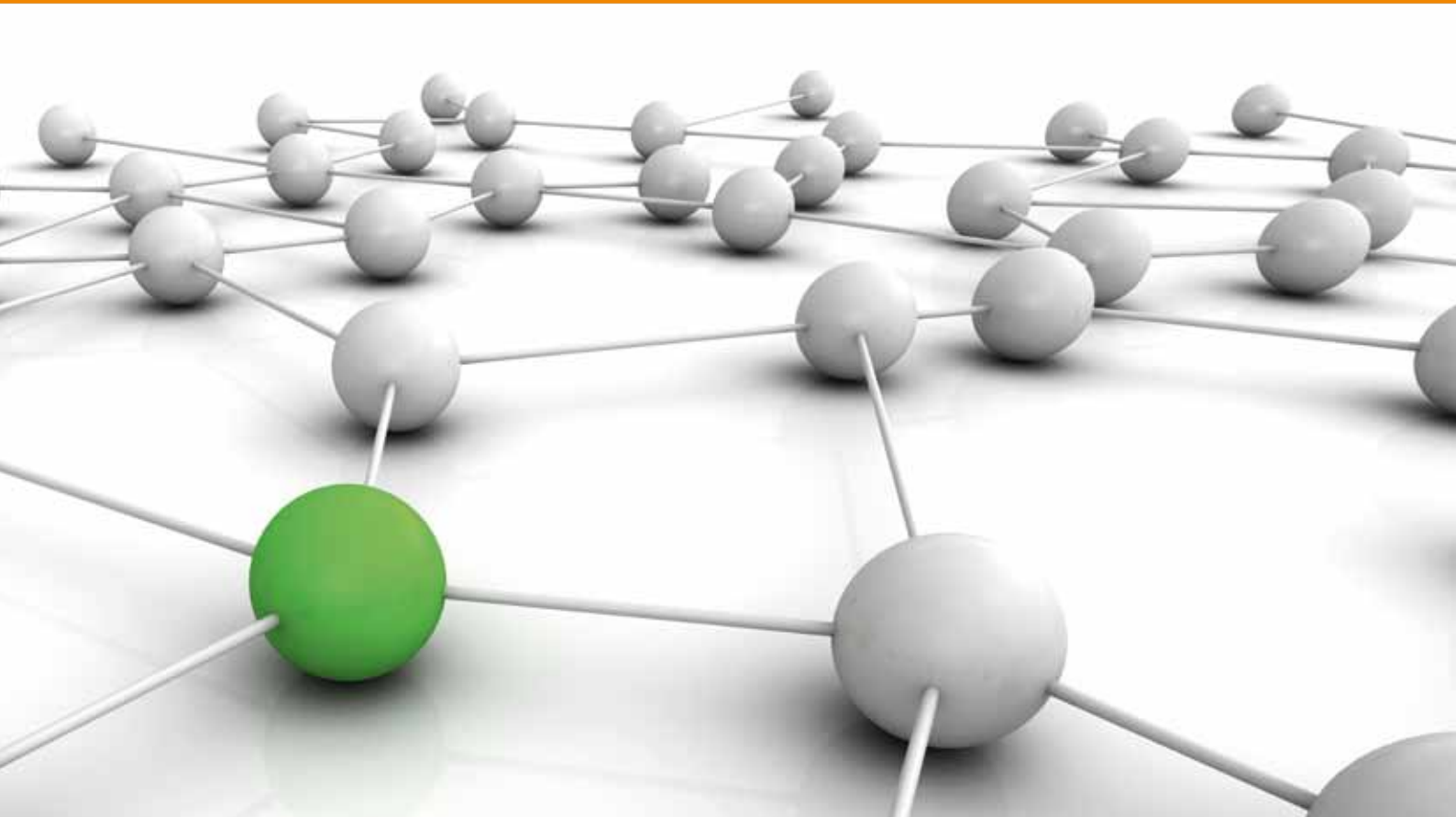


REFERENZARCHITEKTUR TEIL 4:

# Zentrale Dienste – die Übersetzer im Hintergrund

VERSION 1.0



**Über das Bündnis für Bildung e. V.**

Unter dem Dach des Bündnis für Bildung e. V. (BfB) arbeiten Hard- und Software-Hersteller, Entwickler bildungsspezifischer Lösungen, Netzwerk-Spezialisten, Schulbuchverlage sowie Anbieter von Lerninhalten und -medien eng mit Vertretern der Ministerien, Schulträgern sowie Lehrkräften und Eltern zusammen. Das Bündnis für Bildung ist ein gemeinnütziger Verein und finanziert sich ausschließlich über Mitgliedsbeiträge und Spenden.

Weitere Informationen zum BfB finden Sie unter [www.b-f-b.net/](http://www.b-f-b.net/)

REFERENZARCHITEKTUR TEIL 4:

# **Zentrale Dienste – die Übersetzer im Hintergrund**

VERSION 1.0

## Einleitung

Bildung ist die wichtigste Investition in die Zukunft unserer Gesellschaft und einer der Schlüsselfaktoren für wirtschaftliches Wachstum. Dabei muss unser föderales Bildungssystem zahlreichen Herausforderungen gerecht werden: Um der vernetzten Informationsgesellschaft Rechnung zu tragen und die nächste Generation optimal auf die beruflichen Herausforderungen der Zukunft vorzubereiten, muss ein nachhaltiges Bildungssystem stets einen Schritt voraus sein.

Das Bündnis für Bildung e. V. (BfB) hat sich zusammengeschlossen, um einen Beitrag für eine zukunftsgeradte Bildung zu leisten und gemeinsam mit allen Stakeholdern im Bildungsbereich offene und produktneutrale Konzepte für eine IT- Bildungsinfrastruktur für das ganzheitliche Lernen von morgen in Deutschland zu erarbeiten – die sogenannte Referenzarchitektur.

Diese besteht derzeit aus den Kapiteln Pädagogik, Infrastrukturmanagement, Zentrale Dienste (Data Services und Schnittstellen), Content Distribution und ID-Management. Das BfB veröffentlicht nun erste Kapitel der Referenzarchitektur, um den Dialog darüber mit den Akteuren und Entscheidern im Bildungsumfeld zu eröffnen und zur weiteren Mitarbeit an diesem Dokument anzuregen. Ziel des BfB ist es, die Referenzarchitektur ständig weiterzuentwickeln und an neue technische Entwicklungen anzupassen.

Das vorliegende Kapitel der Referenzarchitektur „Zentrale Dienste – die Übersetzer im Hintergrund“ liegt nun in der Version 1.0 vor.

Das BfB freut sich auf konstruktive Vorschläge und die Mitarbeit bei der Weiterentwicklung dieses Kapitels.

# Inhaltsverzeichnis

<b>1</b>	<b>Grundprinzipien und Vorgaben</b>	<b>5</b>
1.1	Flexibilität, Neutralität und Verfügbarkeit	5
1.2	Performance	5
1.3	Skalierbarkeit	6
1.4	Verfügbarkeit	6
1.5	Ausfallsicherheit	6
1.6	Sicherheit	6
1.7	Interoperabilität	6
<b>2</b>	<b>Interessensgruppen</b>	<b>7</b>
2.1	Benutzer	7
2.2	Anbieter	7
2.3	Betreiber	8
<b>3</b>	<b>Entwicklung und Planungsstand</b>	<b>8</b>
<b>4</b>	<b>Architektur der zentralen Dienste</b>	<b>8</b>
4.1	Produktkategorien	10
<b>5</b>	<b>Abgrenzung Systemgrenzen (zentral / dezentral)</b>	<b>10</b>
5.1	Katalogdienste	10
5.2	Vermittlungsdienste (Adapter, Konnektoren, Router etc.)	12
5.3	Datendienste und Schnittstellen	12
<b>6</b>	<b>Spezifikation der zentralen Daten- und Schnittstellendienste</b>	<b>14</b>
6.1	Gemeinsame Verfahrensweisen	14
<b>7</b>	<b>Spezifizierung der Katalogdienste</b>	<b>15</b>
7.1	Service des Katalogdienstes zu den Katalogdiensten generell	18
7.2	Service des Katalogdienstes zu den Katalogdiensten speziell	19
7.3	Lokalisierung	19
<b>8</b>	<b>Spezifizierung der Vermittlungsdienste</b>	<b>20</b>
<b>9</b>	<b>Spezifikation der Basisdienste der Datendienste und Schnittstellen</b>	<b>21</b>
9.1	Definition und Funktion	21
<b>10</b>	<b>Verfahrensabläufe</b>	<b>22</b>
10.1	Anforderungen und Regularien	22
10.2	Berechtigungskonzept	22
<b>11</b>	<b>Qualitätssicherung</b>	<b>23</b>
11.1	Informationsaustausch BfB, Entwickler, Dienstleister	23
11.2	Dokumentation (Versionierung und Freigabe)	23
<b>12</b>	<b>Bestehende Standards</b>	<b>24</b>

## Zentrale Dienste – die Übersetzer im Hintergrund

Die IT-Infrastruktur an Bildungseinrichtungen setzt sich häufig zusammen aus einer Vielzahl dezentraler IT-Anwendungen, unterschiedlichen Content-Angeboten und diversen Datenbanken, die miteinander nicht oder nur begrenzt interagieren können. Dies ist nicht nur teuer<sup>1</sup>, sondern auch aus organisatorischen Gründen nicht sinnvoll.

Aus allgemeinen Anforderungen an die IT-Infrastruktur von Schulen wird deutlich, dass es im Hintergrund ein System geben muss, das die verschiedenen Insellösungen miteinander verknüpft, um Kompatibilität und damit Datenaustausch zu gewährleisten. Solche zentralen Dienste ermöglichen die Verknüpfung unterschiedlicher IT-Systeme über definierte Schnittstellen. Die Vielfalt der Systeme wird dadurch nicht aufgehoben, sondern

im Gegenteil unterstützt, da die Interaktion zwischen den Systemen verbessert wird. Die Datendienste können also als eine gemeinsame Sprache zwischen den Systemen verstanden werden.

Die Vision ist, dass Schulen aus einem breiten Angebot die jeweils erforderlichen Anwendungen und den passenden Content auswählen können, unabhängig vom Hersteller und in der Gewissheit, dass die Systeme interagieren, ihre Daten austauschen und entsprechend verarbeiten können.

Die Grafik veranschaulicht, wie ein zentraler Dienst im Hintergrund die verschiedenen Akteure der gesamten IT-Schullandschaft miteinander verbinden kann und Daten und Inhalte dorthin gelangen, wo sie gebraucht werden.

