EIN PROJEKT DES IT-PLANUNGSRATS

FITKO

Bundesministerium für Digitales und Staatsmodernisierung

Anlage 1 zum Beschluss zur Deutschland-Architektur

Zusammenfassung

Das vorliegende Dokument fasst wesentliche Ergebnisse des Vorprojekts Deutschland-Architektur zusammen, die dem Beschlussvorschlag zur 49. Sitzung des IT-Planungsrats beigelegt werden. Insbesondere werden folgende Ergebnisse dargestellt:

A) Definition und Artefakte der Deutschland-Architektur

B) Architekturprinzipien für Architekturentscheidungen

C) Erste Funktionsbausteine zur Bündelung von umzusetzenden Funktionalitäten

D) Governance-Eckpunkte für den Umgang mit der Deutschland-Architektur

Inhaltsverzeichnis

1 Einleitung

Das vorliegende Dokument fasst ausgewählte Ergebnisse des Vorprojekts Deutschland-Architektur zusammen, die dem Beschlussvorschlag zur 49. Sitzung des IT-Planungsrats beigelegt werden.

Das vorliegende Dokument umfasst konkret folgende Ergebnisse:

- Definition der Deutschland-Architektur
- Artefakte-Zielbild der Deutschland-Architektur
- Architekturprinzipien in Ergänzung zur Nationalen Architekturrichtlinie
- Erste Funktionsbausteine als Basisfunktionalitäten des Referenzmodells Deutschland-Architektur
- Governance-Eckpunkte

Zu beachten ist, dass sich das Vorprojekt auftragsgemäß nur auf den Wertstrom „Inanspruchnahme eine digitalen Verwaltungsleistung“ konzentriert hat.

2 Definition und Artefakte

2.1 Definition der Deutschland-Architektur

Die folgenden Formulierungen definieren die Deutschland-Architektur:

- Die D-Architektur ist die Enterprise Architektur der deutschen Verwaltung und bildet einen kohärenten Ordnungsrahmen für die zielgerichtete Steuerung und systematische Beschreibung gemeinsamer Geschäftsfähigkeiten und ihre Unterstützung durch die IT in Bund und Ländern.
- Die D-Architektur gestaltet einen modularen und interoperablen Plattformansatz basierend auf den strategischen Zielen der Bundesrepublik Deutschland. Sie deckt sowohl Ende-zu-Ende-Prozesse für Verwaltungsleistungen (für Verwaltungskunden) als auch verwaltungs-interne Prozesse (für Verwaltungsmitarbeitende) ab.
- Die D-Architektur regelt das Zusammenspiel der von ihr beschriebenen Bausteine untereinander als auch nach außen (mit externen Systemen/Bausteinen). Dazu gehört eine wirksame Steuerungsstruktur[1], um die Deutschland-Architektur auf Basis der strategischen Zielsetzungen kontinuierlich weiterzuentwickeln.
- Die D-Architektur orientiert sich an der Disziplin „Enterprise Architektur Management“ und beschreibt Funktionsbausteine im Sinne der Funktionen einer abstrakten, angedachten Lösung (bspw. Bezahldienst).
- D-Architektur ist ein konzeptionelles Rahmenwerk mit Weisungscharakter.

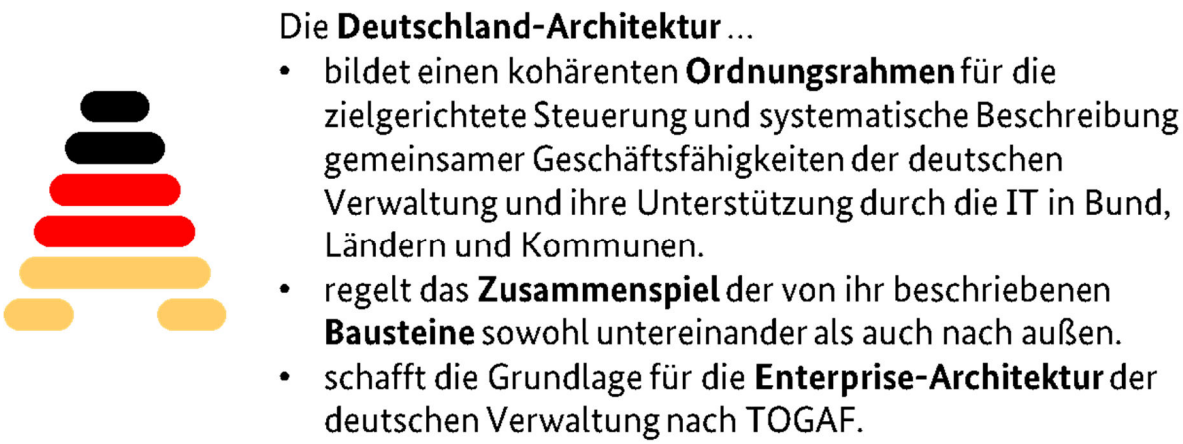

Abbildung 1 Kurzfassung der Definition der Deutschland-Architektur

[1] Die Steuerungsstruktur der Deutschland-Architektur und das IT-Portfoliomanagement des D-Stack müssen zwischen Bund und Ländern noch ausgestaltet werden.

