

Stellungnahme

November 2025

Marktdialog Ökosystem Digitale Verwaltung

Mission 2 des Bundesministeriums für Digitales und
Staatsmodernisierung: Integration und Bereitstellung

Executive Summary

Die BMDS-Mission 2 zielt darauf ab, eine zukunftsfähige, föderal anschlussfähige und technologisch belastbare Integrationsschicht für die digitale Verwaltung in Deutschland aufzubauen. Sie soll das Rückgrat für einen standardisierten, sicheren und effizienten Datenaustausch zwischen Online-Diensten, Registern und Fachverfahren bilden – bis auf die kommunale Ebene. Der Marktdialog zeigt: Die digitale Wirtschaft unterstützt dieses Ziel ausdrücklich und liefert klare Anforderungen, um einen nachhaltig tragfähigen, interoperablen und innovationsfreundlichen Ansatz zu gewährleisten. Die Integrationsschicht muss standardbasiert, föderal anschlussfähig, modular, cloudfähig und semantisch konsistent sein – und sie benötigt eine verbindliche Governance, um Wirkung entfalten zu können.

Im Rahmen des Marktdialogs wurden von den Unternehmen zwanzig Leitfragen beantwortet, die neun Themenfeldern zugeordnet werden können. Aus den Rückmeldungen lassen sich folgende zehn Kernforderungen der digitalen Wirtschaft ableiten:

- **Verbindliche Architektur- und Governance-Strukturen schaffen:** Klare Zuständigkeiten, Versionierungs- und Freigabeprozesse, Mindeststandards für APIs, Sicherheit und Datenmodelle sind zwingend.
- **Verbindliche, transparente Roadmap etablieren:** Eine abgestimmte, föderal getragene Roadmap mit klaren Meilensteinen, Prioritäten, Migrationspfaden und Zeitplänen schafft Planungssicherheit (für Verwaltung und Unternehmen), reduziert Fragmentierung und ermöglicht koordinierte Weiterentwicklung über Bund, Länder und Kommunen hinweg.

- **Mehrstufiges Einführungsmodell:** „Think big, start small“ durch Pilotierungen und skalierbare Ausbaupfade. D.h. insb. Legacy-Kompatibilität mit klaren Migrationspfaden: Adapter und Bridge-Lösungen, aber keine Dauerprovisorien.
- **„API-first“ bzw. „API-by-default“ als verbindliches Leitprinzip:** Neue und weiterentwickelte Fachverfahren müssen standardisierte, offen dokumentierte APIs bereitstellen.
- **Aufbau einer nationalen API-Registry:** Ein zentraler Katalog für APIs, Datenmodelle, Artefakte und Zuständigkeiten ist Voraussetzung für Wiederverwendung.
- **Perspektivisch gilt es, Automatisierungsgrade zu erhöhen:** Self-Healing, Observability und automatisches Schnittstellenmanagement.
- **Einheitliche Standards und Profile definieren & semantische Interoperabilität verankern:** XÖV, OpenAPI/REST, OAuth2/OIDC sowie konsistente Datenmodelle müssen harmonisiert und erweitert werden. Einheitlich interpretierbare Datenstrukturen sind essenziell.
- **Föderiertes, hybrides und cloudfähiges Betriebsmodell:** Cloud, Hybrid und On-Prem müssen unterstützt werden. Cloud-basierte Verfahren werden zukünftig zum Standard.
- **Sicherheits- und Vertrauensanker etablieren:** Zero-Trust, Ende-zu-Ende-Sicherheit, qualifizierte Signaturen & Siegel.
- **Developer Experience stärken:** Templates, Testtools, Monitoring-Zugänge und Schulungen flankieren den Aufbau eines Ökosystems Digitale Verwaltung.

Beantwortung der Leitfragen des Marktdialogs

Leitfragen

Feedback Unternehmen

1. Grundverständnis und Vision

Was verstehen Sie unter einer Integrationsschicht, wenn wir rechtliche, organisatorische oder ressourcenbedingte Rahmenbedingungen einmal ausblenden?

Eine Integrationsschicht ist die technische Vermittlungs- und Standardisierungsebene, die heterogene Fachverfahren, Register, Basisdienste und Portale sicher, interoperabel und nachvollziehbar verbindet. Sie abstrahiert die Vielfalt der Einzelanwendungen, harmonisiert Schnittstellen und Datenflüsse und macht föderale Strukturen anschlussfähig. Im Kern stellt sie offen dokumentierte, einheitliche APIs sowie semantisch konsistente Datenschemata bereit, ermöglicht Routing, Transformation und Validierung von Daten und sorgt für Ende-zu-Ende-Sicherheit, Authentifizierung, Autorisierung und Protokollierung. Dabei konzentriert sie sich auf technische Aufgaben und vermeidet fachliche Geschäftslogik; sie speichert keine Fachdaten dauerhaft, sondern transportiert, vermittelt und standardisiert. Als Infrastrukturkomponente ist sie hochverfügbar und skalierbar, fördert Wiederverwendung und vermeidet Insellösungen, indem bestehende Bausteine und Standards konsequent eingebunden werden.

Über die klassische Kopplung von Antragsportalen und Fachverfahren hinaus unterstützt eine moderne Integrationsschicht lebenslagenorientierte Prozesse über Organisationsgrenzen hinweg (z. B. bei Geburt, Umzug oder Gründung). Sie liefert Transparenz durch zentrale Verzeichnisse und Kataloge für Schnittstellen, Zuständigkeiten und Standards und ermöglicht Self-Service-Onboarding für neue Teilnehmer. Betriebsseitig kann sie zentral bereitgestellte Katalog- und Governance-Funktionen mit dezentralen, nahe den Fachsystemen laufenden Komponenten kombinieren; Deployment-Modelle können on-premises, in der Cloud oder hybrid gestaltet sein, solange Interoperabilität und Offenheit gewahrt bleiben. Perspektivisch eröffnet die standardisierte Schnittstellenlandschaft den geregelten und sicheren Datenaustausch auch mit externen Akteuren (etwa qualifizierte Signaturen, Identitäts- und Nachweisprüfungen) und schafft die Grundlage, um Automatisierung sowie datengetriebene Verfahren gezielt und kontrolliert einzusetzen.

In den Rückmeldungen der Unternehmen zeigen sich dabei drei Spannungsfelder: Erstens vertreten einige die Notwendigkeit einer dezidierten Integrationsschicht als „Rückgrat“, während andere hervorheben, die konsequente Nutzung bestehender Schnittstellen zwischen Portalen, Registern und Fachverfahren könne eine zusätzliche Schicht entbehrlich machen. Zweitens wird die Logikfreiheit der Integrationsschicht überwiegend betont; einzelne Positionen wünschen jedoch domänenspezifische Orchestrierung. Beides lässt sich vereinbaren, wenn Orchestrierung als technische Sequenzierung und Aggregation

	<p>verstanden wird und fachliche Entscheidungen in den Fachverfahren verbleiben. Drittens wird teils ein schlanker, strikt standardbasierter Kern präferiert, der Produkt- und Lock-in-Risiken minimiert, während andere für einen umfassenden Plattformansatz mit durchgängiger API-Governance und Lifecycle-Management plädieren.</p> <p>Aus diesen Punkten lässt sich eine Leitlinie ableiten: Eine integrative, föderal anschlussfähige Integrationsschicht ist eine leichtgewichtige, standardbasierte Infrastruktur mit klarer Trennung zur Fachlogik. Sie setzt auf offene Schnittstellen, sichere und nachvollziehbare Datenvermittlung, semantische Konsistenz und Transparenz über verfügbare Dienste. Damit maximiert sie Nachnutzbarkeit, reduziert Komplexität und ermöglicht es, bestehende Lösungen pragmatisch einzubinden und schrittweise zu skalieren.</p>
--	---