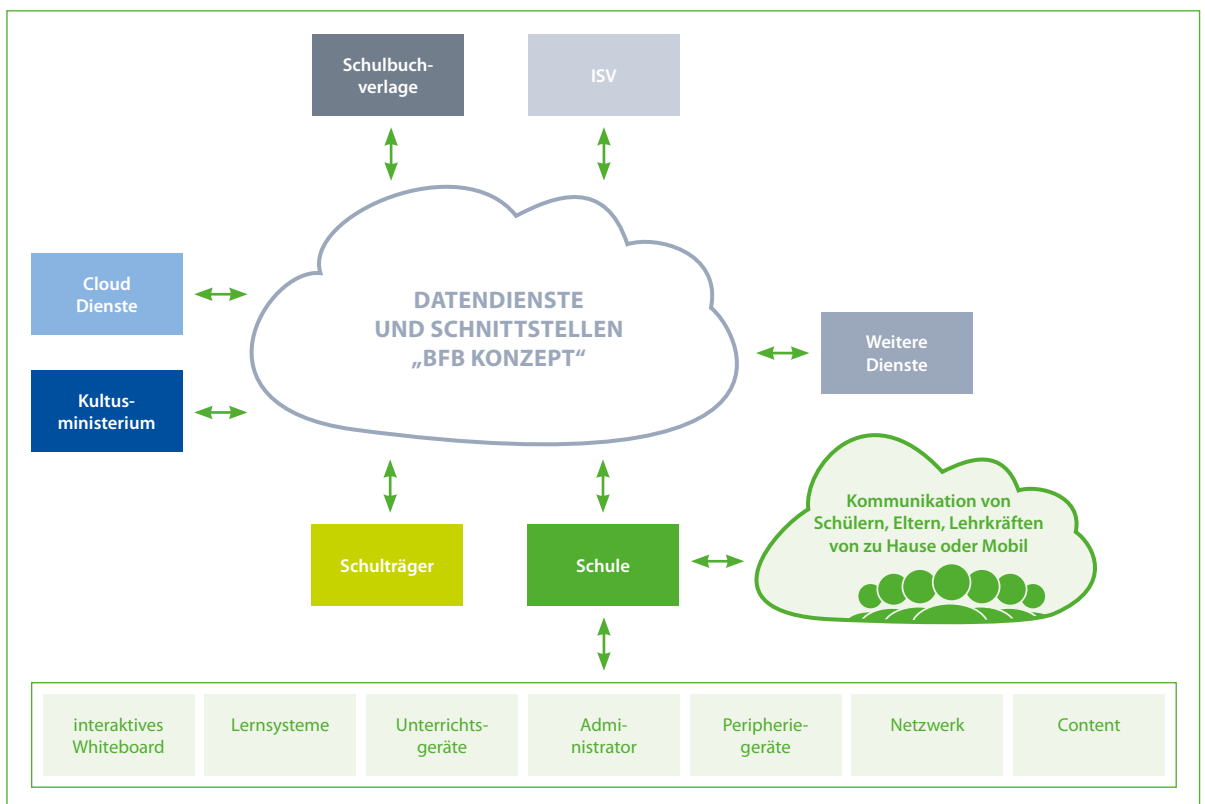


Abb: Darstellung über die Funktion der Datendienste

Nach den aktuellen Zahlen der Statistischen Ämter gibt es ca. 45.000 Institutionen und über 11,5 Millionen Personen im Schulsystem<sup>2</sup>. Wenn alle Schulen künftig solche Basisdienste nutzen wollten, entstünden große Anforderungen an die Skalierbarkeit und Leistungsfähigkeit solcher Dienste.

Dies haben wir berücksichtigt und werden in den nächsten Abschnitten die wichtigsten Parameter und Vorgaben für die zentralen Dienste beschreiben.

## 1 Grundprinzipien und Vorgaben

Dieses Kapitel beschreibt ausschließlich Anforderungen und Strukturen zentraler Dienste, die im Hintergrund einzelne IT-Komponenten miteinander verknüpfen. Es beschreibt ausdrücklich nicht die Ausprägungen und Funktionalitäten der einzelnen IT-Komponenten selbst. Sämtliche für den Nutzer sichtbare Oberflächen sind ebenfalls nicht Gegenstand der Betrachtung. Auch wenn einzelne Oberflächen viele verschiedene Systeme in einer einheitlichen Weise zur Verfügung stellen können, sollten sie dafür die hier angesprochenen Hintergründe verwenden, damit nicht jedes System jeweils aufs Neue die Integration der verschiedensten Lösungen implementieren muss.

Aufgrund des föderalen Bildungssystems in Deutschland und der Entscheidungsfreiheit, die Bildungseinrichtungen beim Einsatz von Software haben, kann nicht

davon ausgegangen werden, dass sich mittel- oder langfristig einzelne Lösungen vollständig durchsetzen. Unterschiedliche Oberflächen werden ihre Verfechter und Anwender finden, was zu einem sehr vitalen Markt und einer belebenden Konkurrenzsituation führen wird.

**Daher halten wir es für wichtig, folgende Grundprinzipien von den zentralen Hintergrunddiensten zu fordern:**

### 1.1 Flexibilität, Neutralität und Verfügbarkeit

Jede Lösung, die standardisierte und / oder gut dokumentierte Schnittstellen hat, kann eingebunden werden. Wenn möglich, greifen die Dienste auf allgemein verfügbare Industriestandards zurück. Der Zugriff wird über gängige Hardware, Betriebssysteme und Webservices sichergestellt.

Die Datendienste sind für Anbieter und Endkunden genau beschrieben und öffentlich verfügbar. Die Standards sind Hersteller- und Produkt-neutral und können als Grundlage für Investitionsentscheidungen und Ausschreibungen genutzt werden.

### 1.2 Performance

Mittelfristig sollten alle ca. 45.000 Institutionen und über 11,5 Mio. Benutzer zentrale Dienste, wie im Folgenden beschrieben, direkt oder indirekt in Anspruch nehmen können. Die Dienste müssen daher von vornherein entsprechend leistungsfähig geplant werden.

Hierbei ist zu berücksichtigen, dass zunächst eine dezentrale Installation der Dienste seitens der IT Anbieter erfolgt, dies entspannt die Anforderungslage zunächst. Dennoch gibt es eine Reihe von Funktionalitäten (z. B. Unterstützung von SSO), die aufgrund ihrer Natur zeitkritisch sind und daher auch zeitnah zur Verfügung gestellt werden sollten.

Anfragen an das System werden priorisiert. Missionskritische Anfragen werden vom System kurzfristig

<sup>1</sup> Einzellösungen sind deshalb teurer, weil Redundanzen vorgehalten werden müssen, dieselben administrativen Tätigkeiten für verschiedene Systeme anfallen (z. B. Nutzergruppen anlegen in Schulverwaltung, in Lernplattformen für Schulnetzwerke), mehrfaches Anlegen von Rollen und Rechten in verschiedenen Systemen etc.

<sup>2</sup> Vgl. Zahlen des Statistischen Bundesamtes: <https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/BildungForschungKultur/Schulen/Schulen.html>

bearbeitet. Ein Großteil der Anforderungen ist jedoch nicht zeitkritisch und kann daher in den Leerlaufzeiten bearbeitet werden. Jeder zentrale Dienst ist mit typischen und maximal zu tolerierenden Latenzzeiten zu beschreiben; und eine Messung ist vorzusehen.

**Direkt aus diesen Anforderungen an die Performance ergeben sich die nächsten Anforderungen:**

### 1.3 Skalierbarkeit

Die zentralen Dienste werden von vielen Nutzern gleichzeitig angefragt werden – in Spitzenzeiten dürften dies mehrere 100.000 (Anzahl der Institutionen\*Mittlere Clientzahl) paralleler Verbindungen sein. Das System muss deshalb von vornherein skalierbar sein. Weder das Abschalten noch das Erweitern einzelner Komponenten darf die Performance einschränken.

Da die Nutzungszahlen an Wochenenden und in den Schulferien voraussichtlich stark zurückgehen, wird eine – in Abhängigkeit von der Auslastung – automatisch skalierende Plattform für den Betrieb der Dienste eingesetzt. Die Skalierbarkeit bringt eine leichte Übertragbarkeit auf Szenarien mit weniger Nutzern mit sich. So ist auch der Betrieb in einzelnen Institutionen oder in einer Private Cloud vorgesehen.

Um die Effizienz der Skalierung vergleichbar zu machen, wird zusätzlich der Stromverbrauch erhoben und in Relation zu IT-Messgrößen gesetzt.

### 1.4 Verfügbarkeit

Die Dienste werden von verschiedensten Applikationen und Individuen in Anspruch genommen. Die Kommunikation erfolgt in der Regel asynchron. Dies bedingt eine Pufferung von Anfragen, und das Gesamtsystem arbeitet bezogen auf das Antwortverhalten nicht deterministisch. Da die Zugriffe weltweit erfolgen, ist eine Verfügbarkeit von 24\*7, also letztlich rund um die Uhr, vorzusehen.

Eine technische Unterbrechung von maximal zehn Minuten innerhalb redundanter Infrastruktur ist vom Anwender zu tolerieren. Der Ausfall nicht redundanter Infrastruktur ist vom Betreiber der Lokation zu steuern und zu verantworten.

Im Falle logischer Fehler ist die Wiederherstellung von zentralen Daten innerhalb von zehn Minuten vorzusehen. Der zu tolerierende Datenverlust darf vier Stunden nicht überschreiten (RPO). Durch geeignete technische und organisatorische Maßnahmen ist nachzuweisen, dass eine Wiederherstellung eines Notbetriebes ab Zeitpunkt des Ausfalls binnen 24 Stunden machbar ist (RTO). Dies gilt auch für schwere Bedienungsfehler.

Insbesondere zum Thema Verfügbarkeit muss eine genaue Bedarfsanalyse durchgeführt werden. Verfügbarkeit kann einer der größten Kostenpunkte sein, die zentrale Dienste verursachen.

### 1.5 Ausfallsicherheit

Die Bereitstellung der zentralen Dienste erfolgt auf Basis einer 24\*7-Verfügbarkeit. Dies bedingt ein automatisches lokationsübergreifendes Failover. Durch mindestens eine jährliche Überprüfung der Notfallpläne ist zu garantieren, dass das Erreichen des definierten Notbetriebes die Wiederherstellung der Dienst-Funktionalitäten nach Vorgaben der Verfügbarkeit auch für den Ausfall einer gesamten Lokation gilt (n+1 oder besser).

### 1.6 Sicherheit

Der Zugang zu sowie die Kommunikation mit den zentralen Diensten wird durch herausgegebene Zertifikate gesichert. Solange dies nicht als hoheitliche Aufgabe des Bundes verstanden wird, muss eine geeignete Organisation als Zertifikatstelle ausgesucht werden. Die Festlegung des Schutzbedarfs von Informationen, Anwendungen und IT-Systemen orientiert sich an den Schutzbedarfskategorien der IT-Grundschutz-Vorgehensweise des BSI<sup>3</sup>.