2.2 Architekturartefakte der Deutschland-Architektur

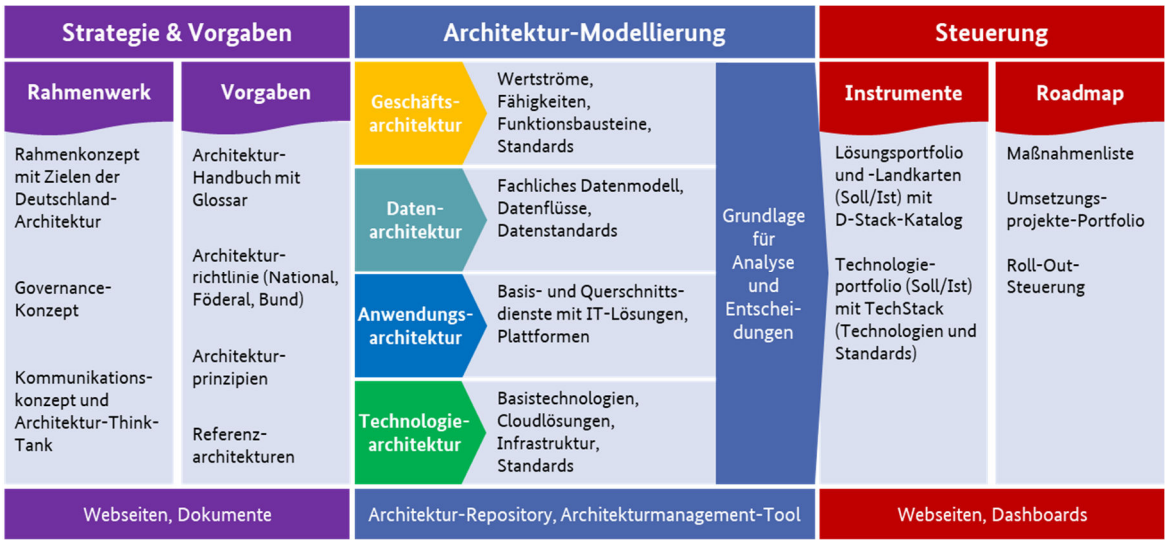

Abbildung 2 Architekturartefakte der Deutschland-Architektur

Aus gehend vom TOGAF-Standard können die Architekturartefakte der Deutschland-Architektur grob in die Kategorien Strategie & Vorgaben, Modellierung sowie Steuerung eingeteilt werden. Diese Kategorien können als Prozessphasen des Architekturentwicklungszyklus verstanden werden. In der Kategorie Strategie & Vorgaben befinden sich grundlegende Konzepte, die ein Rahmenwerk für die Architekturarbeit der D-Architektur schaffen und Dokumente mit Vorgabecharakter. Neben einer Bereitstellung als Textdokument ist eine Veröffentlichung auf einem zu gestaltenden Architekturportal geplant.
In der Unterkategorie Rahmenwerk sind drei Konzepte besonders wichtig:

1. Rahmenkonzept mit Zielen der Deutschlandarchitektur: Dabei kann es sich um eine Fortentwicklung der OZG-Rahmenarchitektur unter Berücksichtigung weitere existierender Rahmen- oder Strategiedokumente handeln.
2. Governance-Konzept: Hier sollen das Regelwerk, die Prozesse, Rollen und Verantwortlichkeiten innerhalb der D-Architektur und ggf. darüber hinaus beschrieben werden.
3. Kommunikationskonzept und Architektur-Think-Tank: Dieses Konzept und die Gestaltung entsprechender Austauschformate mit der Architekten-Community sowie einem ausgewählten Kreis schaffen den Rahmen für Akzeptanz und Ideensammlung zur D-Architektur.

Die Unterkategorie Vorgaben beinhaltet vier Konzeptarten, die Weisungscharakter haben:

4. Architektur-Handbuch mit Glossar: Dies soll beschreiben wie Architekturarbeit innerhalb der deutschen Verwaltung gedacht und ausgeführt werden soll. Wichtig ist zudem, dass über ein Glossar ein gemeinsames Vokabular geschaffen wird.
5. Architekturrichtlinie: In den Ausprägungen national, föderal und Bund werden hier Vorgaben für IT-Architekturen entsprechend dem festgelegten Verbindlichkeitsgrad (Muss/Soll/Darf) definiert.
6. Architekturprinzipien: Diese bilden die Richtschnur für Architekturentscheidungen (insbesondere bei der Auswahl der Lösungsbausteine).

7. Referenzarchitekturen: Dies sind Konzepte, die sich mit einem fachlich und technisch klar abgrenzbaren Architekturfeld beschäftigen und dafür Gestaltungs- und Lösungsvorlagen geben.

Die Kategorie Modellierung orientiert sich an den Architekturebenen von TOGAF:

8. Geschäftsarchitektur: Diese Ebene enthält Architekturelemente aus der fachlichen Sphäre wie zum Beispiel Wertströme, Fähigkeiten, Funktionsbausteine und Standards.
9. Datenarchitektur: Diese Ebene umfasst u.a. fachliche Datenmodelle, Datenflüsse und Datenstandards.
10. Anwendungsarchitektur: In dieser Ebene geht es um Basis- und Querschnittsdienste mit ihren IT-Lösungen bzw. notwendigen Plattformen.
11. Technologiearchitektur: In der untersten Ebene werden Basistechnologien, Cloudlösungen, Infrastruktur und zugehörige Standards betrachtet.

