Verpflichtungen miteinander verbindet.

Einleitung

In einem Kontext, in dem der Schutz personenbezogener Daten und die Verwaltung von Urheberrechten immer wichtiger werden, muss das Projekt der Interaktion zwischen den Plattformen von Synapse und Mein Bildungsraum in einen strengen rechtlichen Rahmen eingebettet sein. Diese Zusammenarbeit, die den Zugang zu digitalen Bildungsressourcen erleichtern soll, wirft große Herausforderungen in Bezug auf die Einhaltung gesetzlicher Vorschriften, die Sicherheit des Austauschs und die Wahrung der Rechte der Nutzer auf.

Ziel dieses Berichts ist es, die Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten und der Nutzung von digitalem Content zu ermitteln, um spezifische Empfehlungen vorzuschlagen, die eine optimale Einhaltung der Allgemeinen Datenschutzverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG) sowie der geltenden Regelungen zum Urheberrecht gewährleisten.

Die Studie beleuchtet die Pflichten der verschiedenen beteiligten Akteure, die Abbildung des Datenflusses zwischen den Systemen und die einzurichtenden Governance-Mechanismen. Sie enthält konkrete Empfehlungen zur vertraglichen Regelung der Beziehungen zwischen den Parteien, zur Umsetzung technischer und organisatorischer Schutzmaßnahmen sowie zur Sensibilisierung der Nutzer und zur Prüfung der Praktiken.

Das Ziel dieses Dokuments besteht also darin, einen robusten und sicheren Rahmen für die künftigen Projektphasen zu schaffen, der ein Gleichgewicht zwischen pädagogischer Innovation und der Einhaltung der gesetzlichen Anforderungen gewährleistet.

Teil I: Der Umgang mit personenbezogenen Daten

Geltender Rechtsrahmen

Analyse der allgemeinen Verpflichtungen der DSGVO[1]

Die DSGVO verlangt von Einrichtungen, die personenbezogene Daten verarbeiten, einen proaktiven und verantwortungsbewussten Ansatz, der eine Anpassung der internen Praktiken und Prozesse erfordert. Die Grundprinzipien (a), die durch die operativen Pflichten (b) ergänzt werden, sind die wesentlichen Elemente, an denen sich die Rechtsträger ausrichten müssen, um konform zu sein.

a. Die Grundprinzipien

In Artikel 5.1 der DSGVO sind die Grundsätze für die Verarbeitung personenbezogener Daten aufgeführt. Wir können diese Grundsätze in vier Prinzipien zusammenfassen: Rechtmäßigkeit, Loyalität und Transparenz (i), Zweckbindung und Datenminimierung (ii) begrenzte Aufbewahrung und Sicherheit (iii) und das Prinzip der Rechenschaftspflicht (iv).

i. Rechtmäßigkeit, Loyalität und Transparenz[2]

Die Stellen, die personenbezogene Daten verarbeiten, müssen dies auf rechtmäßige, redliche und transparente Weise tun. Dies beinhaltet:

- Eine gültige Rechtsgrundlage für die Verarbeitung (z. B. Einwilligung, Vertrag)[3] ;
- Die Verwendung der Daten nur für die ursprünglich vorgesehenen Zwecke und die damit vereinbaren späteren Zwecke[4] ;
- Eine klare Information der betroffenen Personen über die Verwendung ihrer Daten[5] ;

Die Grundsätze der Fairness und Transparenz gehen Hand in Hand mit einer der wesentlichen Herausforderungen der DSGVO, nämlich der Bekräftigung einer größeren

[1] Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ist der europäische Rechtsrahmen für die Verarbeitung personenbezogener Daten in der gesamten Europäischen Union. Da es sich um eine Verordnung handelt, gilt sie unmittelbar und direkt, wird jedoch in einigen Ländern durch nationale Gesetze wie das Bundesdatenschutzgesetz ergänzt, das aus dem Jahr 1977 stammt und 2017 aktualisiert wurde, um es an die DSGVO anzupassen.

[2] Verordnung (EU) 2016/679 des Parlaments und des Rates, Artikel 5.1, a).

[3] *Ebenda,* Artikel 6 Absatz 1

[4] *Ebenda,* Erwägungsgrund 50

[5] *Ibid.,* Artikel 12.1

Kontrolle des Einzelnen über den Verbleib seiner personenbezogenen Daten[6] . Abgesehen von Ausnahmefällen, die insbesondere im Zusammenhang mit Sicherheitsdateien stehen, dürfen personenbezogene Daten nicht ohne das Wissen der Person gesammelt werden. Die Person muss über alle Merkmale der Verwendung ihrer Daten informiert werden, und zwar nicht nur zum Zeitpunkt der Erhebung, sondern auch danach, insbesondere bei aufeinanderfolgenden Verarbeitungen.

ii. Zweckbindung und Datenminimierung[7]

Personenbezogene Daten müssen für festgelegte, eindeutige und rechtmäßige Zwecke verarbeitet werden. Der Zweck entspricht dem "Ziel, das der für die Verarbeitung Verantwortliche im Rahmen des Einsatzes eines Werkzeugs oder einer Software verfolgt.[8] ". Die Bestimmung des Zwecks muss dann der Erhebung vorausgehen, um auf diese Weise die für die Verarbeitung relevanten Daten zu identifizieren.

Nur die Daten, die als angemessen und relevant für die Erreichung der Zwecke der Verarbeitung identifiziert wurden, sind zu erheben. Die Erhebung von Daten für jeden beliebigen Zweck ist nicht zulässig.

Neben der Relevanz müssen die Daten sachlich richtig sein und auf dem neuesten Stand gehalten werden[9] , um Daten zu löschen, die im Hinblick auf die Zwecke, für die sie verarbeitet werden, unrichtig oder irrelevant sind.

iii. Begrenzte Aufbewahrung und Sicherheit[10]

Der für die Verarbeitung Verantwortliche muss sicherstellen, dass technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit getroffen werden, und eine Dauer festlegen, für die die Daten in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Diese Dauer darf nicht länger sein, als es für die Erreichung der Zwecke der Verarbeitung erforderlich ist.

Die Sicherheitsmaßnahmen müssen einen Schutz vor unbefugter Verarbeitung und unbefugtem Zugriff, Datenlecks, versehentlicher Zerstörung oder Veränderung von Daten gewährleisten.

---

[6] Lessi J. et a., *Code de la protection des données personnelles 2025, annoté et commenté*, 2024, 7ième éd., Dalloz, Codes Dalloz Professionnels, S. 66.

[7] *Ebenda,* Artikel 5.1, b) und c).

[8] Banck A., *RGPD: la protection des données à caractère personnel*, 2023, 5ième ed., Gualino, Droit en poche, S. 15.

[9] Verordnung (EU), *a. a. O.*, Artikel 5.1 Buchstabe d.)

[10] *A.a.O.,* Artikel 5.1, e) und f)

iv. Der Grundsatz der Rechenschaftspflicht[11]

Es liegt in der Verantwortung des für die Verarbeitung Verantwortlichen, die Verpflichtungen der DSGVO einzuhalten und in der Lage zu sein, nachzuweisen, dass diese eingehalten werden[12] und dass die Maßnahmen, die zur Einhaltung dieser Verpflichtungen ergriffen wurden, wirksam sind .[13]

Um die Einhaltung nachzuweisen, muss der für die Verarbeitung Verantwortliche die eingeführten Richtlinien und Verfahren dokumentieren, seine Dokumentation auf dem neuesten Stand halten und bereit sein, sie im Falle einer Kontrolle vorzulegen.

b. Die operativen Verpflichtungen

Zusätzlich zu den Grundprinzipien sieht die DSGVO weitere Pflichten vor, die es Unternehmen und Verwaltungen, die personenbezogene Daten verarbeiten, ermöglichen, dem Grundsatz der Rechenschaftspflicht nachzukommen. Diese Pflichten äußern sich insbesondere in der Führung eines Verzeichnisses der Verarbeitungstätigkeiten (i), der Ernennung eines Datenschutzbeauftragten (ii), der Datenschutz-Folgenabschätzung (iii), der Meldung von Datenverletzungen (iv) und den Rechten der betroffenen Personen (v).

i. Das Register der Verarbeitungstätigkeiten

Das Register der Verarbeitungstätigkeiten wird in Artikel 30 erwähnt, und gemäß der EDSB-Leitlinie[14] über den DSB muss dieses Register alle Verarbeitungen der Organisation umfassen, damit sie und die Aufsichtsbehörde auf Anfrage einen Überblick über alle von ihr durchgeführten Tätigkeiten zur Verarbeitung personenbezogener Daten erhalten können .[15]

Das Register muss mindestens enthalten:

- Den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen und gegebenenfalls des gemeinsam für die Verarbeitung Verantwortlichen, des Vertreters und des Datenschutzbeauftragten ;
- Die Zwecke der Verarbeitung ;
- Die Kategorien der betroffenen Personen und der personenbezogenen Daten;
- Die Kategorien der Datenempfänger ;

[11] *Ebenda*, Artikel 24
[12] *Ibid.,* Artikel 5 Absatz 2
[13] *Ibid.*, Erwägungsgrund 74
[14] Europäischer Datenschutzausschuss, ehemals G29 (Artikel 29-Datenschutzgruppe) ist ein unabhängiges, eingebettetes Gremium der Europäischen Union, dessen Ziele die Gewährleistung einer einheitlichen Anwendung der DSGVO und die Förderung der Zusammenarbeit zwischen Datenschutzbehörden sind.
[15] Banck A., *a.a.O.*, S. 34.

- Datenübermittlungen außerhalb der Europäischen Union und die geeigneten Garantien, die zur Ermöglichung dieser Übermittlungen eingeführt wurden.

Es gibt eine Ausnahme für Unternehmen und Organisationen mit weniger als 250 Personen[16] , die nicht verpflichtet sind, das Tätigkeitsregister zu führen. Diese Ausnahme gilt nicht, wenn die durchgeführte Verarbeitung ein Risiko für die Rechte und Freiheiten von Personen mit sich bringt, wenn sie nicht nur gelegentlich erfolgt oder wenn sie besondere Kategorien von Daten oder Daten über Straftaten betrifft. Diese Bedingungen sind nicht kumulativ, sondern alternativ, wobei das Auftreten einer dieser Bedingungen ausreicht, um die Pflicht zur Führung eines Registers aufrechtzuerhalten.

ii. Die Ernennung eines Datenschutzbeauftragten

Laut G29 ist der Datenschutzbeauftragte (DSB) ein "zentraler Akteur, um die Einhaltung der Bestimmungen der DSGVO zu erleichtern.[17] ". Der DSB hat eine doppelte Funktion: Er berät und kontrolliert die Anwendung der DSGVO in einem besonders breiten Bereich, wofür er alle europäischen und nationalen Datenschutzbestimmungen, die auf seine Tätigkeit anwendbar sind, kennen muss.

Die Aufgaben des DSB, die in Artikel 39 aufgeführt sind, dürfen nicht gleichzeitig mit Aufgaben ausgeübt werden, die zur Festlegung der Zwecke und Mittel der Verarbeitung personenbezogener Daten führen. Der DSB wird auf der Grundlage seiner beruflichen Qualitäten, seiner Fachkenntnisse des Rechts und der einschlägigen Praktiken sowie seiner Fähigkeit, seine Aufgaben zu erfüllen, ernannt .[18]

iii. Die Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DIA)

Die DSFA ist ein Ansatz, der darauf abzielt, eine Datenverarbeitung aufzubauen, die der DSGVO entspricht und die Privatsphäre respektiert[19] . Sie bewertet die Risiken für die Rechte und Freiheiten der betroffenen Personen[20] und legt die erforderlichen Maßnahmen zur Abschwächung dieser Risiken fest[21] . Eine PIA ist obligatorisch, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten von Personen mit sich bringt.

---

[16] Verordnung (EU), *a. a. O.*, Artikel 30.5.
[17] Banck A., a.*a.O.*, S. 20
[18] Verordnung (EU), *op. cit.*, Artikel 37.5
[19] "The Data Protection Impact Assessment (DIA)" (Die Datenschutz-Folgenabschätzung) auf https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd
[20] "Datenschutz-Folgenabschätzung" auf https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/analyse-d-impact-relative-a-la-protection-des-donnees
[21] "GDPR/RGPD - Was ist die PIA?" auf https://www.asi.fr/blog/gdpr-rgpd-quest-ce-que-pia-privacy-impact-assessment

Die G29 hat neun Kriterien für die Bewertung des Risikos für die Rechte und Freiheiten von Personen festgelegt. Eine PIA ist obligatorisch, wenn die Verarbeitung mindestens zwei der neun Kriterien erfüllt.

iv. Die Meldung von Datenverletzungen

Die Meldung von Datenverletzungen ist ein Verfahren, das die Verantwortung der Stellen, die personenbezogene Daten verarbeiten, demonstriert und es ermöglicht, schnell Maßnahmen zum Schutz der Rechte der betroffenen Personen zu ergreifen.

Die Meldung an die zuständige Behörde muss so schnell wie möglich, spätestens jedoch 72 Stunden nach Kenntnisnahme der Verletzung erfolgen. Wenn nicht alle Informationen innerhalb der 72-Stunden-Frist verfügbar sind, kann eine Meldung in zwei Schritten erfolgen; eine erste Meldung innerhalb von 72 Stunden und eine weitere Meldung, sobald die fehlenden Informationen verfügbar sind .[22]

v. Die Rechte der betroffenen Personen

Alle Einrichtungen müssen sicherstellen, dass die betroffenen Personen ihre Rechte effektiv ausüben können, einschließlich :

- Recht auf Zugang
- Recht auf Berichtigung
- Recht auf Löschung (Recht auf Vergessenwerden)
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch
- Recht, nicht Gegenstand einer automatisierten Entscheidung zu sein.

Diese Rechte sind nicht absolut und können in bestimmten Situationen eingeschränkt werden, insbesondere aus rechtlichen Gründen, aus Gründen der öffentlichen Sicherheit, der Meinungsfreiheit oder des Interesses des Verantwortlichen, die Verarbeitung personenbezogener Daten vorzunehmen.

[22] " Wie reagiere ich auf eine Datenverletzung? Gebrauchsanweisung und Empfehlungen" auf https://www.village-justice.com/articles/comment-reagir-cas-violation-donnees-personnelles-mode-emploi-attention-des,48154.html

Die Besonderheiten des Bundesdatenschutzgesetzes (BDSG)

Das Bundesdatenschutzgesetz (BDSG) ist das Bundesgesetz über den Datenschutz, das die DSGVO im nationalen deutschen Rahmen ergänzt und präzisiert. Es gilt für Unternehmen mit Sitz in Deutschland, einschließlich ausländischer Niederlassungen. Außerdem verschärft es die Regeln in Schlüsselbereichen wie Beschäftigung, Gesundheit oder öffentliche Sicherheit mit Anforderungen, die die DSGVO ergänzen.

Die Besonderheiten im Vergleich zur DSGVO sind rechtlicher Natur (i) und stehen in Zusammenhang mit anderen Bundesgesetzen (ii).

i. Die rechtlichen Besonderheiten

Das BDSG verschärft und bringt zusätzliche Kriterien zu den Bestimmungen der DSGVO, insbesondere zu :

- Die Verarbeitung von Arbeitnehmerdaten, indem die Rechtsgrundlagen (vertragliche Notwendigkeit oder ausdrückliche Einwilligung) strikt eingeschränkt werden.[23]
- Die digitale Überwachung von Arbeitnehmern wird mit einer strengen Auslegung des Verhältnismäßigkeitsgrundsatzes restriktiver gehandhabt.[24]
- Die obligatorische Ernennung eines Datenschutzbeauftragten (DSB), sobald zwanzig Personen ganz oder teilweise an der automatisierten Verarbeitung beteiligt sind.[25]
- Eine systematische Meldung an die Aufsichtsbehörde bei Verstößen, die sensible Daten betreffen, selbst wenn kein hohes Risiko besteht.[26]
- Die Ausweitung der Pflicht zu einer PIDA auf Verarbeitungen, die nicht unter die DSGVO fallen, wie z. B. Datenübermittlungen in Drittländer ohne Angemessenheitsabkommen.

ii. Die Verknüpfung mit anderen Bundesgesetzen.

---

[23] "Germany: New draft bill for an "Employee Data Act" ("Beschäftigtendatengesetz"), auf https://insightplus.bakermckenzie.com/bm/data-technology/germany-new-draft-bill-for-an-employee-data-act-beschaftigtendatengesetz

[24] "Germany Draft for Employee Data Act issued", auf https://www.hoganlovells.com/en/publications/germany-draft-for-employee-data-act-issued

[25] "Germany's data privacy protection laws: Everything you need to know", auf https://www.didomi.io/blog/germany-data-privacy-protection-laws-everything-you-need-to-know.

[26] *Ibidem*

Das BDSG ist mit einer Reihe von sektoralen Gesetzen verknüpft und schafft so einen mehrdimensionalen Rechtsrahmen. Dieses Zusammenspiel erhöht die Anforderungen an die Einhaltung der Vorschriften, insbesondere für ausländische Unternehmen, die in Deutschland tätig sind. Die wichtigsten betroffenen Gesetze sind :

- TTDSG (Telekommunikation-Telemedien-Datenschutzgesetz) mit der Verpflichtung zu einem ausdrücklichen Opt-in vor der Hinterlegung von nicht wesentlichen Cookies.[27]
- Beschäftigtendatenschutzgesetz, ein Gesetzentwurf zur Schließung der Lücken in §26 BDSG, der vom EuGH als nicht DSGVO-konform eingestuft wurde und der die Rechte von Arbeitnehmern stärken soll, indem er den Einsatz digitaler Überwachungsinstrumente regelt.
- SchulDSG (Schuldatenschutzgesetz), das die Weitergabe persönlicher Daten von Schülern an Dritte (wie Verlage digitaler Schulbücher) ohne ausdrückliche elterliche Zustimmung verbietet.

Analyse der Datenströme

Identifizierung der betroffenen personenbezogenen Daten

Die Analyse der Datenströme zwischen Synapse und MEIN BILDUNGSRAUM veranlasst uns, vorab die an diesem Austausch beteiligten personenbezogenen Daten zu identifizieren. Diese Daten werden nach Kategorien identifiziert und können verschiedenen Zwecken dienen.

Kategorie der Daten	Beispiele	Zwecke
Daten zur Identifizierung	Name, Vorname, E-Mail-Adresse, SSO-Kennung.	Authentifizierung über MeinBildungsraum und Verwaltung von Benutzerprofilen.
Pädagogische Daten	Metadaten der Granule (Titel, Tags, Autor).	Organisation und Indexierung der Inhalte in Datenraum.

[27] *Ibidem*

Daten zum Verhalten.	Nutzungsverlauf, Zeit, die mit den Ressourcen verbracht wird.	Pädagogische Analyse und Personalisierung der Nutzererfahrung.
Daten zum Nutzerprofil	Pädagogische Präferenzen, digitale Abzeichen.	Verwaltung von Profilen in DataWallet zur Personalisierung und Nachverfolgung.
Technische Daten	IP-Adressen, Logs von Verbindungen.	Sicherung der Datenflüsse und Erkennung von Anomalien.

Kartierung der Datenflüsse zwischen Synapse und MEIN BILDUNGSRAUM.

Diese Kartografie listet die persönlichen Daten auf, die zwischen Synapse und der Anwendung MeinBildungsraum, dem Datawallet und dem Datenraum ausgetauscht werden.

Komponente	**Richtung des Datenflusses**	**Ausgetauschte Daten**	**Hauptzweck**
MeinBildungsraum	Bidirektional	SSO-Identifikatoren (Benutzername, Passwort), Token	Einmalige Authentifizierung und Zuweisung von Zugriffsrechten.
Datawallet		Benutzerpräferenzen, digitale Namensschilder	Verwaltung von Benutzerprofilen und pädagogische Personalisierung.
		Daten zur Identifizierung	Aktualisierung von persönlichen Informationen
Datenraum		Metadaten der Granule	Indexierung und Suche von Lernressourcen

		Verhaltensdaten (auf Ressourcen verbrachte Zeit)	Pädagogische Analyse und kontinuierliche Verbesserung

Wichtige Punkte

Mehrere Punkte müssen berücksichtigt werden, um die Einhaltung gesetzlicher Vorschriften zu gewährleisten und einen optimalen Schutz personenbezogener Daten sicherzustellen.

i. Sicherung der Datenströme

- Verschlüsseln Sie den Datenaustausch mit sicheren Protokollen wie TLS 1.3, um ein Abhören zu verhindern, und verwenden Sie OAuth2-Tokens, um Fälschungen zu verhindern.
- Implementieren Sie ein rollenbasiertes Zugriffskontrollsystem, um den Datenzugriff entsprechend den Verantwortlichkeiten der Benutzer zu beschränken.
- Führen Sie ein Prüfprotokoll für alle Zugriffe, Änderungen oder den Austausch von Daten zwischen den Systemen, um eine vollständige Rückverfolgbarkeit zu gewährleisten.

ii. Minimierung der Daten

- Sammeln Sie nur die Daten, die für den jeweiligen Zweck unbedingt erforderlich sind, nach dem Vorbild des Datenraums, der nur die Metadaten erhalten sollte, die für die Indexierung der Granule erforderlich sind.
- Einen automatischen Mechanismus einrichten, um ungenutzte Daten nach einer bestimmten Zeit zu löschen oder zu anonymisieren.

iii. Transparenz gegenüber den Nutzern

- Stellen Sie eine klare Datenschutzrichtlinie zur Verfügung, in der die Arten der gesammelten Daten, die Zwecke der Verarbeitung und die Rechte der Nutzer detailliert aufgeführt sind.
- Einholen einer ausdrücklichen Zustimmung für jede Verarbeitung, die nicht für die Ausführung des Dienstes erforderlich ist, wie z. B. die Verhaltensanalyse zu pädagogischen Verbesserungszwecken.

- Bei Nutzern unter 16 Jahren[28] , muss die ausdrückliche Zustimmung der Person, die die elterliche Verantwortung innehat, eingeholt werden.

iv. Handhabung der grenzüberschreitenden Übermittlung

- Stellen Sie sicher, dass alle Daten in Infrastrukturen innerhalb der Europäischen Union gehostet werden.
- Schließen Sie mit Auftragsverarbeitern Vereinbarungen gemäß Artikel 28 DSGVO ab.

v. Rechte der Nutzer

- Ermöglichen Sie es den Nutzern, ihre Profile aus DataWallet oder Synapse in einem Standardformat zu exportieren (Beispiel: JSON oder CSV).
- Einen klaren Prozess einrichten, mit dem Nutzer die Berichtigung oder Löschung ihrer personenbezogenen Daten beantragen können.
- Bieten Sie den Nutzern die Möglichkeit, ihre Aktivitätsverläufe auf der Plattform einzusehen.

vi. Umgang mit sensiblen Daten

- Wenn sensible Daten (religiöse Überzeugungen, Gesundheit) indirekt über Granule oder geteilte Inhalte verarbeitet werden, holen Sie vor der Verarbeitung eine ausdrückliche Zustimmung ein.
- Systematische Anonymisierung aller sensiblen Daten vor ihrer Analyse oder Speicherung in Datenraum.

vii. Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DIA)

Angesichts des erzieherischen Charakters des Projekts und der potenziellen Verarbeitung sensibler Daten (Minderjährige, pädagogische Profile) ist es zwingend erforderlich, eine PIA gemäß Artikel 35 der DSGVO durchzuführen.

Diese Analyse muss Folgendes umfassen:

- Eine Bewertung der mit dem Datenfluss verbundenen Risiken.

[28] Verordnung (EU), op. cit., Artikel 8.1

- Die technischen und organisatorischen Maßnahmen, die zur Abschwächung dieser Risiken ergriffen wurden.

Zuweisung von Verantwortlichkeiten

Die verschiedenen Rollen der Akteure

i. Verantwortlicher für die Verarbeitung

Der für die Verarbeitung Verantwortliche ist die Stelle, die die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt .[29]

Verantwortlicher für die Verarbeitung	**Synapse**	**MEIN BILDUNGSRAUM**	**Verlage**
Verarbeitungen in Bezug auf	• Pädagogische Daten (erstellte Inhalte, Metadaten der Granule). • Verhaltensdaten (Nutzungsverlauf). • Identifikationsdaten (Name, E-Mail), die für die Verwaltung von Benutzerkonten benötigt werden.	• Die SSO-Kennungen. • Die OAuth2-Tokens. Es bestimmt die Zwecke im Zusammenhang mit der Authentifizierung und der Verwaltung von Zugriffsrechten.	• Die Metadaten, die mit den bereitgestellten Granulen verbunden sind (Titel, Autor, Tags). • Die Daten, die über ihre eigenen, in die Granule integrierten Systeme gesammelt werden.

ii. Mitverantwortlich für die Verarbeitung

Eine gemeinsame Verantwortung für die Verarbeitung liegt vor, wenn mindestens zwei Stellen gemeinsam die Zwecke und Mittel einer Verarbeitung festlegen .[30]

[29] Verordnung (EU), *op. cit.*, Artikel 4.7
[30] Verordnung (EU), a.*a.O.*, Artikel 26

Im vorliegenden Fall handeln Synapse und MEIN BILDUNGSRAUM als gemeinsam Verantwortliche für die Verwaltung von Nutzerprofilen (pädagogische Präferenzen, digitale Abzeichen) :

- Synapse verwendet diese Daten, um die Nutzererfahrung zu personalisieren.
- DataWallet zentralisiert und speichert diese Profile für eine interoperable Verwaltung mit anderen Bildungsplattformen.