### 1.7 Interoperabilität

Die Entwicklung der zentralen Dienste durch Industrieunternehmen sollte ausdrücklich unter prinzipieller Berücksichtigung aller bestehenden Lösungskompo-

<sup>3</sup> Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0, Mai 2008. <http://www.bsi.bund.de/grundschutz>



nenten unabhängig von Hersteller und Betriebsplattform erfolgen.

Die Bereitstellung der Dienste erfolgt über entsprechende Web-Services, Plattformen kommunaler Rechenzentren oder individuelle Installationen an Institutionen. Die Migration bzw. Adaption bestehender Lösungen sollte bei entsprechender Anpassung durch deren Hersteller jederzeit möglich sein.

## 2 Interessensgruppen

**Eine große Herausforderung ist die Berücksichtigung der einzelnen Interessengruppen. Vorerst hat das BfB drei wichtige Gruppen definiert:**

- Benutzer
- Anbieter
- Betreiber

Das Konzept ist jedoch so flexibel, dass weitere Gruppen aufgenommen werden können.

### 2.1 Benutzer

Kultusministerien, Schulträger, Schulen und Pädagogen möchten eine langfristige und kontinuierliche Weiterentwicklung ohne hohe Kosten bei maximaler Stabilität und Verfügbarkeit erreichen. Daher ist ihre Interessenlage, nicht die Infrastruktur zu unterhalten oder deren Komplexität in allen Belangen zu verstehen, sondern nur ihren inhaltlichen Auftrag möglichst störungsfrei zu gewährleisten.

**Wichtig sind daher:**

- Reduktion der direkten Kosten (liquiditätsrelevanten Kosten);
- Verbesserte medienbruchfreie Informationsflüsse;
- Verbesserte Möglichkeiten des Controllings und qualitativ hochstehende Lenkungsinformationen.

SchülerInnen und Eltern haben das primäre Ziel, eine transparente Informationslage über den Ist- und Sollzu-

stand der Ausbildung zu erhalten und die Gewissheit, dass das Gelernte den perspektivischen Übergang von Schule zu Wirtschaft optimal gewährleistet. Dabei spielt das medienbruchfreie, sichere Zusammenspiel aller Informationen eine zentrale Rolle.

**Für diese Gruppe ist wichtig:**

- Medienbruchfreier Zugriff auf die Informationen über Ist (Leistungsdaten, Aufgaben, etc.) und Soll (Lernziele, Entwicklungsmöglichkeiten, Perspektiven);
- Transparenz der Art der Beurteilung der Konsequenzen des aktuellen Ist-Zustandes und der Möglichkeit Informationen zur Verbesserung des zu erwartenden Zustandes in der Zukunft;
- Zeitlich unbegrenzter Zugriff auf Informationen, Medien und Materialien;
- Direkte und zeitlich unbegrenzte Kommunikation zwischen Bildungspartnern;
- Keine Bürokratie oder kein unnötiger Verwaltungsaufwand. Heutzutage ist es für Eltern kaum nachvollziehbar, weshalb mit den vorhandenen Kommunikationsmitteln noch so viele Probleme bei trivialen Dingen wie Schulinformationen, Aufgaben oder Nachhilfe existieren.

### 2.2 Anbieter

**Die Anbieter von Bildungssoftware (von der Schulverwaltung bis zu Schulbuchverlagen) unterliegen in der Regel den folgenden Grundverhalten:**

- Möglichst wenige Veränderungen in lukrativen und bestehenden Marktfeldern, die durch sie beherrscht werden.
- Möglichst hohe Innovation in noch nicht existierenden oder nicht besetzten Marktfeldern, um neue Märkte zu erschließen und eine langfristige Kundenbindung zu ermöglichen.

**Der aktuelle Markt zeigt folgende Charakteristik:**

- Stark fragmentierte, vom Bundesland abhängige Märkte, die sich aufgrund der unterschiedlichen Schultypen und bestehenden Infrastrukturen kaum sinnvoll flächendeckend

- durchdringen lassen.
- Großer Aufwand für die Akquisition und kleine Margen.

Viele Anbieter sind daher eher klein und regional orientiert. Entsprechend sind die Schnittstellen auf die unmittelbar in der jeweiligen Schule oder im entsprechenden Bundesland genutzten Produkte ausgerichtet und existieren in der Regel nur dort, wo sie aus zwingenden Gründen gebaut werden mussten. Schnittstellen werden also nicht proaktiv bereitgestellt, sondern bedarfsgerecht aus den unmittelbaren lokalen Bedürfnissen heraus. Dafür ist immer die Zusammenarbeit der jeweiligen Anbieter zwingend notwendig, und ein wirtschaftlicher Nutzen für die Anbieter bzw. eine Kostenerstattung durch die Benutzer (Schule, Schulträger, Land etc.).

### 2.3 Betreiber

Die Betreiber sind Unternehmen oder Organisationen, die das vorliegende Konzept in lauffähige Produkte umwandeln. Ihr Interesse liegt in einer möglichst großen Verbreitung und Nutzung ihrer Implementationen.

## 3 Entwicklung und Planungsstand

Die Architektur der Datendienste und damit des zentralen Schnittstellen-Managements baut auf einer Analyse der aktuellen Systemlandschaft im deutschen Schulsystem auf. Dabei wurden alle denkbaren Interaktionen zwischen den Bildungspartnern (von SchülerInnen über Lehrkräfte und Eltern bis hin zum Kultusministerium) in Betracht gezogen.

Bisher gibt es keinen übergreifenden systemischen Ansatz, an den sich die Softwarehersteller anlehnen könnten. Und es gibt nur wenige, die über standardisierte Austauschtechnologien und Datenstrukturen verfügen. Letztere sollten aber soweit wie möglich berücksichtigt und integriert werden.

### Wesentliche Ziele der Architektur der Datendienste sind:

- den Herstellern von Bildungssoftware eine maximale Freiheit in der inhaltlichen und technologischen Entwicklung zu gewährleisten, gleichzeitig aber ein Maximum an Anbindungsmöglichkeiten zu ermöglichen;
- den Benutzern eine langfristige Wahl- und Entwicklungsmöglichkeit von neuen und nutzbringenden Zusatzdiensten zu bieten.

Dieses Kapitel soll Bauplan für einen Betreiber der Datendienste und Schnittstellen sein. Nachfolgend werden die wichtigsten Dienstmerkmale und ihre beabsichtigte Wirkungsweise beschrieben. Die technischen Details und deren Umsetzung müssen in einem gesonderten Whitepaper festgelegt werden.

Die folgenden Kapitel werden die einzelnen Daten- und Schnittstellendienste detailliert auflisten und beschreiben. Darüber hinaus werden im Rahmen einzelner Dienste Praxisbeispiele und Abläufe dargestellt, die exemplarisch für die Gruppe der dargestellten Dienste den Zweck und das Verhalten der Dienste besser erläutern sollen.

## 4 Architektur der zentralen Dienste

Die Architektur unterscheidet mehrere Kategorien von Diensten, die in unterschiedlicher Form durch die Anbieter verwendet werden können. Allen Diensten ist jedoch gemeinsam, dass sie keine inhaltlichen Daten speichern oder auswerten. Ihre primäre Aufgabe ist es, den reibungslosen Austausch von Informationen zwischen verschiedenen Systemen zu erlauben.

Die Datendienste und Schnittstellen können also als eine gemeinsame Sprache zwischen den Systemen verstanden werden. Sie nehmen jedoch keinen Einfluss auf das Nutzungsverhalten oder die inhaltliche Ausgestaltung der ausgetauschten Informationen.

Die Architektur sieht neben den informativen **Katalogdiensten** zwei unterschiedliche Komponentengruppen

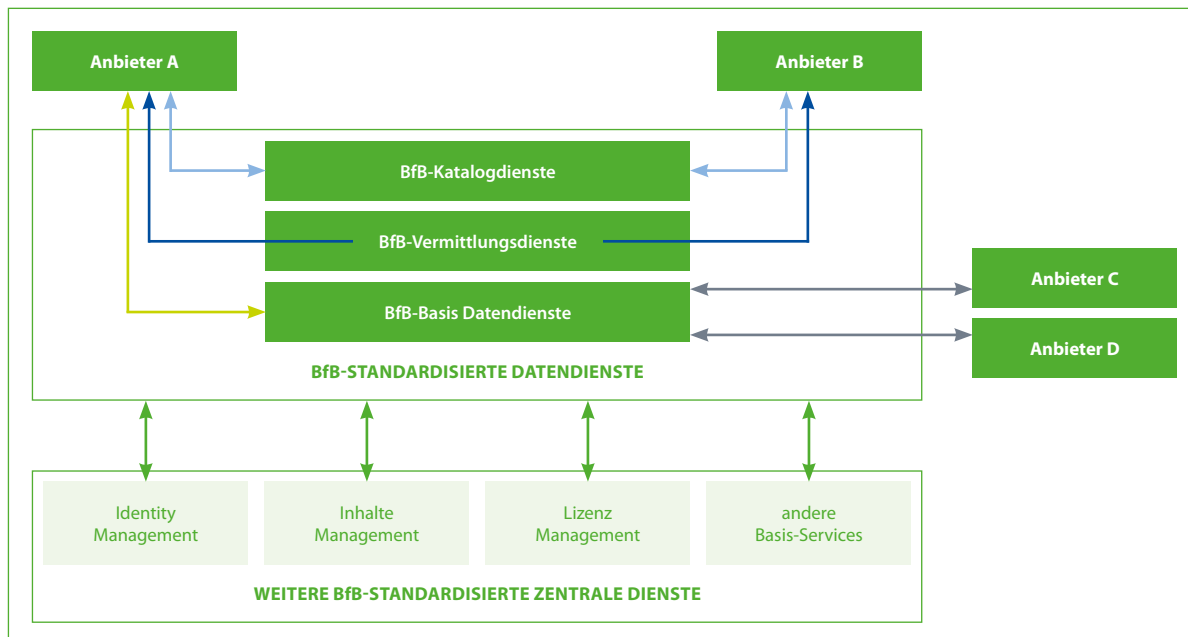


Abb: Daten- und Schnittstellenarchitektur

vor, die sich hauptsächlich durch ihre funktionale Qualität unterscheiden. Während **Vermittlungsdienste** einfach eine Art Tunnel zwischen dem Informationsaustausch zweier oder mehrerer Anbieter darstellt, sind Basisdienste „veredelte“ oder anspruchsvollere Dienste, welche zusätzliche systemische Abklärungen für die Ausführungen des Informationsaustausches voraussetzen.

Zentrale Daten- und Schnittstellendienste, also Katalog- und Vermittlungsdienste, sind zuständig für den horizontalen Austausch von Informationen über die Systemgrenzen hinaus – also themen- oder fachbereichsübergreifend.

Zentrale Basisdienste sind zuständig für den vertikalen Funktionsbereich, z. B. für das Identitätsmanagement. Die Basisdienste müssen sich von fast allen Anbietern immer wieder nutzen lassen, brauchen aber nur von wenigen Anbietern (Landesinstitute oder vergleichbare Institutionen) bereitgestellt zu werden.