2. Problemdefinition & Abgrenzung

Welche Probleme muss eine Integrationsschicht konkret adressieren?	<p>Eine Integrationsschicht muss die strukturellen Brüche einer föderal organisierten, technisch heterogenen Verwaltungslandschaft gezielt schließen. Im Mittelpunkt stehen fehlende Interoperabilität zwischen Bund, Ländern und Kommunen, proprietäre Schnittstellen, uneinheitliche Datenmodelle und konkurrierende Standardwelten. Heute treffen unterschiedliche System- und Betriebsmodelle (on-premises, Cloud, hybrid) aufeinander, Fachverfahren sind historisch gewachsen, und Daten werden oft manuell, mit Medienbrüchen und ohne durchgängige Vertrauensanker ausgetauscht. Die Integrationsschicht hat daher die Aufgabe, einen verlässlichen, standardisierten und sicheren Austausch über Organisations- und Netzgrenzen hinweg zu etablieren – mit klaren Identitäten der beteiligten Systeme, durchgängiger Authentisierung und Autorisierung und nachvollziehbaren Transportketten bis zur zuständigen Behörde.</p> <p>Fachlich-technisch muss sie Schnittstellenvielfalt und Protokollunterschiede beherrschbar machen: Sie vermittelt zwischen Protokollen und Formaten, übernimmt Routing, Transformation und Mapping, und sorgt für semantische Konsistenz über Versionen hinweg. Wo es konkurrierende oder lückenhafte Standards gibt – etwa divergierende Rollen von FIM und XÖV, fehlende Standard-Datenmodelle für Antragsverfahren oder Formatfragen wie XML versus JSON – braucht es entweder konvergierende Profile oder eine robuste Mediationsfähigkeit, ohne neue Insellösungen zu erzeugen. D.h. dort wo Standards konkurrieren oder fehlen, muss die Integrationsschicht entweder Harmonisierung vorantreiben oder verlässlich vermitteln, ohne einseitige Abhängigkeiten zu begünstigen. Ebenso wichtig ist die Entkopplung: Frontends und</p>
--	--

Backends, Antragsportale und Fachverfahren sowie Register und Basisdienste sollen über klar definierte, offen dokumentierte APIs verbunden sein, sodass Änderungen in einem Teil nicht unkontrolliert Folgewirkungen in anderen Systemen auslösen.

Betrieblich adressiert die Integrationsschicht Anforderungen an hohe Verfügbarkeit, Skalierbarkeit und Performance – auch in Mehrmandanten-Szenarien, wie sie in kommunalen Bezugsrahmen typisch sind. Sie muss in hybriden Betriebsmodellen funktionieren, in denen sensible Daten lokal verbleiben, während Design-, Katalog- und Governance-Funktionen zentral auffindbar sind. Dazu gehören Mandantenfähigkeit, differenzierte Netz- und Zonenkonzepte (inklusive sicherem Überwinden von Netzzonen), ein modernes Sicherheitsverständnis und die saubere Trennung von Zuständigkeiten. Transparenz ist kein „Nice to have“: Monitoring, Logging, Tracing, Alerting, revisionssichere Protokollierung und ein konsistentes Fehler- und Incident-Handling sind Voraussetzung für Audit-Fähigkeit, Compliance und schnelle Wiederherstellung im Störfall. Gleichzeitig muss die Plattform wartbar bleiben: Versionierung, Lebenszyklusmanagement von Schnittstellen, konsistente Dokumentation und ein Self-Service-Onboarding neuer Teilnehmer gehören explizit zum Problemraum, den eine Integrationsschicht löst.

Inhaltlich geht es nicht allein um den synchronen Datenaustausch. Die Verwaltung soll von einer rein antragsgebundenen hin zu einer ereignisorientierten Arbeitsweise kommen. Eine Integrationsschicht muss daher Ereignisfähigkeit bereitstellen, damit lebenslagenbezogene Prozesse inter- und intrabehördlich in Echtzeit angestoßen werden können. Das setzt Auffindbarkeit und Adressierbarkeit von Diensten, Queues und APIs voraus, etwa über leistungsfähige Verzeichnisse und Kataloge, die sowohl technische Metadaten (OpenAPI, Schemas, Versionen) als auch organisatorische Informationen (Zuständigkeiten, Endpunkte, Erreichbarkeiten) bündeln. Darüber hinaus sind robuste Vertrauensanker – interoperable Identitäten, Signaturen, Nachweisführung – und konsistente Datenschutzpraktiken erfolgsentscheidend.

Schließlich muss die Integrationsschicht Innovationsfähigkeit ermöglichen, ohne Stabilitätsanforderungen der Fachverfahren zu unterlaufen. Sie reduziert Redundanz und Doppelarbeit, indem sie Wiederverwendung fördert (z.B. über zentrale Kataloge, Templates, klare Richtlinien) und zugleich eine klare (Schnittstellen-) Governance etabliert (Qualität, Standardkonformität, Freigaben, Betrieb und Weiterentwicklung). Ohne diese Governance drohen erneut Insellösungen und uneinheitliche Praktiken.

	<p>Gleichzeitig darf der Scope nicht beliebig wachsen: Grundlagen wie Netz- und IAM-Infrastruktur sind zwingende Vorbedingungen, werden von einigen Unternehmen als Teil der Integrationsschicht verstanden, von anderen eher als flankierende Basiskomponenten gesehen – hier ist eine saubere Schnittstellendefinition entscheidend, damit Verantwortlichkeiten nicht verwischen.</p> <p>Insgesamt heißt das: Eine Integrationsschicht adressiert nicht nur Technikdetails, sondern die Voraussetzungen für einen sicheren, nachvollziehbaren, skalierbaren und wirklich interoperablen Datenaustausch – als Grundlage für weniger Medienbrüche, mehr Wiederverwendung und beschleunigte, vertrauenswürdige digitale Verwaltungsprozesse.</p>
Welche Probleme sollte sie adressieren (Wunschdenken, Zukunftsausbau)?	<p>Im Zielbild sollte eine Integrationsschicht weit über heutige „Verbinder“-Aufgaben hinauswachsen und den durchgängig automatisierten, sicheren und standardisierten Datenaustausch zwischen Registern, Fachverfahren und Portalen ermöglichen – inklusive einmaliger Datenerfassung, rechtssicheren Nachweisen in Echtzeit und der nahtlosen Einbindung europäischer Ökosysteme (z. B. digitale Identitäten und Once-Only-Prinzip). Dazu gehören standardisierte, abgesicherte Schnittstellen, die neue Anwendungen und Anbieter mit minimalem Aufwand anschließbar machen, sowie zentrale, qualitätsgesicherte Kataloge für APIs, Schemas und Zuständigkeiten, damit Wiederverwendung zum Regelfall wird und Integrationsaufwände spürbar sinken. Einheitliche, praxistaugliche Referenzarchitekturen sollten so gestaltet sein, dass auch kleinere Verwaltungen sie ohne große Spezialkompetenzen übernehmen können.</p> <p>Für den Betrieb ist ein deutlich höherer Automatisierungsgrad wünschenswert: Self-Healing-Mechanismen, die Störungen automatisch erkennen und beheben, Observability „by design“ mit durchgängigem Monitoring, Tracing und Alerting sowie „Hot Switching“ von Schnittstellen für unterbrechungsarme Updates. Automatisiertes API-Management – inklusive Policy-Durchsetzung, Dokumentationspflege und Deprecation-Pfaden – reduziert manuelle Arbeit und senkt Fehlerquoten. Low-Code/No-Code-Fähigkeiten ermöglichen es Fachbereichen, einfache Integrationen selbst umzusetzen, während Entwicklerproduktivität durch gute Werkzeuge, Templates und Testbarkeit maximiert wird; so wirkt die Integrationsschicht aktiv dem Fachkräftemangel entgegen.</p> <p>Inhaltlich muss die Zukunftsausbaustufe neben technischer auch semantische Interoperabilität sichern, insbesondere in Richtung historisch gewachsener Legacy-Systeme: Daten sollen über definierte, versionierbare Schemata überall gleich verstanden und verarbeitet werden.</p>