Eine Vereinbarung über die gemeinsame Verantwortung sollte erstellt werden, um die jeweiligen Verpflichtungen zu klären.

iii. Subunternehmer

Ein Auftragsverarbeiter ist eine vom Verantwortlichen getrennte Einheit, die personenbezogene Daten im Namen und auf Anweisung des Verantwortlichen verarbeitet.

Mein Bildungsraum fungiert als Unterauftragsverarbeiter für Synapse[31] , indem er die Metadaten der Granule sowie die Verhaltensdaten speichert und indiziert. Er führt nur die von Synapse erteilten Anweisungen bezüglich der Organisation und der Bildungsanalyse aus.

Die spezifischen Punkte

i. Zustimmung der Nutzer/innen

Die Zustimmung ist eine wesentliche Rechtsgrundlage[32] in einigen spezifischen Fällen, einschließlich :

- Verhaltensanalyse, wenn Synapse Verhaltensdaten für Zwecke verwendet, die nicht unbedingt für die Bereitstellung des Dienstes erforderlich sind (z. B. Marketingstatistiken oder akademische Forschung).

[31] Ein Unterauftragnehmervertrag gemäß Artikel 28 der DSGVO ist erforderlich, um diese Rolle zu regeln.
[32] Verordnung (EU), *a. a. O.*, Artikel 6.1

- Die potenzielle Verarbeitung sensibler Daten, wenn sensible Informationen indirekt über Lerninhalte oder Nutzerpräferenzen verarbeitet werden (Beispiel: religiöse Überzeugungen in einem Auszug).

Der empfohlene Mechanismus ist die Implementierung eines granularen Systems zur Verwaltung von Einwilligungen in Synapse und eine spezifische Sammlung von Einwilligungen durch MEIN BILDUNGSRAUM für jeglichen Datenaustausch zwischen Plattformen.

ii. Umgang mit Minderjährigen

Minderjährige unter 16 Jahren genießen einen verstärkten Schutz, der die elterliche Zustimmung zwingend erforderlich macht. Dies beinhaltet:

- Eine vorherige Überprüfung des Alters bei der Anmeldung.
- Ein Mechanismus, der es den Eltern oder Erziehungsberechtigten ermöglicht, der Verarbeitung personenbezogener Daten ausdrücklich zuzustimmen.

Zusätzlich zur obligatorischen elterlichen Zustimmung muss die Verarbeitung strikt auf Bildungszwecke beschränkt werden. Dies bedeutet, dass :

- Pädagogische Daten und Verhaltensdaten müssen strikt in einem erzieherischen Rahmen verwendet werden.
- Jegliche Analyse oder Weitergabe an Dritte muss anonymisiert oder pseudonymisiert werden, um eine direkte oder indirekte Identifizierung des Minderjährigen zu vermeiden.

Spezifische Empfehlungen

Zu erwartende Verträge

i. Verträge über die Vergabe von Unteraufträgen

Verträge über die Vergabe von Unteraufträgen müssen die Verpflichtungen zur Vertraulichkeit, Datensicherheit und das Verbot der Weiterverwendung von Daten außerhalb des vertraglich festgelegten Zwecks formalisieren.

Diese Verträge sollten auch Standardvertragsklauseln (STVK) oder Binding Corporate Rules (BCR) enthalten, wenn die Daten in Drittländer weitergeleitet werden, als Ergänzung zu technischen Garantien wie der systematischen Anonymisierung sensibler Daten vor der Übermittlung.

ii. Vereinbarung über gemeinsame Verantwortung

Es sollte eine Vereinbarung zwischen Synapse und MEIN BILDUNGSRAUM ausgearbeitet werden, um Folgendes zu klären:

- Die Verteilung der Pflichten im Falle der Ausübung von Nutzerrechten.
- Die Mechanismen für die gemeinsame Benachrichtigung im Falle von Datenverletzungen.

iii. BDSG-spezifische Klauseln

Das BDSG verlangt die Aufnahme von verschärften Klauseln bezüglich :

- Die systematische Meldung an die deutsche Behörde bei Verstößen, bei denen Schülerdaten betroffen sind, auch wenn kein hohes Risiko besteht.
- Die ausdrückliche elterliche Zustimmung bei der Verarbeitung von Daten von Minderjährigen unter 16 Jahren.

Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen werden sich auf die Sicherung der Datenströme, die Datenminimierung und die Durchführung einer Folgenabschätzung beziehen.

i. Die Sicherung der Datenflüsse

Verschlüsselung des Datenaustauschs durch Implementierung von TLS 1.3 für die Datenströme zwischen Synapse und MEIN BILDUNGSRAUM und Verwendung von Token mit begrenzter Gültigkeitsdauer für die Authentifizierung.

ii. Die Minimierung von Daten

Programmieren von automatischen Bereinigungen, die pädagogische Metadaten anonymisieren, sobald sie pädagogisch veraltet sind, und Verhaltensdaten nach drei Jahren Inaktivität löschen.

iii. Die Durchführung einer Folgenabschätzung.

Angesichts des pädagogischen Rahmens ist es zwingend erforderlich, eine Folgenabschätzung für Verarbeitungen durchzuführen, die Daten von Minderjährigen und Verhaltensanalysen kombinieren.

Prozess der Verwaltung von Nutzerrechten

i. Kontextuelle Beschränkungen des erzieherischen Rahmens

Der Bildungsrahmen schränkt die Ausübung bestimmter Rechte ein, darunter :

- Recht auf Berichtigung unterwirft Änderungen an akademischen Daten einem von der Bildungseinrichtung bestätigten Verfahren.
- Recht auf Löschung ist unwirksam bei Daten, die für die Ausstellung eines Diploms erforderlich sind.[33]

ii. Die operativen Verfahren

Sehen Sie Verfahren vor, um :

- Exportieren von Benutzerprofilen
- Das Alter der Schüler zu überprüfen
- Eine doppelte Zustimmung (Schüler + Eltern) für die Verhaltensanalyse einrichten.

iii. Die gesetzlichen Ausnahmen

Das BDSG verschärft die Anforderungen an das Profiling und die automatisierte Entscheidungsfindung.

In Bezug auf den Widerstand gegen Profiling muss ein Opt-Out-Recht für Arbeitnehmer in Bezug auf die pädagogische Überwachung zugelassen werden[34] . In Bezug auf

[33] Das BDSG schreibt vor, dass sie fünf Jahre nach Ausstellung des Abschlusses aufbewahrt werden müssen.
[34] BDSG, §26

automatisierte Entscheidungen sollte jeder Algorithmus, der die Schullaufbahn ohne vorherige menschliche Validierung bestimmt, ausgeschlossen werden.

Teil II: Die Nutzung von digitalem Content

Status von digitalen Werken

Urheberrechtsanalyse für digitale Kataloge

Digitaler Content sind sowohl auf europäischer als auch auf nationaler Ebene urheberrechtlich geschützt. Originelle Schöpfungen genießen einen automatischen Schutz, sobald sie festgehalten werden[35] . Die pädagogische Ausnahme bei der Verwertung geschützter Werke kennt strenge Grenzen[36] wie die 15%-Schwelle für die pädagogische Verwertung eines Buches. TDM[37] für nichtkommerzielle Forschung ist ebenfalls erlaubt, aber Verleger können ihre Rechte durch technische Opt-outs vorbehalten .[38]

Granule, die geschützte Auszüge integrieren, müssen die Ausnahmen beachten oder explizit lizenziert werden. Die zugehörigen Metadaten sind ebenfalls geschützt, wenn sie einen originellen Charakter aufweisen.

Bedingungen für die Bereitstellung von Inhalten durch Verleger

Verleger können Bedingungen über Lizenzverträge mit Klauseln zu :

- Die abgetretenen Rechte: Vervielfältigung, Verbreitung, Bearbeitung.
- Die Vergütung, die in der Regel proportional zu den Verwertungserlösen ist oder auf Basis einer Pauschale festgelegt wird.
- Die territorialen Beschränkungen, um mögliche grenzüberschreitende Rechtekonflikte zu vermeiden.
- Die technischen Modalitäten nach dem Vorbild der Verwendung von DRM-Software.[39]
- Die Bedingungen für die Nutzung durch Endnutzer.
- Die Mechanismen zur Überwachung der Nutzung von Pellets, um eine genaue Rechenschaftslegung zu gewährleisten.

[35] Urheberrechtsgesetz (UrhG), § 2
[36] UrhG, § 60a
[37] Text und Data Mining
[38] UrhG, Artikel 60d
[39] Hierbei handelt es sich um Software zur Verwaltung digitaler Rechte.

- Die regelmäßige Überprüfung der wirtschaftlichen Bedingungen.

Verantwortlichkeiten von Plattformen und Nutzern

Regulatorischer Rahmen

a. Digital Services Act (DSA)

Der DSA verpflichtet Plattformen, die digitale Kreationen hosten und verbreiten, illegale Inhalte zu moderieren, die Transparenz der Algorithmen zu gewährleisten und mit den Behörden zu kooperieren.

Weitere praktische Anforderungen können sich aus der Umsetzung der Richtlinie ergeben .[40]

b. DAMUN-Richtlinie (Artikel 17)

Umgesetzt über das UrhDaG, verpflichtet sie Plattformen, unerlaubte Inhalte zu blockieren, andernfalls droht eine gemeinsame Haftung .[41]

Rechte und Grenzen der Endnutzer

Die Rechte und Grenzen der Endnutzer bei der Nutzung von geschütztem digitalem Content.

Rechte	Grenzen
- Zugang zu Granulen für den pädagogischen Gebrauch. - Datenübertragbarkeit unter bestimmten Bedingungen.	- Kommerzielle Weiterverbreitung - Veränderung außerhalb der pädagogischen Nutzung - Pflicht zur Quellenangabe (Erwähnung des Verlages in den Metadaten).

[40] Die Richtlinie wird ab April 2025 in deutsches Recht umgesetzt.

[41] "The German Model to Protect User Rights when implementing Article 17", auf https://communia-association.org/2020/07/02/german-model-protect-user-rights-implementing-article-17/.

Erkannte Risiken

Unberechtigter Zugriff auf lizenzierte Inhalte.

- Risiko: Weitergabe über Drittplattformen oder Umgehung von DRM
- Vorbeugende Maßnahmen: Verschlüsselung, Multi-Faktor-Authentifizierung und regelmäßige Sicherheitsprüfungen.

Mögliche Streitigkeiten über grenzüberschreitende Verbreitungsrechte.

- Risiko: Ein ausländischer Verleger könnte den Zugang zu einem Granulat in Deutschland anfechten, wenn die Lizenz beschränkt ist.
- Vorbeugende Maßnahmen: Aufnahme von Rechtswahlklauseln in Verträge.

Nutzungsbedingungen werden von Endnutzern nicht eingehalten.

- Risiko: Umwandlung von Granulen in PDF zur Verbreitung außerhalb von Synapse, kommerzielle Nutzung.
- Präventivmaßnahme: Überwachung durch Verkehrsanalysetools.

Spezifische Empfehlungen

Die Nutzung digitaler Ressourcen erfordert ein Gleichgewicht zwischen pädagogischer Innovation und der strikten Einhaltung des rechtlichen Rahmens. Diese Empfehlungen setzen eine enge Zusammenarbeit mit den Verlegern voraus, gekoppelt mit robusten technischen Maßnahmen, um die Risiken zu minimieren und die Nutzererfahrung zu optimieren.

Verträge mit Verlegern

- Aufnahme von FRAND-Klauseln[42] für den Zugang zu Katalogen.
- Möglichkeit der Nutzung von Gesamtlizenzen über Verwertungsgesellschaften.

[42] Das bedeutet, dass die Lizenzbedingungen objektiv, transparent und diskriminierungsfrei auf alle Antragsteller angewendet werden müssen.

Techniken zum Schutz

- Implementieren Sie ein interoperables DRM-System und nutzen Sie Blockchain, um die Nutzung von Granulen nachzuverfolgen.
- APIs für die Indexierung im Datenraum verwenden.

Sensibilisierung der Nutzer

- Integrieren Sie Tutorials zum Thema Urheberrecht in den Lernraum.
- Ein Belohnungssystem für Nutzer einrichten, die Verstöße melden.

Regelmäßige Audits

- Überprüfen Sie die Einhaltung der DSGVO und des UrhG über unabhängige Dritte.
- Veröffentlichen Sie jährliche Transparenzberichte über Anträge zur Entfernung von Inhalten.

Zusammenfassung der Empfehlungen

Um die Konformität des Projekts zu gewährleisten und die Risiken zu minimieren, haben wir Empfehlungen für den Schutz personenbezogener Daten sowie für die Nutzung von geschütztem digitalem Content formuliert.

Im Bereich des Umgangs mit personenbezogenen Daten ist es zwingend erforderlich, die Beziehungen zwischen den Beteiligten zu formalisieren. Dies geschieht durch die Einführung von Unterverträgen, die einen strengen Rahmen für die Nutzung der Daten vorgeben und jede Weiterverwendung außerhalb des vorgesehenen Zwecks verbieten. Darüber hinaus muss zwischen Synapse und MEIN BILDUNGSRAUM eine Vereinbarung über die gemeinsame Verantwortung geschlossen werden, um die Verwaltung der Nutzerrechte und die jeweiligen Verpflichtungen im Falle einer Datenverletzung zu klären. In Übereinstimmung mit dem BDSG müssen auch spezifische Klauseln aufgenommen werden, darunter die Forderung nach einer systematischen Meldung an die Behörden bei Vorfällen mit Minderjährigen und die Einholung einer ausdrücklichen elterlichen Zustimmung für Kinder unter 16 Jahren.

Aus technischer und organisatorischer Sicht ist die Sicherheit des Datenaustauschs ein zentrales Anliegen. Es wird empfohlen, die Datenströme systematisch zu verschlüsseln und temporäre Authentifizierungs-Tokens zu verwenden, um das Risiko einer Kompromittierung zu begrenzen. Die Datenminimierung sollte eine Priorität sein, mit einer Politik der automatischen Löschung veralteter Daten, insbesondere solcher, die mit pädagogischen Interaktionen in Verbindung stehen. Darüber hinaus muss angesichts der Sensibilität der verarbeiteten Informationen eine Folgenabschätzung durchgeführt werden, um die Risiken und die einzuführenden Minderungsmaßnahmen zu bewerten.

Die Verwaltung der Nutzerrechte erfordert einen an den Bildungskontext angepassten Ansatz. So müssen die Verfahren den Nutzern das Hochladen und Übertragen ihrer persönlichen Daten ermöglichen und gleichzeitig eine Altersverifikation für Minderjährige gewährleisten. Besondere Aufmerksamkeit muss der Nutzung von Verhaltensdaten gewidmet werden: Ihre Analyse zu Zwecken der pädagogischen Verbesserung darf nur mit

einer doppelten Zustimmung erfolgen, die die ausdrückliche Zustimmung der Schüler und ihrer Eltern beinhaltet.

In Bezug auf die Nutzung von digitalem Content müssen die Beziehungen zu den Verlegern durch transparente Lizenzverträge geregelt werden, die FRAND-Klauseln (Fair, Reasonable, and Non-Discriminatory) enthalten, um einen fairen Zugang zu den digitalen Katalogen zu gewährleisten. Um Urheberrechtsverletzungen zu verhindern, wird empfohlen, ein interoperables DRM-System zu integrieren und die Blockchain zu nutzen, um eine optimale Nachvollziehbarkeit der Nutzung zu gewährleisten.

Schließlich kann die Einhaltung der Vorschriften nicht ohne ständige Bemühungen um Bewusstseinsbildung und Kontrolle aufrechterhalten werden. Es ist von entscheidender Bedeutung, die Nutzer in den Regeln des geistigen Eigentums zu schulen, indem interaktive Tutorials und Anreizmechanismen zur Meldung von Missbrauch integriert werden. Darüber hinaus müssen regelmäßige Audits durchgeführt werden, um die Einhaltung der rechtlichen Verpflichtungen sowohl im Bereich des Datenschutzes als auch der Verwaltung von Urheberrechten zu überprüfen. Die Veröffentlichung von Transparenzberichten wird die Glaubwürdigkeit des Projekts stärken und eine strenge Governance der genutzten Daten und digitalen Inhalte sicherstellen.

2. Architektur Katalog und Metadaten

2.1. Einführung

Im Rahmen des Projekts Synapse zielt das Arbeitspaket 2 darauf ab, eine effektive Methode zur Standardisierung von Ressourcen für die Integration in die Metadatenplattform zu etablieren. Das Hauptziel besteht darin, einen umfassenden Katalog von Ressourcen aus verschiedenen Quellen und Akteuren des Bildungssektors zu erstellen, diese in einer robusten Datenbank zu zentralisieren und die wichtigsten Elemente für eine optimale Nutzung im Datenraum zu extrahieren.

Dieser Standardisierungsprozess ist Teil eines Qualitätskonzepts gemäß den Grundsätzen der ISO 9000 und zielt darauf ab, die Verwaltung und Nutzung digitaler Bildungsressourcen zu optimieren. Darüber hinaus berücksichtigt der gewählte Ansatz Aspekte der Informationssicherheit in Übereinstimmung mit den Empfehlungen von ISO 27001, um die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten zu gewährleisten.

Um diesen Katalog zu bereichern und seine Nutzung zu erleichtern, haben wir auch den Einsatz von künstlicher Intelligenz zur automatischen Generierung von Tags erforscht. Diese Initiative soll die Kategorisierung und Suche von Ressourcen verbessern, wobei wir uns der Herausforderungen und Grenzen dieser Technologie in einem Bildungskontext bewusst sind.

Die Einführung dieses standardisierten Systems zur Verwaltung digitaler Bildungsressourcen stellt einen bedeutenden Fortschritt bei der Organisation und Zugänglichkeit von Bildungsinhalten dar. Sie ebnet den Weg für eine effizientere und personalisierte Nutzung der Ressourcen durch die verschiedenen Akteure des Bildungssystems und legt gleichzeitig den Grundstein für eine entwicklungsfähige und sichere digitale Infrastruktur.

2.2. Methode

Um dieses Projekt zur Standardisierung digitaler Bildungsressourcen erfolgreich durchzuführen, haben wir einen methodischen und strukturierten Ansatz gewählt. Diese Methodik lässt sich in mehrere Schlüsselschritte unterteilen:

Untersuchung der bestehenden Standards

Unser erster Schritt bestand darin, eine umfassende Bestandsaufnahme der derzeit im Bereich der digitalen Bildungsressourcen verwendeten Standards durchzuführen. Diese Analyse umfasste :

- Die Formate zur Darstellung von Daten in digitalen Katalogen.
- Die spezifischen Standards für Bildungsressourcen.
- Die Standards für die Beschreibung von Lerngranulaten. Dieser Schritt ist entscheidend, um das bestehende Ökosystem zu verstehen und die Best Practices zu identifizieren, die wir in unseren Ansatz integrieren können.

Auswahl einer geeigneten Datenbank

Nach der Untersuchung der Standards konzentrierten wir uns auf die Identifizierung einer Datenbank, die in der Lage ist, eine große Menge strukturierter Daten effizient zu verwalten. Zu den Auswahlkriterien gehörten:

- Die Fähigkeit, große Datenmengen zu verarbeiten.
- Die Flexibilität, sich an verschiedene Ressourcenformate anzupassen.
- Die Skalierbarkeit, um mit dem Wachstum des Katalogs Schritt zu halten.
- Die Kompatibilität mit den zuvor identifizierten Standards.

Erforschung von Technologien der künstlichen Intelligenz

Um die Nutzung und Kategorisierung von Ressourcen zu verbessern, haben wir uns vorgenommen, die Möglichkeiten der künstlichen Intelligenz zu erforschen, insbesondere für die automatische Generierung von Tags. Diese Analysephase umfasste:

- Die Identifizierung von KI-Technologien, die für unseren Kontext relevant sind.
- Die Definition von Testprotokollen zur Bewertung ihrer Effektivität.
- Die Analyse der ethischen und praktischen Auswirkungen der Nutzung von KI in diesem Rahmen.

Gestaltung des Standardisierungsprozesses

Basierend auf den Ergebnissen der vorherigen Schritte haben wir einen Standardisierungsprozess entworfen, der darauf abzielt:

- Eine gemeinsame Datenstruktur für alle Ressourcen festzulegen.
- Konvertierungsprotokolle für die verschiedenen vorhandenen Formate festlegen
- Qualitätskontrollmechanismen einzurichten, um die Konsistenz der Daten zu gewährleisten.

2.3. Analyse des Vorhandenen

Die Analyse des Bestehenden im Rahmen unseres Projekts zur Standardisierung digitaler Bildungsressourcen konzentrierte sich auf die Verwendung des Datenraums und die von ihm vorgeschlagene Datenstruktur. Dieser Ansatz zielt darauf ab, die Integration und Nutzung von Bildungsressourcen in einem kohärenten und effizienten digitalen Ökosystem zu optimieren.

Struktur des Datenraums

Der Datenraum bietet eine robuste Architektur, die die Verwaltung und Organisation von Bildungsressourcen ermöglicht. Seine Struktur ist so konzipiert, dass sie Folgendes erleichtert:

- Die Generierung von Lernangeboten aus Schulbüchern.
- Die Integration von qualifizierten Ressourcen-Sets.
- Die Kompatibilität mit verschiedenen Arten von Lerninhalten.

Diese strukturelle Flexibilität ermöglicht eine breite und vielfältige Nutzung der Ressourcen und entspricht damit den unterschiedlichen Bedürfnissen der Akteure im Bildungssektor.

Kompatibilität und Interoperabilität

Ein entscheidender Aspekt unserer Analyse war die Bewertung der Kompatibilität zwischen der Datenstruktur des Datenraums und den verschiedenen bestehenden Formaten für Bildungsressourcen. Diese Kompatibilität ist entscheidend für die Gewährleistung:

- einer nahtlosen Integration von Ressourcen aus verschiedenen Quellen.
- einer effizienten Standardisierung ohne Verlust von entscheidenden Informationen.
- einer Anpassungsfähigkeit an zukünftige Entwicklungen von Bildungsformaten und -standards.

Potenzial für die Nutzung

Die Analyse hat auch das Nutzungspotenzial aufgezeigt, das der Datenraum bietet für:

- Die Erstellung von personalisierten Lernpfaden
- Die Anreicherung der Metadaten, die mit den Ressourcen verknüpft sind.
- Die Verbesserung der Zugänglichkeit und Auffindbarkeit von Bildungsinhalten. Diese Infrastruktur ermöglicht innovative Nutzungsmöglichkeiten von Ressourcen, die den Weg für neue pädagogische Ansätze und eine bessere Anpassung an die spezifischen Bedürfnisse von Lernenden und Lehrenden ebnen.

Zusammenfassend lässt sich sagen, dass die Analyse des Bestehenden die Relevanz der Wahl des Datenraums als Grundlage unseres Standardisierungsansatzes bestätigt hat. Seine flexible Struktur und seine Kompatibilität mit aktuellen Standards machen ihn zu einem vielversprechenden Instrument für die Erreichung unserer Ziele und bieten gleichzeitig Entwicklungsperspektiven, die mit den von ISO 9000 propagierten Grundsätzen der kontinuierlichen Verbesserung in Einklang stehen.

2.4. Technische und regulatorische Anforderungen

Die Umsetzung des Projekts zur Standardisierung digitaler Bildungsressourcen erfordert eine robuste und skalierbare Infrastruktur. Die Datenbanken müssen so konzipiert sein, dass sie ein beträchtliches Volumen von Ressourcen verwalten können, wobei die Architektur eine effiziente Skalierbarkeit ermöglicht. Die Interoperabilität mit dem Datenraum wird durch die Nutzung bestehender APIs gewährleistet, die eine nahtlose Integration der standardisierten Daten garantieren. Im Hinblick auf die Sicherheit wird das System die in AP 5.1 beschriebenen Empfehlungen befolgen, um den Schutz der Daten und die Einhaltung der geltenden Normen zu gewährleisten.

2.5 Ergebnisse der Recherche

Analyse der Standards

Unsere eingehende Untersuchung der Standards ergab, dass sich der **GS1 XML-Standard** besonders gut für unser Projekt zur Standardisierung digitaler Bildungsressourcen eignet. Dieser Standard bietet die Flexibilität und Robustheit, die für die effiziente Verwaltung von Lieferketten für Bildungsinhalte unerlässlich sind.
Die detaillierte Analyse der Formate xAPI, SCORM, LTI und XML-GS1 ist im beigefügten Dokument "AP 2.1 Analyse Datenaustauschformate" zu finden. Diese vergleichende Studie ermöglichte es uns, eine Datenstruktur zu entwerfen, die mit diesen Standards kompatibel und in unserem gewählten DBMS nutzbar ist.

Wahl des DBMS und Datawarehouse

Um die Bildungsressourcen zu zentralisieren und zu standardisieren, haben wir uns für **PostgreSQL** als Datenbankmanagementsystem entschieden. Der Grund für diese Wahl waren seine Leistungsfähigkeit, Stabilität und relationalen Fähigkeiten, die für die effiziente Verwaltung von mindestens 7 Millionen Datensätzen bei gleichzeitig hervorragender Skalierbarkeit unerlässlich sind.

Unsere Datawarehouse-Architektur umfasst:

1. ETLs für die Umwandlung von Daten in strukturierte Felder.
2. QlikSense als Business-Intelligence-Tool für die Datenanalyse und -visualisierung.
3. Einen Staging-Bereich zur vorübergehenden Speicherung von Rohdaten vor der Transformation.