Basisdienste sind z. B. Identitätsmanagement, Inhaltsmanagement, Lizenzmanagement etc. Sie werden gesondert ausführlicher behandelt.

Die hier beschriebenen Dienste können zentral (bundesweit) oder dezentral durch einen oder mehrere Anbieter bereitgestellt werden. Auch wenn eine zentrale Bereitstellung für alle Schulen in Deutschland wünschens- und anstrengenswert erscheint, muss davon ausgegangen werden, dass die zentrale Bereitstellung (wie z. B. für Telefonie oder Autobahn) erst in einer zweiten Phase realisiert werden kann, sofern gesetzliche, politische und wirtschaftliche Rahmenbedingungen dies zulassen.

Daher wird das System so konzipiert, dass eine parallele Bereitstellung gleichartiger Dienste an mehreren Orten durch unterschiedliche Anbieter (öffentlich-rechtliche oder private) möglich ist und eine gegenseitige Registrations- und Abgleichmöglichkeit über die Katalogdienste erfolgt. Dies kann im einfachsten Fall durch einen Nachweis der Existenz geschehen (Eintrag in den Katalog).

## 4.1 Produktkategorien

Auf dem Bildungsmarkt lassen sich folgende Produktkategorien für Software ausmachen:

- Infrastruktursoftware (Steuerung von Bildschirmen, Heizung, Energie etc.);
- Verwaltungssoftware (Schulverwaltung, Finanzen, Zutritt und Identitätsmanagement, Lizenzverwaltung, Bibliothek etc.);
- Software für die pädagogische Verwaltung (Klassenbuch, Leistungen etc.);
- Pädagogische Software (Lernplattformen, Medien, Materialien, interaktive Whiteboards etc.);
- Standardsoftware (Betriebssysteme für eigene Server, Office-Pakete etc.);
- Software für die Verpflegung (Mensa etc.).

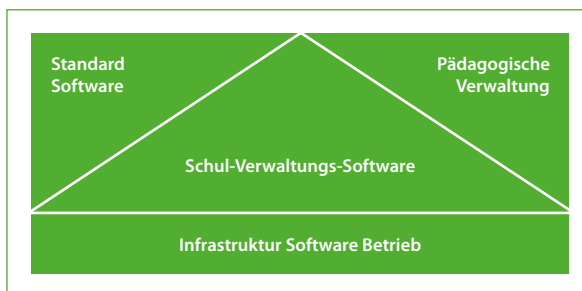


Abb: Produktkategorien

Ziel der Datendienste ist es, dass Anwendungen aus den verschiedenen Produktkategorien medienbruchfrei zusammenarbeiten können.

Derzeit gibt es noch immer den Trend, dass Anbieter aus der Not eine Tugend machen und immer mehr Funktionalitäten in die eigene Software integrieren, um das Ziel der medienbruchfreien Arbeit zu gewährleisten. Dadurch werden die Produkte einander immer ähnlicher und gleichzeitig monolithischer. Der Austausch von Daten und Inhalten wird dadurch nicht erleichtert.

Einfach viele Applikationen (Apps) zu bauen, um viele Funktionalitäten anzubieten, führt ebenfalls nicht zum Ziel, da dadurch das Zusammenspiel der einzelnen Funktionalitäten noch weniger gewährleistet wird bzw.

die Problematik der unterschiedlichen Datenhaltungen oder Logins nach wie vor existiert.

Die Lösung hierfür bieten Datendienste im Hintergrund, die die Vielfalt an Produkten, neuen Funktionalitäten und Apps so verknüpfen, dass der Datenaustausch unter sicheren, gleichartigen und geordneten Rahmenbedingungen stattfinden kann.

## 5 Abgrenzung Systemgrenzen (zentral / dezentral)

Die generellen Systemgrenzen von Daten- und Schnittstellendiensten können wie folgt definiert werden:

- Die Datendienste und Schnittstellen stellen nur den Informationsaustausch von Produkten unterschiedlicher Anbieter und von zentralen Basisdiensten sicher. Es werden keine inhaltlichen Prüfungen von Daten vorgenommen und auch keine inhaltlichen Datenhaltungen angelegt.
- Die Datendienste und Schnittstellen sind unabhängig von Produkten oder Organisationen und stellen nur den Betrieb des Informationsaustauschs sicher. Daten werden nur für technisches Caching oder Weiterleitungsfunktionen sowie für die technische Sicherstellung der Transaktionssicherheit vorgesehen.

### 5.1 Katalogdienste

Die Katalogdienste haben die Aufgabe, alle genutzten oder verfügbaren Dienste aufzulisten und deren Grundparameter sowie eventuelle funktionale Beschreibungen, soweit verfügbar, bereitzustellen. Dazu gehören Technik, Parameter, Interaktionsverhalten, Anbieter, geographische Verfügbarkeit und Status der Betriebsverfügbarkeit (Prototyp, Test, Freigabe, Sperrung etc.).

Es werden nur Dienste ausgewiesen, die im Rahmen der Zertifizierung der Implementierung den Ansprüchen des vorliegenden Konzepts entsprechen. Der Betreiber dieser Katalogdienste verpflichtet sich, die gesetzlichen, technischen und fachlichen Vorgaben dieses Konzepts zu gewährleisten.

Die Katalogdienste müssen durch den Betreiber gepflegt und ergänzt bzw. verwaltet werden können. Dies sollte weitgehend automatisiert möglich sein. Auch der Austausch mit anderen Katalogdiensten muss sichergestellt werden, bzw. muss jeder Katalogdienst alle parallelen oder ergänzenden Katalogdienste referenzieren

können, damit die Kenntnis eines Katalogdienstes als Einstiegspunkt genügt. Es muss ein rollenbasiertes Berechtigungssystem vorliegen, welches vom Gast (für eine einfache elektronische Übersicht der verfügbaren Dienste) bis zum Administrator des Katalogdienstes alle wichtigen Funktionen abdeckt.

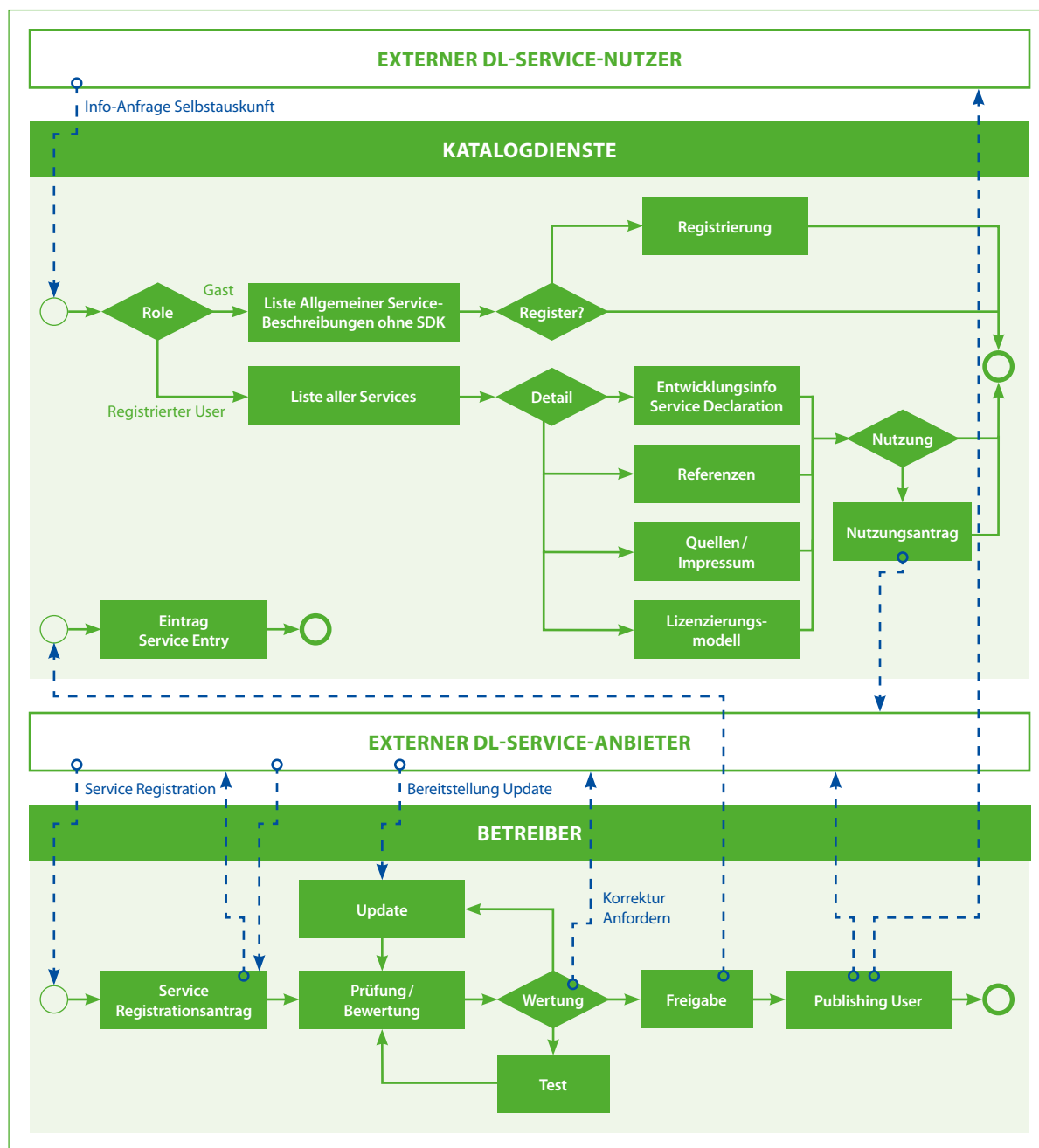


Abb: Genereller Ablauf Katalogdienste

## 5.2 Vermittlungsdienste (Adapter, Konnektoren, Router etc.)

Ein Vermittlungsdienst hat nur eine passive Rolle, die darin besteht, Funktionsaufrufe unterschiedlicher Anbieter oder deren Produkte technisch weiterzuleiten. Dabei ist es unerheblich, was dieser Dienst macht oder mit welchen Daten er arbeitet. Es wird weder eine inhaltliche noch eine funktionale Prüfung vorgesehen. Eine Zuordnung bzw. ein Mapping zwischen einzelnen Datenmodellen und Taxonomien ist jedoch zu implementieren, sobald dies erforderlich ist.

Der Betreiber haftet weder für den Datenschutz der angeschlossenen Dienste noch für die Art der Kommunikation zwischen den Anbietern. Diese Dienstleistung dient nur der Gewährleistung des Daten- und Signalaustauschs zwischen den Funktionen unterschiedlicher Anbieter.