	<p>Für Governance und Marktpraktiken wäre es wünschenswert, Integrationsfähigkeit messbar zu machen (z. B. Reifegrade, Konformität zu Profilen) und in Ausschreibungen als Kriterien zu verankern. Die Integrationsschicht sollte Hersteller- und Community-Ansätze fördern, den kontrollierten Einsatz neuer Technologien (z. B. KI-Dienste, Automatisierung) erleichtern und eine transparente KI-Governance unterstützen, damit sich Innovationen schnell, sicher und rechtskonform einbinden lassen. Förderierte Datenräume könnten kollaborative, sektorenübergreifende Prozesse ermöglichen – mit klaren Regeln für Zugriff, Zweckbindung und Auditierbarkeit.</p> <p>Einige Unternehmen wünschen eine Fokussierung auf bestehende Standards (z.B. FIM), andere schlagen den Ausbau der XÖV-Standardisierung und vollständige Integrationsszenarien vor. Diese Positionen lassen sich perspektivisch vereinen, wenn konvergierende Profile definiert, Lücken (etwa fehlende Standard-Datenmodelle für Antragsverfahren) geschlossen und Übersetzungsmechanismen bereitgestellt werden – stets mit dem Ziel, Komplexität zu reduzieren, statt neue Inseln zu erzeugen.</p> <p>Zusammenfassend ist die Zukunftsversion eine Integrationsschicht, die sich weitgehend selbst verwaltet, semantisch wie technisch interoperabel ist, Innovation strukturiert einbettet, auch in kleinen Organisationen tragfähig bleibt und dadurch Produktivität, Sicherheit und Bürgernutzen nachhaltig steigert.</p>
<p>Was muss sie nicht leisten (klare Abgrenzung zu anderen Vorhaben)?</p>	<p>Die Integrationsschicht ist klar als technische Vermittlungs- und Standardisierungsebene zu verstehen – nicht als Fachanwendung oder UI/UX-Ebene. Sie übernimmt keine fachliche Steuerung, keine Geschäftsregeln und speichert keine Fachdaten; Antragsdatenerhebung findet in Portalen, Antragsbearbeitung in Fachverfahren statt. Politische Steuerung, Registermodernisierung oder die Bereitstellung/der Betrieb fachlicher Anwendungen gehören ebenfalls nicht zu ihren Aufgaben. Kurz: Die Integrationsschicht ist Infrastruktur.</p> <p>Sie ersetzt keine bestehenden, (teil-)mandatierten Komponenten wie FIT-Connect, NOOTS, EUDI-Wallet oder Datenraum-Lösungen, sondern ergänzt sie als Gateway und sorgt für Anschlussfähigkeit an deren Standards und Protokolle. Komplexe Query-Funktionalität (z. B. NOOTS) oder langfristige, gesicherte Datenhaltung (z.B. Wallet) sind nicht Teil ihres Scopes.</p> <p>Ebenfalls sollten folgende Aufgaben nicht im Bereich der Integrationsschicht liegen: Die Erstellung nicht-technischer Inhalte</p>

	<p>(Rechtstexte, Bürgerinformationen, Richtlinien), der Aufbau leistungsfähiger Netze oder die Definition/Bereitstellung von IAM-Standards – diese sind notwendige Voraussetzungen, aber gesondert zu adressieren. Zur Abgrenzung gehört auch die Wahrung der Produktneutralität und die Vermeidung von Lock-in-Effekten: Die Schicht darf keine festen Lösungsbausteine „setzen“ oder fachliche Spezifika enthalten.</p> <p>Während die Mehrzahl der Unternehmen die Komplementärrolle zu NOOTS/FIT-Connect betont, gibt es einzelne Stimmen, die eine Konkurrenz bzw. Nicht-Erforderlichkeit einer gesonderten Integrationsschicht sehen. Diese Divergenz betrifft jedoch die Positionierung im Ökosystem – nicht die oben skizzierten Zuständigkeitsabgrenzungen.</p> <p>In Summe: Die Integrationsschicht standardisiert, vermittelt und verbindet – sie gestaltet keine Fachlichkeit, betreibt keine Fachsysteme, ersetzt keine mandatierten Infrastrukturen und übernimmt keine Netz-/IAM-Grundlagen.</p>
--	---

3. Nachhaltigkeit & Zukunftsfähigkeit

Wie sehr sehen Sie die Integrationsschicht als längerfristige Lösung?	<p>Die überwiegende Mehrheit der Unternehmen sieht die Integrationsschicht als langfristige, strategische Infrastruktur - vergleichbar mit Basisdiensten oder Netzinfrastrukturen - die dauerhaft betrieben, weiterentwickelt und finanziert werden muss. Nachhaltigkeit entsteht durch klare Governance (staatliche Trägerschaft, Betrieb ggf. durch Partner bei staatlicher Kontrolle), transparente Finanzierung, verbindliche Versionierung sowie eine aktive, offene Community-Weiterentwicklung. Technisch wird eine modular aufgebaute, containerbasierte Architektur gefordert, die auf offenen Standards und modernen Plattformprinzipien (z. B. Kubernetes) beruht, hybride Betriebsmodelle (on-prem, Cloud, hybrid) unterstützt und Vendor-Lock-ins vermeidet. Schnittstellen sollen technologie-agnostisch gestaltet werden, sodass konkrete Technologien austauschbar bleiben; Protokolle und Standards wie XÖV und OpenAPI/REST gelten als Pflicht. Die Integrationsschicht fungiert als dauerhaftes Rückgrat für föderale Interoperabilität über Kommunen, Länder und Bund hinweg, verbindet heterogene Landschaften (Fachverfahren, Register, Portale) und ermöglicht Orchestrierung, ohne bestehende, (teil-)mandatierte Infrastrukturen zu ersetzen. Sie sollte den Wettbewerb unterschiedlicher Anbieter digitaler Lösungen fördern und sich in eine ganzheitliche Zielarchitektur (Deutschland-Architektur/D-Stack) einfügen.</p>
---	---