Diese Artefakte werden in einem gemeinsamen Architektur-Repository gepflegt. Dazu gehören grafische Modelle und detaillierte Beschreibungen der Architekturelemente (u.a. Funktionsbausteine, Lösungen), aber auch Abfrageergebnisse. Aus dem entsprechenden Tool können Sichten, Analysen und Dashboard für unterschiedliche Zielgruppen generiert werden.
Die Kategorie Instrumente umfasst Werkzeuge zum Portfoliomanagement in den Ebenen IT-Lösungen und Technologien.

12. Lösungsportfolio: Dieses Portfolio stellt Instrumente zum Management der Lösungen im Ist und Soll zur Verfügung. Neben der Lösungslandkarte ist hier der D-Stack-Katalog zu verorten.
13. Technologieportfolio: Dieses Portfolio verwaltet den TechStack aus Technologien und Standards.

In der Unterkategorie Roadmap geht es um die Planung und Steuerung der Maßnahmen auf verschiedenen Ebenen.

14. Maßnahmenliste: Diese Liste benennt die existierenden und die geplanten Maßnahmen zur Umsetzung der D-Architektur. Daraus können insbesondere der zeitliche Ablauf und insbesondere Produktivstellungstermine koordiniert werden.
15. Umsetzungsprojekte-Portfolio: Informationen zu Umsetzungsprojekten werde hier gesammelt, um Prioritäten, Werthaltigkeit und Status der Projekte zu steuern.
16. Roll-out-Steuerung: In diesem Artefakt geht es um Bereitstellung von Flächen-Roll-out-Informationen durch die Umsetzenden bzw. IT-Dienstleister und deren ebenengerechte Aufbereitung, um Roadmap-Entscheidungen vorzubereiten.

3 Architekturprinzipien

3.1 Überblick

Ein Architekturprinzip ist eine grundlegende Regel oder Leitlinie, die Architekturentscheidungen lenkt. Im Gegensatz zu einem Architekturziel geht dabei darum, WIE etwas erreicht werden soll und nicht um das WAS. Architekturprinzipien sollen möglichst stabil über längere Zeiträume und entscheidungsleitend sein. Sie dienen der Konsistenz und Qualität der Umsetzungsergebnisse. Aus dem BMDS wurden zehn Architekturprinzipien mitgegeben, die als besonders wichtig für den D-Stack bewertet wurden. Diese wurden im Rahmen der Deutschland-Architektur konkretisiert und auf die OZG-Rahmenarchitektur und die Föderale IT-Architekturrichtlinie gemappt.

Prinzip	Erläuterung
API-first	Programmierschnittstellen (APIs) werden von Anfang an als zentrale Elemente der Lösungsarchitekturen konzipiert und spezifiziert sowie im Betrieb laufend dokumentiert. Technische API-Zugriffe werden stets gegenüber manuellen Zugriffen bevorzugt eingesetzt.
Serviceorientierung & lose Kopplung	Dienste (Services) sind zentrale Architekturbausteine, die Funktionen bündeln. Sie und ihre Lösungsbausteine sind modular konzipiert, weitgehend unabhängig austauschbar und klar abgegrenzt.
Wiederverwendbarkeit & Portierbarkeit	Architekturelemente und bereitgestellte IT-Lösungen sind weitgehend wiederverwendbar und leicht in andere fachliche und technische Kontexte portierbar.
DevSecOps Only	Die Entwicklung, die Sicherheit und der Betrieb von IT werden als integrierter Prozess betrachtet. Lösungen der D-Architektur verfolgen einen „secure-by-design“ Ansatz, von Beginn an.
Zero-Trust	Lösungsbausteine müssen vollständig kompatibel mit Zero-Trust-Architekturen sein.
Technologisch aktuell	Der aktuelle Stand der Technik ist bestimmend für Architekturentscheidungen.
Made in EU first	Zur längerfristigen Stärkung der Souveränität setzt die Deutschland-Architektur auf Produkte aus EU-Ländern.
Prefer Reuse over Buy over Make	Sofern noch keine nachnutzbaren Angebote existieren, sollen bevorzugt Standardprodukte am Markt beschafft werden - statt individuelle Lösungen zu entwickeln. Die Nutzung und Förderung von Open-Source-Lösungen werden hierbei stets vorgezogen.
Ende-Zu-Ende-Digitalisierung	Der Standard-Verwaltungsprozess ist digital und über Organisationsgrenzen hinweg optimiert: Damit sollen Verwaltungskunden in den Fokus gestellt, Medienbrüche vermieden und Automatisierungspotenziale genutzt werden.

Prinzip	Erläuterung
Managed Services only	Die Nutzung bestehender, zentral gemanagter IT-Dienste ist stets zu bevorzugen, um Effizienz, Sicherheit, Verfügbarkeit und Skalierbarkeit zu erhöhen.

Abbildung 3 Architekturprinzipien der D-Architektur bzw. des D-Stack

Neben diesen einzelnen Prinzipien gelten alle Vorgaben der Nationalen IT-Architekturrichtlinie im dort vorgeschriebenen Verbindlichkeitsgrad (kann/soll/muss).