In diesen Vermittlungsdiensten wird lediglich geprüft, ob die beiden Austauschpartner registrierte Anbieter sind bzw. ob deren Dienste in dieser Form einen Austausch erlauben. Umgekehrt unterbindet das System automatisch den Austausch, wenn eine Seite den Austausch unterbinden will.

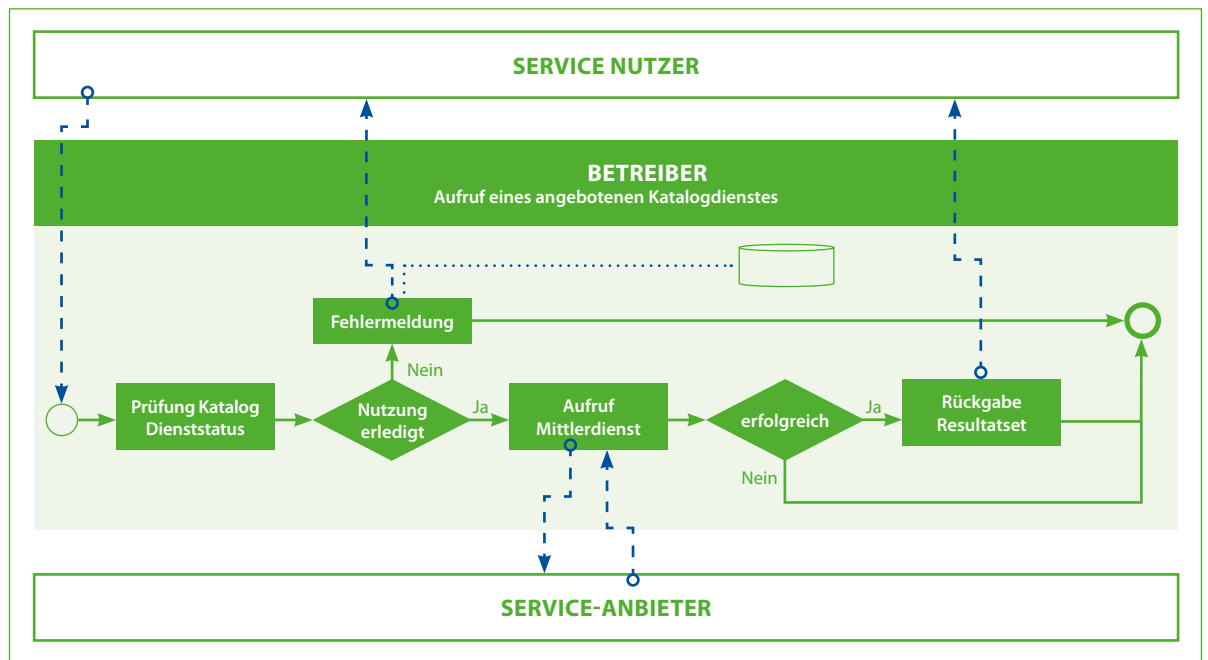


Abb: Vermittlungsdienst

## 5.3 Datendienste und Schnittstellen

**Basis-Daten- und -Schnittstellendienste haben einen erweiterten Aufgabenbereich. Sie prüfen nicht nur, ob eine Punkt-zu-Punkt-Verbindung erlaubt ist, sondern führen u. a. Folgendes durch:**

- Eigenständige Prüfungen;
- Zusammenführung verschiedener Quellen;
- Logische Verknüpfungen zwischen unterschiedlichen Daten.

**Typische Beispiele sind:**

- Prüfung der Identität einzelner User, des Aufrufs und der Weiterleitung an 1-n Zielgruppen, die ebenfalls geprüft werden müssen;
- Prüfungen, ob vorliegende Lizenzen ausreichen. Wobei die angeführten Beispiele nicht inhaltlich abgehandelt werden, sondern kommunikationstechnisch (nur die Aufrufe und die Auswertung der Resultate, um die Weiterleitung zu gewährleisten);
- Inhaltssuche in verschiedenen Quellen in den gesamten verfügbaren Content-Repositoryn aller Anbieter.

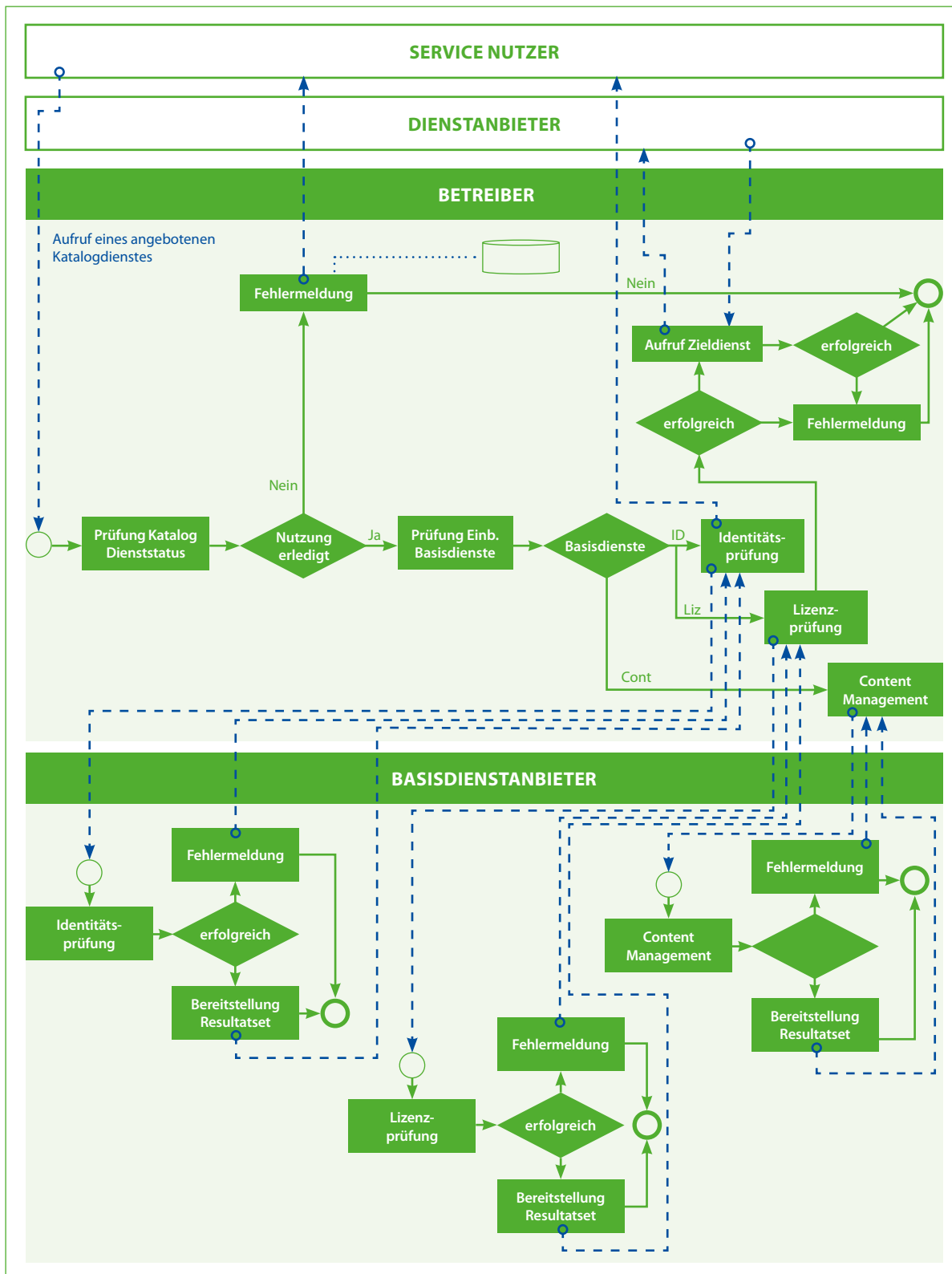


Abb: Basisdienste, Datenservices und -schnittstellen

## 6 Spezifikation der zentralen Daten- und Schnittstellendienste

**Prinzipiell unterscheiden wir zwei Arten von Diensten bzw. Schnittstellen:**

- die zentralen oder internen Dienste der Daten- und Schnittstellendienste (in der Hoheit des Betreibers);
- und die Hersteller oder externen Dienste (in der Hoheit der Hersteller bzw. Anbieter).

Hierbei geht es um die internen Dienste der Daten- und Schnittstellendienste, die mit den externen Diensten kommunizieren. Wenn es beispielsweise  $x$  Hersteller gibt, die das Management von  $y$  Bereitstellungen von Content ansprechen müssen, stellen diese sicher, dass nur  $x + y$  Schnittstellen (und nicht  $x \cdot y$ ) von den Herstellern implementiert werden müssen, da der zentrale Dienst einen Knoten zur Kommunikation zur Verfügung stellt.

### 6.1 Gemeinsame Verfahrensweisen

#### Versionierung der Schnittstellen

Für jeden Anbieter von Schnittstellen oder jeden Betreiber eines Daten- und Schnittstellendienstes ist es notwendig, diese kontinuierlich weiterzuentwickeln und zu erweitern. Trotz ständiger Veränderungen muss die fehlerfreie Nutzung der Schnittstellen im automatisierten Umfeld des Betreibers gewährleistet bleiben. Daher werden Schnittstellen des hier betrachteten Dienstkomplexes einer Versionierung unterstellt. Eine solche Versionierung wird sowohl physisch (Parameter und Technologie) als auch logisch-inhaltlich (Daten und Businesslogik) sichergestellt.

Das bedeutet, dass die Schnittstellen grundsätzlich abwärtskompatibel konzipiert und im Falle von technologischer oder inhaltlicher Veränderung, die eine Abwärtskompatibilität nicht mehr gewährleistet, durch einen organisatorischen Workflow ergänzt werden müssen.

Somit erhält jede Schnittstelle eine Versionsnummer, die eine Aussage über die Veränderung ersichtlich macht. Ein mögliches Beispiel wäre: AAB 1.0. Hierbei

bringt die erste Ziffer die Abwärtskompatibilität zum Ausdruck, die zweite Ziffer die Aussage, ob es sich um eine funktionale Erweiterung handelt, und die dritte Ziffer, ob es Bugfixes enthält. Die eigentliche Versionsnummer 1.0 und folgende gibt die Unterscheidung einer neuen Schnittstelle in Major- und Minor-Version zum Ausdruck.

In der Konsequenz erhält jeder Dienst auch im Katalogdienst diese Kennung in der Liste der verfügbaren Dienste. Damit wird eine vollständige Historisierung gewährleistet.

#### Warnhinweise bei wegfallenden Diensten

Außerdem sind Warnhinweise der einzelnen Schnittstellen zu implementieren, die rechtzeitig auf zukünftige Inkompatibilitäten hinweisen, damit Nutzern dieser Schnittstelle genügend Zeit für eine Reaktion bleibt. Dies kann dann der Fall sein, wenn vorhandene Schnittstellen wegfallen oder sich die Spezifikationen inhaltlich so ändern, dass ein weiteres Bedienen der alten Funktionalität nicht mehr möglich ist. Veränderungen sollten aber nach Möglichkeit so implementiert werden, dass solche Situationen so wenig wie möglich auftauchen. Als organisatorische Komponente muss den bekannten Nutzern das Vorliegen einer neuen Version über den Kommunikationsdienst der Anbieter, die diese Schnittstelle nutzen, bekannt gegeben werden.