Die Steuerung dieser Dienste erfolgt durch:

- Zabbix für das Hardware- und Software-Monitoring.
- Wazuh für die Überwachung von Sicherheitslücken und die Kontrolle von Anomalien.

– Ein System zur Überwachung der Verlage und Vertreiber von Ressourcen, das in AP-6.4 näher erläutert wird.

Standardisierung des Datawarehouse

Wir haben eine Reihe von Hauptfeldern für die Verwaltung von Lernpfaden ausgewählt. Diese Informationen sind in einem Format strukturiert, das mit dem Datenraum kompatibel ist.

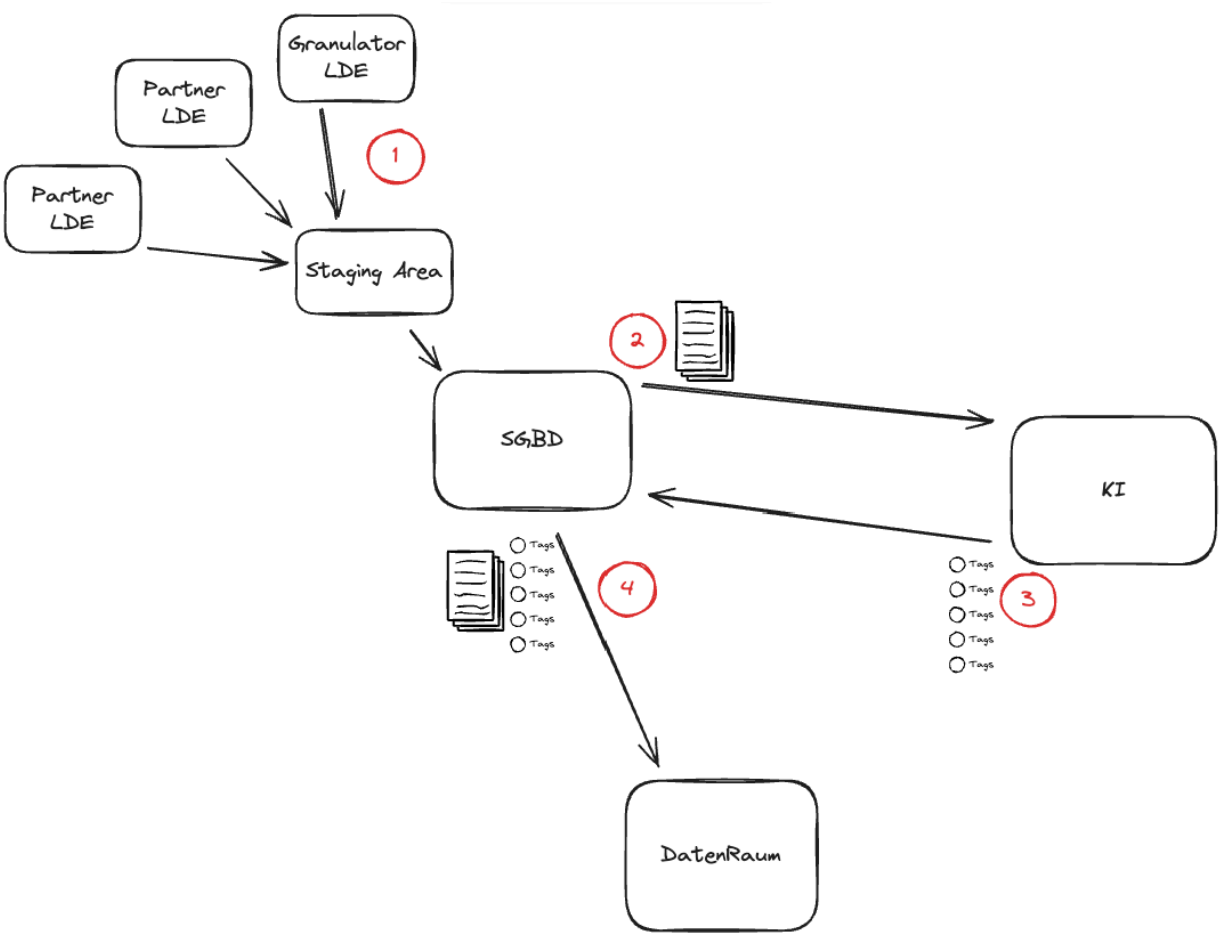
Name	Typ	Beschreibung
ean	string (13)	Eindeutige Kennung des Produkts.
Titel	string	Titel des Buches
Beschreibung	string	Beschreibung des Buches
date_publication	Datum	Datum der Veröffentlichung im ISO GMT-Format.
Kategorie	string	Derzeit werden zwei Kategorien identifiziert: Schulbuch oder Lernmedium. Das digitale Schulbuch ist die digitale Übersetzung eines Buches, während sich das Lernmedium in der Regel auf Lernparcours, Lernapps oder sogar digitale Zeitungen bezieht.
Verlag	string	Name des Verlags
ref_editor	String	Referenz, mit der der Artikel beim Verlag gefunden werden kann.
Sammlung	string	Gesamtheit der Publikationen, zu denen das Buch gehört.
Disziplinen	[string,...]	Bei Schulbüchern das Fach oder die Fächer, die behandelt werden (z. B. Mathematik, Geschichte, ...).
Niveaustufen	[string,...]	Bei Schulbüchern die jeweilige(n) Klassenstufe(n) (z. B. Grundschule, Gymnasium,...).
Klassen	[string,...]	Für Schulbücher, die entsprechende(n) Klasse(n) (z. B. 1.Klasse, 10. Klasse, ...)
öffentliche	[string,...]	Die Zielgruppe(n) (z. B.: Schüler, Lehrer, allgemeines Publikum).
Verfügbarkeit	bool	Gibt an, ob der Artikel derzeit verfügbar ist.
Technologie	string	Name der Technologie, mit der der Artikel aufgerufen werden kann.
url_demonstration	string	URL der Demoversion.
url_cover	string	URL zum Anzeigen des Titelbilds.

Name	Typ	Beschreibung
url_download	string	URL zum Herunterladen des Artikels.
datei_gewicht	doppelt	Gewicht der Datei in Kilobyte.
ean_papier	[string,...]	Papierbuchversion(en) des digitalen Lehrbuchs

Einsatz von KI zur Generierung von Tags

Um die Metadaten anzureichern, haben wir mit dem Einsatz von KI experimentiert, um relevante Tags für jede Ressource zu generieren. Der Prozess läuft wie folgt ab:

1. ETL (Extract, Transform, Load): Daten aus einer Vielzahl von Quellen werden so verarbeitet, dass sie mit der Metadatenplattform übereinstimmen.
2. Jeder Datensatz wird von der KI durchsucht.
3. Die KI liefert uns tags , die für jede Ressource relevant sind.
4. Ein Satz relevanter und Daten über die Ressource wird an den Datenraum gesendet, um von den Partnern genutzt zu werden.



Teil 2 des Schemas läuft wie folgt ab (siehe Code und Details im Anhang):

5. Extraktion der Daten aus dem DBMS.
6. Nutzung eines speziellen Prompts für die Analyse der Bildungsdaten.
7. Generierung relevanter Tags durch die KI.
8. Menschliche Validierung der generierten Tags.

2.6 Analyse der Risiken

Auch wenn unser Projekt zur Standardisierung digitaler Bildungsressourcen nicht direkt mit personenbezogenen Daten zu tun hat, müssen einige wichtige Risiken berücksichtigt werden:

Datensicherheit

Die Zentralisierung einer großen Menge an Bildungsressourcen erfordert eine erhöhte Wachsamkeit in Bezug auf die Sicherheit. Es ist entscheidend, die in AP 5.1 ausführlich beschriebenen Empfehlungen genau zu befolgen, um die Integrität und Vertraulichkeit der Daten zu gewährleisten.

Einsatz von KI

Die Integration von künstlicher Intelligenz zur Tag-Generierung bietet erhebliche Vorteile, birgt aber auch die Risiken, die mit dieser aufstrebenden Technologie einhergehen. Wir haben ein spezielles Dokument, "KI-Empfehlung.pdf", erstellt, in dem die zu treffenden Vorsichtsmaßnahmen und bewährten Praktiken ausführlich beschrieben sind.

Qualität und Relevanz von Metadaten

Ein großes Risiko besteht darin, dass ungenaue oder irrelevante Metadaten erzeugt werden, was die Effizienz des Systems zur Suche und Kategorisierung von Ressourcen beeinträchtigen könnte. Eine konstante menschliche Aufsicht und strenge Überprüfungsprozesse sind notwendig, um dieses Risiko zu mindern.

Skalierbarkeit und Leistung

Mit dem vorhersehbaren Anstieg des Datenvolumens besteht das Risiko, dass die Leistung des Systems beeinträchtigt wird. Eine sorgfältige Planung der Architektur und regelmäßige Performance-Tests sind entscheidend, um Skalierbarkeit, Effizienz und Ausfallsicherheit des Systems langfristig zu gewährleisten.

Zusatz 1 zu 2.: Das ONIX-Format

Überblick

Das ONIX-Format für Bücher ist der internationale Standard für die Darstellung und Kommunikation von "Produkt"-Informationen der Buchbranche (Metadaten) in elektronischer Form.

ONIX ist ein XML-basierter Standard für angereicherte Buchmetadaten, der Verlagen, Einzelhändlern und ihren Partnern in der Lieferkette eine einheitliche Möglichkeit bietet, eine breite Palette von Produktinformationen zu kommunizieren. Es ist ein kommerziell ausgerichtetes Datenformat, das ausdrücklich für den weltweiten Einsatz konzipiert wurde und nicht auf eine Sprache oder die Merkmale eines bestimmten nationalen Buchhandels beschränkt ist. Es wird in der gesamten Lieferkette für Bücher und eBooks in Nordamerika, Europa und Ozeanien weit verbreitet eingesetzt und wird auch im asiatisch-pazifischen Raum und in Südamerika zunehmend übernommen.

Als XML-basierter Standard enthält jede Version von ONIX für Bücher eine Dokumentation, die den Dateninhalt einer ONIX-Standarddatendatei oder einer "Nachricht" festlegt, sowie ein zugehöriges XML-Schema, das zur Validierung einer ONIX-Datei verwendet werden kann.

ONIX selbst ist keine Datenbank oder gar eine Designvorlage für eine Datenbank - es ist ein Mittel zur Kommunikation von Daten zwischen

Datenbanken. Es ist keine Registrierung, Gebühr oder Mitgliedschaft erforderlich, um ONIX zu implementieren.

Anwendungsfälle von ONIX-Nachrichten

1. **Automatisierter Austausch** - ONIX-Nachrichten ermöglichen den automatisierten Austausch und die Verarbeitung komplexer Informationen, wodurch Fehler reduziert und Bestell-, Rechnungs- und Katalogverwaltungsprozesse beschleunigt werden.

2. **Reichhaltige Produktinformationen**: Nachrichten im ONIX-Standard liefern umfassende Daten zu jedem Produkt, wie z. B. Titel, Autor, Sprache, Preis (der je nach Land oder Weltregion unterschiedlich sein kann), Verfügbarkeit, Themen, Bildungsstufen und andere Metadaten.

3. **Bestands- und Aktualisierungsmanagement**: Die Verwendung von ONIX ermöglicht es, Produktkataloge mit Informationen über neue Ausgaben, Nachdrucke und Änderungen der Verfügbarkeit auf dem neuesten Stand zu halten. Dies hilft bei der Verwaltung von Angeboten für Bildungseinrichtungen oder Kommunen, da genaue und aktuelle Daten bereitgestellt werden.

4. **Integration digitaler Ressourcen**: Vor allem ONIX Version 3 ist für digitale Formate (Ebooks, interaktive Ressourcen) optimiert. Es ermöglicht die Beschreibung von Nutzungsrechten, Dateiformaten und Zugangsbedingungen für digitale Bildungsinhalte.

Vorteile des ONIX-Formats für den EDI-Austausch

1. **Interoperabilität**: Die Verwendung von ONIX gewährleistet, dass die "Produkt"-Informationen in einem Format ausgetauscht werden, das von allen Akteuren der Buchkette anerkannt und verstanden wird.
2. **Erfüllung spezifischer Kundenanforderungen**: In einer Ausschreibung ermöglicht ONIX die Erfüllung spezifischer Anforderungen, wie z. B. detaillierte Beschreibungen digitaler Schulbücher oder Informationen zu Vertriebsrechten.

Dieser Rahmen ermöglicht es, den Austausch zwischen den Akteuren zu standardisieren und zu vereinfachen und gleichzeitig die Konformität mit den Anforderungen der Ausschreibung zu gewährleisten.

Unterschiede zwischen den Versionen 2 und 3

Die meisten ONIX-Austauschvorgänge beruhen auf der Übermittlung vollständiger Datensätze, entweder als neue Informationen oder als Ersatz für zuvor bereitgestellte Informationen.

In ONIX 2.1 steht ein separates Format namens "Supply Update" zur Verfügung, mit dem Preis- und Verfügbarkeitsdetails aktualisiert werden können, ohne dass ein vollständiger Datensatz als Ersatz gesendet werden muss. In ONIX 3.0 und 3.1 wird ein flexiblerer und granularerer Aktualisierungsansatz, genannt "Block Updates", unterstützt, der die Notwendigkeit eines separaten und spezialisierten Aktualisierungsformats beseitigt.

ONIX 3 ist flexibler bei der Beschreibung digitaler Formate und besser auf neue Technologien abgestimmt, während ONIX 2.1 bei einigen Aspekten digitaler Produkte stärker eingeschränkt ist.

ONIX 3 verbessert die Verwaltung von Sammlungen, Serien und gebündelten Inhalten, was für die Verteilung von Lerninhalten in mehreren Bänden oder Modulen wichtig ist.

Fokus auf Version 3.1

Die im März 2023 veröffentlichte Version 3.1 des ONIX-Formats ist ein Update der Version 3.0 und führt Verbesserungen und Klarstellungen ein, ohne die Struktur des Standards grundlegend zu verändern. Hier sind einige bemerkenswerte Unterschiede, die ONIX 3.1 mit sich bringt:

1. **Besserer Umgang mit digitalen Inhalten**: ONIX 3.1 bringt Verbesserungen, um digitale Formate wie Ebooks oder interaktive Inhalte besser zu beschreiben. Dies beinhaltet eine genauere Beschreibung von Nutzungsrechten, Lizenzen, geografischen Beschränkungen und Zugriffszeiten für digitale Ressourcen.

2. **Mehr Granularität bei Aktualisierungen**: Version 3.1 stärkt das Konzept der "block updates", mit dem spezifische Teile der Produktdaten aktualisiert werden können, ohne dass der gesamte Datensatz gesendet werden muss, was die Effizienz des Datenaustauschs verbessert.

3. **Neue Metadaten für Nachhaltigkeit**: ONIX 3.1 führt Felder ein, um Informationen über die Nachhaltigkeit von Produkten zu liefern, z. B. über

die Verwendung von recycelten Materialien oder über Umweltpraktiken im Zusammenhang mit der Herstellung von Büchern.

4. **Verbesserte Verwaltung von Sammlungen und Serien**: ONIX 3.1 bietet Klarstellungen und neue Funktionen für die Verwaltung von Werken, die Teil von Sammlungen oder Serien sind, und ermöglicht eine einheitlichere Beschreibung von Produktgruppierungen.

5. **Kompatibilität mit neuen Preisstandards**: Version 3.1 verbessert die Verwaltung von preisbezogenen Informationen, insbesondere für digitale Produkte, mit Ergänzungen wie der Unterstützung neuer Preismodelle (z. B. Abonnements oder zeitlich begrenzter Zugang).

6. **Klarstellungen und Korrekturen**: ONIX 3.1 enthält kleinere Anpassungen zur Klärung von Unklarheiten in Version 3.0 und zur Korrektur von Fehlern oder Inkonsistenzen, die von den Nutzern des Standards erkannt wurden.

Empfehlungen

- Wir schlagen die einheitliche Nutzung des ONIX 3.1-Formats für den Austausch von produktbezogenen Daten vor. Dies wird eine Entwicklung zur Aktualisierung des ONIX-Mikroservices mit sich bringen, einschließlich der Aktualisierung der JOnix-Bibliothek und der Durchführung notwendiger Anpassungen.

- Optimierung der Granularität der vom Mikroservice erzeugten JSON-Daten, um die Genauigkeit der Aktualisierungen zu verbessern und den Austausch reaktionsschneller zu gestalten.

Diese Entwicklungen werden eine harmonisierte Kommunikation mit unserer aktuellen Kataloganwendung und -datenbank (4D), sowie mit einer dedizierten Anwendung und Datenbank für das MBR-Projekt ermöglichen.

Zusatz 2 zu 2.: xAPI-Analyse

Eine xAPI-Nachricht, oder "*Experience API*", ist eine strukturierte Dateneinheit, die zur Verfolgung und Aufzeichnung von Lernerinteraktionen in Online-Lernsystemen verwendet wird. xAPI wurde entwickelt, um unterschiedliche Lernerfahrungen zu erfassen, und ermöglicht es, Daten über die Aktivitäten eines Lernenden aufzuzeichnen, unabhängig davon, ob diese online, über eine mobile Anwendung oder sogar offline durchgeführt werden. Das Ziel dieser Nachrichten ist es, Lerndaten zu zentralisieren und zugänglich zu machen, um den Weg eines Lernenden zu verfolgen und die Lernerfahrungen zu verbessern.
xAPI-Nachrichten sind um eine dreigliedrige Struktur herum aufgebaut: **Subjekt - Verb - Objekt**. Jedes dieser Elemente repräsentiert einen grundlegenden Aspekt der Erfahrung:

1. **Subjekt**: Identifiziert den Lernenden oder Benutzer, der die Handlung ausführt. Er wird typischerweise durch einen Namen oder eine E-Mail-Adresse repräsentiert.
2. **Verb**: beschreibt die vom Subjekt durchgeführte Aktion, wie z. B. hat *angesehen, hat vervollständigt* oder *hat versucht*.
3. **Betreff**: Beschreibt das Ziel der Aktion, das ein Lernmodul, ein Quiz, ein Dokument oder eine andere Lernressource sein kann.

Eine xAPI-Nachricht kann auch zusätzliche Informationen enthalten:

- **Kontext**: Fügt Details zu den Umständen der Interaktion hinzu, z. B. das verwendete Gerät, den Ort oder das Ziel der Aktion.
- **Ergebnis**: Ermöglicht die Speicherung der Ergebnisse einer Interaktion, z. B. Punktzahl, Erfolg oder Dauer.

Diese Nachrichten werden gesendet und in einem *Learning Record Store* (LRS) gespeichert, der die Daten zentralisiert und es Administratoren und Lehrern ermöglicht, den Fortschritt und die Leistung der Lernenden zu verfolgen und zu analysieren.
Beispiel für eine xAPI-Nachricht im JSON-Format.
Hier ein vereinfachtes Beispiel für eine XAPI-Nachricht:
{"actor": {"name": "Alice Dupont", "mbox": "mailto:alice@example.com"}}, "verb": {"id": "http://adlnet.gov/expapi/verbs/completed", "display": { "en-US": "completed" }}, "object":

{"id": "http://example.com/activities/module-intro", "definition": {"name": { "en-US": "XAPI-Einführungsmodul" }}}, "result": {"score": { "scaled": 0.85 }}}
In diesem Beispiel hat die Schauspielerin *Alice Dupont* das *XAPI-Einführungsmodul* mit einer Punktzahl von 85 % *abgeschlossen.*

SCORM-Analyse :

- Was ist eine SCORM-Nachricht?

Eine SCORM-Nachricht, oder "Sharable Content Object Reference Model", ist ein Kommunikationsformat, das verwendet wird, um den Fortschritt und die Ergebnisse von Lernenden in Lernmanagementsystemen (LMS - Learning Management Systems) zu verfolgen und zu berichten. SCORM wurde vom US-Verteidigungsministerium und Advanced Distributed Learning (ADL) entwickelt und ist ein Standard, der es ermöglicht, digitale Lerninhalte in verschiedene kompatible LMS zu integrieren und Lerndaten auf einheitliche Weise zu zentralisieren.
SCORM basiert auf einem Modell von Datenstrukturen und Protokollen zur Aufzeichnung von Informationen, einschließlich der Interaktionen des Lernenden mit den Lernmodulen. Dazu gehören Aktionen wie das Aufrufen einer Lektion, das Abschließen eines Tests oder auch die erzielten Ergebnisse. SCORM-Nachrichten ermöglichen es daher, Informationen wie die aufgewendete Zeit, die erreichte Punktzahl und den Abschlussstatus zu verfolgen und zu speichern.
SCORM-Nachrichten sind um einige Schlüsselelemente herum strukturiert:
1. **Das Lernziel**: Stellt den Lerninhalt oder die Lernressource dar (z. B. eine Lektion oder ein Quiz).
2. **Die Aktionen des Lernenden**: umfasst Aktionen wie das Starten von Inhalten, das Voranschreiten im Modul oder die Interaktion mit Fragen und Tests.
3. **Ergebnisse**: Enthält Daten wie die Endpunktzahl, den Abschlussstatus (abgeschlossen oder nicht) und die Zeit, die für jede Aktivität aufgewendet wurde.
SCORM-Nachrichten werden häufig im XML-Format ausgetauscht und im LMS gespeichert, wo die Lerngeschichte jedes Lernenden aufzeichnet wird und Berichte über den Fortschritt abgelegt werden.

- Beispiel für eine SCORM-Nachricht.

Eine SCORM-Nachricht könnte wie folgt strukturiert sein:

- Startet das Lernmodul: cmi.launch_data

- Verstrichene Zeit: cmi.core.session_time

- Abschlussstatus: cmi.core.lesson_status (kann "completed", "incomplete" usw. angeben).

- Punktzahl: cmi.core.score.raw, um die in einem Test erzielte Punktzahl anzugeben.

- Vergleich mit xAPI

Obwohl SCORM ein weit verbreiteter Standard im Bereich der LMS war, hat er einige Einschränkungen, wie z. B. das Fehlen von Offline-Tracking und eine eingeschränkte Kompatibilität mit LMS-Umgebungen. Das neuere xAPI ("Experience API") wurde entwickelt, um die Möglichkeiten des Trackings zu erweitern. Es ermöglicht die Verfolgung von Interaktionen über das LMS hinaus, indem es Online- und Offline-Interaktionen in verschiedenen Lernumgebungen integriert.

LTI-Analyse :

- Was ist eine LTI-Nachricht?

Eine LTI-Nachricht, oder "Learning Tools Interoperability", ist ein Kommunikationsstandard, der vom IMS Global Learning Consortium entwickelt wurde, um die Integration externer Lerninhalte und -tools in Lernmanagementsysteme (LMS) zu erleichtern. Mithilfe von LTI können Lernplattformen mit Anwendungen von Drittanbietern - wie Videokonferenztools, interaktiven Quizzes oder Simulationen - verbunden werden, ohne dass die Benutzer neue Konten anlegen oder sich erneut anmelden müssen. LTI vereinfacht und sichert die Lernerfahrung, indem es verschiedene Bildungsdienste und -tools innerhalb einer einzigen Plattform verbindet.

LTI-Nachrichten funktionieren über einen sicheren Informationsaustausch, der auf dem OAuth-Protokoll basiert, einem Authentifizierungs- und Autorisierungsmechanismus, der verwendet wird, um sicherzustellen, dass nur autorisierte Benutzer auf Inhalte zugreifen können. Wenn ein Lernender vom LMS aus auf einen externen Inhalt oder ein externes Tool zugreift, sendet das System eine LTI-Nachricht, um den Benutzer zu authentifizieren, die erforderlichen Informationen auszutauschen und den Inhalt oder das externe Tool in das LMS zu laden.

LTI-Nachrichten beinhalten mehrere wesentliche Elemente:

1. **Benutzer**: Informationen über den Lernenden oder Lehrer, der mit dem Tool interagiert, die aus Gründen der Vertraulichkeit oft auf wesentliche Informationen beschränkt sind.
2. **Lernkontext**: Details über den Kurs oder das Modul, in dem das Tool verwendet wird, um eine Personalisierung der Erfahrung zu ermöglichen.
3. **Benutzerrolle**: Gibt an, ob der Benutzer ein Lernender, ein Lehrer oder ein Administrator ist, was die Zugriffsrechte bestimmt.
4. **Ergebnisrückmeldung** (optional): Wenn das externe Tool eine Bewertung des Nutzers ermöglicht (z. B. über ein Quiz), können die Ergebnisse an das LMS zurückgesendet werden, damit der Fortschritt festgehalten wird.

- Beispiel für eine LTI-Nachricht

In einem Anwendungsszenario könnte eine LTI-Nachricht die folgenden Informationen enthalten:
- Benutzer: user_id=12345 (eindeutige Benutzerkennung)
- Rolle: roles= Instructor (oder "Learner" für einen Schüler).
- Kurskontext: context_id=course-001 (Kennung des Kurses oder Moduls).
- Notenrückmeldung: lis_result_sourcedid=score-12345 (wenn das Tool eine Punktzahl an das LMS sendet).