3.2 Beschreibung

API-first

Programmierschnittstellen (APIs) werden von Anfang an als zentrale Elemente der Lösungsarchitekturen konzipiert und spezifiziert sowie im Betrieb laufend dokumentiert.
Der API-first-Ansatz fordert, dass Programmierschnittstellen (APIs) von Anfang an als zentrale Bausteine einer IT-Architektur konzipiert und spezifiziert werden – noch bevor Anwendungen entwickelt werden. Neben der frühzeitigen Entwicklung technischer APIs stellt dieses Prinzip auch deren Nutzung in den Vordergrund. Technische APIs sind als Kommunikationsweg grafischen Benutzeroberflächen stets zu bevorzugen, um eine hohe Effizienz und Skalierbarkeit durch Automatisierung zu erzielen.
Für die D-Architektur bringt dieser Ansatz tiefgreifende strategische und technische Implikationen mit sich:

- Schnittstellen zuerst denken: Die APIs werden nicht nachträglich aus bestehenden Anwendungen abgeleitet, sondern bereits im Rahmen der Referenzarchitekturen geplant und designt.
- Standardisierung und Governance: Tools wie OpenAPI, JSON-Schema oder AsyncAPI helfen, Schnittstellen konsistent und versionierbar zu gestalten. Dazu muss ein zentrales Repository geschaffen werden (z.B. openCode).
- Security-by-Design: Sicherheitsmechanismen (z.B. OAuth2, mTLS, JWTs) werden bereits in der Anwendungsspezifikation berücksichtigt und in der Umsetzung laufend automatisiert getestet.
- DevSecOps & CI/CD: Die APIs sind integraler Bestandteil automatisierter Entwicklungs- und Deployment-Prozesse.

Damit werden folgende strategischen Ziele verfolgt:

- Interoperabilität fördern: API-first ermöglicht den effizienten Datenaustausch zwischen Behörden, Ländern, Kommunen und externen Partnern.
- Silos aufbrechen: Durch standardisierte Schnittstellen können behördliche Datenquellen geöffnet und gemeinsam genutzt werden.
- Innovationsökosysteme schaffen: Öffentliche APIs ermöglichen GovTech-Unternehmen und zivilgesellschaftlichen Akteuren, neue digitale Lösungen zu entwickeln.
- Registermodernisierung und OZG-Umsetzung: APIs sind Schlüsseltechnologie für moderne Verwaltungsportale, Registerzugriffe und Ende-zu-Ende-digitalisierte Services.

Das Prinzip "API first" lässt sich auf folgende Visionen der OZG-Rahmenarchitektur beziehen:

- UE4. Interoperabilität ist, auch innerhalb Europas, durch die Verwendung von internationalen und marktüblichen Standards sowie offenen Schnittstellen gewährleistet.
- F10|03. Alle für die digitale Verwaltung verwendeten Standards, leicht testbaren Schnittstellen und Informationen zu Basiskomponenten sind aktuell und zentral dokumentiert.
- F12|04. Einzelne Komponenten externer Dienstleister lassen sich über standardisierte Schnittstellen in Verwaltungsanwendungen einbinden.

Das Prinzip "API first" lässt sich auf folgende Vorgaben der Nationalen Architekturrichtlinie beziehen:

- TV-02 Schnittstellen: Die Schnittstellen sollen standardisiert implementiert und genutzt werden.
- AV-02 Interoperabilität: Informationstechnik und Digitalisierung sollen interoperabel gestaltet sein.
- FV-02 Dienste- und Schnittstellenbeschreibung: Die Beschreibung von Diensten und Schnittstellen muss standardisiert dokumentiert sein.

Serviceorientierung & Lose Kopplung

Dienste (Services) sind zentrale Architekturbausteine, die Funktionen bündeln. Sie und ihre Lösungsbausteine sind modular konzipiert, weitgehend unabhängig austauschbar und klar abgegrenzt.

Serviceorientierung beschreibt ein Architekturparadigma, bei dem IT-Funktionalitäten als Dienste bereitgestellt werden. Diese Dienste sind fachlich abgeschlossen und unabhängig nutzbar, standardisiert über definierte Schnittstellen, plattformunabhängig und über Netzwerke verfügbar, wiederverwendbar in verschiedenen Geschäftsprozessen. Ziel ist es, komplexe Geschäftsprozesse durch die Orchestrierung einzelner Dienste flexibel abzubilden. Ein Dienst wie „Bonitätsprüfung“ kann z. B. von verschiedenen Anwendungen genutzt werden, ohne dass deren interne Logik bekannt sein muss.

Lose Kopplung fordert, dass die einzelnen IT-Komponenten und Dienste möglichst geringe Abhängigkeiten zueinander haben. Das wird erreicht durch:

- Offene Standards und standardisierte Schnittstellen,
- Minimierung von Abhängigkeiten zu spezifischen Laufzeitumgebungen,
- Serverbasierte Bereitstellung und browserbasierter Zugriff.

Dadurch wird die Wartung, Weiterentwicklung und Skalierung von IT-Systemen erleichtert. Änderungen an einem Dienst wirken sich nicht direkt auf andere aus, was die Agilität und Anpassungsfähigkeit erhöht.

In der Nationale IT-Architekturrichtlinie ist lose Kopplung ein zentrales Prinzip (FV-09 Entkopplung). Sie ermöglicht effiziente Wiederverwendung von Diensten, Standardisierung über Behörden hinweg, Flexibilität bei der Integration neuer Technologien sowie erleichterte Governance durch Schnittstellenmanagement.

Serviceorientierung und lose Kopplung sind also Schlüsselprinzipien, um die digitale Verwaltung des Bundes modular, skalierbar und zukunftssicher zu gestalten.

Das Prinzip "Serviceorientierung & Lose Kopplung" lässt sich auf folgende Visionen der OZG-Rahmenarchitektur beziehen:

- F12|05: Externe Dienstleister können digitale Verwaltungsleistungen über standardisierte Schnittstellen in ihre Services einbinden.