4. Herausforderungen & Innovationsansätze

<p>Welche Herausforderungen sehen Sie für eine Integrationsschicht?</p>	<p>Die größten Herausforderungen liegen weniger in der Technik als in der föderalen Realität: stark heterogene IT-Landschaften und Digitalreifegrade bei Kommunen, Ländern und Bund, unterschiedliche bzw. konkurrierende Standards sowie eine oft fehlende Verbindlichkeit in Governance, Rollen und Roadmaps. Ohne klare Zuständigkeiten je „logischem Dienst“ (einschließlich Migrationspfaden von Alt- zu Zielstandards) drohen Fragmentierung, inkonsistente Implementierungen und Akzeptanzprobleme. Gleichzeitig sind begrenzte Fachkräftekapazitäten, begrenzte Developer Experience (Sichtbarkeit, Wiederverwendung, dokumentierte Best Practices) und die Gefahr von Überkomplexität zentrale Risiken - insbesondere mit Blick auf Erfahrungen aus klassischen ESB-Ansätzen, die häufig an Bedien- und Wartungskomplexität scheiterten.</p> <p>Technisch sind Interoperabilität und Anbindung sehr unterschiedlicher Bestands- und Legacy-Systeme zu sichern—über Domänen und Betriebsmodelle hinweg. Hinzu kommen Skalierbarkeit und Performance bei wachsender Zahl von Anbindungen, Mehrmandantenfähigkeit, sowie die robuste Durchsetzung und Pflege sich weiterentwickelnder Standards (z. B. XÖV, OpenAPI) und Compliance-Anforderungen (u.a. DSGVO, eIDAS, BSI-Grundschutz). Datenschutz, Sicherheit und Betrieb müssen „security-by-design“ gedacht werden. Gleichzeitig sind Lieferketten- und Technologieabhängigkeiten risikobasiert zu managen sowie Vendor-Lock-ins zu vermeiden.</p> <p>Inhaltlich-organisatorisch gilt es, Migration und Modernisierung ohne Serviceunterbrechungen zu ermöglichen, Datensilos zu überwinden und eine „intuitiv erklärbare“ Integrationslogik zu etablieren, die Erweiterungen mit vertretbarem Aufwand zulässt. Der Spagat besteht darin, ausreichend Standardisierung und Verbindlichkeit herzustellen, ohne die Architektur zu überfrachten. Einige Unternehmen verweisen in diesem Zusammenhang auf neue Ansätze (etwa KI-gestützte Interoperabilität) als Chance—gleichzeitig wird angemahnt, Komplexität strikt zu kontrollieren. Produktneutral betrachtet entsteht damit ein doppelter Auftrag: strenge, verbindliche Governance und schlanke, erklärbare Architekturprinzipien, die Heterogenität, Sicherheit, Souveränität und Weiterentwicklungsfähigkeit dauerhaft in Einklang bringen.</p>
<p>Welche Lösungsansätze oder „Wünsche“ haben Sie dazu –auch über den Tellerrand hinaus?</p>	<p>Notwendig ist ein übergreifender Ansatz, der Governance, Standardisierung und Community-Aufbau zusammenführt: ein gemeinsames Architektur- und Governance-Board definiert und pflegt</p>

verbindliche Standards, Roadmaps und Versionierung; dazu ein förderter API-Katalog (mit semantischer Versionierung), „Interoperability Certificates“ für Integrationskomponenten sowie ggf. auch Open-Source-Referenzimplementierungen. Eine offene Community-Plattform von Bund, Ländern, Kommunen und Wirtschaft bündelt Best Practices sowie Lessons Learned und fördert die Nachnutzung bewährter Lösungen. Erkenntnisse aus bestehenden Initiativen (z.B. Gaia-X, 8ra, SCS) sollten systematisch eingebunden werden, um Doppelarbeiten zu vermeiden. Insgesamt sollte es kein nationaler Alleingang sein, sondern ein Anschluss an bewährte internationale Muster erfolgen – bei gleichzeitiger Förderung digitaler Innovationen am Standort Europa.

Architektonisch werden klar fokussierte Prinzipien gewünscht: „API-first“ (teilweise zugespitzt als „API-only“), Microservices, ereignisgetriebene Muster (Event Mesh, CQRS) und ein „agentic-ready“-Denken für künftige Automatisierung. Offene Protokolle und Industriestandards (z.B. REST, OpenAPI, OAuth2) sind Pflicht; Privacy-/Security-by-Design, qualifizierte Vertrauensdienste (Signatur, Siegel, Zeitstempel) als Trust-Layer sowie die Prüfung von Confidential-Computing für sensible Cloud-Szenarien ergänzen dies. Semantische Interoperabilität wird als Schlüssel hervorgehoben, um Daten domänenübergreifend gleich zu verstehen und verarbeiten zu können. Für die Anbindung heterogener Legacy-Landschaften werden vorkonfigurierte Integrationsbausteine („building blocks“) für Kommunen, Bridge-/Migrationslösungen und KI-gestützte Tools (für Mapping, Schema-Konversion, Test/Validierung) vorgeschlagen – jedoch mit klaren Ausstiegs- und Ablösepfeilen, damit Übergänge nicht zu Dauerprovisorien werden.

Organisatorisch braucht es – neben regulatorischer Flankierung für Interoperabilität – ein Vorgehensmodell „Think big, start small“: mit wenigen Diensten pilotieren, messbare Mehrwerte zeigen und dann schrittweise skalieren. Gewünscht sind zudem bessere Developer Experience (Sichtbarkeit, Kataloge, Templates, Referenzen), verbindliche Zertifizierungs-/Konformitätsprozesse und die Möglichkeit, bewährte iPaaS-Muster zu nutzen, ohne Produktbindung zu erzwingen (d. h. technologie-agnostische Schnittstellen, austauschbare Implementierungen).

Einige Unternehmen plädieren sehr strikt für „API-only/Microservices-only/Agentic-first“-Ansätze, andere betonen pragmatische Übergänge (Bridge-Lösungen, iPaaS-Ansätze) – D.h. es besteht ein Spannungsfeld zwischen schneller Anbindung alter Systeme und dem Anspruch auf saubere semantische Harmonisierung.

5. Standards & Schnittstellen

Welche Schnittstellenstandards müssen berücksichtigt werden (rechtlich/technisch verpflichtend)?

Welche Schnittstellenstandards sollten berücksichtigt werden (Best Practices, Zukunftssicherheit)?

[Beide Fragen werden zusammenfassend beantwortet]

Für den Datenaustausch zwischen Portalen und Fachverfahren gelten FIT-Connect samt XÖV-Profilen als maßgeblich; XÖV bleibt zentraler semantischer Standard, ergänzt um Metadaten/Verwaltungsvokabulare (FIM, LeiKa) und offene Datenstandards (DCAT-AP.de, RDF; teils SKOS/OWL). Technisch wird mehrheitlich „API-first“ befürwortet: REST/JSON mit OpenAPI (3.x) als Default; SOAP/XML bleibt übergangsweise relevant; weitere Schnittstellen wie gRPC und – je nach Use Case – GraphQL/OData können ergänzen.

Zu OSCI/XTA und XÖV gibt es jedoch unterschiedliche Akzente: Einige Unternehmen betonen deren fortgesetzte Relevanz (inkl. XJustiz, XRechnung, XÖV-Base), andere warnen vor deutschen Partikularlösungen, wenn etablierte internationale Standards dasselbe Problem bereits lösen. Konsensfähig erscheint: bestehende, (teil-)mandatierte Standards respektieren, zugleich international anschlussfähig bleiben und migrationsfähige Pfade schaffen (Bestandsschutz vs. Erprobungsstatus).