- Vorteile von LTI

Der Hauptvorteil von LTI besteht darin, dass es die Integration von externen Tools und Inhalten in LMS vereinfacht und gleichzeitig eine nahtlose Nutzererfahrung gewährleistet. Mithilfe von LTI-Nachrichten können Einrichtungen ein reichhaltigeres und vielfältigeres Lernerlebnis bieten, ohne dass für jede Integration mehrere Authentifizierungsprozesse oder komplexe technische Entwicklungen erforderlich sind.

- Vergleich mit SCORM und XAPI

Im Gegensatz zu SCORM und XAPI, die Standards für die Verfolgung von Lerndaten sind, ist LTI ein Integrationsstandard, der darauf abzielt, verschiedene Lernwerkzeuge in einer zentralen Umgebung zu verbinden. XAPI und SCORM konzentrieren sich mehr auf die Verfolgung der Interaktionen des Lernenden, während LTI sich auf die Authentifizierung und den Zugriff auf externe Tools und Inhalte konzentriert.

GS1 XML-Studie

GS1 XML ist ein internationaler Standard, der die Datenkommunikation zwischen Unternehmen unter Verwendung des XML-Formats ("eXtensible Markup Language") ermöglicht. Er wurde von der GS1-Organisation entwickelt, die auch die Barcodes und andere Handelsstandards hervorgebracht hat. Ziel dieses Standards ist es, eine bessere Interoperabilität zwischen Computersystemen zu gewährleisten und so den Informationsaustausch in komplexen Lieferketten zu erleichtern.

Ziele von GS1 XML

GS1 XML zielt darauf ab, den Informationsaustausch zu standardisieren, um :

1. Kommunikationsfehler zwischen den Systemen der verschiedenen Handelspartner **zu reduzieren.**
2. **Die Prozesse in der Lieferkette zu optimieren**, indem der Datenaustausch schneller und effizienter gestaltet wird.
3. **Die Integration neuer Geschäftspartner** durch eine standardisierte Kommunikationssprache **zu erleichtern.**
4. **Die Transparenz der Informationen** in den Warenströmen **erhöhen.**

Architektur und Struktur von GS1 XML

GS1 XML basiert auf einer standardisierten Architektur, die verschiedene Arten von Nachrichten umfasst, die mehrere Aspekte der Lieferkette abdecken. Jede Nachricht folgt einer Struktur, die in XML-Schemata festgelegt ist. Hier sind einige Schlüsselkomponenten :

- **Nachrichtenköpfe**: Sie enthalten Informationen wie den Nachrichtentyp, die Identifikation von Absender und Empfänger sowie das Übertragungsdatum.
- **Nachrichtentext**: Er enthält spezifische Informationen, die sich auf das logistische Ereignis beziehen, wie Versanddetails oder den Wareneingang.
- **GS1 Codes**: Verwendung von GTIN (Global Trade Item Number), SSCC (Serial Shipping Container Code) und GLN (Global Location Number) zur eindeutigen Identifizierung von Produkten und Orten.

Beispiel für eine GS1 XML-Nachricht

Hier ein vereinfachtes Beispiel einer XML-Nachricht für eine Bestellung (Order) :

<Order><Header><MessageID>123456</MessageID><CreationDate>2024-10-27</CreationDate></Header><OrderDetails><Buyer><GLN>1234567890123<./GLN></Buyer><Supplier><GLN>9876543210987</GLN></Supplier><OrderLine><GTIN>00012345678905</GTIN><Quantity>100</Quantity><Price>25.00</Preis></OrderLine></OrderDetails></Order>.

Kopieren

Arten von GS1 XML-Nachrichten

GS1 XML Nachrichten lassen sich je nach Verwendungszweck in verschiedene Kategorien unterteilen. Hier einige Beispiele:

1. **Bestellung (Order)**: Zum Ausstellen von Bestellungen.
2. **Versandbenachrichtigung (Despatch Advice)**: um den Versand von Waren anzukündigen.
3. **Warenempfang (Receiving Advice)**: um den Erhalt einer Sendung zu bestätigen.
4. **Rechnung (Invoice)**: Zum Austausch von Rechnungsinformationen.

Jeder Nachrichtentyp folgt einem standardisierten Format, das modifiziert werden kann, um es an die spezifischen Bedürfnisse der Unternehmen anzupassen.

Anwendungen von GS1 XML

GS1 XML wird in verschiedenen Branchen eingesetzt, u. a. :

- **Einzelhandel**: um den Fluss von Bestellungen, Sendungen und Empfängen zu verwalten.
- **Gesundheitswesen**: Zur Verfolgung von Medikamenten und medizinischen Hilfsmitteln in der Lieferkette.
- **Lebensmittelindustrie**: um die Rückverfolgbarkeit von Lebensmitteln zu gewährleisten.
- **E-Commerce**: um den Datenaustausch zwischen Partnern zu standardisieren.

Vorteile der Verwendung von GS1 XML

- **Erhöhte Interoperabilität**: Kompatibel mit verschiedenen ERP-Systemen und anderen Logistikanwendungen.
- **Geringere Kosten und Fehler**: Dank einer standardisierten Sprache und eines maschinenlesbaren Formats werden Kommunikationsfehler minimiert.
- **Bessere** Übersicht: Unternehmen können sich in Echtzeit einen Überblick über ihre Bestände, Sendungen und Verkäufe verschaffen.
- **Einhaltung regulatorischer Anforderungen**: GS1 XML wird in einigen Branchen häufig aus Gründen der Rückverfolgbarkeit und Transparenz gefordert.

Schlussfolgerung

GS1 XML ist ein mächtiges Werkzeug für Unternehmen, die die Effizienz ihrer Lieferketten steigern wollen. Seine zunehmende Einführung in verschiedenen Branchen zeugt von seiner Bedeutung in einem zunehmend globalisierten Geschäftsumfeld. Durch die Standardisierung des Datenaustauschs bietet GS1 XML eine zuverlässige und flexible Lösung, die den vielfältigen Bedürfnissen moderner Unternehmen gerecht wird.

Zusatz 3 zu 2. Empfehlungen zu KI

Die wichtigste Frage ist, ob Sie eine lokale KI oder eine KI von Drittanbietern verwenden wollen. Die Wahl wird sich auf verschiedene Aspekte des Projekts auswirken:

1. Sicherheit

Wir empfehlen, den direkten Zugriff auf die KI zu beschränken, um das Risiko von Prompt-Injection-Angriffen oder böswilligem Hijacking deutlich zu verringern. Dieser Ansatz erhöht den Schutz sensibler Daten und gewährleistet eine bessere Kontrolle über die Funktionsweise des Modells. Es ist besser, die KI nur intern für die automatische Generierung von Metadaten zu nutzen, um die Sicherheit zu wahren und gleichzeitig die Qualität und Konsistenz der Daten zu verbessern.

2. Vertraulichkeit der Daten

Wir empfehlen, eine lokale KI zu verwenden, um die volle Kontrolle über den Datenschutz und die Datensicherheit zu haben und zu vermeiden, dass Daten über externe Server geleitet werden. Lösungen von Drittanbietern können zwar aufgrund ihrer einfachen Implementierung attraktiv sein, bedeuten aber häufig, dass die Informationen zu Anbietern übertragen und dort gespeichert werden, den anderen Gesetzen oder Sicherheitsrichtlinien unterliegen. Im Hinblick auf den Schutz sensibler Daten ist es daher besser, trotz der Kosten und der technischen Komplexität, die dies mit sich bringen kann, dem internen Hosting und der kontrollierten Infrastruktur den Vorzug zu geben.

3. Nutzung durch die verschiedenen Partner

Wenn mehrere Partner das KI-System anfordern, müssen Sie sich darauf einstellen, ein großes Volumen an Inferenzanfragen zu bewältigen, was zu Engpässen führen und die Reaktionsfähigkeit beeinträchtigen kann. Eine höhere Anzahl gleichzeitiger Anrufe treibt auch die Ausgaben für die Infrastruktur in die Höhe, da mehr Rechenleistung benötigt wird.

4. RPGD

Wenn Sie sich für eine lokale Lösung entscheiden, behalten Sie die volle Kontrolle über die Verarbeitung und Speicherung Ihrer Daten, was die Einhaltung der DSGVO erheblich erleichtert. Diese Art des Hostings verringert das Risiko eines unrechtmäßigen Datentransfers außerhalb Deutschlands (oder der EU) und ermöglicht eine bessere Kontrolle über Zugriffe,

Logs und die Verwaltung von Einwilligungen. Sie trägt somit dazu bei, das Vertrauen der Nutzer zu stärken und die Abhängigkeit von Drittanbietern zu begrenzen, während sie gleichzeitig die Rückverfolgbarkeit und die Sicherheit sensibler Informationen verbessert.

5. Risiken

Der Einsatz von KI zur Generierung von Metadaten ist mit mehreren Risiken verbunden, darunter algorithmische Verzerrungen aufgrund der Qualität und Repräsentativität der Trainingsdaten, die die Relevanz und Objektivität der erzeugten Informationen beeinflussen können. Daher ist es von entscheidender Bedeutung, das richtige Modell zu wählen und Mechanismen zur regelmäßigen Überwachung und Bewertung der Ergebnisse einzurichten.

6. Modellempfehlung (01/2025)

Im Hinblick auf KI von Drittanbietern ist das von OpenAI erstellte Modell "o1" das effizienteste Modell, wie die Ergebnisse mehrerer unabhängiger Benchmarks zeigen. Die Größe seines maximalen Kontexts ist ausreichend, um verschiedene Metadaten zu generieren. Es ist auch möglich, ihn für bestimmte Aufgaben zu fine-tunen. Es ist jedoch wichtig zu beachten, dass dieses Modell sehr teuer ist.

Beim lokalen Hosting ermöglicht die große Auswahl an Modellen die Wahl eines Modells, das der Infrastruktur und den Bedürfnissen entspricht.

Weltweit bekannte Unternehmen wie Meta stellen Open-Source-Modelle wie LLama3 zur Verfügung, die auf 70 Milliarden Parametern basieren, aber die Infrastruktur, die für den Betrieb dieses Modells erforderlich ist, ist sehr groß.

Ein Modell, das in letzter Zeit aufgrund seiner Leistung und Leichtigkeit in aller Munde ist, ist DeepSeek, das bei einigen Aufgaben mit o1 konkurrieren kann. Es ist von 1,5 bis 671 Milliarden Parametern verfügbar.

7. Ethische Betrachtung

Aus ethischer Sicht wirft der Einsatz von KI zur Generierung von Metadaten insbesondere die Frage der Verzerrung auf: Wenn die Trainingsdaten oder die zugrunde liegenden Algorithmen verzerrt sind, kann dies zu einer unfairen oder diskriminierenden Klassifizierung führen.

3. POC und Analysen zu den neuen Abläufen bei der Einspeisung von Verlagskatalogen (ETL und Staging Area)

3.1 Beschreibung

1. Hintergrund

a. Katalogumgebung und MBR

Im Rahmen des MBR-Projekts und wurde eine zentrale Katalogdatenbank gefordert, die es ermöglicht, alle technischen Informationen zu den verschiedenen digitalen Ressourcen der Verlage zu enthalten, um sie an verschiedene Kunden des Systems verteilen zu können.

b. Ziele

Der Proof of Concept (POC) soll zeigen, wie effizient es ist, die Produktdatenblätter der Verlage in einen einheitlichen Katalog zu importieren, indem verschiedene Austauschmethoden EDI (Electronic Data Interchange) verwendet werden. Ziel dieser Studie ist es, die Bereitstellung dieser wichtigen Informationen zu optimieren.

Zusätzlich zu diesem POC bieten wir auch eine Analyse anderer Importmöglichkeiten an, die im NPB-Kontext angeboten werden können.

Wir untersuchen drei Fälle:

1. **Automatisierung von EDI-Sendungen für die Informationssysteme der Herausgeber.**
    - **Hintergrund**: Einige Herausgeber verfügen über Informationssysteme, die den Versand von EDI-Nachrichten an ihre Geschäftspartner automatisieren können.

- **Ziel**: Integration dieser EDI-Nachrichten in den Katalog unter Verwendung der verschiedenen vorhandenen Modi, z. B. des standardisierten ONIX-XML-Formats oder über ein ETL für proprietäre Formate. Diese Integration soll eine reibungslose und konforme Übertragung der Informationen aus den Produktblättern gewährleisten.

2. **Verwaltung von Flat Files (Typ CSV) für kleine Strukturen**
   - **Hintergrund**: Kleine Strukturen verfügen zwar nicht über eine Automatisierung des EDI-Versands, sind aber in der Lage, Flat Files mit Informationen aus Produktdatenblättern zu generieren.
   - **Ziel**: Es soll ein Prozess eingeführt werden, der die Integration dieser Flat Files in den Katalog ermöglicht und so sicherstellt, dass die Informationen aus den Produktblättern für das MBR-Netzwerk zugänglich und nutzbar sind. Dieser Prozess wird über eine sichere Webschnittstelle implementiert.
3. **Alternative Verwaltung für kleinere Strukturen**
   - **Hintergrund**: Kleinere Strukturen benötigen eine alternative Lösung für die Verwaltung von Produktdatenblättern, da sie weder über EDI-Automatisierung noch über die Fähigkeit zur Erzeugung von Flat Files verfügen.
   - **Ziel**: Entwicklung einer sicheren Webschnittstelle (wie oben für Flat Files erwähnt), die die vollständige Verwaltung von Produktdatenblättern ermöglicht, einschließlich Erstellen, Bearbeiten, Duplizieren, Archivieren und Löschen. Diese Schnittstelle soll es auch kleineren Strukturen ermöglichen, ihre Produktinformationen auf effiziente und sichere Weise zur Verfügung zu stellen.

2. Systemarchitektur und Datenfluss

a. Externe Datenströme

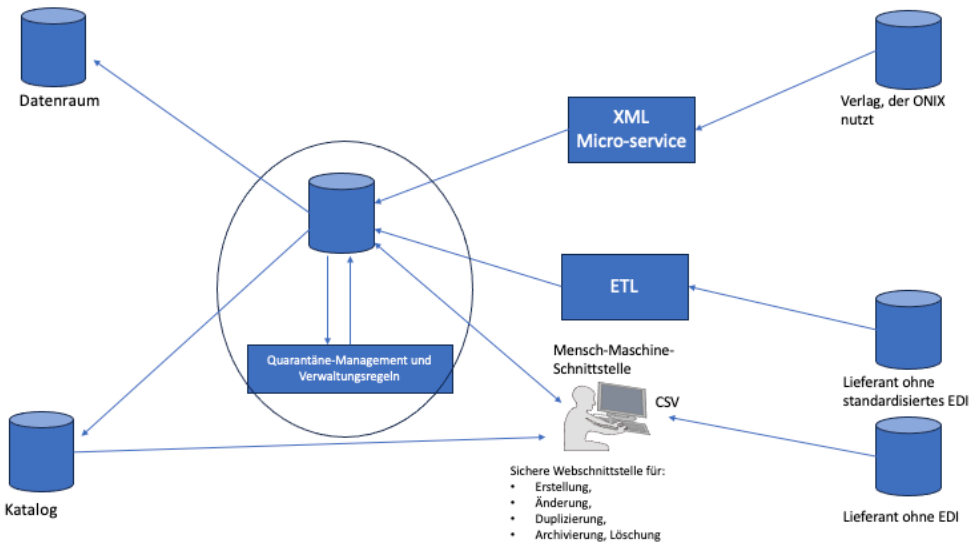
Es ist von entscheidender Bedeutung, robuste Sicherheitsmaßnahmen zum Schutz sensibler Informationen einzuführen.

Zu diesem Zweck wurde beschlossen, eine Zwischendatenbank zu implementieren, damit die Ein- und Ausgänge von Informationen, die von außerhalb des Informationssystems "Synapse" stammen, nicht direkt in die Hauptdatenbank des Katalogs integriert werden.

Um dieses Ziel zu erreichen, wurde ein zwischengeschaltetes ETL-Set eingerichtet, das aus folgenden Elementen besteht:

a. Eine dedizierte Datenbank zur Speicherung der Zwischeninformationen.
b. Ein System zur Verwaltung der Quarantäne und der Verwaltungsregeln (System zur Qualifizierung der eingehenden Daten, damit zuverlässige Informationen an alle MBR-Partner weitergeleitet werden können), zusammen mit einer Verwaltungsschnittstelle. Zunächst und im Rahmen unserer Studie wird diese Schnittstelle direkt in das Verwaltungssystem integriert, es wird jedoch empfohlen, sie zu einem späteren Zeitpunkt auf eine sichere Schnittstelle zu übertragen.

Der Zugriff auf alle Katalogdaten wird über den Datenraum durch die Datenbank des zwischengeschalteten ETL erfolgen. Dieser Ansatz gewährleistet eine sichere und effiziente Datenverwaltung und erleichtert gleichzeitig den kontrollierten Zugriff auf die Daten und ihre Verarbeitung gemäß den geltenden Sicherheitsstandards.



Schritt 1: Erste Integration

- **Ziel**: Verbindung von Verlegern, die ONIX verwenden, und Anbietern, die kein standardisiertes EDI oder kein EDI verwenden.
- **Komponenten**:
    - **XML Microservice** : Ermöglicht die Verwaltung von Daten von Herausgebern, die das ONIX-Format verwenden.
    - **ETL**: Verarbeitet Daten von Anbietern, die kein standardisiertes EDI oder kein EDI verwenden, indem CSV-Dateien ausgewertet werden.
    - **Secure Web Interface (SMI)**: Ermöglicht die manuelle Erstellung von Daten**.**

Schritt 2: Zwischenverwaltung

- **Ziel**: Einführung eines zwischengeschalteten ETL, um die Daten zu zentralisieren und bestimmte Verwaltungsregeln anzuwenden.
- **Komponenten**:
    - **Intermediate ETL**: Führt die Quarantäneverwaltung durch und wendet die festgelegten Verwaltungsregeln an.
    - **XML-Mikroservice und klassischer ETL**: Versorgen den zwischengeschalteten ETL weiterhin mit ihren jeweiligen Daten.
    - **Secure Web Interface (MMI)**: Behält die gleichen Funktionen bei, um Daten im CSV1-Format zu verwalten.

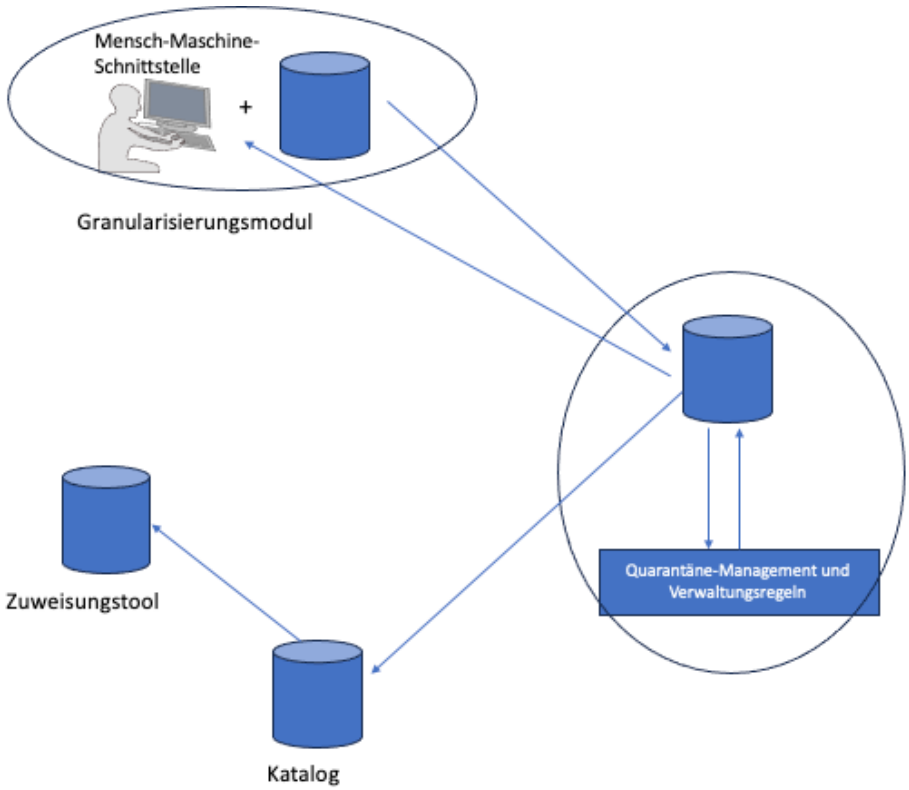
Schritt 3: Verbindung zu Datenraum und Katalog.

- **Ziel**: Erweiterung der Integration durch Verbindung des intermediären ETL mit dem Datenraum (zentraler Datenraum) und dem Katalog.
- **Komponenten** :
    - Der intermediäre ETL sendet die Daten aus Schritt 1 und 2 an den Katalog und den Datenraum und sorgt so für eine effiziente Zentralisierung.

Schritt 4: Finalisierung mit dem Katalog.

- **Ziel**: Integration des Katalogs in den intermediären ETL für eine vollständige Datenverwaltung.
- **Komponenten**:
    - Der Katalog versorgt das GUI mit Daten.
    - Das GUI bleibt funktional, um die manuelle Datenverwaltung durch die Benutzer zu ermöglichen, und speist direkt den intermediären ETL, der die Geschäftsregeln und Quarantänen anwendet, um:
        - Änderung
        - Duplizierung
        - Archivieren und Löschen.

b. Interne Datenströme.



Schritt 1: Granulator

- Dieser Schritt beinhaltet ein System namens *Granulator*, das eine Mensch-Maschine-Schnittstelle (MMI) und eine Datenbank miteinander verbindet.

- Der *Granulator* interagiert mit einem System zur Verwaltung von Quarantänen und Geschäftsregeln.
- Die Datenbank des *Granulators* sendet Informationen an das Quarantäneverwaltungsmodul, wo die Geschäftsregeln zur Verarbeitung der Daten angewendet werden.

Schritt 2: Katalog

- Ausgehend vom Quarantäneverwaltungsmodul und den Geschäftsregeln werden die verarbeiteten Daten an einen *Katalog* weitergeleitet.
- Der *Katalog* scheint eine Datenbank zu sein, die dazu dient, die durch die Geschäftsregeln gefilterten und validierten Informationen zu zentralisieren oder zu organisieren.

Schritt 3: Zuordnungswerkzeug

- Schließlich interagiert der *Katalog* mit einem Zuordnungswerkzeug.
- Dieses Zuweisungswerkzeug ruft Informationen aus dem *Katalog* ab, um sie in einem bestimmten Prozess zu verwenden, wahrscheinlich um Ressourcen oder Aufgaben anhand der verfügbaren Daten zuzuweisen oder zu verteilen.

Jeder Schritt stellt einen Informationsfluss zwischen verschiedenen Modulen oder Systemen dar, wobei die Verarbeitungslogik schrittweise erfolgt.

Es ist auch von entscheidender Bedeutung, die internen Flüsse des Synapse-Systems zu verstehen und zu verwalten.

Diese Flüsse lassen sich in zwei Hauptkategorien unterteilen:
Granulator-Fluss (siehe AP-7): Um die Daten aus diesem System zu qualifizieren, werden die Informationen in die Datenbank des zwischengeschalteten ETL integriert. In diesem Schritt wird die Konformität der Daten vor ihrer weiteren Verwendung überprüft.

Fluss zum Zuweisungstool (siehe AP-6): Um die Zuweisung digitaler Ressourcen zu erleichtern, werden die für diese Aktion notwendigen Informationen automatisch bereitgestellt. Dies gewährleistet eine effiziente Verwaltung der Ressourcen ohne manuelle Eingriffe.

Dieser Ansatz gewährleistet eine strenge und sichere Datenverwaltung und optimiert gleichzeitig die Prozesse der Qualifizierung und Zuweisung digitaler Ressourcen.

3. Hauptbestandteile des POC

Es wurde entschieden, die Machbarkeit des automatischen Imports zwischen den Verlagen anhand der standardisierten ONIX-Dateien und der Katalogdatenbank zu demonstrieren.

a. ONIX-Nachricht

Ursprünglich haben wir uns für die Verwendung von ONIX 2.0 entschieden, aber bislang arbeiten nur wenige Verleger mit diesem standardisierten Format im Verlagswesen. Wir empfehlen jedoch die Verwendung des neuesten Standards, nämlich ONIX 3.1.(https://www.editeur.org/93/release-3.0-downloads/).

b. XML-Microservice

Der XML-Microservice wird es ermöglichen, eine ONIX-Notiz in eine JSON-Datei umzuwandeln und die Datenbank des intermediären ETL mit dem Katalog und dem XML-Microservice zu füllen.

c. Zwischen-ETL,

Der Zwischen-ETL besteht aus zwei Hauptteilen:

- Einer Datenbank unter PostgreSQL.

- Einem Anwendungsprogramm, das die Verwaltung der Quarantänen und der zuvor festgelegten Verwaltungsregeln ermöglicht und so die Qualifizierung der Daten sicherstellt.

4. Datenfluss zwischen dem Granulator und der Katalogdatenbank,

   Um die Informationsmerkmale der vom Granulator erzeugten digitalen Ressourcen verfügbar zu machen, sendet der Granulator einen Informationsfluss an den Katalog, der mit dem zwischengeschalteten ETL übereinstimmt.

5. Datenfluss zur Zuweisungssoftware

   Bei der Synchronisierung mit der Zuweisungssoftware (und dem Katalog) werden alle in einer Tabelle erfassten Abteilungen über Änderungen mittels einer POST-Anfrage benachrichtigt.