Das Prinzip "Serviceorientierung & Lose Kopplung" lässt sich auf folgende Vorgaben der Nationalen Architekturrichtlinie beziehen:

- FV-09 Entkopplung: Die Entkopplung (lose Kopplung) soll optimiert werden.
- AV-09 Digitale Souveränität: Informationstechnik und Digitalisierung müssen digital souverän gestaltet sein.

Wiederverwendbarkeit & Portierbarkeit

Architekturelemente und bereitgestellte IT-Lösungen sind weitgehend wiederverwendbar und leicht in andere fachliche und technische Kontexte portierbar.

Wiederverwendbarkeit bezieht sich auf die Fähigkeit, bestehende IT-Komponenten, Architekturelemente oder Lösungen mehrfach und in unterschiedlichen Kontexten einzusetzen. In der Architekturrichtlinie des Bundes bedeutet das:

- Modulare Architektur: Systeme und Komponenten sollen so gestaltet sein, dass sie unabhängig voneinander funktionieren und in verschiedenen Projekten wiederverwendet werden können.
- Standardisierung: Durch die Verwendung einheitlicher Schnittstellen und Technologien wird die Wiederverwendung erleichtert.
- Effizienzsteigerung: Wiederverwendbare Komponenten reduzieren Entwicklungsaufwand, Kosten und Zeit bei neuen Vorhaben.
- Nachnutzung: Die Richtlinie empfiehlt ausdrücklich die Nachnutzung bestehender Architekturvorgaben bei Neuentwicklungen

Portierbarkeit beschreibt die Fähigkeit, IT-Lösungen oder Komponenten einfach auf andere technische Umgebungen oder Plattformen zu übertragen, ohne dass umfangreiche Anpassungen nötig sind. In der D-Architektur bedeutet das:

- Technologische Unabhängigkeit: Systeme sollen nicht an proprietäre Plattformen gebunden sein.
- Cloud-Fähigkeit: Die Architekturrichtlinie berücksichtigt zunehmend die Anforderungen an Cloud-Umgebungen und hybride Infrastrukturen.
- Offene Standards: Die Nutzung offener, interoperabler Standards erleichtert die Portierung zwischen verschiedenen Systemen und Organisationen.

Beide Prinzipien sind Teil der technischen Vorgaben der Architekturrichtlinie und dienen dazu, die Interoperabilität zwischen Behörden und Systemen zu verbessern, die Digitalisierung der Verwaltung nachhaltig zu gestalten und die Flexibilität bei zukünftigen Entwicklungen zu erhöhen. Sie sind eng verknüpft mit europäischen Rahmenwerken wie dem European Interoperability Framework (EIF) und dem TOGAF-Modell, die als Grundlagen für die D-Architektur dienen.

Das Prinzip "Wiederverwendbarkeit & Portierbarkeit" lässt sich auf folgende Visionen der OZG-Rahmenarchitektur beziehen:

- F10|04: Open-Source-Code von bestehenden Komponenten kann an zentraler Stelle eingesehen, überarbeitet und wiederverwendet werden.

Das Prinzip "Wiederverwendbarkeit & Portierbarkeit" lässt sich auf folgende Vorgaben der Nationalen Architekturrichtlinie beziehen:

- AV-10 Skalierbarkeit: Informationstechnik und Digitalisierung sollen skalierbar gestaltet sein.
- TV-05 Entwicklung: Die Entwicklung soll standardisiert erfolgen.

DevSecOps Only

Die Entwicklung, die Sicherheit und der Betrieb von IT werden als integrierter Prozess betrachtet. Die D-Architektur bekennt sich dazu, dass alle IT-Entwicklungs- und Betriebsprozesse ausschließlich nach dem DevSecOps-Prinzip gestaltet werden sollen. Dabei handelt es sich um ein integriertes Vorgehensmodell, bei dem Sicherheit nicht nachträglich, sondern von Anfang an in den Entwicklungsprozess eingebunden wird. Ziel ist es, durch Automatisierung und Zusammenarbeit Sicherheitslücken frühzeitig zu erkennen, kontinuierliche Auslieferung sicherer Software zu ermöglichen und die Reaktionsfähigkeit bei Bedrohungen zu erhöhen.
Die D-Architektur muss daher die Anwendung des DevSecOps-Prinzips in allen IT-Vorhaben , automatisierte Sicherheitsprüfungen in CI/CD-Pipelines, transparente und nachvollziehbare Prozesse für Sicherheit und Compliance sowie eine Kultur der gemeinsamen Verantwortung für Entwickler, Sicherheitsverantwortliche und Betrieb verpflichtend vorschreiben.
Dies zahlt ein auf die Ziele:

- Erhöhte Sicherheit durch frühzeitige Integration,
- Schnellere Entwicklungszyklen bei gleichzeitiger Einhaltung von Sicherheitsstandards,
- Skalierbarkeit und Wiederverwendbarkeit durch standardisierte Prozesse,
- Effiziente Governance durch automatisierte Prüfmechanismen.