Für Authentifizierung/Autorisierung werden BundID und perspektivisch EUDI-Wallet (eIDAS 2.0) genannt.

Protokolle: OAuth2/OpenID Connect und teils SAML 2.0.

Sicherheit/Transport: HTTPS/TLS mit Mutual-TLS, ggf. VPN/SINA, Ende-zu-Ende-Verschlüsselung sowie qualifizierte Vertrauensdienste nach ETSI-TS-119 (Signatur, Siegel, Zeitstempel).

Für föderierte, asynchrone Kopplung werden ereignisbasierte Muster empfohlen (Event Mesh/CQRS); Messaging/Event-Standards wie Kafka, AMQP, MQTT (teilweise auch JMS) sollten unterstützt werden; Linked Data Event Streams (LDES) werden als Option für Datensynchronisation erwähnt. Für Datenräume werden u.a. NGS-ILD und DCAT-AP-DE genannt.

Breite Interoperabilität mit Bestandswelten erfordert zusätzliche Protokolle/Formate (z. B. FTP/SFTP, CSV, PDF/A) sowie branchenspezifische/B2B-Standards (EDI: X12, UN/EDIFACT, cXML) und – wo nötig – ERP-nahe Schnittstellen (IDoc, RFC, XI).

Prozess-/Transaktionsbeschreibungen können via BPMN 2.0/BPEL abgebildet werden; Observability könnte auf offene Standards wie OpenTelemetry setzen.

Über den Tellerrand hinaus werden technologie-agnostische Schnittstellen und Open-Source-Referenzimplementierungen gewünscht, um Vendor-

Leitfragen

Feedback Unternehmen

	<p>Lock-ins zu vermeiden; „de-facto“ Industriestandards sind zu unterstützen, sofern breit erprobt und planbar. Für die Zukunft werden Low-Latency-/Low-Level-Optionen (z. B. NATS, ggf. WASM/WIT/WRPC) nicht ausgeschlossen.</p>
<p>Welche Rolle spielt Open Source für Sie (Betrieb, Weiterentwicklung, Lizenzmodell, Community)?</p>	<p>Open Source wird von vielen Unternehmen als zentraler Hebel für Transparenz, Nachnutzbarkeit, Interoperabilität und Digitale Souveränität gesehen—sofern Governance, Sicherheit und Pflege dauerhaft gesichert sind. Gewünscht sind offene Schnittstellen und offene, nachvollziehbare Lizenzmodelle; Standards und Spezifikationen sollen in offenen Community-Prozessen entstehen und versioniert werden. Eine aktive, kuratierte Community (z.B. über OpenCoDE) mit klaren Rollen, Qualitätsregeln, Security-Reviews, Roadmaps und verlässlicher Finanzierung gilt als Voraussetzung für eine nachhaltige Weiterentwicklung. Auch die Förderung externer OSS-Projekte mit hoher Relevanz für staatliche IT wird als Baustein gesehen, um Abhängigkeiten zu reduzieren und Einfluss auf kritische Komponenten zu gewinnen.</p> <p>Gleichzeitig wird von den Unternehmen Pragmatismus betont: Die Integrationsschicht soll keine konkreten Produkte festschreiben, sondern technologie- und produktneutral bleiben und multiple Implementierungen erlauben. Häufig befürwortet wird ein hybrider Ansatz—Open-Source-Grundlagen (etwa Container-/ Kubernetes-Ökosystem, etablierte OSS-Frameworks) kombiniert mit zusätzlichen, ggf. proprietären Komponenten dort, wo umfassende Enterprise-Funktionen, Support, Haftung oder Zertifizierungen erforderlich sind. Beschaffung und Bewertung sollen risikobasiert erfolgen (Kritikalität, Reifegrad, Security, Lieferketten, Skills, Wartbarkeit). Sicherheitsaspekte (Security-by-Design, strukturierte Schwachstellenmeldungen, kontrollierte Veröffentlichung) sind dabei zu berücksichtigen. Zudem kann in besonders sensiblen Bereichen die Quelloffenheit eingeschränkt sein.</p>

6. Architektur, Betrieb & Skalierung

<p>Wenn die Integrationsschicht zentral bereitgestellt wird –wie kann Skalierung und Performanz sichergestellt werden?</p>	<p>Skalierung und Performanz hängen weniger an einer Einzeltechnologie als an klaren Architektur- und Betriebsprinzipien: Ein zentrales, verbindliches Betriebsmodell (Rollen, SLOs, Incident- und Kapazitätsmanagement) mit föderierter Umsetzung ermöglicht, dass Länder und Kommunen mit unterschiedlichen Reifegraden teilnehmen und vorhandene Infrastrukturen weiterverwenden. Technisch wird mehrheitlich eine cloud-native, modular containerisierte Architektur (Kubernetes/OpenShift) mit Microservices, konsequenter horizontal-Skalierung, Georedundanz und automatischem Scaling gefordert.</p>
--	--

	<p>Die Lösung muss in allen Aspekten konsequent als horizontal skalierbare Software ausgelegt werden. Bei einer zentralen Bereitstellung sind für die Sicherstellung von Skalierung und Performanz folgende Aspekte konsequent in der gesamten Systemauslegung zu berücksichtigen: Statelessness, Asynchronität, dynamisches Scaling sowie Partitionierung / Sharding unter Berücksichtigung der Mandantenzuordnung.</p>
Welche Deployment-Modelle (Cloud, Hybrid, föderiert) sind denkbar?	<p>Mehrheitlich wird ein flexibles, föderiertes Hybrid-Modell empfohlen: gemeinsame Standards und zentrale Steuerung (z.B. Kataloge, Policies, Governance), bei dezentral organisierten Fachverfahren zur Wahrung von Latenz, Datenschutz und Souveränität. Die Integrationsschicht selbst sollte alle Betriebsformen unterstützen—On-Prem, Private/Community Cloud sowie Public/Sovereign Cloud—unter konsequenter Nutzung von Cloud-Prinzipien (Container, IaC, Automatisierung) auch im On-Prem-Betrieb. Für sensible Workloads werden bevorzugt Sovereign-Cloud-Angebote, Sicherheitszonen und ggf. Confidential-Computing genannt, teils wird eine „souveräne Infrastruktur“ gefordert; weniger sensible Dienste können in gemanagten Cloud-Umgebungen skaliert werden. Viele Unternehmen plädieren für eine klare Cloud-First-Ausrichtung als zukunftsfähigstes Modell, andere warnen insb. vor einer rein zentralen Bereitstellung und betonen dezentrale Elemente als zwingend. Grundsätzlich gilt: „Cloud, Hybrid, föderiert“ sind keine Alternativen, sondern als kombinierbare Bausteine je nach Schutzbedarf, Datenresidenz und Fachkontext zu betrachten.</p>
Ist es sinnvoll, eine mehrstufige Einführung (z.B. zunächst Landesebene, dann bundesweite Konsolidierung) vorzusehen?	<p>Eine mehrstufige Einführung ist zu empfehlen. Dies trägt zur Risikominimierung und zum Akzeptanzaufbau bei und schafft die Möglichkeit, in realen Kontexten schnell zu lernen. Eine sehr kurzfristige und zugleich umfassende Anpassung ist wenig realistisch; tatsächlich würden fachliche Vorhaben ohnehin zeitlich versetzt anlaufen und Regionen unterschiedlich schnell vorankommen. Damit ist die Frage weniger eine technische, sondern primär eine organisatorische: Es braucht klare Prioritäten, Governance, transparente Kommunikation und ein strukturiertes Change-Management, um die Anpassungen erkennbar, anschlussfähig und politisch tragfähig zu machen.</p> <p>Empfohlen wird, „groß zu denken und klein zu starten“: Pilotierungen auf Landes- oder Kommunalebene (ggf. mit Verwaltungen unterschiedlichen Reifegrads) validieren früh Skalierbarkeit, Sicherheit, Standardisierung und Interoperabilität. Zentrale Lernziele der ersten Stufe sind: technische Machbarkeit, Betriebssicherheit, Nutzenbelege für Fachverfahren, praktikable Betriebs- und Supportmodelle sowie die Identifikation wiederverwendbarer Bausteine. Parallel sollte ein Kompetenzaufbau (z. B.</p>