6. Gesicherte Webschnittstelle zur Verwaltung von Produktdatenblättern.

   a. Import-Funktionalität

   Diese Funktion wird es KMU und MIT ermöglichen, ihre Produkt- und Artikelinformationen, die sie in das Netzwerk MBR integrieren möchten, über eine standardisierte Flat-File-Datei zur Verfügung zu stellen. Diese Informationen werden in den zwischengeschalteten ETL integriert, um die Qualifizierung der eingehenden Daten für den Gesamtkatalog zu ermöglichen.

   b. Schnittstelle, um die Produktinformationen zum Leben zu erwecken.

Um allen Akteuren im Bereich der Veröffentlichung digitaler Lernressourcen, einschließlich KMU, die Möglichkeit zu geben, ihre Produktinformationen verfügbar zu machen, wurde eine Mensch-Maschine-Schnittstelle entwickelt.

Diese Schnittstelle wird es den KMU und ETI auch ermöglichen, bestimmte nicht qualifizierende Informationen zu korrigieren.

i. Funktionalität für die Erstellung,

Diese Funktion wird die Erstellung von Produktdatenblättern über eine sichere Webschnittstelle ermöglichen, die automatisch die Geschäftsregeln integriert, um eine Quarantäne zu vermeiden.

ii. Funktionalitäten für die Bearbeitung,

Diese Funktion ermöglicht es, die Informationen der Produktkarte zu ändern, um sie zu qualifizieren (Beispiel: für eine Quarantäne), oder ihre Verfügbarkeit zu ändern, um sie für das gesamte Netzwerk MBR zugänglich zu machen oder nicht.

iii. Duplizierungsfunktionalität,

Bei fast identischen Artikeln wird vorgeschlagen, eine bereits vorhandene Produktkarte zu duplizieren, wobei der EAN-13-Code angegeben werden muss.

iv. Funktion Löschen/Archivieren.

Diese Aktion ermöglicht die Archivierung oder Löschung des Produktblatts und macht es für das gesamte Netzwerk nicht mehr verfügbar MBR .

7. Implementierung des POC

- Entwicklungs- und Einsatzphasen des POC.

- Konfiguration

application-local.yml: Konfiguration für die lokale Entwicklung application-MBR.yml: Konfiguration, die auf den MBR-Servern implementiert wird.

In der Konfiguration gibt es zwei Datasources :

- etl ist die Konfiguration der Verbindung zur Datenbank "etl".
- catalog ist die Konfiguration der Verbindung zur Datenbank "catalog".

Es gibt auch, zwei Konfigurationen für flyway (Migrationen) :

- etl mit dem Pfad zu Migrationen, der für die Datenbank und die Entitäten "etl" spezifisch ist (derzeit leer).
- catalog mit dem Pfad zu den datenbank- und entitätsspezifischen Migrationen "catalog".

Die Konfiguration zeigt an, dass flyway nicht aktiviert ist, das ist normal! Denn dies wird in einer datenbankspezifischen Konfiguration in der Klasse "KatalogMigration" verwaltet, zum Beispiel.

- Integration der Daten

Die Integration der in der etl-Datenbank vorhandenen Daten erfolgt in einem Runner "IntegrationRunner".

Führen Sie den Befehl aus: java -jar -Dspring.profiles.active= MBR target/etl-0.0.1.jar integration.

- Tests und Validierung

  - Testmethodologie zur Validierung der Machbarkeit und Effektivität von Feed-Flows.

  Bei jedem Schritt des Feeds ermöglichte eine Schnittstelle die Überprüfung der Verarbeitung.

  - Ergebnisse der Tests

- Schritt 1

  Der Herausgeber stellt uns eine ONIX-Datei mit den Informationen aus den Produktblättern der Ressourcen zur Verfügung.digitalen

- Schritt 2

articles.xml

```
            <MediaFileFormatCode>03</MediaFileFormatCode>
            <MediaFileLinkTypeCode>01</MediaFileLinkTypeCode>
            <MediaFileLink>https://res.cloudinary.com/pim-red/image/upload/ht/titles/covers/W1803
        </MediaFile>
        <Publisher>
            <PublishingRole>01</PublishingRole>
            <NameCodeType>04</NameCodeType>
            <NameCodeValue>12545</NameCodeValue>
            <PublisherName>Verlag</PublisherName>
        </Publisher>
        <PublicationDate>20200608</PublicationDate>
        <Measure>
            <MeasureTypeCode>01</MeasureTypeCode>
            <Measurement>297</Measurement>
            <MeasureUnitCode>mm</MeasureUnitCode>
        </Measure>
        <Measure>
            <MeasureTypeCode>02</MeasureTypeCode>
            <Measurement>210</Measurement>
            <MeasureUnitCode>mm</MeasureUnitCode>
        </Measure>
        <SupplyDetail>
            <SupplierIdentifier>
                <SupplierIDType>04</SupplierIDType>
                <IDValue>12545</IDValue>
            </SupplierIdentifier>
            <SupplierName>Verlag</SupplierName>
            <SupplierRole>00</SupplierRole>
            <ProductAvailability>20</ProductAvailability>
            <Price>
                <PriceTypeCode>04</PriceTypeCode>
                <PriceAmount>5.95</PriceAmount>
                <CurrencyCode>EUR</CurrencyCode>
                <CountryCode>DE</CountryCode>
                <TaxRateCode1>R</TaxRateCode1>
                <PriceEffectiveFrom>20240101</PriceEffectiveFrom>
            </Price>
            <Price>
                <PriceTypeCode>04</PriceTypeCode>
                <PriceAmount>6.00</PriceAmount>
                <CurrencyCode>EUR</CurrencyCode>
                <CountryCode>AT</CountryCode>
                <TaxRateCode1>R</TaxRateCode1>
            </Price>
            <Price>
                <PriceTypeCode>04</PriceTypeCode>
                <PriceAmount>5.95</PriceAmount>
                <CurrencyCode>EUR</CurrencyCode>
                <CountryCode>DE</CountryCode>
                <TaxRateCode1>R</TaxRateCode1>
                <PriceEffectiveFrom>20230101</PriceEffectiveFrom>
                <PriceEffectiveUntil>20231231</PriceEffectiveUntil>
            </Price>
        </SupplyDetail>
    </Product>
    </ONIXMessage>
```

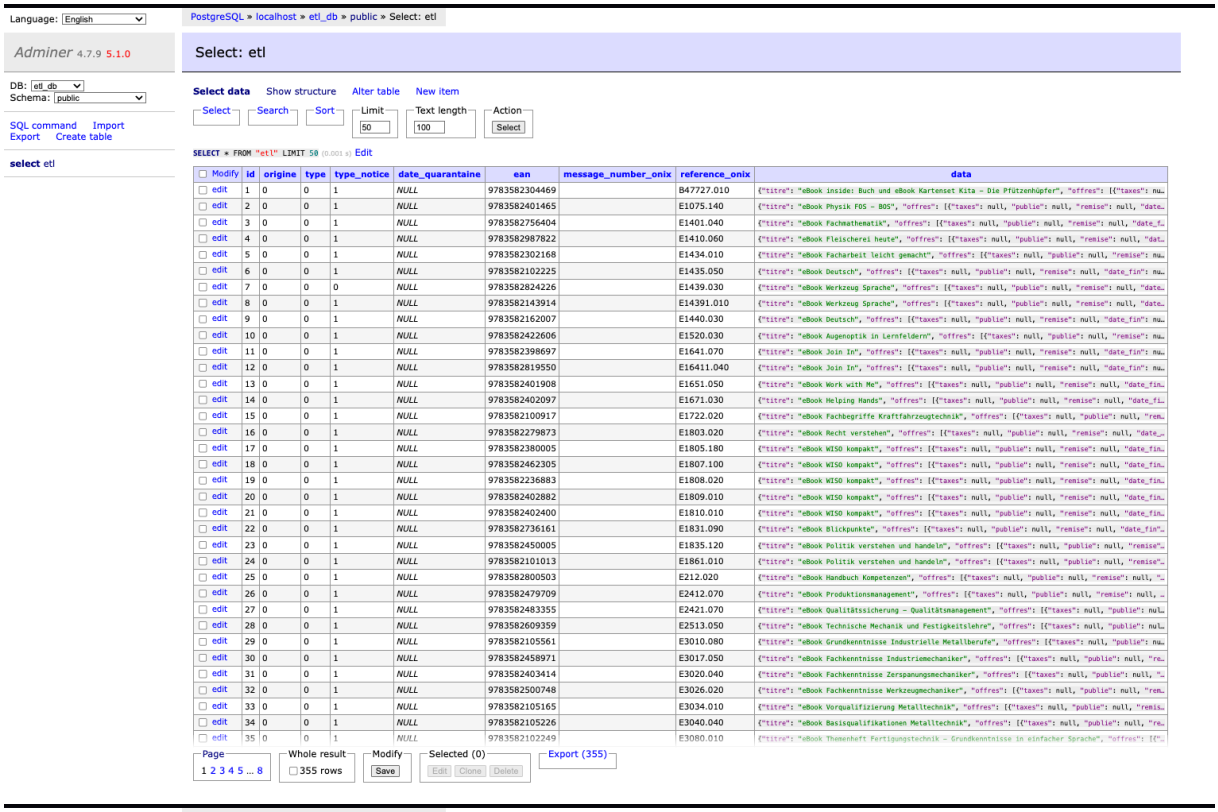
articles.xml

```
<MainSubject sourcename="Publisher">
    <MainSubjectSchemeIdentifier>93</MainSubjectSchemeIdentifier>
    <SubjectSchemeVersion>1.0</SubjectSchemeVersion>
    <SubjectCode>YP</SubjectCode>
</MainSubject>
<Subject>
    <SubjectSchemeIdentifier>24</SubjectSchemeIdentifier>
    <SubjectSchemeName>VLB-Sachgruppen</SubjectSchemeName>
    <SubjectCode>111</SubjectCode>
    <SubjectHeadingText>VLB-Schulbuch</SubjectHeadingText>
</Subject>
<Subject>
    <SubjectSchemeIdentifier>20</SubjectSchemeIdentifier>
    <SubjectHeadingText>WISO</SubjectHeadingText>
</Subject>
<Subject>
    <SubjectSchemeIdentifier>20</SubjectSchemeIdentifier>
    <SubjectHeadingText>Lösung</SubjectHeadingText>
</Subject>
<Subject>
    <SubjectSchemeIdentifier>20</SubjectSchemeIdentifier>
    <SubjectHeadingText>Berufsschule</SubjectHeadingText>
</Subject>
<Subject sourcename="Publisher">
    <SubjectSchemeIdentifier>94</SubjectSchemeIdentifier>
    <SubjectSchemeVersion>1.0</SubjectSchemeVersion>
    <SubjectCode>1DFG</SubjectCode>
</Subject>
<Subject sourcename="Publisher">
    <SubjectSchemeIdentifier>94</SubjectSchemeIdentifier>
    <SubjectSchemeVersion>1.0</SubjectSchemeVersion>
    <SubjectCode>1DFA</SubjectCode>
</Subject>
<Subject sourcename="Publisher">
    <SubjectSchemeIdentifier>94</SubjectSchemeIdentifier>
    <SubjectSchemeVersion>1.0</SubjectSchemeVersion>
    <SubjectCode>1DFH</SubjectCode>
</Subject>
<Subject sourcename="Publisher">
    <SubjectSchemeIdentifier>97</SubjectSchemeIdentifier>
    <SubjectSchemeVersion>1.0</SubjectSchemeVersion>
    <SubjectCode>4C</SubjectCode>
</Subject>
<AudienceCode>04</AudienceCode>
<AudienceDescription>Schülerinnen und Schüler sowie Lehrkräfte an berufsbildenden und all
<OtherText>
    <TextTypeCode>01</TextTypeCode>
    <TextFormat>02</TextFormat>
    <Text>&lt;p&gt;Der eL&amp;ouml;ser im PDF-Format zu dem Lehr- und Arbeitsbuch "Recht
    br /&gt;&lt;/p&gt;</Text>
</OtherText>
<MediaFile>
    <MediaFileTypeCode>04</MediaFileTypeCode>
    <MediaFileFormatCode>03</MediaFileFormatCode>
    <MediaFileLinkTypeCode>01</MediaFileLinkTypeCode>
    <MediaFileLink>https://res.cloudinary.com/pim-red/image/upload/ht/titles/covers/W1803
</MediaFile>
```