Der D-Stack wird DevSecOps-Werkzeuge für folgende Funktionsbereiche bereitstellen:

- Codeanalyse & Sicherheitsscans; Statische Codeanalyse zur Erkennung von Bugs, Sicherheitslücken und Code-Smells (z.B. SonarQube); Scannen Open-Source-Abhängigkeiten auf bekannte Schwachstellen (CVEs) (z.B. Snyk, WhiteSource, Black Duck); Enterprise-Tools für tiefgehende Sicherheitsanalysen im Quellcode (z.B. Checkmarx, Fortify).
- Container-Sicherheit: Schutz von Container-Images und Laufzeitumgebungen (z.B. Aqua Security, Twistlock); Leichtgewichtiges Tool zur Schwachstellenanalyse von Docker-Images (z.B. Trivy).
- CI/CD-Pipelines: Automatisierung von Build-, Test- und Deployment-Prozessen (z.B. GitLab CI, Jenkins, GitHub Actions); Kubernetes-native CI/CD-Tools mit Fokus auf Sicherheit und Governance (z.B. Tekton, ArgoCD).
- Infrastructure-as-Code (IaC) & Sicherheit: Infrastrukturdefinition mit Sicherheitsprüfungen (z.B. Terraform + tfsec, Terrascan); Automatisierte Konfiguration mit Sicherheitschecks (z.B. Ansible + Ansible-Lint).
- Monitoring & Logging: Überwachung von Systemmetriken (z.B. Prometheus + Grafana); Zentrale Loganalyse (z.B. ELK Stack (Elasticsearch, Logstash, Kibana)); Echtzeit-Sicherheitsüberwachung für Container (z.B. Falco).
- Secrets Management: Sichere Verwaltung von Zugangsdaten, Tokens und Zertifikaten (z.B. HashiCorp Vault).

Das Prinzip "DevSecOps Only" lässt sich auf folgende Visionen der OZG-Rahmenarchitektur beziehen:

- keine

Das Prinzip "DevSecOps Only" lässt sich auf folgende Vorgaben der Nationalen Architekturrichtlinie beziehen:

- TV-01 Administration: Die Administration soll über standardisierte Prozesse erfolgen. Die Administration soll über automatisierte kontinuierliche Bereitstellung (Continuous Integration, Deployment, Delivery - DevOps) erfolgen.
- TV-05 Entwicklung: Die Entwicklung soll standardisiert erfolgen.

Zero-Trust

Lösungsbausteine müssen für Zero-Trust-Architekturen vorbereitet sein (u.a. Rechteprüfung, Logging).

Zero-Trust basiert u.a. auf dem Prinzip „Assume Breach" – also der Annahme, dass ein Angriff bereits stattgefunden hat oder jederzeit stattfinden kann. Daraus folgt, dass es kein automatisches Vertrauen gegenüber Nutzern, Geräten oder Anwendungen, weder innerhalb noch außerhalb des Netzwerks geben darf. Zudem darf jede Entität nur die Zugriffsrechte erhalten, die sie unbedingt benötigt (Least Privilege). Eine weitere Maßnahme ist die kontinuierliche Verifikation: Identitäten, Kontexte und Sicherheitszustände werden laufend überprüft.
Das BSI schlägt ein Zero Trust-Integrationsmodell vor, das die relevanten IT-Infrastrukturbereiche identifiziert und strukturiert. Dieses Modell ist flexibel und muss je nach Organisation angepasst werden. Für die D-Architektur bedeutet dies, dass die verschiedenen Zero-Trust-Konzepte verbindlich abgestimmt werden müssen. Die Interoperabilität von Produkten ist dabei eine große Herausforderung, insbesondere wegen fehlender Standardisierungen. Dennoch ist die Zero Trust-Fähigkeit der Lösungen im Rahmen der D-Architektur stets sicherzustellen.
Das Prinzip "Zero-Trust" lässt sich auf folgende Visionen der OZG-Rahmenarchitektur beziehen:

- keine

Das Prinzip "Zero-Trust" lässt sich auf folgende Vorgaben der Nationalen Architekturrichtlinie beziehen:

- FV-08 Schutz: Der Schutz von sensiblen Informationen muss durch bedarfsgerechte Schutzmechanismen gewährleistet werden.

Technologisch aktuell

Das Prinzip „Technologisch aktuell" bedeutet für die Architektur in Bund und Ländern, dass Architekturentscheidungen konsequent am aktuellen Stand der Technik ausgerichtet werden müssen.

Dies hat weitreichende Auswirkungen auf Planung, Umsetzung und Betrieb von IT-Systemen im Kontext der D-Architektur. Laut dem BSI ist der „Stand der Technik" ein dynamischer Begriff, der sich nicht gesetzlich abschließend definieren lässt, sondern sich aus internationalen Normen und Standards (z. B. ISO, DIN, IEC), bewährten Best Practices sowie erfolgreich eingesetzten Technologien ableitet.

Die Nationale IT-Architekturrichtlinie fordert, dass Entscheidungen systematisch, nachvollziehbar und transparent getroffen werden – und dabei stets den aktuellen technischen Möglichkeiten Rechnung tragen. Die IT-Architektur des Bundes soll zukunftssicher sein. Daher dürfen veraltete Technologien nicht Grundlage neuer Projekte sein. Darüber hinaus müssen technologische Weiterentwicklungen proaktiv in Architekturvorgaben integriert werden. Zudem werden Interoperabilität zwischen Behörden und Systemen, Standardisierung von Schnittstellen und Komponenten sowie Effizienz in der Umsetzung und Wartung durch technologisch aktuelle Lösungen gefördert.
Das Prinzip „technologisch aktuell“ ist kein Nice-to-have, sondern ein verpflichtender Maßstab für die D-Architektur. Es sorgt dafür, dass die IT-Systeme sicher, effizient, zukunftsfähig und gesetzeskonform bleibt.
Zuordnung
Das Prinzip "Technologisch aktuell" lässt sich auf folgende Visionen der OZG-Rahmenarchitektur beziehen:

- UE5: Es werden Technologien eingesetzt, die dem aktuellen Stand der Technik entsprechen.