	<p>Center of Excellence) erfolgen, um Know-how zu verstetigen und die spätere Skalierung zu beschleunigen.</p> <p>Technisch empfiehlt sich, zunächst die Integrationsschicht in Richtung Zielbild funktionsfähig zu machen („Endausbaustufe“ als Leitstern), ohne auf die bundesweite Ausbringung zu warten. Auf dieser Basis werden Services und Fachverfahren entlang einer priorisierten Roadmap schrittweise angebunden. Bereits existierende Schnittstellen und etablierte Komponenten sind nach Möglichkeit früh mitzunehmen, sofern sie sinnvoll in Richtung Zielzustand weiterentwickelt werden können. So lässt sich eine Übergangsphase gestalten, in der Legacy-APIs koexistieren, aber planvoll abgelöst werden.</p> <p>Für die Skalierung in späteren Stufen erscheint eine bundesweite Konsolidierung auf Basis gemeinsamer Standards sinnvoll, mit expliziter europäischer Anschlussfähigkeit. Zentral ist hierfür ein verbindlicher Schnittstellen- und Standards-Katalog, klare Zertifizierungs- und Abnahmeprozesse sowie ein Governance-Modell, das föderale Autonomie respektiert und dennoch Konsistenz sichert. Iterative, agile Vorgehensweisen mit kurzen Feedback-Schleifen, regelmäßigen Release-Zyklen und transparenten Metriken (z.B. Time-to-Integrate, Ausfallzeiten, Nutzungsgrad) helfen, Qualität und Tempo zu steuern.</p> <p>Es ergibt sich folgendes Spannungsfeld: Einerseits sollen Piloten bewusst fokussiert starten, andererseits sollen keine Akteure „ausgeschlossen“ werden. Auflösbar ist dies durch eine enge Pilotperimeterisierung bei gleichzeitiger technischer Offenheit: frühe, klar definierte Use Cases mit begrenztem Kreis, jedoch von Beginn an standardisiert und skalierbar angelegt, sodass sich weitere Länder/Kommunen ohne aufwendige Einarbeitung anschließen können.</p> <p>Fazit: Eine mehrstufige Einführung ist sinnvoll und strategisch geboten - sie reduziert Risiken, fördert Wiederverwendung und Kompetenzaufbau und ermöglicht eine geordnete, föderal anschlussfähige Skalierung bis zur bundesweiten Ausrollung.</p>
--	--

7. Erfolgsmessung & Mehrwert

Wie kann Rückmeldung zur Nutzung (Zufriedenheit, Verbesserungspotenzial) systematisch eingeholt werden?	<p>Zu empfehlen ist ein kombinierter Ansatz aus qualitativen und quantitativen Verfahren, der von Beginn an verbindlich geregelt wird. Qualitativ sollten eng begleitete Pilotierungen mit repräsentativen Behörden (unterschiedliche Größen und Reifegrade) systematisch Erfahrungswissen heben - u. a. über regelmäßige Reviews mit Ländern und Kommunen, Community-of-Practice-Formate, Nutzerforen, Helpdesk-</p>
---	---

	<p>Auswertungen, Anwenderkonferenzen sowie ein mehrstufiges Feedbackverfahren. Für Nutzerfeedback wird eine zentrale, leicht zugängliche Rückmeldekomponente empfohlen (inkl. Barrierefreiheit und Mehrsprachigkeit).</p> <p>Quantitativ sollte Telemetrie/Monitoring/Logging standardmäßig aktiviert sein, um Probleme präventiv zu erkennen (Fehlerraten, Latenzen, Timeouts, Verfügbarkeit, MTTR, Ressourcenauslastung, Security-Findings) und um Nutzungs- und Qualitätsindikatoren zu messen. Zentrale Kennzahlen sind z. B. Integrationszeit neuer Dienste, Anzahl/Verfügbarkeit/Versionierung von APIs, Wiederverwendungsraten standardisierter Schnittstellen, Transaktionsvolumina, Datenqualität (z. B. Validierungsfehler), Abbruch- und Fehlerquoten, Support-Ticket-Durchlaufzeiten sowie Zufriedenheitsmaße (CSAT/NPS) je Zielgruppe. Diese Metriken sollten in konsolidierten Dashboards aufbereitet und - wo sinnvoll - öffentlich bereitgestellt werden, um Transparenz und Vertrauen zu stärken. Da die föderale Organisation eine einheitliche technische Erfassung erschweren kann, ist es wichtig, Rahmenbedingungen verbindlich zu regeln: ein gemeinsames Feedback-Datenmodell (Taxonomie, Prioritätsklassen, Datenschutzvorgaben), standardisierte Erhebungszyklen (z. B. monatliche Betriebsreviews, quartalsweise Zufriedenheitsumfragen), ein einheitlicher Prozess zur Triage/Priorisierung (inkl. Rückmeldung an Meldende), Release-Notes und Änderungsprotokolle. Bereits bestehende Schnittstellen und Komponenten werden in das Monitoring einbezogen, damit von Anfang an ein möglichst vollständiges Lagebild entsteht. Insgesamt entsteht so ein geschlossener Lern- und Verbesserungszyklus: erfassen → auswerten → priorisieren → umsetzen → rückmelden—mit klaren Verantwortlichkeiten, föderal anschlussfähig und skalierbar in den Regelbetrieb.</p>
Was hat sich nach erfolgreicher Umsetzung für die Kommune / das Land konkret verbessert?	<p>Nach erfolgreicher Umsetzung verbessert sich die Lage für Kommunen und Länder entlang vier Linien: Erstens steigen Tempo und Planbarkeit der Fachverfahrensintegration deutlich. Eine standardisierte Integrationsschicht reduziert Abstimmungsaufwand zwischen Ebenen, verringert Punkt-zu-Punkt-Kopplungen und verkürzt die Implementierungszeit neuer Dienste; Wiederverwendung von Schnittstellen und vorkonfigurierten Konnektoren beschleunigt Folgeverfahren. Zweitens sinken Betriebs- und Wartungslasten: stabilere Verfügbarkeit, geringere Fehlerraten, einfacheres Monitoring sowie einheitliche Sicherheits- und Compliance-Mechanismen senken Kosten und entlasten Fachpersonal; bestehende Komponenten können geordnet weiterbetrieben und schrittweise modernisiert werden, statt sie parallel individuell zu pflegen. Drittens wird das Leistungsangebot konsistenter und nutzerfreundlicher: weniger Medienbrüche, schnellere Antragsbearbeitung, verifizierbare Nachweise und Datenaustausch in</p>