articles.xml

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE ONIXMessage SYSTEM "http://www.editeur.org/onix/2.1/reference/onix-international.dtd">
<ONIXMessage release="2.1">
    <Header>
        <SenderIdentifier>
            <SenderIDType>04</SenderIDType>
            <IDValue>12545</IDValue>
        </SenderIdentifier>
        <FromCompany>Verlag</FromCompany>
        <FromPerson/>
        <FromEmail/>
        <SentDate>20250401</SentDate>
    </Header>
        <Product>
        <RecordReference>98031.010</RecordReference>
        <NotificationType>03</NotificationType>
        <ProductIdentifier>
            <ProductIDType>03</ProductIDType>
            <IDValue>9782374084657</IDValue>
        </ProductIdentifier>
        <ProductIdentifier>
            <ProductIDType>15</ProductIDType>
            <IDValue>9782374084657</IDValue>
        </ProductIdentifier>
        <ProductIdentifier>
            <ProductIDType>01</ProductIDType>
            <IDValue>18031</IDValue>
        </ProductIdentifier>
        <ProductForm>DG</ProductForm>
        <Title>
            <TitleType>01</TitleType>
            <TitleText>Lösungen zu Recht verstehen</TitleText>
            <Subtitle>in Ausbildung, Beruf und Alltag</Subtitle>
        </Title>
        <Contributor>
            <ContributorRole>A01</ContributorRole>
            <SequenceNumberWithinRole>1</SequenceNumberWithinRole>
            <PersonName>Julia Ruch</PersonName>
            <PersonNameInverted>Ruch, Julia</PersonNameInverted>
            <NamesBeforeKey>Julia</NamesBeforeKey>
            <KeyNames>Ruch</KeyNames>
        </Contributor>
        <EditionTypeCode>NED</EditionTypeCode>
        <EditionNumber>1</EditionNumber>
        <Language>
            <LanguageRole>01</LanguageRole>
            <LanguageCode>ger</LanguageCode>
        </Language>
        <NumberOfPages>10</NumberOfPages>
        <MainSubject>
            <MainSubjectSchemeIdentifier>26</MainSubjectSchemeIdentifier>
            <SubjectSchemeVersion>2.0</SubjectSchemeVersion>
            <SubjectCode>9830</SubjectCode>
        </MainSubject>
        <MainSubject sourcename="Publisher">
            <MainSubjectSchemeIdentifier>93</MainSubjectSchemeIdentifier>
            <SubjectSchemeVersion>1.0</SubjectSchemeVersion>
```

- Schritt 3



Language: English

Adminer 4.7.9 5.1.0

DB: etl_db
Schema: public

SQL command Import
Export Create table

select etl

PostgreSQL » localhost » etl_db » public » Select: etl

Select: etl

Select data Show structure Alter table New item

Select Search Sort Limit: 50 Text length: 100 Action: Select

SELECT * FROM "etl" LIMIT 50 (0.001 s) Edit

Modify	id	origine	type	type_notice	date_quarantaine	ean	message_number_onix	reference_onix	data
edit	1	0	0	1	NULL	9783582304469		B47727.010	{"titre": "eBook inside: Buch und eBook Kartenset Kita – Die Pfützenhüpfer", "offres": [{"taxes": nu…
edit	2	0	0	1	NULL	9783582401465		E1075.140	{"titre": "eBook Physik FOS – BOS", "offres": [{"taxes": null, "public": null, "remise": null, "date…
edit	3	0	0	1	NULL	9783582756404		E1401.040	{"titre": "eBook Fachmathematik", "offres": [{"taxes": null, "public": null, "remise": null, "date_f…
edit	4	0	0	1	NULL	9783582987822		E1410.060	{"titre": "eBook Fleischerei heute", "offres": [{"taxes": null, "public": null, "remise": null, "dat…
edit	5	0	0	1	NULL	9783582302168		E1434.010	{"titre": "eBook Facharbeit leicht gemacht", "offres": [{"taxes": null, "public": null, "remise": nu…
edit	6	0	0	1	NULL	9783582102225		E1435.050	{"titre": "eBook Deutsch", "offres": [{"taxes": null, "public": null, "remise": null, "date_fin": nu…
edit	7	0	0	0	NULL	9783582824226		E1439.030	{"titre": "eBook Werkzeug Sprache", "offres": [{"taxes": null, "public": null, "remise": null, "date…
edit	8	0	0	1	NULL	9783582143914		E14391.010	{"titre": "eBook Werkzeug Sprache", "offres": [{"taxes": null, "public": null, "remise": null, "date…
edit	9	0	0	1	NULL	9783582162007		E1440.030	{"titre": "eBook Deutsch", "offres": [{"taxes": null, "public": null, "remise": null, "date_fin": nu…
edit	10	0	0	1	NULL	9783582422606		E1520.030	{"titre": "eBook Augenoptik in Lernfeldern", "offres": [{"taxes": null, "public": null, "remise": nu…
edit	11	0	0	1	NULL	9783582398697		E1641.070	{"titre": "eBook Join In", "offres": [{"taxes": null, "public": null, "remise": null, "date_fin": nu…
edit	12	0	0	1	NULL	9783582819550		E16411.040	{"titre": "eBook Join In", "offres": [{"taxes": null, "public": null, "remise": null, "date_fin": nu…
edit	13	0	0	1	NULL	9783582401908		E1651.050	{"titre": "eBook Work with Me", "offres": [{"taxes": null, "public": null, "remise": null, "date_fin…
edit	14	0	0	1	NULL	9783582402097		E1671.030	{"titre": "eBook Helping Hands", "offres": [{"taxes": null, "public": null, "remise": null, "date_fi…
edit	15	0	0	1	NULL	9783582100917		E1722.020	{"titre": "eBook Fachbegriffe Kraftfahrzeugtechnik", "offres": [{"taxes": null, "public": null, "rem…
edit	16	0	0	1	NULL	9783582279873		E1803.020	{"titre": "eBook Recht verstehen", "offres": [{"taxes": null, "public": null, "remise": null, "date_…
edit	17	0	0	1	NULL	9783582380005		E1805.180	{"titre": "eBook WISO kompakt", "offres": [{"taxes": null, "public": null, "remise": null, "date_fin…
edit	18	0	0	1	NULL	9783582462305		E1807.100	{"titre": "eBook WISO kompakt", "offres": [{"taxes": null, "public": null, "remise": null, "date_fin…
edit	19	0	0	1	NULL	9783582236883		E1808.020	{"titre": "eBook WISO kompakt", "offres": [{"taxes": null, "public": null, "remise": null, "date_fin…
edit	20	0	0	1	NULL	9783582402882		E1809.010	{"titre": "eBook WISO kompakt", "offres": [{"taxes": null, "public": null, "remise": null, "date_fin…
edit	21	0	0	1	NULL	9783582402400		E1810.010	{"titre": "eBook WISO kompakt", "offres": [{"taxes": null, "public": null, "remise": null, "date_fin…
edit	22	0	0	1	NULL	9783582736161		E1831.090	{"titre": "eBook Blickpunkte", "offres": [{"taxes": null, "public": null, "remise": null, "date_fin"…
edit	23	0	0	1	NULL	9783582450005		E1835.120	{"titre": "eBook Politik verstehen und handeln", "offres": [{"taxes": null, "public": null, "remise"…
edit	24	0	0	1	NULL	9783582101013		E1861.010	{"titre": "eBook Politik verstehen und handeln", "offres": [{"taxes": null, "public": null, "remise"…
edit	25	0	0	1	NULL	9783582800503		E212.020	{"titre": "eBook Handbuch Kompetenzen", "offres": [{"taxes": null, "public": null, "remise": null, "…
edit	26	0	0	1	NULL	9783582479709		E2412.070	{"titre": "eBook Produktionsmanagement", "offres": [{"taxes": null, "public": null, "remise": null, …
edit	27	0	0	1	NULL	9783582483355		E2421.070	{"titre": "eBook Qualitätssicherung – Qualitätsmanagement", "offres": [{"taxes": null, "public": nul…
edit	28	0	0	1	NULL	9783582609359		E2513.050	{"titre": "eBook Technische Mechanik und Festigkeitslehre", "offres": [{"taxes": null, "public": nul…
edit	29	0	0	1	NULL	9783582105561		E3010.080	{"titre": "eBook Grundkenntnisse Industrielle Metallberufe", "offres": [{"taxes": null, "public": nu…
edit	30	0	0	1	NULL	9783582458971		E3017.050	{"titre": "eBook Fachkenntnisse Industriemechaniker", "offres": [{"taxes": null, "public": null, "re…
edit	31	0	0	1	NULL	9783582403414		E3020.040	{"titre": "eBook Fachkenntnisse Zerspanungsmechaniker", "offres": [{"taxes": null, "public": null, "…
edit	32	0	0	1	NULL	9783582500748		E3026.020	{"titre": "eBook Fachkenntnisse Werkzeugmechaniker", "offres": [{"taxes": null, "public": null, "rem…
edit	33	0	0	1	NULL	9783582105165		E3034.010	{"titre": "eBook Vorqualifizierung Metalltechnik", "offres": [{"taxes": null, "public": null, "remis…
edit	34	0	0	1	NULL	9783582105226		E3040.040	{"titre": "eBook Basisqualifikationen Metalltechnik", "offres": [{"taxes": null, "public": null, "re…
edit	35	0	0	1	NULL	9783582102249		E3080.010	{"titre": "eBook Themenheft Fertigungstechnik – Grundkenntnisse in einfacher Sprache", "offres": [{"…

Page: 1 2 3 4 5 … 8 Whole result: 355 rows Modify: Save Selected (0): Edit Clone Delete Export (355)

Language: English

Adminer 4.7.9 5.1.0

DB: etl_db
Schema: public

SQL command Import
Export Create table

select etl

PostgreSQL » localhost » etl_db » public » Select: etl

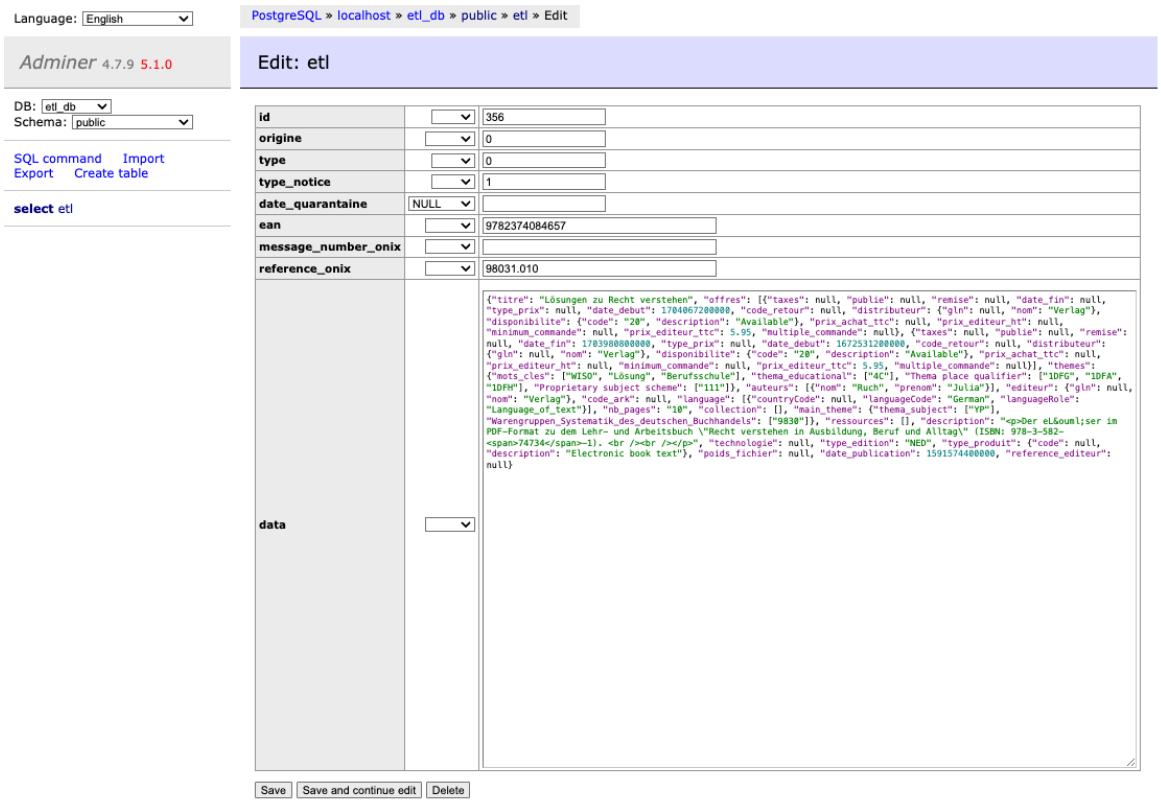
Select: etl

Select data Show structure Alter table New item

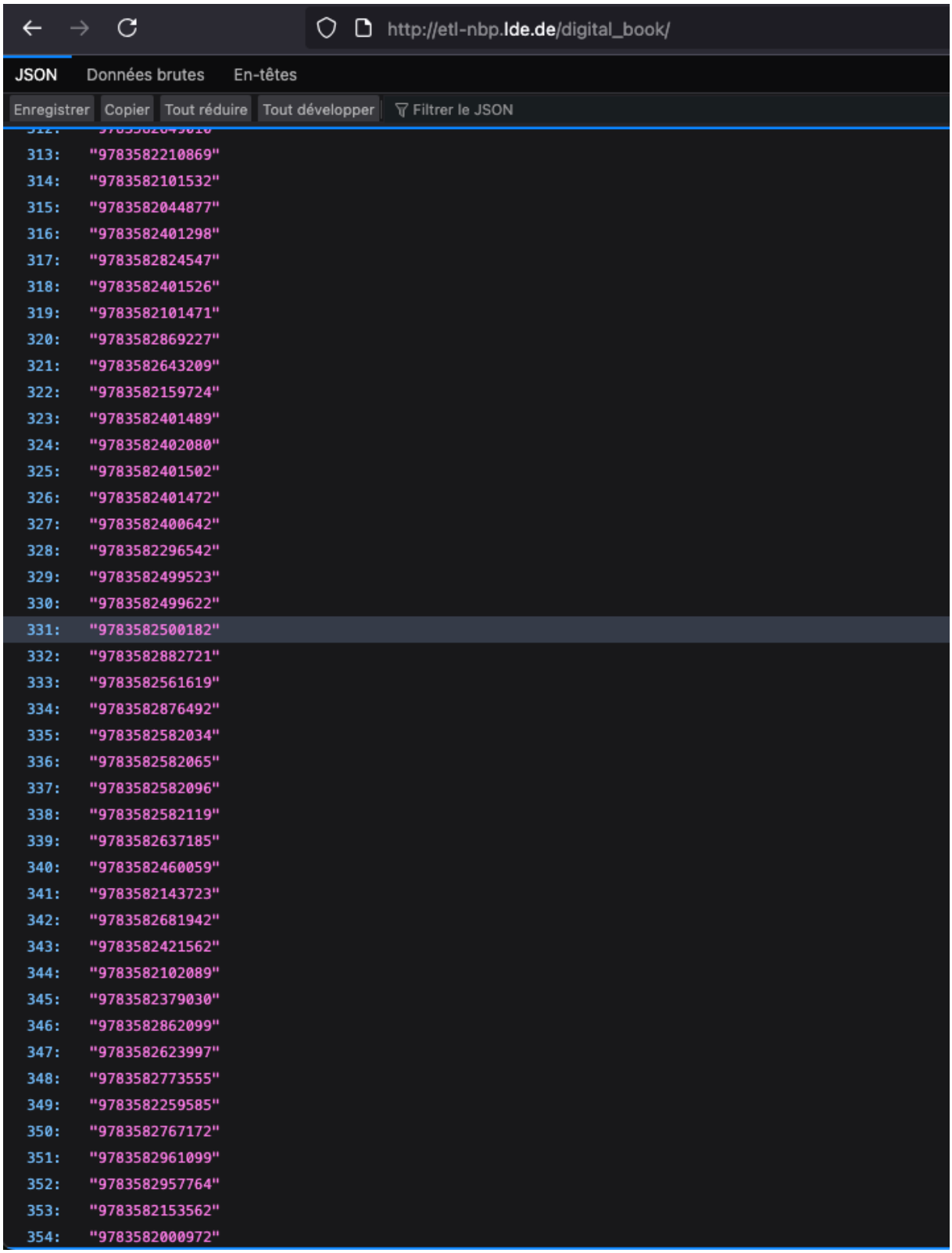
Select Search Sort Limit: 50 Text length: 100 Action: Select

SELECT * FROM "etl" LIMIT 50 (0.001 s) Edit

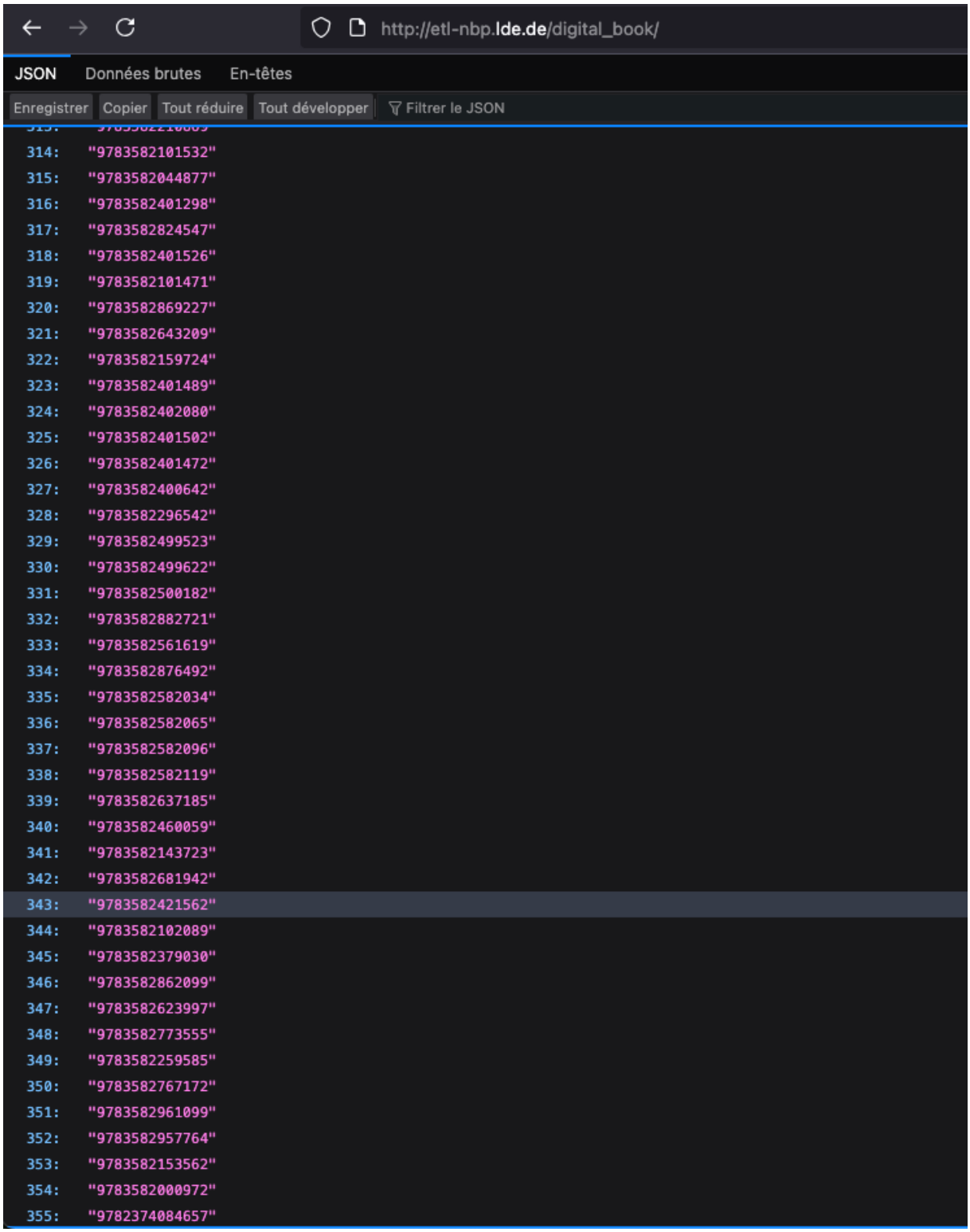
Page: 1 2 3 4 5 … 8 Whole result: 355 rows Modify: Save Selected (0): Edit Clone Delete Export (355)



- Schritt 4
  - Vor der Integration



- Nach der Integration



8. Ergebnisse und Diskussionen

- Analyse der Ergebnisse
    - Präsentation der Ergebnisse, die während des POC erzielt wurden.

  Bei jedem Schritt wurden Screenshots zur Verfügung gestellt.
    - Vergleich mit den ursprünglichen Zielen.

Die ursprünglichen Ziele wurden eingehalten und sind auf dem dedizierten MBR-Server verfügbar.

- Gelernte Lektionen
    - Aufgetretene Schwierigkeiten und gefundene Lösungen.

Das einzige Problem, das auftrat, war die Tatsache, dass deutsche Verleger kaum standardisierte EDI und/oder internationale GS1-Standards (Produktcodierung) verwenden, was uns dazu zwang, fingierte ONIX-Notizen zu erstellen.

- Empfehlungen für zukünftige Implementierungen.

Um den Datentransfer zwischen den verschiedenen Partnern von MBR effizient zu gestalten, wird empfohlen, auf Verlagsebene Vorarbeiten zu leisten zu :

- Internationale Kodierungsregeln, damit die digitale Ressource im gesamten MBR-System einen eindeutigen Code vom Typ GTIN 13 (Global Target Identification Number oder besser bekannt unter dem Begriff EAN13) haben kann,
- Die Befürwortung der Verwendung von standardisiertem EDI, trotz der Tatsache, dass das System "SYNAPSE" offen ist für den Import von "proprietären" Dateien, flachen Dateien und die manuelle Verwaltung von Karteikarten über eine sichere Schnittstelle ermöglicht.

9. Schlussfolgerung.

Der im Rahmen des Projekts MBR durchgeführte POC hat die Machbarkeit und Effizienz des Imports von Produktdatenblättern der Verlage in einen einheitlichen Katalog unter Verwendung verschiedener Datenaustauschmethoden (EDI, Flat Files und sichere Webschnittstellen) demonstriert. Die ursprünglichen Ziele wurden erreicht, und die erzielten Ergebnisse bestätigen die Relevanz der implementierten Lösungen.

Die wichtigsten Erkenntnisse aus diesem POC sind folgende:

1. **Effizienz der automatisierten Abläufe** : Die Integration von EDI-Nachrichten und Flat Files erwies sich als leistungsfähig und gewährleistete eine reibungslose und konforme Informationsübermittlung.
2. **Zugänglichkeit für alle Strukturen**: Die vorgeschlagenen Lösungen (gesicherte Webschnittstelle, manuelle Verwaltung) ermöglichen die Einbeziehung auch der kleinsten Strukturen, die über keine automatisierten Systeme verfügen.
3. **Anpassungsfähigkeit an Standards**: Obwohl einige Herausgeber noch keine internationalen Standards (wie ONIX oder GTIN 13) verwenden, wurden Anpassungen vorgenommen, um die Kompatibilität mit dem MBR-System zu gewährleisten.

4. Empfehlungen für die Zukunft :

- **Harmonisierung der Standards**: Ermutigen Sie die Herausgeber, internationale Standards (standardisiertes EDI, GTIN 13) zu übernehmen, um den Austausch zu vereinfachen und die Interoperabilität zu verbessern.
- **Stärkung der Sicherheit**: Aufrechterhaltung einer strengen Verwaltung der Datenströme über das zwischengeschaltete ETL und die sichere Schnittstelle, um die Vertraulichkeit und Integrität der Informationen zu gewährleisten.
- **Skalierbarkeit des Systems**: Weitere Entwicklung und Verbesserung der eingesetzten Tools, um den wachsenden Anforderungen des MBR-Netzwerks gerecht zu werden.

Zusammenfassend lässt sich sagen, dass dieses POC eine solide Grundlage für die zukünftige Einführung des einheitlichen Systems zur Verwaltung digitaler Ressourcen im Rahmen des MBR-Projekts darstellt und gleichzeitig eine Flexibilität bietet, die den verschiedenen Profilen von Verlegern gerecht wird.

3.2 Technische Dokumentation

1. ETL

Diese Anwendung ermöglicht die Umwandlung von Rohdaten aus der "etl"-Datenbank in strukturierte Daten im endgültigen Katalog.

2. Konfiguration

application-local.yml: Konfiguration für die lokale Entwicklung application-MBR.yml: Konfiguration, die auf den MBR-Servern eingerichtet wurde.

In der Konfiguration gibt es zwei Datasourcen:

- etl ist die Konfiguration für die Verbindung zur Datenbank "etl".
- catalog ist die Konfiguration für die Verbindung zur Datenbank "catalog".

Es gibt auch, zwei Konfiguration für flyway (migrations) :

- etl mit dem Pfad zu Migrationen, der für die Datenbank und die Entitäten "etl" spezifisch ist (derzeit leer).
- catalog mit dem Pfad zu den datenbank- und entitätsspezifischen Migrationen "catalog".

Die Konfiguration zeigt an, dass flyway nicht aktiviert ist, das ist normal! Denn dies wird in einer datenbankspezifischen Konfiguration in der Klasse "KatalogMigration" verwaltet, zum Beispiel.

3. Integration der Daten

Die Integration der in der etl-Datenbank vorhandenen Daten erfolgt in einem Runner "IntegrationRunner".

Führen Sie den Befehl aus: java -jar -Dspring.profiles.active= MBR target/etl-0.0.1.jar integration.

4. API

Starten Sie die API auf dem MBR-Server: java -jar -Dspring.profiles.active= MBR target/etl-0.0.1.jar.

- Adresse: http://etl-MBR.lde.de
- Authentifizierung :
  - username: MBR
  - password: MBR2025#
- Endpunkte:
  - /digital_book/ um eine Liste der EANs im Katalog zu erhalten.
  - /digital_book/{ean}, um Informationen über ein Handbuch anhand seiner EAN abzurufen.
  - /digital_book/integration, um die Integration von der API aus zu starten.

5. Kompilieren und Aktualisieren des Dienstes

./mvnw clean package -DskipTests cp target/etl-0.0.1.jar /var/www/etl.jar service etl restart

6. SSO, Rechte und Rechte-übertragung

1. Einführung

Meilenstein 4 ist Teil eines Prozesses zur Optimierung des Daten- und Rechteaustauschs zwischen der MBR-Plattform (Mein Bildungsraum) und ihren verschiedenen Partnern. Dabei konzentriert sich die Studie auf zwei grundlegende Aspekte: die Integration des LTI-Standards (Learning Tools Interoperability) und die Verwaltung der Benutzerrechte.

Hintergrund des Meilensteins

Das MBR-Ökosystem erfordert eine robuste Architektur, die eine effiziente Verwaltung von Benutzerrechten und eine reibungslose Interoperabilität zwischen den verschiedenen Partnerplattformen ermöglicht. Diese Architektur muss die Normen ISO 27001 für die Informationssicherheit und ISO 9001 für die Prozessqualität erfüllen.

Rahmen des Meilensteins

Der Umfang des Meilensteins ist in zwei verschiedene Teile unterteilt:

LTI POC (Meilenstein 4.1)

- Demonstration der LTI-Integration mit BookWidgets.
- Implementierung von Single Sign-On (SSO).
- Implementierung von Deep Linking für die Verwaltung von Ressourcen.

Verwaltung von Rechten (Meilenstein 4.2)

- Vernetzung zwischen den Systemen zur Rechteverwaltung.
- Standardisierung der Austauschformate
- Einführung von eindeutigen Identifikatoren für die Einrichtungen.

Ziele der technischen Machbarkeitsstudie

- Die Machbarkeit einer vollständigen LTI-Integration bewerten.
- Definition einer skalierbaren Architektur für die Rechteverwaltung.
- Technische Lösungen vorschlagen, die den Sicherheitsstandards entsprechen.
- Validierung der Möglichkeit einer Vernetzung zwischen den verschiedenen Systemen.

2. Methodologie

Ansatz für die Recherche

Die Studie wurde nach einem schrittweisen Ansatz durchgeführt:

9. Analyse der technischen und funktionalen Anforderungen
10. Bewertung der bestehenden Standards
11. Entwicklung von Proof-of-Concepts
12. Validierung der vorgeschlagenen Lösungen.

Verwendete Tools und Techniken

- Authentifizierungsprotokolle SSO und OIDC
- LTI-Standards für die Interoperabilität
- RESTful APIs für den Datenaustausch.
- Datawallet für die zentrale Verwaltung von Rechten.

3. Analyse der bestehenden Plattformen

Beschreibung der betroffenen Plattformen

Das MBR-Ökosystem basiert auf zwei Hauptkomponenten, die besonderer Aufmerksamkeit bedürfen. Einerseits wird der LTI-Standard beispielsweise durch die Anwendung PopLab implementiert, die als Plattform für die Verwaltung von Lerninhalten mit einer modernen Webschnittstelle dient, die externe Integrationen unterstützt. Andererseits sorgt das System Themis für die Verwaltung der Benutzerrechte, indem es eine Schnittstelle zum Datawallet für die Verwaltung der Profile bildet.

Identifizierte technische Einschränkungen

Die identifizierten technischen Einschränkungen beziehen sich hauptsächlich auf drei kritische Aspekte: die Notwendigkeit, die absolute Vertraulichkeit der personenbezogenen Daten zu wahren, die Leistungsanforderung für den Echtzeitaustausch zwischen den Systemen und das Gebot der Kompatibilität mit den verschiedenen Partnerplattformen.

4. Technische und regulatorische Anforderungen

Funktionale Spezifikationen

Die funktionalen Spezifikationen lassen sich in zwei verschiedene Bereiche unterteilen.

13. Für die LTI-Integration muss das System eine einmalige Benutzerauthentifizierung gewährleisten, eine nahtlose Integration externer Ressourcen ermöglichen und Deep Linking unterstützen.
14. In Bezug auf die Rechteverwaltung erfordert die Architektur eine standardisierte Formatierung der Nutzerdaten, ein System zur eindeutigen Identifizierung von Einrichtungen und robuste Mechanismen zur Synchronisierung von Rechten.

Überlegungen zur Sicherheit und zum Datenschutz

- Verschlüsselung des Datenaustauschs
- Verwaltung von Authentifizierungs-Tokens
- Schutz personenbezogener Daten gemäß der DSGVO.

5. Phasen der vorgeschlagenen Implementierung

1. **Vorbereitende Phase**
   - Einrichten der Umgebungen
   - Einrichtung der technischen Voraussetzungen
2. **Entwicklungsphase**
   - Implementierung der LTI-Konnektoren
   - Entwicklung der APIs für die Rechteverwaltung
3. **Testphase**

- Validierung der Integrationen
- Leistungs- und Sicherheitstests

4. **Phase der Bereitstellung**

- Schrittweise Einführung in die Produktion
- Schulung der Nutzerinnen und Nutzer

6. Ergebnis der Untersuchungen

Die Analyse der drei Anwendungsfälle (CF 4.2) führte zur Identifizierung der optimalen Lösung. Fall 3, eine Kombination aus OIDC und API, bietet die beste Antwort auf die ermittelten Anforderungen an die Rechteverwaltung und ist für LTI anwendbar . Dieser hybride Ansatz ermöglicht eine Feinsteuerung der Zugriffsrechte bei gleichzeitiger Aufrechterhaltung eines optimalen Sicherheitsniveaus durch die kombinierte Nutzung des Datawallet, von OIDC und einer dedizierten API.

Die Integration mit den bestehenden Tools von MBR erweist sich als besonders effizient, insbesondere mit Mein Bildungsraum für die Bereitstellung von Benutzerkennungen und dem Datawallet für die Verwaltung von Profilen und Berechtigungen. Die Lösung ermöglicht auch eine regelmäßige Aktualisierung der Informationen durch die "Token Refreshs" von OIDC.

7. Analyse der Risiken

Identifizierung der potenziellen Risiken

- Komplexität der Integration heterogener Systeme.
- Sicherheitsrisiken im Zusammenhang mit dem Datenaustausch
- Abhängigkeit von externen Systemen

Strategien zur Eindämmung

- Einführung von Fallback-Mechanismen
- Ausführliche Sicherheitstests
- Detaillierte Dokumentation der Prozesse.

8. Schlussfolgerung und Empfehlungen

Die gewählte Lösung stellt einen bedeutenden Fortschritt für das MBR-Projekt dar, indem sie ein robustes und sicheres digitales Bildungsökosystem etabliert. Der hybride Ansatz, der Datawallet, OAuth, LTI und eine dedizierte API kombiniert, bietet ein optimales Gleichgewicht zwischen Sicherheit, Flexibilität und Benutzerfreundlichkeit. Mit dieser Architektur lassen sich die Probleme der Verwaltung von Schulverzeichnissen, der Kommunikation und des sicheren Zugriffs auf Bildungsressourcen effektiv lösen.

Zusammenfassung der Ergebnisse

Die POCs haben die technische Machbarkeit der vorgeschlagenen Lösungen sowohl für die LTI-Integration als auch für die Rechteverwaltung nachgewiesen[43]. Die vorgeschlagene Architektur erfüllt die Anforderungen an Sicherheit und Leistung.

Abschließende technische Empfehlungen

Für eine erfolgreiche Umsetzung müssen vier Hauptachsen berücksichtigt werden. Erstens sollte die Einführung von Fall 3 für die Rechteverwaltung unter Verwendung von OIDC und APIs Vorrang haben.

Zweitens ist die Implementierung von Deep Linking LTI für die nahtlose Integration von Ressourcen von entscheidender Bedeutung.

Drittens muss die Standardisierung von Datenaustauschformaten nach festgelegten Standards etabliert werden.

Schließlich ist die Einführung eines Systems zur eindeutigen Identifizierung der Einrichtungen eine grundlegende Voraussetzung für das reibungslose Funktionieren des Ganzen.

[43]Die ausführliche Detaillierung der Ergebnisse kann auf Anfrage nachgeliefert werden.

Zusatz 1 zu 4.: Kommunikationsarchitektur und -standards

1. Einleitung

AP4.2 konzentriert sich speziell auf den Vorschlag einer gemeinsamen Kommunikationsarchitektur und -standards für alle NBP-Partner.
Im Zentrum dieses Projekts steht die Verwaltung personenbezogener Daten (PBD), mit besonderem Schwerpunkt auf der Sicherheit und der Einschränkung der Verbreitung von PBD.
Das Hauptziel von AP4.2 besteht darin, ein System zu entwerfen, das die Anmeldung von Nutzern und die Verwaltung von Rechten auf den Plattformen der NBP-Partner ermöglicht und gleichzeitig den Abruf der erforderlichen Einrichtungsverzeichnisse und Kontakte sicherstellt.

Das vorgeschlagene System zielt auf eine Vereinheitlichung der Rechteverwaltung ab, so dass sich jeder Nutzer entsprechend seinem Profil und seinen Rechten bei den verschiedenen NBP-Partnern anmelden kann. Dieser Ansatz beinhaltet die obligatorische Nutzung der von NBP bereitgestellten Tools, wie z. B. des Datawallet.

2. Rahmen des Projekts

Umfang und Ausschlüsse

AP4.2 konzentriert sich auf die Verwaltung von Benutzerrechten innerhalb der Partnerplattformen von NBP. Es ist wichtig zu beachten, dass dieses Projekt **nicht die Verwaltung von Nutzerlizenzen auf Ressourcen umfasst**, die separat in AP5.2 behandelt wird. Stattdessen konzentriert es sich auf die Konzeption eines Systems, das auf SSO-Verbindungen (Single Sign-On) und einem Mechanismus zur Verbreitung von Rechten basiert.

Vorgeschlagener Ansatz

Das geplante System basiert auf zwei Schlüsselelementen:

5. Die SSO-Verbindungen (Single Sign-On).
6. Eine API- oder Datawallet-basierte Architektur zur Verbreitung von Rechten. Die zentrale Idee besteht darin, das Datawallet bei der Anmeldung des Benutzers abzufragen, um die korrekt formatierten Rechteinformationen abzurufen.

Standardisierung und Interoperabilität

Um eine effektive Interoperabilität zwischen den verschiedenen Akteuren zu gewährleisten, schlägt das Projekt vor :

- Eine eingeschränkte Formatierung für die Speicherung und Nutzung von Benutzerfunktionen.
- Die Schaffung einer eindeutigen nationalen Kennung für jede Einrichtung, die potenziell auf einem Präfixsystem für jedes Bundesland basiert.

Spezifische Ziele

Die Hauptziele des vorgeschlagenen Systems sind:

7. Die Anmeldung von Nutzern und die Verwaltung von Rechten auf den Plattformen der NBP-Partner zu ermöglichen.
8. Den Abruf von Schulverzeichnissen für die Zuweisung von Lehrbüchern und Ressourcen zu erleichtern.
9. Ermöglichen Sie den Erhalt einer Kontaktmail pro Schule für technische und partnerschaftliche Aspekte.

Proof of Concept (POC)

Um die Machbarkeit des Projekts zu belegen, wird ein Proof of Concept entwickelt, der die Verbindung zwischen dem Themis-System (dem derzeit auf den EDL-Plattformen verwendeten Rechteverwaltungssystem) und dem Datawallet für die Nutzer veranschaulicht.

Untersuchte Anwendungsfälle

Die Studie wird sich auf drei mögliche Fälle der Rechteverwaltung stützen:

10. Verwaltung durch SSO

11. Verwaltung durch eine externe API
12. Verwaltung der Zugriffe durch OIDC und API.

5. Untersuchte Anwendungsfälle

Voraussetzungen

Für jeden der im Folgenden entwickelten Fälle müssen bestimmte technische Voraussetzungen geschaffen werden, die für ihre Funktionsweise notwendig sind. Wir sehen drei davon:

1. Einrichtung einer eindeutigen ID pro Lernzentrum: Eine eindeutige und allen Partnern vorgeschriebene ID erleichtert die Kommunikation zwischen den Anbietern, den Nutzern und den Lernzentren. Diese ID muss nicht standardisiert sein, aber sie muss eindeutig sein. Eine zweiteilige Kennung, bei der der erste Teil das Bundesland und der zweite Teil die Bildungseinrichtung definiert, würde daher eine große Flexibilität ermöglichen.
2. Wir halten die Einführung eines Leitdokuments für wichtig: Dieses Dokument muss die Profile, Rechte und Rollen definieren, die bei der Vernetzung verfügbar sind und verwendet werden. Jeder Partner kann dann seine eigenen Tabellen mit den Rechten und Profilen erstellen, die in seinen eigenen Systemen verwendet werden.
3. Wir sind davon überzeugt, dass nur NBP das Werkzeug zur Verfügung stellen kann, das die Erstellung und Zuweisung von Profilen, Rechten und Berechtigungen für jeden Benutzer ermöglicht. Dieser zentrale Verwaltungspunkt garantiert NBP die vollständige Kontrolle über die bereitgestellten Ressourcen.

5.1 Fall 1: Rechteverwaltung durch SSO

In diesem ersten Fall untersuchen wir die Verwendung von SSO für die Verwaltung und Übertragung von Rechten. Es werden keine weiteren Systeme hinzugefügt.

So werden über den JSON-Rückkanal im Anschluss an die SSO-Verbindung die Profile und Rechte der Nutzer an die Partnerplattform übermittelt.

Dieses System ermöglicht den Zugriff auf die Wallet über die eindeutige Benutzer-ID und schränkt die Verbreitung personenbezogener Informationen so weit wie möglich

ein. Da SSO-Protokolle in der Regel sehr sicher sind, hat diese Methode den Vorteil, dass sie ein gutes Sicherheitsniveau der Benutzerinformationen gewährleistet.

Einschränkungen und Probleme

Zugang zu einem Minimum an Daten Einrichtung

Im Rahmen einer Leistungsbeziehung mit Schulen ist es wichtig, dass die Anbieter, die die vorgeschriebenen Dienstleistungen erbringen, direkt kontaktiert werden können. Wenn ein Vertrag direkt mit einer Schule oder einer Bildungseinrichtung eingerichtet wird, ist dies kein Problem, da die Vertragsbeziehung die Informationen festlegt, die für die Erfüllung der Verpflichtungen erforderlich sind.
Bei Ausschreibungen, die von Zusammenschlüssen von Schulen oder Regionen eingerichtet werden, ist die Identifizierung jeder einzelnen Schule jedoch nicht garantiert.

Abruf von Nutzerverzeichnissen

Einige Dienste ermöglichen die Zuweisung von Handbüchern oder Ressourcen an einzelne Benutzer. In dem Fall, dass dem Partner nur die Benutzer bekannt sein können, die sich eingeloggt haben, wäre es sehr schwierig, die Zuweisungen von Handbüchern und Ressourcen zu verwalten.
Die Schulen wären gezwungen, alle Schüler aufzufordern, sich in ein System einzuloggen, bevor sie überhaupt mit den Zuweisungen beginnen könnten. Dies ist natürlich nicht optimal.

Schlussfolgerung

Die einfache Implementierung dieser Lösung und das hohe Sicherheitsniveau sind Schlüsselfaktoren. Aufgrund der Problematik des Zugriffs auf bestimmte Informationen, die von den Dienstleistern benötigt werden, ist diese Lösung jedoch nicht optimal.
Wir sind daher der Ansicht, dass dieser Anwendungsfall nicht weiter verfolgt werden sollte.

5.2 Fall 2: Verwaltung von Rechten über eine externe API.

In diesem zweiten Fall untersuchen wir die Verwendung einer externen API für die Verwaltung und Übertragung von Rechten als Ergänzung zum bestehenden SSO-System.

Funktionsweise

Die vorgeschlagene API wäre eine einfache Schnittstelle, über die die Partner die für ihre Leistungen erforderlichen Informationen abrufen können. Das Funktionsprinzip ist wie folgt:

- Ein Partner führt einen Aufruf der API durch, indem er eine Benutzer- oder Einrichtungskennung angibt.
- Die API gibt die relevanten Informationen zurück:
  - Für einen Nutzer: seine Rechte und Berechtigungen.
  - Für eine Einrichtung: Kontaktinformationen und/oder Schülerverzeichnisse.

Dieser Ansatz orientiert sich an ähnlichen Systemen, die bereits in anderen Regionen eingeführt wurden, und beweist damit seine Machbarkeit und Effizienz.

Vorteile

Dieser Ansatz bietet mehrere bedeutende Vorteile. Zunächst einmal ermöglicht er es den Partnern, die erforderlichen Daten vor der ersten Anmeldung eines Nutzers zu erhalten, wodurch die proaktive Bereitstellung von Diensten erleichtert wird. Darüber hinaus können die Informationen regelmäßig aktualisiert werden, ohne auf die Anmeldung des Nutzers warten zu müssen, was eine dynamischere Verwaltung der Rechte ermöglicht. Diese Lösung löst die in Fall 1 identifizierten Probleme wirksam, insbesondere den Zugriff auf die Daten der Einrichtungen und den Abruf der Benutzerverzeichnisse, der die Zuweisung von Ressourcen, Rechten und Kursen durch eine Lehrkraft vor der ersten Anmeldung ermöglicht.

Überlegungen zur Sicherheit

In diesem Fall ist es notwendig, eine Zugriffskontrolle zu implementieren: Ein System zur Verwaltung des Zugriffs auf die Verzeichnisdaten ist notwendig, um eine freie

Abfrage zu verhindern. Selbstverständlich müssen alle notwendigen Vorkehrungen getroffen werden, um den Zugang der Partner zu dieser API angemessen zu sichern. Dazu gehören beispielsweise die Verwendung starker Verschlüsselungsschlüssel und die Einrichtung einer sicheren RESTful API.

Einschränkungen und Probleme

Das Hauptproblem ist der Schutz sensibler Daten, insbesondere von Benutzerverzeichnissen. Es muss ein robuster Mechanismus für die Zugriffskontrolle implementiert werden, um sicherzustellen, dass nur autorisierte Partner auf diese Informationen zugreifen können. Hierfür sind mehrere Lösungen denkbar, die meisten sind jedoch umständlich und belastend.

Schlussfolgerung

Diese Lösung ist interessanter als Fall 1, da sie die ermittelten Probleme wirksam löst und gleichzeitig mehr Flexibilität bietet. Sie ermöglicht eine dynamischere Verwaltung von Rechten und einen kontrollierten Zugriff der Partner auf die benötigten Informationen bei gleichzeitiger Aufrechterhaltung eines hohen Sicherheitsniveaus. Allerdings kann die Implementierung eines Zugriffskontrollmechanismus besonders verwaltungsaufwändig und komplex sein.

5.3 Fall 3: Zugriffsverwaltung über OIDC und API.

Dieser dritte Fall schlägt einen hybriden Ansatz vor, der die Verwendung des Datawallet, OIDC und einer API kombiniert, um eine umfassende und sichere Verwaltung von Zugriffen und Rechten zu gewährleisten.

Betrieb

In diesem Szenario meldet sich ein Benutzer, z. B. ein Schulleiter, per SSO bei einer Partnerplattform an, um den Benutzern Handbücher und Ressourcen zuzuweisen. Er stellt fest, dass er auf der Plattform für die Ressourcenzuweisung keinen Zugriff auf die erforderlichen Verzeichnisse hat. Um dieses Problem zu lösen, klickt er in der Partnerplattform auf eine Schaltfläche, um die Verzeichnisse zu synchronisieren. Die Autorisierung dieser Synchronisierung wird von OIDC verwaltet, je nach den Rechten des Benutzers, der die Synchronisierung anfordert. Sobald die Berechtigung

erteilt wurde, wird das Verzeichnis abgerufen, sodass der Benutzer die Zuweisungen vornehmen kann.

Vorteile

Dieser Ansatz löst alle in den Fällen 1 und 2 identifizierten Probleme. Er ermöglicht einen frühzeitigen Zugriff auf die für die Leistung erforderlichen Informationen, ohne auf die Anmeldung aller Nutzer warten zu müssen. Darüber hinaus bietet er eine Feinsteuerung der Zugriffsrechte auf Verzeichnisse, was die Flexibilität für die Partner erhöht.
Die Funktionsweise des IODC ermöglicht die Verwendung von "token refresh¨, wodurch die Verzeichnisinformationen regelmäßig aktualisiert werden können.

Integration mit NBP-Tools

Die Integration mit den bestehenden NBP-Tools ist nahtlos. Meinbildungsraum stellt die Benutzer-ID bereit, während die Datawallet API den Abruf des Benutzerprofils ermöglicht. Es ist wichtig zu beachten, dass der Datenraum nicht direkt an diesem Prozess beteiligt ist.

Für die Speicherung der Benutzerprofile im Datawallet können wir das folgende Format vorschlagen:


```
{
  "content":                                                    {
    "expiresAt":                                  "2025-12-19T14:29:17.676Z",
    "items":                                                    [
      {
        "@type":                                          "Request",
        "items":                                                [
          {
          "@type":                          "CreateAttributeRequestItem",
          "mustBeAccepted":                                  true,
          "attribute":                                          {
            "@type":                          "RelationshipAttribute",
            "owner":                                              "",
            "key":                                        "PROFILS",
            "confidentiality":                              "public",
```

```
            "Wert": {
              "@type": "ProprietaryJSON",
              "title": "Zugriffsrechte",
              "value": {
                "DIR": "Schulleiter",
                "VAL": "Rechnungsprüfer",
                "OP": "Zuweisungsoperator".
              }
            }
          }
          }
        ]
      }
    ]
  },
  "peer": "did:e:nmshd-bkb.demo.meinbildungsraum.de:dids:069c476a18241e19ffc950".
}
```


Dieses Format würde die gemeinsame Nutzung eines bestimmten Nutzerprofils für jeden Nutzer ermöglichen.
Beispiel: Durch eine Suche nach dem Schlüssel "PROFILS" kann ein Partner herausfinden, dass es sich um den Leiter einer Einrichtung handelt, der für die Validierung von Rechnungen verantwortlich ist und auch Zuweisungen vornimmt.

Die Schlüssel, die den Austausch zwischen den verschiedenen Partnern ermöglichen, müssen von NBP definiert und kontrolliert werden. Im Falle von Profilen ist es auch wichtig zu beachten, dass die Verwaltung der Profile unbedingt zentralisiert werden muss, um Interessenkonflikte zu vermeiden.

Überlegungen zur Sicherheit

Die in diesem Ansatz verwendeten Protokolle tragen zu einem optimalen Sicherheitsniveau bei. Die kombinierte Verwendung von OIDC und Enmeshed stellt sicher, dass nur befugte Personen auf sensible Informationen zugreifen können.

Komplexität und Herausforderungen

Diese Lösung weist jedoch aufgrund der Implementierung einer speziellen Vernetzung eine erhöhte Komplexität auf. Dies erfordert besondere Aufmerksamkeit bei der Entwicklung, um eine erfolgreiche Integration zu gewährleisten.

Schlussfolgerung

Zusammenfassend lässt sich sagen, dass dieser Ansatz eine umfassende Lösung für das Sicherheitsmanagement und die erforderlichen Anwendungsfälle darstellt. Er ergänzt die beiden anderen untersuchten Fälle wirksam und erfüllt die im Rahmen des NBP-Projekts ermittelten Anforderungen umfassend. Durch die Kombination der Vorteile der verschiedenen Technologien bietet dieser Anwendungsfall maximale Flexibilität bei gleichzeitiger Aufrechterhaltung eines hohen Sicherheitsniveaus.

6. Empfehlungen und nächste Schritte

Als Folge der eingehenden Untersuchung der drei Anwendungsfälle empfehlen wir die Umsetzung von Fall 3, der die Verwendung von Datawallet, OIDC und einer API für die Verwaltung von Zugängen und Rechten kombiniert. Diese Lösung bietet die beste Antwort auf die im Rahmen des NBP-Projekts ermittelten Bedürfnisse und vereint Flexibilität, Sicherheit und eine optimale Integration in bestehende Tools.

Um diese Lösung zu implementieren :

1. Detaillierter Entwurf der Architektur :
   Dies bedeutet, dass die genauen Interaktionen zwischen dem Datawallet, dem OIDC-System und der API definiert werden müssen. Außerdem wird es notwendig sein, die Datenflüsse und Kommunikationsprotokolle festzulegen, um eine reibungslose Integration zwischen allen Komponenten und den verschiedenen Partnern zu gewährleisten. Dies wird nur von NBP gesteuert und den Partnern auferlegt werden können.

2. Entwicklung der API :
   Es wird eine sichere RestFull-API entwickelt werden, die das Abrufen von Verzeichnissen und anderen notwendigen Informationen ermöglicht. Dieser Schritt wird die Implementierung der Endpunkte beinhalten, die für die verschiedenen Funktionen, die die Lösung bieten soll, erforderlich sind.

3. OIDC-Integration :
   Dies wird die Implementierung eines Berechtigungssystems erfordern, das den Zugriff auf Verzeichnisse (z. B.) verwaltet. Die Sicherheitseinstellungen und Autorisierungsskopen müssen sorgfältig konfiguriert werden, um sicherzustellen, dass nur autorisierte Personen auf sensible Informationen zugreifen können.

4. Anpassung des Datawallet :
   Das Datawallet muss angepasst werden, um die Verwaltung von Benutzerprofilen durch den einzigen dazu befugten Partner zu ermöglichen. Diese Anpassung muss die Kompatibilität des Berechtigungssystems mit der Gesamtheit der Partner gewährleisten.

5. Entwicklung der Benutzeroberfläche :
   Partner, die das Benutzerverzeichnis abrufen möchten, müssen die notwendigen Schnittstellenelemente entwickeln, z. B. eine Schaltfläche, mit der die Verzeichnisse synchronisiert werden können. Die Integration der OIDC-Autorisierungsströme in diese Schnittstelle wird dazu beitragen, die Benutzererfahrung reibungsloser zu gestalten.

Die Umsetzung dieser Schritte wird eine effiziente Implementierung der empfohlenen Lösung ermöglichen, die eine nahtlose Integration in das bestehende NBP-Ökosystem gewährleistet und den ermittelten spezifischen Bedürfnissen gerecht wird.

7. Schlussfolgerung

Die im Rahmen von AP4.2 des NBP-Projekts (Digital for Education) durchgeführte Studie untersuchte eingehend die verschiedenen möglichen Ansätze für die Verwaltung von Rechten und Zugriffen im deutschen digitalen Bildungsökosystem. Durch die Analyse von drei verschiedenen Anwendungsfällen konnten wir eine optimale Lösung identifizieren, die den komplexen und vielfältigen Bedürfnissen der verschiedenen beteiligten Akteure gerecht wird.

Die empfohlene Lösung, die auf einem hybriden Ansatz basiert, der die Nutzung des Datawallet, OAuth und eine dedizierte API kombiniert, bietet ein optimales Gleichgewicht zwischen Sicherheit, Flexibilität und Benutzerfreundlichkeit. Mit diesem Ansatz lassen sich die zu Beginn der Studie ermittelten entscheidenden Probleme

lösen, darunter die effiziente Verwaltung der Verzeichnisse der Einrichtungen, die Kommunikation mit den Einrichtungen und der sichere Zugriff auf Bildungsressourcen.

Die nahtlose Integration mit den bestehenden NBP-Tools, wie Meinbildungsraum und Datawallet, gewährleistet die Gesamtkonsistenz des Systems und bietet gleichzeitig wichtige neue Funktionen. Die Einführung eines auf OAuth basierenden Autorisierungsmechanismus erhöht die Sicherheit des Systems erheblich und ermöglicht gleichzeitig eine Feinsteuerung der Zugriffsrechte.

Es ist wichtig zu betonen, dass die Umsetzung dieser Lösung eine enge Zusammenarbeit zwischen den verschiedenen Akteuren des NBP-Projekts sowie eine besondere Aufmerksamkeit von NBP für die Umsetzung des Rahmens auf die technischen und sicherheitsrelevanten Aspekte während der Entwicklung und des Einsatzes erfordern wird.

Zusammenfassend lässt sich sagen, dass die vorgeschlagene Lösung einen bedeutenden Fortschritt bei der Erreichung der Ziele des NBP-Projekts darstellt. Sie legt den Grundstein für ein robustes, sicheres digitales Bildungsökosystem, das den sich ändernden Bedürfnissen des Bildungssektors gerecht wird. Dieser innovative Ansatz wird nicht nur dazu beitragen, die Effizienz der Bildungsprozesse zu verbessern, sondern auch den Schutz der persönlichen Daten von Schülern und Bildungspersonal zu stärken.

Ergebnis des POCs

Einleitung

Im Rahmen von AP6.2 haben wir mit der Entwicklung eines Proof of Concept (POC) begonnen, um unseren Mikroservice für die Profilverwaltung mit dem Namen Themis mit dem System datawallet zu verbinden. Dieses Projekt ist Teil eines Ansatzes zur kontinuierlichen Verbesserung unserer Systeme, um die Verwaltung der Benutzerrechte zu optimieren und gleichzeitig eine größere Interoperabilität zwischen den Diensten zu gewährleisten.

Das Datawallet soll als zentraler Dreh- und Angelpunkt für die Verwaltung der Benutzerberechtigungen dienen und einen sicheren und kontextbezogenen Ansatz für die Rechte ermöglichen, wobei die Grundsätze des Schutzes personenbezogener Daten eingehalten werden müssen.

Ziele der Technischen Machbarkeitsstudie

Das Hauptziel dieser Studie besteht darin, die technische Machbarkeit der Integration zwischen Themis und dem Datawallet zu validieren. Im Einzelnen geht es darum :

- Zu überprüfen, ob die Benutzerprofile ordnungsgemäß in das Datawallet übertragen werden können.
- Sicherzustellen, dass die mit diesen Profilen verbundenen Rechte abgerufen und in unseren bestehenden und künftigen Systemen angewendet werden können.
- Sicherzustellen, dass diese Integration die geltenden technischen und rechtlichen Auflagen erfüllt.

Methodologie

Zur Durchführung dieses POC wurden zwei Instanzen des Enmeshed-Systems auf unseren lokalen Umgebungen installiert, um zwei verschiedene Aktionen zu simulieren:

6. Die Übermittlung von Informationen über Benutzerprofile an das Datawallet durch einen "Administrator".

7. Das Abrufen der Profile für einen Benutzer bei einem Anmeldeversuch an unserem System.

Die Entwicklung wurde auf unserem Produkt Themis durchgeführt. Dieser interne Mikroservice, der der Verwaltung von Benutzerprofilen gewidmet ist, ermöglicht eine kontextbezogene Verwaltung der Rechte in Abhängigkeit von den SSO-Attributen (Single Sign-On) der Benutzer, ihrer Herkunft (z. B. ein bestimmtes ENT) oder auch ihrer Ziele innerhalb unserer Produkte.

Erklärung des Bestehenden

Thémis ist ein Mikrodienst, der entwickelt wurde, um Benutzerrechte auf nicht namentliche Weise zu verwalten. Er stützt sich auf mehrere Parameter wie :

- Die SSO-Attribute der Benutzer.
- Die URL des Ziels.
- Die externen Rollen, die von Partner-APIs stammen.

Anhand dieser Informationen kann Thémis die anwendbaren Kontexte identifizieren und eine Liste von Rollen bereitstellen, die für jedes Produkt in spezifische Benutzerrechte übersetzt werden.

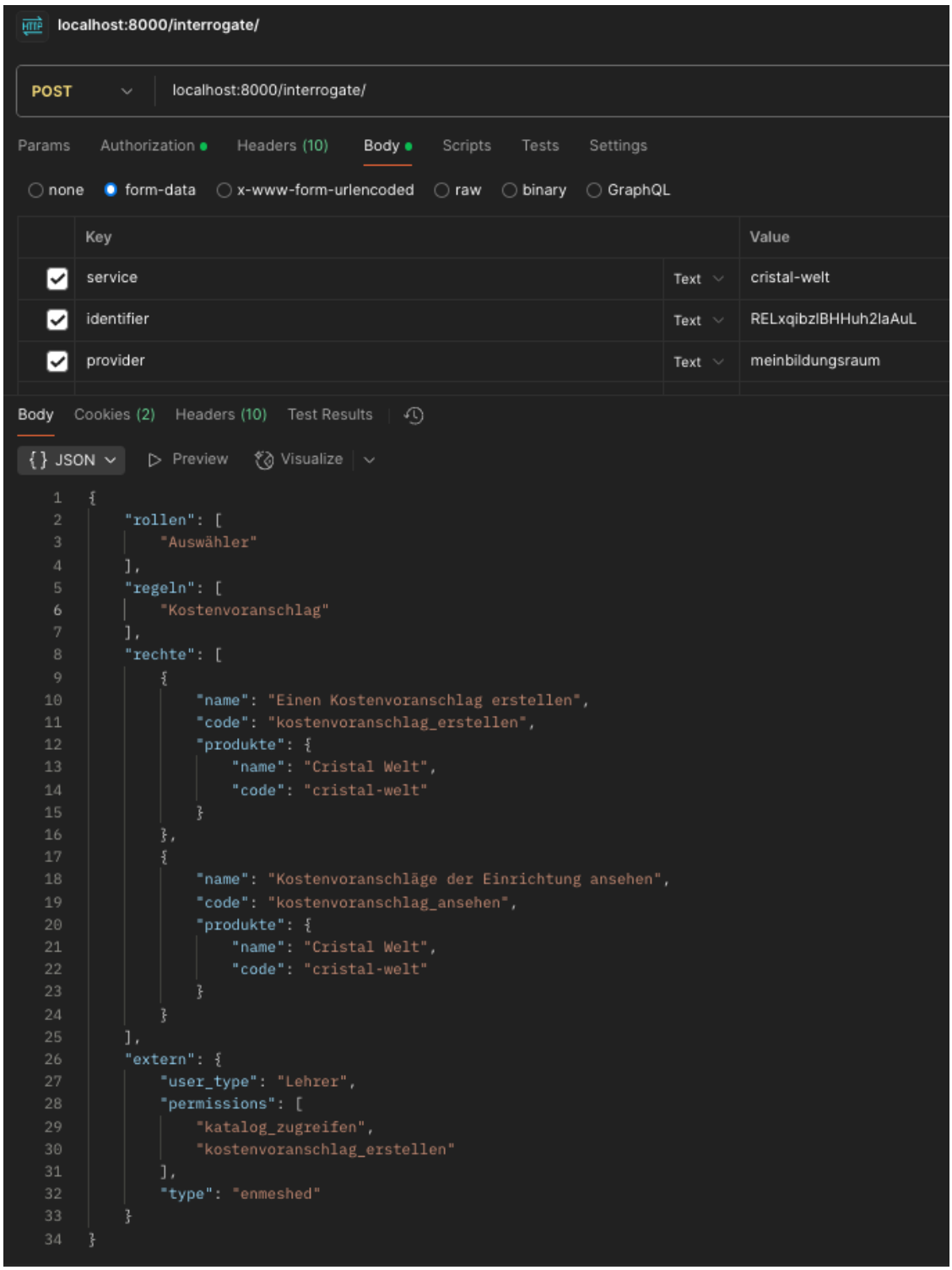
Ein Schlüsselpunkt der aktuellen Funktionsweise ist, dass Thémis keine persönlichen Daten speichert. Die Kontexte, die die Rechte definieren, basieren auf nicht-personenbezogenen Kriterien, wodurch die Einhaltung der Datenschutzbestimmungen (insbesondere der DSGVO) gewährleistet wird.

Phase der Implementierung

Die Implementierung des POC erfolgte in mehreren strukturierten Schritten:

8. **Datenübertragung an das Datawallet**: Die Informationen zu den Berechtigungen werden von Themis über einen dedizierten Dienst für die Zuweisung von Rechten gesendet.
9. **Aufbau einer Beziehung zwischen Dienst und Benutzer**: Der Dienst, der diese Rechte benötigt, baut über Enmeshed eine "RelationShip" mit dem Benutzer auf und übermittelt diese Kennung bei Aufrufen an Themis.

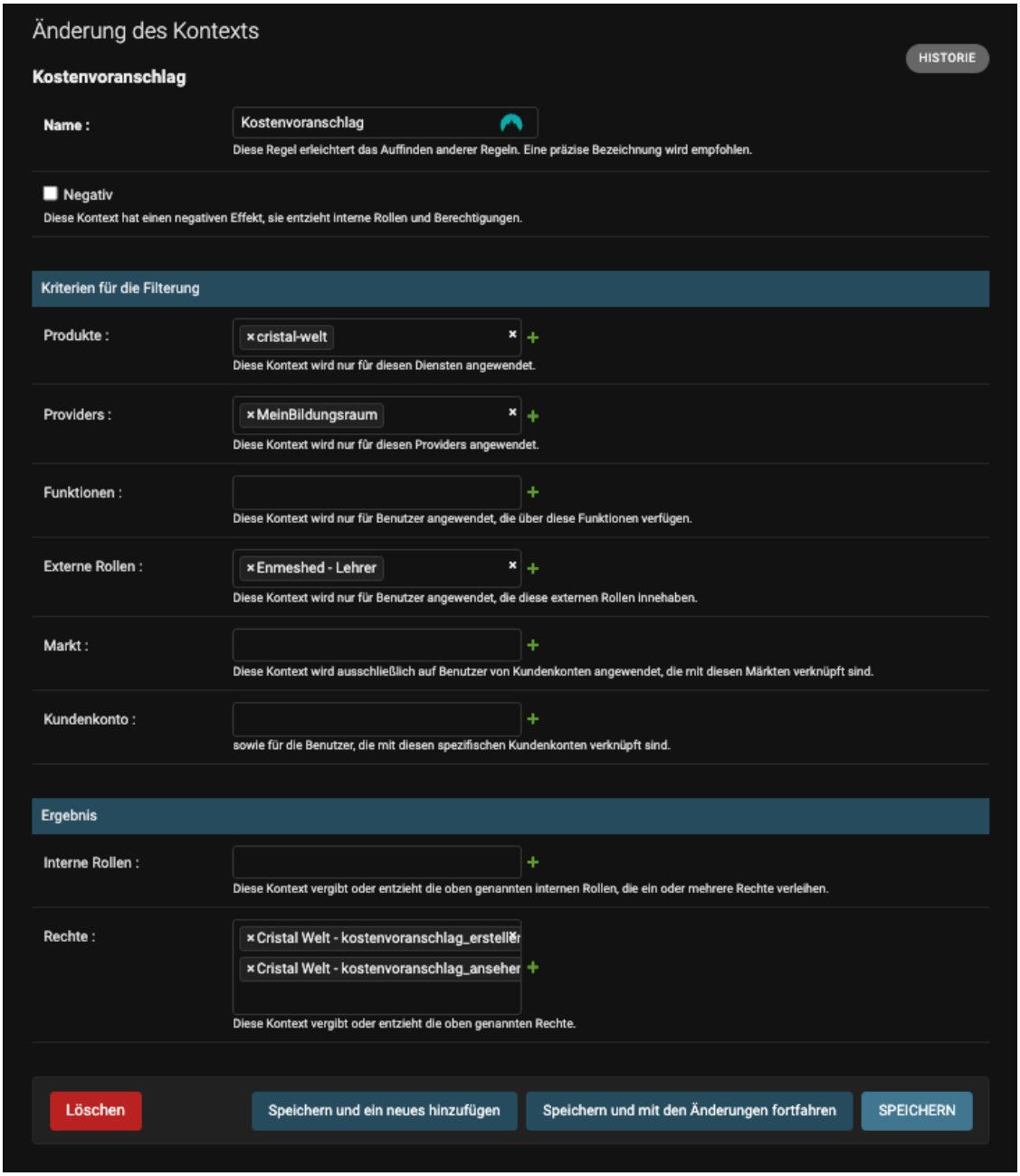
10. **Datenabruf und -verarbeitung**: Themis fragt das Datawallet ab, um die für die Berechnung der Rechte erforderlichen Daten abzurufen. Diese Informationen werden dann verwendet, um die für den Benutzer geltenden Kontexte zu ermitteln.



11. **Anwendung der Kontexte** : Jeder Kontext stellt einen Satz von Parametern dar, der die Rechte definiert, die einem Benutzer gewährt oder entzogen

werden sollen. Beispielsweise kann einem Lehrer, der von einem bestimmten NTU kommt, je nach Produkt das Recht eingeräumt werden, ein Angebot zu erstellen oder ein Ticket zu eröffnen.

12. **Dynamische** Aktualisierung: Da die Kontexte kumulierbar sind, wird ihre Aktualisierung vereinfacht, wodurch eine einheitliche Verwaltung der Berechtigungen zwischen Anwendungen gewährleistet wird.



Schlussfolgerung und Empfehlungen

Das im Rahmen von AP6.2 durchgeführte POC hat die technische Machbarkeit der Verbindung zwischen Themis und dem Datawallet bewiesen.

Die ersten Tests zeigen, dass :

- Daten können zwischen Themis und dem Datawallet effizient übertragen und abgerufen werden.
- Die erzeugten Kontexte ermöglichen eine korrekte Anwendung von Rechten in unseren bestehenden Systemen.
- Bisher wurden keine größeren Probleme in Bezug auf die Sicherheit oder die Einhaltung der technischen Transaktionen festgestellt.

Es ist jedoch zu betonen, dass dieses POC eine konzeptionelle Projektion und keine voll funktionsfähige Lösung darstellt. Derzeit weist das Datawallet erhebliche Einschränkungen auf, insbesondere das Fehlen von Mechanismen, mit denen bestimmte Attribute eingeschränkt werden können. Diese Lücke könnte die Sicherheit der Systeme gefährden, da sie es unberechtigten Akteuren ermöglicht, Benutzerprofile zu erstellen oder zu ändern. Um eine vollständige Kontrolle über die Rechte und Berechtigungen zu gewährleisten, ist es zwingend erforderlich, dass nur NBP und seine autorisierten Partner in die Profilverwaltung eingreifen können. Eine technische Weiterentwicklung des Datawallet ist daher unerlässlich, um die Sicherheitsanforderungen zu erfüllen und eine zentralisierte und kontrollierte Verwaltung der Berechtigungen zu gewährleisten.

7. Technische Architektur Wallet – Enmeshed - Synapse

Framing

Dieser Meilenstein konzentriert sich auf drei grundlegende Aspekte der technischen Architektur.
Erstens hat die Sicherheit der Infrastruktur oberste Priorität, wobei den Empfehlungen des BSI sowie den besten Praktiken des OWASP besondere Aufmerksamkeit gewidmet wird. Diese Richtlinien dienen als Grundlage für die Schaffung eines soliden Sicherheitsrahmens, der den höchsten Standards entspricht.

Zweitens: die Verwaltung der Kommunikation, einschließlich E-Mails und Benachrichtigungen zwischen Nutzern. Die Integration des von LDE entwickelten Hermes-Projekts wird als potenzielle Lösung zur Zentralisierung und Optimierung dieses Austauschs mit Synapse in Betracht gezogen.

Schließlich bilden der Zugang zu Ressourcen und die Verwaltung von Lizenzen die dritte Säule dieses Meilensteins. Die Studie untersucht die innovative Nutzung von Wallet für eine optimierte und sichere Verwaltung von Zugriffsrechten auf pädagogische Inhalte digitale Inhalte und granularisierte Inhalte.

Sicherheitsrahmen

Im Rahmen des Projekts MBR haben wir einen gründlichen Ansatz unternommen, um ein hohes Maß an Sicherheit zu gewährleisten. Dieser Ansatz basierte auf einem sorgfältigen Studium der Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik), der deutschen Behörde für Cybersicherheit, die eng mit der französischen ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) zusammenarbeitet. Ergänzend dazu haben wir die Grundprinzipien der Top 10 des OWASP (Open Web Application Security Project), der weltweiten Referenz für die Sicherheit von Webanwendungen, integriert.

Auf der Grundlage dieser umfassenden Analyse haben wir eine Zusammenfassung der Sicherheitspunkte erstellt, die für den Erfolg und den Fortbestand eines Projekts von der Größenordnung von MBR entscheidend sind. Diese Zusammenfassung, die das Ergebnis kollaborativer Arbeit und gründlicher Überlegungen ist, wurde weiter unten im Dokument im *Zusatz 1 zu 5* festgehalten. Dieses Kapitel stellt nun eine zentrale Ressource dar, an der wir unsere Entscheidungen und Handlungen im Bereich der Sicherheit ausrichten können.

Verwaltung von E-Mails und Benachrichtigungen zwischen Nutzern

Vorwort zu Hermes

Das von LDE schon vor Synapse entwickelte Produkt *Hermes* stellt eine zentrale Lösung für die Verwaltung elektronischer Kommunikation dar, die E-Mails und Benachrichtigungen für unsere gesamte Produktreihe umfasst. Die auf Microservices basierende Architektur ermöglicht eine nahtlose Integration mit mehreren Produkten über Programmierschnittstellen (APIs).
Wir werden in der Lage sein, Hermes mit dataWallet zu vernetzen und damit einen Standard für die API-Struktur zu etablieren.

Personalisierung von Alerts

Das System bietet eine feine Granularität bei der Konfiguration der Kommunikationspräferenzen. Jeder Nutzer hat die volle Kontrolle darüber, welche Arten von Warnungen, E-Mails und Benachrichtigungen er erhalten möchte.

Intelligente Verwaltung der Frequenzen

Um eine optimale Nutzererfahrung zu gewährleisten, integriert Hermes einen Mechanismus zur automatischen Regulierung der Sendungen. Dieses System verhindert eine Überreizung der Nutzer, indem es die Häufigkeit der Kommunikation intelligent begrenzt.

Verteilte Architektur

Die Zentralisierung der Benachrichtigungen, gekoppelt mit einer offenen Architektur, ermöglicht allen angeschlossenen Plattformen den Zugriff und die Anzeige von Benachrichtigungen auf konsistente und synchronisierte Weise.

Unser Vorschlag

Durch eine vollständige Integration der Produkte MBR, können wir die MBR-Nutzer auf unseren Plattformen erkennen und die Funktionsweise anpassen. Jede Benachrichtigung kann dann einfach von Hermes aus zu Enmeshed weitergeleitet werden.
Das Hermes-Projekt ist Teil der von LDE erdachten Produkte, dieses Produkt befindet sich noch nicht in der Entwicklung.

Verwaltung von Ressourcen und Lizenzen

Untersuchung des aktuellen Marktes

Eine eingehende Analyse des aktuellen Marktes zeigt, dass die Systeme, die von Verlagen und Händlern zur Verbreitung von Lehrbüchern und digitalen Ressourcen eingesetzt werden, nicht für die Nutzung in einem globalen Rahmen wie dem MBR geeignet sind. Diese Unzulänglichkeit unterstreicht die Notwendigkeit einer stärker integrierten und flexiblen Lösung.

Unsere technische Expertise konzentriert sich hauptsächlich auf drei große Verlage: Handwerk und Technik, Merkur und Europa Lehrmittel. Die Interaktionen mit diesen Verlagen veranschaulichen die Vielfalt der derzeitigen Ansätze. In einem Fall erfolgt der Austausch über Excel-Dateien, die wir automatisch in unsere Prozesse integrieren. Im anderen werden die Interaktionen über APIs gesteuert. Bei anderen Anbietern, mit denen wir zusammenarbeiten, sind die Methoden spezifisch und beruhen in der Regel auf der Übertragung von Excel- oder CSV-Dateien zwischen dem Anbieter, LDE und den Endnutzern.

Ein entscheidender Aspekt, den es zu beachten gilt, ist die Gültigkeitsdauer der Lizenzen. Einige der von Kunden erworbenen Lizenzen bleiben mehrere Jahre lang

gültig, was ein System erfordert, das diese langen Validitätszeiträume effizient verwalten kann.

Derzeit erfolgt die Lizenzvergabe individuell pro Benutzer direkt auf der Plattform des Herausgebers. Dieser Ansatz hat mehrere Nachteile: Er erfordert entweder eine vorherige Anmeldung der Schüler oder das manuelle Hochladen von Schülerlisten in die Plattformen der Herausgeber. Außerdem werden Änderungen der Lehrer- und Schülerzahlen nicht automatisch propagiert, was die Verwaltung der Lizenzen erschwert.

Eine weitere große Herausforderung ist das Fehlen von Lizenzen, die für eine komplette Schule gelten. Dieser Mangel führt zu besonderen Problemen bei bestimmten Arten von Ressourcen, wie z. B. Enzyklopädien, die eine individuelle Zuweisung der Ressourcen an jeden Nutzer in jeder Bildungseinrichtung erfordern.

Schließlich haben wir festgestellt, dass die Lizenzen in der Regel nicht wiederverwendbar sind. Diese Starrheit erschwert die Korrektur von Eingabefehlern, was zu administrativen Komplikationen und Ineffizienzen bei der Ressourcenverwaltung führen kann.

Diese Marktanalyse verdeutlicht den Bedarf an einer flexibleren, zentralisierten Lösung, die auf die spezifischen Bedürfnisse von MBR und seinen Partnern zugeschnitten ist. Sie unterstreicht die Bedeutung der Entwicklung eines Systems, das langfristige Lizenzen effizient verwalten, den Zuweisungsprozess vereinfachen und eine größere Flexibilität bei der Verwaltung digitaler Bildungsressourcen bieten kann.

Unser Vorschlag

Unser technischer Vorschlag basiert auf der Nutzung der dataWallet für die gemeinsame Nutzung und Verwaltung von Lizenzen. Zu den Hauptmerkmalen dieser Lösung gehören die Speicherung von Lizenzinformationen direkt in der dataWallet des Nutzers, die Verwendung eines standardisierten JSON-Formats zur Darstellung von Lizenzen, die Überprüfung der Gültigkeit von Lizenzen über die dataWallet durch die Ressourcenverteiler sowie eine zentrale Verwaltung der Lizenz- und Ressourcenzuweisungen.

Da jede Lizenz einem bestimmten Benutzer zugewiesen wird, ist es logisch, die Lizenzinformationen dem Benutzer im DataWallet hinzuzufügen. Indem sichergestellt wird, dass jede Lizenz von allen MBR-Partnern korrekt und identisch formatiert wird, wäre es möglich, die Zuweisungen direkt im Datawallet zu speichern.

So könnte ein Ressourcenverteiler beim Zugriff eines Nutzers die Gültigkeit der Lizenz direkt im Datawallet überprüfen. Dies würde auch eine vollständige Portabilität zwischen den verschiedenen Akteuren ermöglichen.

Das Format, das wir mit den Elementen, die wir im Moment haben, vorschlagen können, ist das folgende:

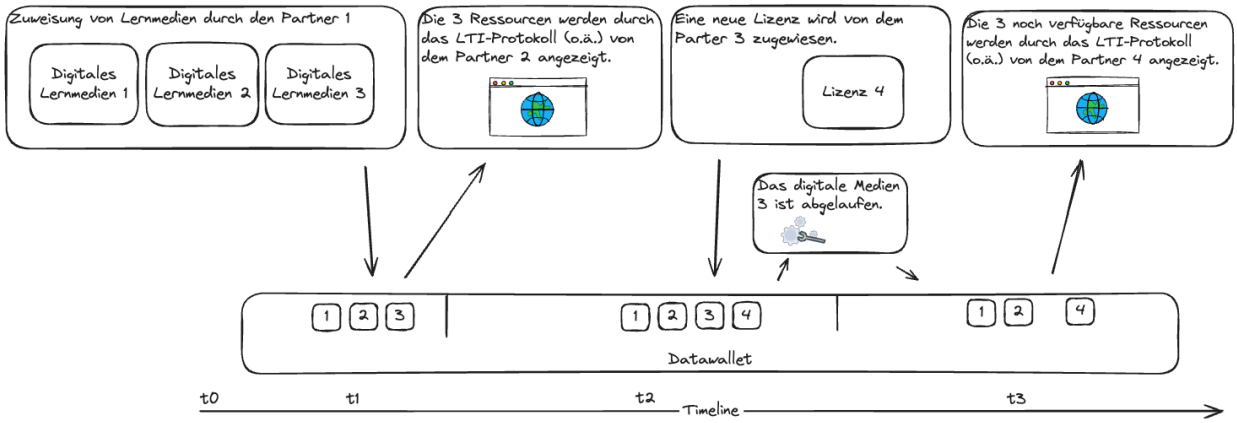
```
{
  "content": {
    "expiresAt": "2025-12-19T14:29:17.676Z",
    "items": [
      {
        "@type": "Request",
        "items": [
          {
          "@type": "CreateAttributeRequestItem",
          "mustBeAccepted": true,
          "attribute": {
            "@type": "RelationshipAttribute",
            "owner": "",
            "key": "LICENSE-KEY-<EAN>",
            "confidentiality": "public",
            "value": {
              "@type": "ProprietaryJSON",
              "title": "<NAME DES HANDBUCHS>",
              "value": {
                // Wir können weitere Informationen hinzufügen, wenn wir wollen.
                "origin": "LDE",
                "token": "<LIZENZSCHLÜSSEL, DER DAS TOKEN VON LDE GENERIERT
IST>".
              }
```