Das Prinzip "Technologisch aktuell" lässt sich auf folgende Vorgaben der Nationalen Architekturrichtlinie beziehen:

- TV-08

Made in EU first

Das Prinzip „Made in EU first“ fordert, dass bei der Auswahl von IT-Produkten und IT-Dienstleistungen europäische Anbieter bevorzugt werden.
Damit sollen die digitale Souveränität Deutschlands gestärkt und strategische Abhängigkeiten reduziert werden. Dies gilt für alle Ebenen der digitalen Souveränität: Technologie, Betrieb und Daten. Von der Bundesregierung werden technologische Abhängigkeiten von Drittstaaten (z. B. USA, China) als strategisches Risiko gesehen. Daher soll die Kontrolle über kritische Infrastrukturen, Datenhoheit und politische Handlungsfreiheit durch europäische Lösungen gesichert werden.
Die D-Architektur und der D-Stack müssen in diesem Sinne sicherstellen, dass Produkte aus EU-Ländern vorrangig berücksichtigt werden oder Anbieter außerhalb der EU nur dann zum Einsatz kommen, wenn keine gleichwertige europäische Lösung verfügbar ist. Ein weiterer Aspekt ist, dass der Bund und die Länder IT-Aufträge gezielt bündeln, um als Ankerkunden die europäische Digitalwirtschaft zu stärken. Aus Gründen der digitalen Souveränität Deutschlands werden hierbei zunächst deutsche Anbieter bevorzugt betrachtet.
"Made in EU first" ist mehr als eine politische Absicht. Es ist ein verbindliches Architekturprinzip, das die technologische Eigenständigkeit Deutschlands stärkt, die Resilienz der Verwaltungs-IT erhöht und die europäische Innovationskraft gezielt fördert.
Zuordnung
Das Prinzip "Made in EU first" lässt sich auf folgende Visionen der OZG-Rahmenarchitektur beziehen:

- F13|02

Das Prinzip "Made in EU first" lässt sich auf folgende Vorgaben der Nationalen Architekturrichtlinie beziehen:

- AV-09

Prefer Reuse over Buy over Make

Das Prinzip „Prefer Reuse over Buy over Make“ bedeutet für die D-Architektur, dass Standardprodukte vom Markt bevorzugt beschafft werden, anstatt individuelle Eigenentwicklungen zu realisieren.
Ziel ist es, Effizienz, Wirtschaftlichkeit und Zukunftsfähigkeit der IT-Systeme zu steigern. Die Nationale IT-Architekturrichtlinie fordert, dass Architekturentscheidungen systematisch und transparent getroffen werden – dabei ist die Marktsichtung ein zentraler Bestandteil.
Vor jeder Entscheidung zur Systementwicklung muss daher geprüft werden:

- Gibt es geeignete Standardprodukte?
- Können bestehende Lösungen wiederverwendet oder angepasst werden?
- Ist eine Open-Source-Komponente verfügbar? Nur wenn diese Optionen ausscheiden, wird eine Eigenentwicklung in Betracht gezogen.

Die Entscheidung basiert grundsätzlich auf wirtschaftlichen Kriterien (z. B. Anschaffungskosten, Wartung, Anpassungsaufwand), strategischen Vorgaben (z. B. Souveränität, Wiederverwendbarkeit) und technischen Risiken (z. B. Integrationsfähigkeit, Kompatibilität). Daher werden Open-Source-Lösungen bei gleicher Eignung stets bevorzugt.
„Prefer Reuse over Buy over Make“ ist ein strategisches Architekturprinzip, das die Effizienz der IT-Beschaffung erhöht, die Entwicklungsrisiken minimiert sowie die Wartbarkeit und Skalierbarkeit der IT-Systeme verbessert. Eigenentwicklungen sind begründungspflichtig und nur dann zulässig, wenn sie nachweislich wirtschaftlicher oder technisch zwingend erforderlich sind (s. V-Modell XT, Produkt Make-or-Buy-Entscheidung).
Zuordnung
Das Prinzip "Prefer Reuse over Buy over Make" lässt sich auf folgende Visionen der OZG-Rahmenarchitektur beziehen:

- keine

Das Prinzip "Prefer Reuse over Buy over Make" lässt sich auf folgende Vorgaben der Nationalen Architekturrichtlinie beziehen:

- keine

Ende-Zu-Ende-Digitalisierung

Das Prinzip „Ende-zu-Ende-Digitalisierung“ bedeutet für die D-Architektur, dass Verwaltungsprozesse vollständig digitalisiert werden – von der Antragstellung über die Bearbeitung bis zur Bescheiderstellung und Archivierung.
Es geht um medienbruchfreie Abläufe, die auf allen föderalen Ebenen umgesetzt und an die Anforderungen der Digitalisierung angepasst sind. Die Ende-zu-Ende-Digitalisierung ist nicht nur eine technische Maßnahme, sondern ein architekturprägendes Prinzip, das folgende Ziele verfolgt:

- Vermeidung von Medienbrüchen: Keine Papierformulare, keine manuelle Übertragung.
- Automatisierungspotenziale nutzen: Prozesse sollen teil- oder vollautomatisiert ablaufen.
- Einheitliche Standards und Schnittstellen: Für eine reibungslose Integration über Bund, Länder und Kommunen hinweg.