#### Transaktionssicherheit

Jede Schnittstelle (sowohl des Betreibers als auch des Diensteanbieters) muss Transaktionssicherheit gewährleisten. Der Daten- und Schnittstellendienst stellt dies für die eigenen Funktionen und Services sicher.

Transaktionssicherheit bedeutet die Wiederherstellung auf einen kontrollierten Wiederaufsetzpunkt. Gleichzeitig muss eine Wiederholbarkeit sichergestellt werden.

Die Datendienste protokollieren die Fehlersituationen und intervenieren im Wiederholungsfall (Kriterien hierfür müssen noch festgelegt werden) ab einer kritischen Größe beim Verursacher. Die Systeme legen intern einen Wiederaufsetzpunkt fest, damit ein kontrolliertes Wiederaufsetzen durch einen Rollback einer Transaktion möglich ist. Analog verfährt der Betreiber mit den Datendiensten.



## Fehlerauskunft

Die aufgezeichneten Fehlersituationen stehen dem aufrufenden Anbieter bzw. Dienstleister zur weiteren Verarbeitung zur Verfügung und werden im Regelfall automatisch an ihn weitergeleitet. Eine weitergehende Auswertung über die Zeitachse ist vorzusehen, jedoch nicht zwingend.

## Dienstselbstauskunft

**Jeder Dienst (dies gilt also für Dienste von externen Herstellern und internen Diensten von Betreibern) verfügt über eine Schnittstelle, um Auskunft zu geben über**

- Status (Test, Prototyping, betriebsbereit, Sperrung, Außerbetriebnahme)
- Funktionsumfang (Beschreibung)
- Parameter (Liste mit Erläuterung)
- Interaktionsverhalten (Status, Fehlermeldungen)

## Kommunikationsrichtungen

Die zentralen Daten- und Schnittstellendienste müssen berücksichtigen, in welcher Form die beteiligten IT-Systeme miteinander kommunizieren möchten.

- **Unidirektional**  
Eine Komponente schickt bspw. Informationen an eine andere zum dortigen Verbleib.  
**Beispiel:** Benutzerinformationen aus der Schulverwaltung werden an das pädagogische Netz übermittelt. Änderungen im pädagogischen Netzwerk reflektieren jedoch nicht in die Schulverwaltungssoftware.
- **Bidirektional**  
Eine Komponente übermittelt zum Zweck der Verarbeitung Informationen an eine andere und erwartet ein Ergebnis.  
**Beispiel:** Export von der Schulverwaltung in die Stundenplanerstellung. Das Ergebnis fließt zur Führung von Stundenkonten wieder zurück.
- **Automatisch**  
Eine Komponente übermittelt Informationen automatisch ohne Benutzereingriff.  
**Beispiel:** Im pädagogischen Netzwerk wird ein Benutzer angelegt, woraufhin automatisch ein entsprechender Account in einem LMS o. Ä. angelegt wird.

- **Erst nach Autorisierung**

Aufgrund datenschutzrechtlicher Erwägungen dürfen Informationen, insbesondere wenn sie die Schule verlassen, nicht automatisch übermittelt werden.

**Beispiel:** Der Vertretungsplan wird bearbeitet und erst nach Autorisierung durch den Planer an schulische Info-Boards in der Pausenhalle oder ins schulische Web-Portal übermittelt.

- **Aktiv**

Eine aktive Kommunikation beschreibt die Möglichkeit einer Komponente, direkt über die zentralen Basis-Dienste Informationen an eine andere Komponente zu schicken und dort eine unmittelbare Reaktion zu erzielen. Die aktive Kommunikation bedingt medienbruchfreie Übertragungswege und Erreichbarkeit der Kommunikationspartner.

- **Passiv**

Passive Kommunikation ist notwendig, wenn ein Kommunikationspartner nicht direkt erreichbar ist, sei es aus technischen oder Sicherheits-Gründen. In solchen Fällen ist die Kommunikation über einen Mittler zwecks Pufferung notwendig. Das heißt, eine Komponente hinterlegt Informationen an zentraler Stelle, der Kommunikationspartner holt sie in regelmäßigen Abständen von dort ab.

## 7 Spezifizierung der Katalogdienste

**Katalogdienste haben die Aufgabe, Informationen bereitzustellen über:**

- den Daten- und Schnittstellendienst generell
- die Vermittlungsdienste generell
- die Vermittlungsdienste im Speziellen (verfügbare Dienste)
- die Basis-Datendienste und -Schnittstellen generell
- die Basis-Datendienste und -Schnittstellen im Speziellen (Liste)

Unter dem Begriff „generell“ verstehen wir, dass die allgemeine Handhabung und Nutzung der Basis-Daten- und -Schnittstellendienste (Katalog-, Vermittlung und Basisdienste) erläutert werden – also die Verhaltensmuster, die alle speziellen Dienste gemeinsam aufweisen. Unter „speziell“ verstehen wir, dass jeder einzelne Dienst im Detail beschrieben und erläutert wird.

Jeder Eintrag des Katalogdienstes ist versioniert und ermöglicht einen Rückblick in die Historie.

**Jeder Eintrag zu einem Dienst muss mindestens folgende Informationen beinhalten:**

- Bezeichnung
- Version
- Status (Test, Prototyping, betriebsbereit, Sperrung, Außerbetriebnahme)
- Funktionsumfang (Beschreibung)
- annotierte Parameterliste
- Interaktionsverhalten (Status, Fehlermeldungen)
- Anbieter
- Links zu SOK
- Benutzer (Liste der effektiven Benutzer)
- Lizenzierungsmodell (Lizenztyp der Nutzung, von offen uneingeschränkt bis exklusiver Benutzerkreis)
- Sicherheitsstufe der Kommunikation
- Sicherheitsstufe der Datenhaltung

**Optional:**

- Userfeedback (\*\*\*\*\* Bewertung durch Hersteller von Diensten)

### **Zielgruppe des Dienstes**

Die Zielgruppen des Katalogdienstes sind primär die Anbieter bestehender Produkte bzw. Services und in zweiter Priorität neue Anbieter für neue Services. Indirekt Benutzer (weil nicht primäre Informationsquelle) können auch Kultusministerien, Forschungs- oder vergleichbare Institutionen sein.

### **Nutzen**

**Der Nutzen von Katalogdiensten ist über die Zeitachse betrachtet sehr nachhaltig:**

- Der Hauptnutzen von Katalogdiensten ist eine einfache Übersicht für Anbieter, Benutzer und Entwicklungsfirmen über bestehende Funktionsservices.
- Ihr mittelfristiger Nutzen ist eine Übersicht über die Marktnischen und die Möglichkeit, auf spezielle Dienstleistungen zu fokussieren.

### **Organisatorische Verfahren**

**(Registration, Aufruf, Löschung etc.)**

**Die Ablauforganisation des Katalogdienstes orientiert sich an folgendem grobem Ablauf:**

- Der Anbieter informiert sich über die Verfahrensweise einer Dienstzertifizierung beim BfB.
- Der Anbieter erhält die Verfahrensanforderungen und die URL für die Katalogdienste.
- Der Anbieter kann sich über das BfB für die Registrierung von 1-n Services anmelden.
- Das Gremium für die Zertifizierung wird informiert, und der Interessent wird angemeldet.
- Der Interessent meldet sich für die Testphase bei einem Betreiber in seiner Nähe oder im Zielgebiet seines Interesses.
- Der Interessent bekommt vom Betreiber ein Testzertifikat (technisches Zertifikat) und kann seine Katalogdienste im System aufnehmen.
- Das evolutionäre Prototyping mit bestehenden Anbietern des Betreibers oder direkt mit dem Betreiber wird abgesprochen.
- Sind die Tests erfolgreich, meldet der Interessent die Schnittstellen zur Zertifizierung beim Zertifizierungspartner des BfB an.
- Die Prüfung der Schnittstellendienste wird durchgeführt.
- Eventuelle Korrekturen werden durchgeführt, und eine Nachprüfung wird angeordnet.
- Mit der Freigabe durch die Zertifizierungsstelle wird der Dienst im Katalogdienst für die Öffentlichkeit freigeschaltet. Gleichzeitig werden die anderen Betreiber über die Freigabe informiert.
- Mit der Freigabe wird eine Vereinbarung mit dem Betreiber und der Zertifizierungsstelle

getroffen, in welcher sich der Anbieter des Dienstes für die Einhaltung der datenschutzrechtlichen Rahmenbedingungen verpflichtet.

Für einen neuen Release (neue Version) werden vereinfachte Verfahren angewendet. Typischerweise wird der Betreiber des Dienstes nur zur Freigabe des Dienstes eingeladen. Dennoch muss die Testphase mit dem Betreiber durchlaufen und entsprechend abgenommen werden.

Die Löschung eines Dienstes wird mit entsprechendem Vorlauf durch eine schriftliche Mitteilung des Betreibers bzw. des Anbieters kommuniziert. Dasselbe Verfahren gilt für neue Daten- oder Schnittstellendienste des Betreibers.

#### **Technische Verfahrensanforderungen**

Das technische Verfahren, um in den Katalogservice als Dienst aufgenommen zu werden, unterliegt schwerwiegend dem Verfahren, die der jeweilige Betreiber festlegt. Generell muss der Betreiber den bereits erwähnten Testablauf protokollieren.

#### **Jeder Dienst muss den Nachweis erbringen, dass:**

- im Normalbetrieb alles stabil läuft (eine vorgegebene Anzahl von Aufrufen des Dienstes wurde für den Empfänger vollständig, fachlich korrekt und ohne Fehlersituation durchlaufen);
- der Last-Test mit n parallelen Aufrufen durch unterschiedliche Quellen erfolgreich war;
- im Ausnahmefall eine Transaktion durch einen Rollback zurückgesetzt wird;
- das Wiederanlaufverfahren vollständig automatisch durchgeführt wird;
- die verwendeten technologischen Konzepte nicht den geforderten Ansprüchen der Zieltechnologie widerspricht (nicht die Hersteller-abhängige, sondern die Architektur der gewählten Zieltechnologie);
- jede Ausnahmesituation, soweit sie technisch möglich ist, mit qualifizierten Fehlercodes protokolliert und die Zielgruppen adäquat informiert werden;

- die datenschutzrechtlichen Anforderungen eingehalten werden und die notwendigen Kontrollen durchgeführt werden können.