```
            }
          }
          }
        ]
      }
    ]
  },
  "peer":        "did:e:nmshd-bkb.demo.meinbildungsraum.de:dids:069c476a18241e19ffc950".
}
```


Wenn alle Partner das gleiche Format verwenden, kann jeder Partner die Attribute des aktuell angemeldeten Benutzers abrufen und so die Ressourcen auflisten, die ihm zugewiesen sind. Er kann diese dann auf seiner eigenen Plattform verwenden, um dem Nutzer ein möglichst reibungsloses und umfassendes Erlebnis zu bieten. Ein solches System würde es jedem Partner ermöglichen, sich auf natürliche Weise in der Zuweisungs- und Zugangskette zu positionieren.

In dem unten dargestellten Beispiel fügen mehrere Partner einem Benutzer digitale Ressourcen oder Lehrbücher hinzu . Andere Partner sind in der Lage, diese Ressourcen auf ihren Plattformen anzuzeigen und zu nutzen.
Diese Abbildung zeigt den Prozess der Zuweisung und Verwaltung von digitalen Ressourcen oder Lizenzen über eine Zeitachse mit verschiedenen beteiligten Partnern.
t0 - Anfangszustand: Der erste Block zeigt drei digitale Ressourcen (1, 2 und 3), die unter für die Partner verfügbar sind.
t1 - Erste Zuweisung:Partner 2 zeigt die Ressourcen an, die über das LTI-Protokoll oder je nach technischen Möglichkeiten auf andere Weise verfügbar sind.
t2 - Hinzufügen von Ressourcen
- Partner 3 stellt eine neue digitale Ressource (4) bereit.
- Die Ressourcen 1, 2, 3 und 4 sind nun im Datawallet verfügbar.
t3 - Endgültiger Status
- Ressource 3 wird als abgelaufen markiert.

- Partner 4 zeigt die verbleibenden verfügbaren Ressourcen (1, 2 und 4) an.



Das Datawallet bleibt das zentrale Element für die Verwaltung von Lizenzen und digitalen Ressourcen. Die Verwaltung über Enmeshed ermöglicht die sichere Verwaltung von Lizenzen und DCPs (Persönliche Daten) Benutzer.
Die Anzeige von Ressourcen wird durch die Synergie aller zur Verfügung gestellten Protokolle ermöglicht: SSO - Datawallet-API - LTI ...

Analyse der Risiken

Es wurden mehrere potenzielle Risiken identifiziert, darunter der Widerstand gegen Veränderungen seitens einiger Partner, die technische Komplexität der Implementierung für einige Akteure, Kompatibilitätsprobleme mit Legacy-Systemen sowie Sicherheitsrisiken im Zusammenhang mit der Zentralisierung von Lizenzdaten. Um diese Risiken zu mindern, schlagen wir verschiedene Strategien vor. Wichtig wird eine klare Kommunikation und eine Schulung der Partner über die Vorteile des neuen Systems sein. Eine persönliche technische Unterstützung bei der Implementierung wird ebenfalls erforderlich sein.
Schließlich wird die Einführung verstärkter Sicherheitsmaßnahmen und regelmäßiger Audits den Schutz der Daten gewährleisten.

Schlussfolgerung

Im Bereich der Sicherheit schafft die Übernahme der Empfehlungen des BSI und der OWASP, die weiter unten festgehalten sind, einen robusten Rahmen, der den anspruchsvollsten Standards entspricht. Dieser proaktive Ansatz zur Cybersicherheit

ist perfekt auf die Grundsätze der ISO 27001 abgestimmt und gewährleistet so den optimalen Schutz von Daten und Systemen.

Das Kommunikationsmanagement, insbesondere durch das Hermes-Projekt von LDE, bietet eine zentrale und flexible Lösung für Benachrichtigungen und E-Mails. Ihre Integration mit der dataWallet und ihre Fähigkeit, sich an die spezifischen Bedürfnisse von MBR anzupassen, versprechen eine reibungslose und personalisierte Benutzererfahrung, die den Qualitätsstandards von ISO 9000 entspricht.

Schließlich stellt der Vorschlag, das dataWallet für die Verwaltung von Ressourcen und Lizenzen zu verwenden, einen bedeutenden Fortschritt dar. Dieser innovative Ansatz, der auf einem standardisierten JSON-Format basiert, ermöglicht eine effizientere und flexiblere Verwaltung von Lizenzen und erleichtert die Interoperabilität zwischen den verschiedenen Projektbeteiligten.

Obwohl es noch einige Herausforderungen gibt, insbesondere in Bezug auf die Akzeptanz und die Sicherheit, sind wir der Ansicht, dass die vorgeschlagenen Lösungen einen soliden Rahmen für die zukünftige Entwicklung von MBR bieten.

Zusatz zu 5.: Sicherheitsempfehlungen Synapse

Es ist von entscheidender Bedeutung, robuste Sicherheitselemente für die verschiedenen eingerichteten Interkonnektionen zu etablieren. Dieses Dokument enthält eine gründliche Analyse der Sicherheitsmaßnahmen, die für jede der drei wichtigsten Interkonnektionen implementiert werden sollten: SSO mit OAuth, Datawallet mit Enmeshed und Datenraum für den Austausch nicht-personenbezogener Daten.
Die Analyse basiert auf der OWASP-Studie10 und den Empfehlungen des BSI.

Absicherung des SSO mit OAuth

Die Einführung eines auf dem OAuth-Standard basierenden Single-Sign-On-Systems (SSO) erfordert besondere Aufmerksamkeit in Bezug auf die Sicherheit. Es wird empfohlen, die folgenden Maßnahmen zu implementieren:
Verwendung von HTTPS: Die gesamte Kommunikation zwischen den verschiedenen Komponenten des SSO-Systems sollte über HTTPS (TLS 1.3 oder 1.2) verschlüsselt werden, um Abhörung und Man-in-the-Middle-Angriffe zu verhindern.
Die Verwendung von Refresh-Tokens wird empfohlen. Sie ermöglicht ein Gleichgewicht zwischen Sicherheit und Benutzerfreundlichkeit.
Verwaltung von Token : Zugriffs- und Refresh-Tokens sollten sicher und mit einer begrenzten Gültigkeitsdauer gespeichert werden. Es wird empfohlen, signierte und verschlüsselte JWT-Tokens (JSON Web Tokens) zu verwenden (mindestens in SHA-256).
Strenge Validierung: Alle Parameter, die während des OAuth-Austauschs empfangen werden, müssen streng validiert werden, um Injektionen und Flow-Change-Angriffe zu verhindern.
PKCE-Implementierung: Für mobile Anwendungen oder öffentliche Clients wird die Verwendung von PKCE (Proof Key for Code Exchange) dringend empfohlen, um die Sicherheit des Autorisierungsflusses zu erhöhen.

Absicherung von Datawallet mit Enmeshed

Die Anwendung Enmeshed, die für die Verwaltung des Datawallet und die gemeinsame Nutzung personenbezogener Daten (DCP) verwendet wird, erfordert besondere Sicherheitsmaßnahmen :

Datenverschlüsselung: Alle im Datawallet gespeicherten DCPs müssen verschlüsselt werden, sowohl im Ruhezustand als auch bei der Übertragung. Die Verwendung von robusten Verschlüsselungsalgorithmen wie AES-256 wird empfohlen.

Granulare Zugriffskontrolle: Es sollte ein feingliedriges Zugriffskontrollsystem eingerichtet werden, das es den Nutzern ermöglicht, genau zu verwalten, welche Daten mit wem geteilt werden.

Sichere Protokollierung: Alle Vorgänge der gemeinsamen Nutzung und des Zugriffs auf DCPs sollten zu Prüf- und Compliance-Zwecken in sicheren und unveränderbaren Protokollen festgehalten werden.

Multi-Faktor-Authentifizierung (MFA): Der Zugriff auf das Datawallet sollte durch eine MFA geschützt werden, um die Sicherheit der Benutzerkonten zu erhöhen.

Absicherung von Datenraum

Obwohl Datenraum keine DCPs verarbeitet, bleibt die Sicherung der Kataloginformationen, der Lernpfade und der gemeinsam genutzten Taxonomie von größter Bedeutung :

Datenisolierung : Gespeicherte Daten müssen logisch von anderen Systemen isoliert sein, insbesondere von solchen, die DCPs verarbeiten.

Zugriffsverwaltung: Ein rollenbasiertes System zur Verwaltung von Zugriffsrechten (RBAC) muss implementiert werden, um zu kontrollieren, wer die Daten in Datenraum lesen, ändern oder löschen kann.

Nachvollziehbarkeit: Alle Änderungen an den Daten müssen mit der Identität des Urhebers und dem Zeitstempel der Aktion nachvollziehbar sein.

Allgemeine Sicherheitsüberlegungen

Zusätzlich zu den spezifischen Maßnahmen für jede Vernetzung ist es entscheidend, globale Sicherheitspraktiken zu implementieren:

Cybersicherheitsmonitoring: Für alle Systemkomponenten sollte eine ständige

Überwachung auf neue Schwachstellen und Sicherheitsaktualisierungen durchgeführt werden.

Penetrationstests: Es sollten regelmäßige Penetrationstests für die gesamte Infrastruktur durchgeführt werden, um potenzielle Schwachstellen zu identifizieren und zu beheben.

Die Einführung automatisierter Sicherheitstests in PipLine CI/CD mithilfe von Tools wie OWASP ZAP wäre eine gute Praxis.

Benutzerschulung: Die Benutzer des Systems sollten in bewährten Sicherheitspraktiken geschult werden, insbesondere in Bezug auf die Verwaltung von DCPs und die Verwendung des Datawallet.

Plan zur Reaktion auf Vorfälle: Es sollte ein detaillierter Plan zur Reaktion auf Sicherheitsvorfälle erstellt und regelmäßig aktualisiert werden.

Zusammenfassend lässt sich sagen, dass die Sicherung der Interconnections im NBP-Projekt einen ganzheitlichen Ansatz erfordert, der die Besonderheiten jeder Komponente berücksichtigt und gleichzeitig eine globale Kohärenz der Sicherheitsmaßnahmen gewährleistet. Die strikte Anwendung dieser Empfehlungen wird die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten gewährleisten und gleichzeitig die geltenden Normen und Vorschriften zum Schutz personenbezogener Daten einhalten.