	<p>(nahezu) Echtzeit führen zu einheitlicheren Service-Erlebnissen über Verwaltungsgrenzen hinweg—eine Grundlage für proaktive Leistungen und datenbasierte Entscheidungen. Viertens steigt die Innovationsfähigkeit: neue fachliche Use Cases (z. B. zusätzliche Datenquellen, Ereignis-/API-basierte Prozesse) lassen sich schneller umsetzen; hybride und föderierte Betriebsmodelle werden technisch einfacher, ohne föderale Autonomie aufzugeben.</p> <p>Messbar wird der Fortschritt über klar definierte Kennzahlen, etwa Integrationszeit und -aufwand pro Dienst, API-Verfügbarkeit und -Nutzungsgrad, Wiederverwendungsraten, Datenqualität, Time-to-Restore/MTTR, Ticket-Durchlaufzeiten sowie Zufriedenheit der beteiligten Verwaltungen und Endnutzenden.</p>
Wann ist die Mission 2 aus Ihrer Sicht erfolgreich abgeschlossen?	<p>Erfolgreich abgeschlossen ist Mission 2, wenn die Integrationsschicht im Regelbetrieb nachweislich wirkt: Sie wird von Bund, Ländern und Kommunen breit genutzt, ist standardisiert und interoperabel (einschließlich Anschluss an EU-Standards), und wird als gemeinsames Fundament akzeptiert. Dazu gehören eine verbindliche, föderal getragene Referenzarchitektur mit festgelegten (Sicherheits-)Standards und Governance, die produktiv erprobt, geprüft und freigegeben wurde, sowie verfügbare zentrale Dienste/Produkte für den dezentralen Betrieb. Erfolg zeigt sich messbar: deutlich verkürzte Anbindungszeiten für neue und bestehende Fachverfahren (unter einem definierten Schwellenwert), hohe Verfügbarkeit und Qualität der Schnittstellen, belegte Wiederverwendungsraten, sinkender Betriebs-/Wartungsaufwand, verbesserte Datenqualität und stabil steigende Zufriedenheitswerte bei Verwaltungen und Endnutzenden. Ein weiterer Erfolgsindikator ist die gelebte „Developer Experience“: die Lösung gilt in der Praxis als Standard (ohne Grundsatzdebatten), es existieren qualifizierende Angebote (Doku, Trainings, Community-Formate) und eine relevante Zahl von Personen hat sie genutzt.</p> <p>Leichte Akzentunterschiede in den Marktstimmen lassen sich als Meilensteine entlang einer Erfolgsleiter lesen: Einige sehen die Mission mit der verbindlichen Festlegung von Architektur/Standards und erfolgreichem PoC als erreicht; die überwiegende Position verlangt darüber hinaus die bundesweite, produktive Nutzung mit fortlaufender Weiterentwicklung und nachweisbaren Mehrwerten (u. a. End-zu-End-Digitalisierung, geringere Komplexität/Kosten, schnellere Umsetzung neuer Leistungen).</p>

8. Weiterentwicklung & Positionierung

Was könnte in einer weiteren Iteration verbessert werden?

Die Marktstimmen empfehlen für die nächste Iteration drei Schwerpunkte: Governance & Verbindlichkeit, technische Vertiefung der Interoperabilität sowie nutzungszentrierte Weiterentwicklung.

Erstens braucht es mehr Verbindlichkeit in der Nachnutzung und eine enge Verzahnung mit Mission 1 (Basisdienste) und Mission 3 (Nutzung & Wirkung). Dazu gehören eine transparent dokumentierte Roadmap, gemeinsame Gremien mit Bund, Ländern und Marktakteuren, verbindliche Mindeststandards (API-Governance, Versionierung, SLAs/SLOs, Security/Privacy-Vorgaben) sowie durchgesetzte Regeln zur Wiederverwendung statt paralleler Neuentwicklungen. Ein gemeinsames semantisches Zielbild (Datenmodelle/Taxonomien) und durchgängige DevSecOps-Prozesse sollen sicherstellen, dass Standards aktuell bleiben und Schnittstellen kontinuierlich gepflegt werden.

Zweitens sollte die Integrationsschicht technisch „intelligenter“ und breiter anschlussfähig werden. Genannt werden kontextsensitive, semantisch verstehende Integrationsmechanismen (statt rein regelbasierter Flows), dynamische Interoperabilität (neue Teilnehmer werden leichter eingebunden), sowie eine lebenslagen- und prozessorientierte Orchestrierung über Behörden- und Ebenengrenzen. Perspektivisch sind weitere Register- und Datenquellen anzubinden; föderale und europäische Systeme (z. B. Wallet/NOOTS) sollen nahtlos integriert werden. Emerging Tech (z. B. KI-gestützte Assistenz, automatisierte Vorbefüllung, Datenqualitätsprüfungen; teils auch Blockchain) wird als Option gesehen - allerdings klar eingebettet in Governance und Datenschutz.

Drittens rückt die Nutzung in den Fokus: Systematisches Nutzerfeedback aus den ersten Rollouts soll konsequent in Verbesserungen einfließen (Metriken, Reviews, Community-Formate). Parallel sind „Developer Experience“ und Befähigung zentral: Dokumentation, Schulungen, ggf. auch Low-/No-Code-Optionen für einfache Integrations- und Automationsfälle, damit Fachbereiche entlastet und IT-Teams Kapazität für strategische Themen gewinnen. Als langfristiges Bild wird eine zentrale, modulare Plattform genannt, die als einheitlicher Einstiegspunkt für Bürgerinnen und Bürger sowie Unternehmen dient und über die Integrationsschicht alle digitalen Verwaltungsleistungen verbindlich vernetzt—bei Wahrung föderaler Autonomie.

Kurzum: Die nächste Iteration sollte Nachnutzung verbindlich machen, semantische und technische Interoperabilität vertiefen, Sicherheit und Governance fortschreiben, KI & Automatisierung kontrolliert nutzbar machen und die Erfahrungen aus Betrieb und Nutzung kontinuierlich in Roadmap und Plattformausbau zurückspielen.