#### **Beispiel**

Ein einfaches Beispiel könnte sein, dass ein Anbieter eine bidirektionale Schnittstelle zur Übertragung von Schülerdaten registrieren lassen möchte, so dass weitere Systeme eine direkte Anbindung an sein Produkt vornehmen können. In diesem einfachen Beispiel werden nur der Anbieter und der Betreiber sowie die Zertifizierungsstelle tangiert (einfache Vermittlungsdienste).

In einem komplexeren Beispiel möchte der gleiche Anbieter vor der Übertragung dieser Daten den aufrufenden Benutzer über einen Basis-Daten- und -Schnittstellendienst einen Identity Check durchführen lassen. Diese Anbindung an einen zentralen Basisdienst setzt die Einbindung des Betreibers zur Bereitstellung dieser Zusatzfunktion voraus.

## 7.1 Service des Katalogdienstes zu den Katalogdiensten generell

Methode	Beschreibung
<p><b>Katalogdienst:</b> Identität &amp; Status prüfen (also: Kann ich den gewünschten Katalogdienst erreichen?)</p>	<p><b>Parameter:</b> [ID (Identifikation des Betreibers), Target Service (Service-Name, der gesucht wird), Version (Version des Services)]</p> <p><b>Gibt einen Informations-Stream zurück mit folgenden Informationen:</b></p> <ul style="list-style-type: none"> <li>• Version</li> <li>• Betreiber</li> <li>• CheckResult</li> <li>• Status</li> </ul>
<p>Selbstauskunft über die Betreiberdienste (gibt die wichtigsten Daten an den Betreiber zurück)</p>	<p><b>Parameter:</b> Keine</p> <p><b>Gibt einen Informations-Stream zurück mit folgenden Informationen:</b></p> <ul style="list-style-type: none"> <li>• Version</li> <li>• Betreiber</li> <li>• Anzahl der Einträge je Status (Baum)</li> <li>• Ansprechpartner: Name, E-Mail-Adresse, Telefon</li> <li>• Status</li> </ul>
<p>Liste der Dienste, die der Betreiber für den Katalogdienst vorgesehen hat</p>	<p><b>Parameter:</b> Status optional</p> <p><b>Gibt einen Informations-Stream zurück mit folgenden Informationen:</b></p> <ul style="list-style-type: none"> <li>• Servicename</li> <li>• Anbieter</li> <li>• URL-Service-Beschreibung</li> <li>• Version</li> <li>• Status</li> <li>• Benutzer-Referenzliste</li> </ul>

Darüber hinaus kann der Betreiber weitere Methoden zur Verfügung stellen.

## 7.2 Service des Katalogdienstes zu den Katalogdiensten speziell

Methode	Beschreibung
Liste der verfügbaren Dienste ausgeben	<b>Parameter:</b> Status optional  <b>Gibt einen Informations-Stream zurück mit folgenden Informationen:</b> <ul style="list-style-type: none"><li>• Servicename</li><li>• Anbieter</li><li>• Nutzungstyp (public, Ticket, Identity-check, private)</li><li>• URL-Service-Beschreibung</li><li>• Version</li><li>• Status</li><li>• Benutzer-Referenzliste</li></ul>
Auskunft über andere Katalogdienste	<b>Parameter:</b> Keine  <b>Gibt einen Informations-Stream zurück mit folgenden Informationen:</b> <ul style="list-style-type: none"><li>• Katalogdienstanbieter (Name)</li><li>• URL des Katalogdienstes</li><li>• Letzte Änderung / Abgleich des Katalogdienstes</li></ul>

Optional:

Methode	Beschreibung
Synchronisationsprozesse, die der Katalogdienst repliziert	<b>Parameter:</b> keine  <b>Gibt einen Informations-Stream zurück mit folgenden Informationen:</b> <ul style="list-style-type: none"><li>• Katalogdienstanbieter (Name)</li><li>• URL des Katalogdienstes</li><li>• Letzte Änderung / Abgleich des Katalogdienstes</li><li>• Beschreibung URL der detaillierten Replikation</li></ul>

## 7.3 Lokalisierung

Der Betreiber stellt sicher, dass die allgemeinen Informationen in der Landeshauptsprache oder auf Englisch vorliegen.

## 8 Spezifizierung der Vermittlungsdienste

Die Vermittlungsdienste dienen der sicheren und medienbruchfreien Kommunikation aller auf der Betreiberplattform registrierten Lösungskomponenten. Die hierzu notwendige Kommunikationssprache wird durch ein zentrales, standardisiertes Kommunikationsschema definiert, das es den beteiligten Lösungskomponenten ermöglicht, sich unabhängig von ihrer eigenen Datenstruktur und -haltung miteinander zu verständigen.

Das Kommunikationsschema ermöglicht die Integration verschiedener Lösungskomponenten, indem es zwischen ihnen vermittelt und die korrekte Übersetzung (Mapping) der zu übermittelnden Daten sicherstellt. Im Falle einer asynchronen Kommunikation wird zudem für eine datenschutzkonforme Pufferung der zu übertragenden Daten gesorgt. Dies kann ggf. auch über einen längeren Zeitraum hinweg notwendig sein, wenn etwa Lösungskomponenten in Ferienzeiten mehrere Wochen nicht erreichbar sind.

### Nutzen

- Das Kommunikationsschema dient als Zuordnungshilfe zwischen Lösungskomponenten und etabliert eine gemeinsame „Sprache“ für die Abfrage und Aktualisierung von gemeinsam genutzten Daten.
- Standardisierte Kommunikation mit bzw. über die zentralen Dienste unter Berücksichtigung höchster Sicherheitsstandards.
- Puffert die zu übertragenen Daten bei asynchroner Verbindung über längere Zeiträume.

### Zielgruppe des Dienstes

Zielgruppe der Vermittlungsdienste sind in erster Linie die IT-Hersteller von Lösungskomponenten.

### Organisatorische Verfahren (Registration, Aufruf, Löschung etc.)

Da die Vermittlungsdienste primär ein Austausch von Informationen zwischen Lösungskomponenten innerhalb einer Lösungsgruppe (Module desselben Herstellers) oder unterschiedlicher Programme unter unterschiedlichen Herstellern sind, unterliegen sie prinzipiell den gleichen Verfahren wie die bereits dargestellten Verfahren für die Katalogdienste.

Hier soll jedoch ergänzend hinzugefügt werden, dass zwei Arten von Vermittlungsdiensten bereitgestellt werden können:

- Vermittlungsdienste, die allen Diensten des Systems zur Verfügung gestellt werden (allgemeine Schnittstelle / Schnittstellen von einem Produkt).
- Vermittlungsdienste, die nur eingeschränkt öffentlich sind (typischerweise produktinterne Dienste). Diese werden aus architektonischen Gründen oder im Hinblick auf eine spätere Publizierung bereitgestellt.

Die Hersteller sind aufgefordert, möglichst viele öffentliche Vermittlungsdienste anzubieten, damit nur der Inhaber der Datenhoheiten entscheiden kann, ob er sich an andere Dienste anschließen will (abgesehen von der Lizenzierung).

### Technische Verfahrensanforderungen

Auch hier bestimmt der Betreiber die technischen Details der Implementierung der Vermittlungsdienste. Im Regelfall ist ein Vermittlungsdienst ein einfacher Hub oder eine Router-Funktion. Dennoch müssen die Aufrufe technisch sauber implementiert werden.

Das heißt, dass der Betreiber prüfen muss, ob:

- es bereits aufgeführte Anforderungen der Katalogdienste gibt,
- die Aufrufe mit den richtigen Zertifikaten, Zeichensätzen (ASCII etc.) vorliegen,
- ein Timeout zwischen den Aufrufen korrekt abgehandelt wird (wenn die Weiterleitungsfunktionalität unterbrochen wird),
- das Fehlverhalten bei unautorisierten Zugriffsversuchen korrekt abgehandelt wird,
- Mehrfachversuche nach einer fixierten Anzahl mit einer kontrollierten Information abgebrochen werden.

### Beispiel: produktinterne Vermittlungsdienste

Will ein Hersteller seine Lösung, die modular genutzt wird, für die künftige Ausbreitung vorbereiten, wird er in der Regel zuerst einen eingeschränkten Vermittlungsdienst bereitstellen, der nur für die Nutzung durch Programmkomponenten seiner eigenen Lösung funktioniert.

## 9 Spezifikation der Basisdienste der Datendienste und Schnittstellen

Basisdienste der Datendienste und Schnittstellen zeichnen sich dadurch aus, dass sie erweiterte Funktionalitäten beim Aufruf eines Dienstes bieten. Diese können vorgelagert (typischerweise Authentifizierungsverfahren oder Lizenzprüfungen) – oder nachgelagert werden (Abschlussrechnung oder Protokollierung von abgeschlossenen Aufträgen).

### Mindestanforderungen von Diensten, die generell durch den Betreiber bereitgestellt werden:

- Prüfung der Berechtigung von Nutzern, einen Dienst zu nutzen (nur im Fall eines Fehlers wird die Nutzung durch den Basisdienst unterbunden);
- Prüfung der Verfügbarkeit einer Lizenz zur Nutzung eines Dienstes durch den aufrufenden Benutzer;
- Kauf von Lizenzen als Transaktionen-Content und den Content-Provider prüft und die Transaktion abschließt;
- Suchdienste über Shop-Angebote mehrerer Anbieter.

### 9.1 Definition und Funktion

Der Aufbau eines Basisdienstes der Daten- und Schnittstellendienste umfasst abstrakt betrachtet immer Folgendes:

- Serviceheader
  - \_ Aufruf der Identifikation
  - \_ Aufruf Kontext (wenn Delegationsservice)
- Service Vorprüfungskontext (optional)
  - \_ Referenz des gewünschten Dienstes, wie beispielsweise Autorisierungsdienst OID X
  - \_ Funktion des Dienstes
  - \_ Übergabeparameter für die Prüfung (XML-Struktur)
- Service Hauptverarbeitung (1-n)
  - \_ Liste der Services für die Hauptverarbeitung
    - OID des Services
    - Parameter für die Verarbeitung (XML Struktur)

- Service Nachprüfungskontext (optional)
  - \_ Referenz des gewünschten Dienstes, wie beispielsweise Kaufabschluss OID X
  - \_ Funktion des Dienstes
  - \_ Übergabeparameter für die Prüfung (XML Struktur)

Der Betreiber sollte die Möglichkeit einer parallelen Nutzung von Diensten beschreiben und die Zusammenführung der Resultate koordinieren.

### Nutzen

Der Mehrwert dieser komplexeren Dienste liegt in der Verarbeitung mehrerer Schritte in einem Transaktionskontext und der Ausführung der Services im gesicherten Umfeld des Betreibers.

### Zielgruppe des Dienstes

Zielgruppe der Basis-Daten- und -Schnittstellendienste sind in erster Linie die IT-Hersteller von Lösungskomponenten.

### Organisatorische Verfahren

#### (Registration, Aufruf, Löschung etc.)

Das Verfahren ist identisch mit dem Verfahren der Vermittlungsdienste. Darüber hinaus wird jedoch eine zusätzliche Einbindung des Betreibers notwendig (bei standardisierten Verfahren, z. B. Authentifizierung, wird dies nicht immer zwingend sein, doch in spezielleren Fällen wird vermutlich auch ein Bestandteil durch den Betreiber bereitgestellt werden müssen).

Ein Basis-Daten- und -Schnittstellendienst wird immer mit der verfügbaren Zertifizierung ausgewiesen. Werden zusätzliche Dienste bereitgestellt, so sind diese bis zu ihrer Zertifizierung durch die Zertifizierungsstelle als „nicht zertifiziert“ zu markieren.

## Technische Verfahren

Auch hier bestimmt der Betreiber die technischen Details zur Implementierung der Basis-Daten- und -Schnittstellendienste. Das heißt, der Betreiber prüft:

- bereits aufgeführte Anforderungen der Vermittlungsdienste;
- die korrekte Interpretation der gewünschten vorgeschalteten Dienste im Normal- und Fehlerfall;
- die korrekte Abwicklung im Fehlerfall über mehrere Dienste (Dienste müssen ein nachträgliches Rollback ermöglichen -> Savepoints);
- die Kommunikation unter Berücksichtigung mehrerer beteiligter Dienste und damit weiterer Hersteller.

## Beispiel

Ein E-Learning-Anbieter möchte seinen Nutzern ermöglichen, den Content eines Anbieters einzukaufen.

In diesem Szenario werden folgende Dienstleistungen (als ideales Szenario) aufgerufen:

- Aufruf des zentralen Content-Suchdienstes über alle Anbieter (Basis-Daten- und -Schnittstellendienst) mit einem Filterkriterium zum Thema „Spanabhebende Verfahren“.
  - \_ Der Basisdienst ruft nun alle bekannten Suchdienste für Content mit dem gleichen Filterkriterium auf und konkateniert, also sammelt, die Resultate in einer Liste für den Aufrufer.
- Nun wählt der Benutzer des E-Learning-Systems eines der angebotenen Produkte aus und bestellt es.
  - \_ In diesem Falle wird ein Basis-Daten- und -Schnittstellendienst aufgerufen, welcher
    - zuerst eine Authentifizierung des Nutzers gegenüber einem ausgewählten Identitätsmanagement ausführt und nur im Erfolgsfalle
    - einen Aufruf eines Vermittlungsdienstes des Shops zum Kauf eines ihrer jeweiligen Produkte anstößt.
    - Im Erfolgsfall wird der Kauf gleich mit einem Lizenzschlüssel für das Produkt, den Lizenzbedingungen (Laufzeit etc.) und den

Abrechnungsdaten zurückgeliefert und

- im Erfolgsfall in einem Lizenzregister-Dienst beim Benutzerportfolio (bzw. bei der Schule) eingetragen.

## 10 Verfahrensabläufe

### 10.1 Anforderungen und Regularien

Das Gremium der Daten- und Schnittstellendienste implementiert und betreibt nicht. Dennoch wacht es über das vorliegende Konzept und entwickelt es kontinuierlich zum Nutzen der Benutzer, Anbieter und Betreiber weiter.

Entsprechend gilt es, Regularien zu definieren, die den Fortbestand des Gremiums sicherstellen.

Diese Regularien betreffen folgende Bereiche:

- Zusammensetzung des Gremiums und Aufgabenbereiche
- Periodizität der Sitzungen und Besprechungen
- Priorisierung der Aufgabenbereiche
- Definition der operativen und strategischen Zielsetzungen des Gremiums
- Kommunikationsrichtlinien
  - \_ innerhalb des Gremiums und des BfB
  - \_ mit Betreibern, Forschung und anderen direkten Interessengruppen im Kontext der Implementierung
  - \_ mit der Zertifizierungseinheit für Expertisen
- Entwicklung von Qualitätskriterien für die Bewertung der Daten- und Schnittstellendienste

### 10.2 Berechtigungskonzept

Das Berechtigungskonzept innerhalb der Daten und Schnittstellen basiert auf Rollen und Funktionsrechten. Dabei können beliebige Rollen definiert werden. Diese Rollen können einerseits Benutzern oder Benutzergruppen und andererseits den Diensten und deren Funktionen zugeordnet werden. Darüber hinaus werden Datenrechte auf diese Rollen zugeordnet, soweit dies sinnvoll oder nötig ist.



Im Minimum werden folgende Rollen vorliegen müssen: **11.1 Informationsaustausch BfB, Entwickler, Dienstleister**

- Gast
- Anbieter
- Benutzer
- Supervisor Vermittlungsdienste
- Supervisor Basis-Daten- und -Schnittstellendienste
- Supervisor Katalogdienste
- Administrator
- Entwicklung Schnittstellen-Unternehmen

## 11 Qualitätssicherung

In der IT bezeichnet die Qualitätssicherung die Einhaltung von organisatorischen und technischen Anforderungen, um den Schutz und die Verfügbarkeit von Daten, Diensten und Funktionen sicherzustellen. Dazu wird die Umsetzung aller relevanten Gesetze, Richtlinien, Normen, Standards, Vereinbarungen und technischen Anforderungskataloge geprüft. Je automatisierter (z. B. durch technisches Monitoring und dokumentierte Prozesse nach ISO 9001, Audit) die Prüfungen ausgeführt werden, desto schneller können Abweichungen von den Anforderungen festgestellt werden (Qualität).

**Erkannte Abweichungen von den Anforderungen folgern ggf. temporären Workaround und Korrektur durch**

- Ergreifen organisatorischer Maßnahmen, z. B. Ausbildung, Training, Arbeitsanweisung, Prozessverbesserung, Neudelegierung, Personalentscheidung;
- Service bei Hardware durch Reparatur, Wartung, Austausch;
- Service bei Software durch Konfigurationsänderung, Korrektur (Patch), Upgrade, Migration.

Ebenso kann es notwendig sein, die Anforderungen an neue Gegebenheiten anzupassen.

**Qualitätsmanagement umfasst:**

- Technische Funktionen (Bedienung, Funktion, Verfügbarkeit, Performance, Kapazität etc.);
- Arbeitsergonomie (Sprache, Haptik, Bedienungsfreundlichkeit, Aufwand, Barrierefreiheit, Fehlhaltung etc.);
- Arbeitssicherheit (Gefährdung durch Verletzung bei sach- und unsachgemäßem Gebrauch, äußere Einflüsse, Defekte);
- Risiko (durch höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen, vorsätzliche Handlungen);
- Umwelt (Schonung von Ressourcen, Energie etc.);
- Gesetzliche Vorgaben und kulturelle Gepflogenheiten.

Der Dialog zwischen den Verantwortlichen der Vorgaben, den technischen Entwicklern, den Betreibern, den Prüfern und den Nutzern ist unverzichtbar und etablierten Verfahren unterworfen. Das BfB könnte die Institution sein, die als Vermittler für die Schnittstellen der Dialogpartner fungiert.

### 11.2 Dokumentation (Versionierung und Freigabe)

Jede technische und organisatorische Funktion kann ausschließlich durch Dokumentation der Anforderungen in ihrer Qualität gesichert werden. Fortlaufende Änderungen durch Innovation, Vermeidung neuer erkannter Risiken, aber auch die Reduzierung von Aufwand und Ressourcen bedingen eine lückenlose Dokumentation. Das Änderungsmanagement hält dabei mittels Versionierung den jeweils aktuellen Stand der Dokumentation und deren Umsetzung fest. Ein Freigabe-Prozess (Release Management) regelt die Umsetzung von der Feststellung des Handlungsbedarfs bis zur Prüfung der erfolgreichen Umsetzung. Technische Begriffe hierfür sind auch Produkt-Lebenszyklus (Lifecycle Management) von der Entstehung über die Nutzung bis zur endgültigen Einstellung.

### Die Versionierung wird angewendet auf

- Gesetze, Regelungen, Verträge, sonstige Vereinbarungen;
- Technische und organisatorische Beschreibungen (Dokumente) von Anforderungen, Funktionen, Anweisungen und Prüflisten;
- Software-Pakete und Korrekturen (Patches) für Betriebssysteme, IT-Anwendungen, Programme, Dateien;
- Hardware-System-Modelle und -Komponenten;
- Revisionsrelevante Datenbestände (auf Transaktionsebene).

### Die Hauptaufgabe der Versionierung ist

- Protokollierung der Änderungen: Es kann jederzeit nachvollzogen werden, wer wann was geändert hat.
- Wiederherstellung von alten Ständen einzelner Dateien: Somit können versehentliche Änderungen jederzeit wieder rückgängig gemacht werden.
- Archivierung der einzelnen Stände eines Projekts: Dadurch ist es jederzeit möglich, auf alle Versionen zuzugreifen.
- Koordinierung des gemeinsamen Zugriffs von mehreren Entwicklern auf die Dateien.
- Gleichzeitige Entwicklung mehrerer Entwicklungszweige (Branches) eines Projekts.

## 12 Bestehende Standards

Die Services werden soweit wie möglich und sinnvoll mit entsprechenden Standards versehen oder daran angelehnt. Gleiches wird den Anbietern der speziellen Services nahegelegt. Empfehlungen für die Verwendung werden punktuell gegeben, wenn diese in den speziellen Kontexten einen Sinn ergeben.

### Beispiele für mögliche Standards sind:

- IMS Enterprise Services
- IMS Enterprise v1.1 Import
- File Import (CSV)
- Course Webservices
- REST API
- Authentifizierung gegen LDAP, AD
- OpenID
- Shibboleth
- SAML 1.1 und SAML 2
- SSO Client
- u. v. m.

## Impressum

### **Bündnis für Bildung e. V.**

Reinhardtsraße 38, 10117 Berlin

T. +49 30 5 26 87 22 53

F. +49 30 5 26 87 22 60

info@b-f-b.net

www.b-f-b.net

### **Leiter der Arbeitsgruppe Zentrale Dienste (Dataservices und Schnittstellen):**

Jan Joswig, ANTARES PROJECT GmbH

### **Redaktion:**

Anja Janus, Bündnis für Bildung e. V.

### **Lektorat:**

Miriam Buchmann-Alisch, text\_transfer

### **Gestaltung:**

Schleuse01 Werbeagentur GmbH, Berlin

### **Titelfoto:**

Fotolia, Parris Cope / fotolia.com

### **Druck:**

LASERLINE Digitales Druckzentrum

Bucec & Co. Berlin KG

### **Stand:**

Februar 2013



BÜNDNIS FÜR BILDUNG  
vernetztes Lernen

**Bündnis für Bildung e. V.**  
Reinhardtstraße 38  
10117 Berlin

Telefon: +49 30 5 26 87 22 53  
E-Mail: [info@b-f-b.net](mailto:info@b-f-b.net)

[www.b-f-b.net](http://www.b-f-b.net)