Leitfragen

Feedback Unternehmen

<p>Wie positioniert sich die Integrationsschicht im Kontext bestehender Initiativen (z. B. NOOTS, Wallet, ...)?</p>	<p>Die Integrationsschicht wird mehrheitlich als verbindendes Rückgrat verstanden: Sie bündelt und orchestriert bestehende Initiativen (u. a. NOOTS/FIT-Connect, Registermodernisierung, BundID/EUDI-Wallet, OZG) über standardisierte Schnittstellen, anstatt neue Silos zu schaffen oder Einzelkomponenten zu ersetzen. Ihre Rolle ist, technische und organisatorische Interoperabilität sicherzustellen - durch verbindliche API- und Datenstandards (inkl. semantischer Modelle), klare Governance, Versionierung, SLAs/SLOs sowie DevSecOps-Prozesse - und so Synergien zwischen den Initiativen nutzbar zu machen. Dazu gehören ein Developer-Portal (APIs, Spezifikationen, Artefakte), definierte Onboarding-Prozesse, Monitoring/Telemetrie sowie—gemäß D-Architektur—die Einbindung sicherheitsrelevanter Bausteine (z. B. IAM/Zero-Trust) für den geschützten Zugriff auf Systeme und Daten.</p> <p>Inhaltlich rückt der End-to-End-Nutzen in den Mittelpunkt: Bürgerinnen und Bürger sowie Unternehmen interagieren über bestehende Portale/Wallets; die Integrationsschicht sorgt „unter der Haube“ für die verlässliche Weiterleitung, Orchestrierung und Nachweisführung zwischen Online-Diensten, Fachverfahren und Registern. Wo es Überschneidungen oder Graubereiche gibt, soll die Integrationsschicht als Anschluss- und Übersetzungsebene fungieren—komplementär zu mandatieren Infrastrukturen wie NOOTS/FIT-Connect. Einzelne Stimmen sehen potenziellen Wettbewerb zu solchen Systemen; der mehrheitliche Standpunkt betont hingegen die Komplementarität: Spezialinfrastrukturen übernehmen definierte externe Zustellungen/Standards, die Integrationsschicht adressiert die interne Vielfalt, verbindet Komponenten und macht sie föderal skalierbar.</p> <p>Zur Wallet differieren die Einschätzungen: Teils wird sie als primär frontendläufig (Identifizierung/Nachweis im Antrag) bewertet, teils als wichtiger Baustein im Gesamtsystem. Konsens ist: Die Integrationsschicht stellt die anschlussfähige, standardisierte API-Schicht bereit, damit Identitäts- und Nachweisdienste sicher und einheitlich in Verwaltungsprozesse eingebunden werden können. Insgesamt positioniert sie sich somit als interoperable Plattformebene des D-Stacks, die bestehende Vorhaben verbindet, deren Nachnutzung durchsetzt und eine einheitliche, skalierbare Grundlage für föderale Digitalleistungen schafft.</p>
<p>Welche Ansätze sehen Sie, um Synergien zu nutzen und Überschneidungen konstruktiv zu gestalten, ohne die Innovationsfähigkeit einzuschränken?</p>	<p>Die Marktstimmen schlagen einen doppelt gerichteten Ansatz vor: klare Leitplanken, damit Synergien gehoben werden können und keine Doppelarbeit entsteht – und gleichzeitig ausreichend Freiräume, damit Innovation nicht ausgebremst wird. Organisatorisch bedeutet das: eine gemeinsam getragene Referenzarchitektur (Bund–Länder–Kommunen) mit schlanker, verbindlicher Governance; eine koordinierende Stelle (z. B. beim</p>

	<p>BMDS) zur Abstimmung laufender Vorhaben sowie regelmäßige Markt- und Community-Dialoge, damit Ergebnisse früh sichtbar und nachnutzbar sind. Technisch heißt es: konsequente Standardisierung von Schnittstellen, Protokollen und Datensemantik, ein gemeinsames Identitäts-/Nachweisverständnis (eID/eIDAS-Vertrauensanker) und Security-by-Design (IAM/Zero-Trust) – kombiniert mit loser Kopplung und modularen Architekturen, damit Komponenten austauschbar bleiben.</p> <p>Um Doppelungen und Überschneidungen zu vermeiden, werden zwei Hebel betont. Erstens: klare Zuständigkeits- und Schichtzuschnitte (z. B. System-, Prozess-, Experience-Ebene) und ein Developer-Portal mit konsistenten API-Spezifikationen, Artefaktkatalog, Onboarding und Versionierung. So können Initiativen wie NOOTS/FIT-Connect, Wallet/BundID, Registermodernisierung und Fachverfahren problemlos andocken, ohne dass neue Silos entstehen. Zweitens: Wiederverwendung vor Neuentwicklung – über qualitätsgesicherte, standardkonforme Assets (APIs, Schemas, Transformationsbausteine), die verbindlich kuratiert, zertifiziert und in einem gemeinsamen Katalog bereitgestellt werden.</p> <p>Damit Innovationsfähigkeit gewahrt bleibt, müssen entsprechende Freiheitsräume geschaffen werden: minimal notwendige (aber verbindliche) Standards statt Überregulierung; Sandbox- und Pilotkorridore für neue Technologien (z. B. KI-gestützte Assistenz), flankiert von Datenschutz- und Sicherheitsleitplanken, Schulungen und Self-Service-Werkzeugen.</p> <p>Kurz: Synergien entstehen durch verbindliche, schlanke Standards, kuratierte Nachnutzung und klare Schnittstellen – Innovation durch Modularität, offene Prozesse und kontrollierte Experimentierräume.</p>
--	--

9. Technische Machbarkeit

Haben die Fachverfahrens-/Onlinedienst-Applikationen bereits technische Schnittstellen, die mit einer Integrationsschicht kommunizieren können?	<p>„Teilweise ja.“: Viele Fachverfahren und Onlinedienste bringen heute bereits Integrationspunkte mit—typisch REST-/SOAP-Webservices, teils XÖV/OSCI/XTA-konform oder via FIT-Connect/M2M-Schnittstellen. Die Realität ist jedoch heterogen: uneinheitlich dokumentierte APIs, inkonsistentes Antwortverhalten, unterschiedliche Sicherheitszonen/Netzisolierung und Lücken bei bestehenden Verfahren. Daraus folgt: Die größte Aufgabe ist weniger die reine Bereitstellung von Schnittstellen als deren Harmonisierung und verlässliche Standardisierung. Grundsätzlich gilt: Die Integrationsschicht kann auf vorhandene Integrationspunkte aufbauen und diese durch Middleware-Konnektoren und Trust-Services ergänzen, um sichere, signierte und nachvollziehbare Transaktionsketten zu ermöglichen.</p>
---	--

Empfohlen wird daher ein gestuftes, produktneutrales Vorgehen: Erstens eine systematische Bestandsaufnahme (Inventur) der vorhandenen Schnittstellen samt Reifegradbewertung und die Einrichtung eines nationalen API-Registry/Developer-Portals (Spezifikationen, Artefakte, Versionen, Kontaktpunkte). Zweitens verbindliche Mindeststandards nach D-Architektur/D-Stack, damit Neu- und Weiterentwicklungen konsistent anschließen. Drittens: Brücken für Legacy: Adapter-/Gateway-Muster, Konnektoren und - wo keine APIs absehbar sind - temporäre Überbrückung über UI-/Datei-Automatisierung und dokumentierte Migrationspfade. Viertens eine klare Roadmap: priorisierte Anbindung häufig genutzter Register und Fachverfahren, Wiederverwendung qualitätsgesicherter Transformationsbausteine, sowie Leitlinien, wann FIT-Connect/NOOTS für die externe Zustellung genutzt und wann interne Schnittstellen bedient werden.

Für Onlinedienste gilt perspektivisch: „API by default“—jede neue Leistung und wesentliche Weiterentwicklung sollte standardisierte, dokumentierte Schnittstellen mitbringen (fachlich und semantisch konsistent), damit Integrationszeit und Pflegeaufwand sinken. Messbar wird der Fortschritt u.a. über Anbindungsgeschwindigkeit, API-Verfügbarkeit/Fehlerquoten, Wiederverwendungsraten, Anteil standardkonformer Endpunkte und Rückgang individueller Punkt-zu-Punkt-Integrationen. Insgesamt zeigt sich: Anschlussfähigkeit ist größtenteils vorhanden, aber nur durch konsequente Standardisierung, Registry/Dev-Portal, Legacy-Brücken und verbindliche Governance wird sie breit und nachhaltig nutzbar.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Marc Danneberg | Leiter Public Sector

Verantwortliches Bitkom-Gremium

AK Digitale Verwaltung

Copyright

Bitkom 2024

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.