Für die Prozessgestaltung bedeutet dies:

- Prozesse müssen von Anfang an digital gedacht werden („Digital by Design“), immer ausgehend von der Nutzendenperspektive. Der digitale Prozess gilt als Standard, ggf. erforderliche manuelle Alternativen sind nur ergänzend zulässig.
- Vorhandene Prozesse müssen in ihrem gesamten fachlichen Kontext (z.B. andere Prozesse, beteiligte Rollen) auch organisationsübergreifend geprüft und optimiert werden.
- Jeder Prozess wird auf Notwendigkeit und Automatisierbarkeit geprüft.
- Die Architektur muss anschlussfähig für zentrale Basisdienste wie BundID bzw. DeutschlandID und digitale Postfächer sein.

Für die Technische Infrastruktur bedeutet dies:

- Backend-Systeme (Fachverfahren) müssen an digitale Frontends angebunden werden.
- Elektronische Aktenführung und digitale Bescheidzustellung sind Pflichtbestandteile.
- Die Architektur muss skalierbar und interoperabel sein – auch für zukünftige EU-Vorgaben wie das Single Digital Gateway.

Für rechtliche und organisatorische Rahmenbedingungen bedeutet dies:

- Das geänderte Onlinezugangsgesetz (OZG 2.0) macht Ende-zu-Ende-Digitalisierung zum gesetzlichen Standard.
- Schriftformerfordernisse werden durch digitale Identitäten ersetzt (z. B. eID, Elster-Zertifikat).
- Das Once-Only-Prinzip wird rechtlich verankert: Daten müssen nur einmal eingereicht werden und können behördenübergreifend genutzt werden.

„Ende-zu-Ende-Digitalisierung“ ist ein zentraler Baustein der Deutschland-Architektur, der auf durchgängige digitale Prozesse, verbindliche Standards und eine nutzerzentrierte Verwaltung ausgerichtet ist.

Zuordnung

Das Prinzip "Ende-Zu-Ende-Digitalisierung" lässt sich auf folgende Visionen der OZG-Rahmenarchitektur beziehen:

- UE3

Das Prinzip "Ende-Zu-Ende-Digitalisierung" lässt sich auf folgende Vorgaben der Nationalen Architekturrichtlinie beziehen:

- AV-04
- AV-05
- AV-06

Managed Services only

Das Prinzip „Managed Services only“ bedeutet für die D-Architektur, dass bestehende, zentral bereitgestellte IT-Dienste bevorzugt genutzt und wiederverwendet werden – anstatt neue, individuelle Lösungen zu entwickeln oder selbst zu betreiben.

Die D-Architektur setzt auf standardisierte, zentral gemanagte IT-Dienste, um Effizienz, Sicherheit, und Skalierbarkeit zu erhöhen. Dabei gilt: Wiederverwendung vor Neuentwicklung – insbesondere bei Basisdiensten wie Identitätsmanagement, Dokumentenmanagement, Hosting, Monitoring oder Sicherheitslösungen.

Vor jeder neuen Entwicklung muss daher geprüft werden, ob ein bestehender, zentral betriebener IT-Dienst mit dem erforderlichen Funktionsumfang bereits verfügbar ist oder ein solcher Dienst wirtschaftlich dahingehend erweitert werden kann. Die Systemarchitektur muss zudem anschlussfähig an zentrale Dienste oder die föderale Cloud-Infrastruktur sein.
Die D-Architektur wird so durch die Dienstekonsolidierung geprägt, indem zentrale Dienste nur einmal entwickelt und mehrfach genutzt werden. Dies reduziert Komplexität, Kosten und Fehleranfälligkeit.
Die Nutzung von Managed Services erfolgt koordiniert über Steuerungskreise, die über Wiederverwendung und Qualität entscheiden. Die Verantwortung für Betrieb und Pflege liegt beim Dienstanbieter – z. B. ITZBund oder andere zentrale Stellen.
„Managed Services only“ ist ein strategisches Architekturprinzip, das die Effizienz der IT-Landschaft des Bundes erhöht, die Wiederverwendung bestehender Lösungen fördert und die digitale Souveränität durch zentrale Steuerung stärkt. Eigenentwicklungen sind nur dann zulässig, wenn kein geeigneter Managed Service verfügbar ist (dies muss entsprechend begründet werden).
Zuordnung
Das Prinzip "Managed Services only" lässt sich auf folgende Visionen der OZG-Rahmenarchitektur beziehen:

- keine

Das Prinzip "Managed Services only" lässt sich auf folgende Vorgaben der Nationalen Architekturrichtlinie beziehen:

- keine

4 Erste Funktionsbausteine

4.1 Vorgehen

Die ersten Funktionsbausteine der Deutschland-Architektur wurden anhand mehrerer Schritte auf Basis des Wertstroms „Inanspruchnahme einer Verwaltungsleistung“ abgeleitet. Eine Fortschreibung und Validierung der Funktionsbausteine muss fortlaufend beim Aufbau der Deutschland-Architektur und der dabei weiteren betrachteten Wertströme erfolgen.

Definition von Funktionsbausteinen

Ausgehend von den zuvor beschriebenen Prozessschritten wurden voneinander separierbare Funktionalitäten identifiziert, welche den jeweiligen Prozessschritte (oder mehrere) unterstützen. Aus diesen können später IT-Lösungen abgeleitet werden, welche die benötigte Funktionalität bereitstellen. Ziel ist es hierbei querschnittliche Basisfunktionalitäten zu identifizieren, die möglichst einmalig entwickelt und zentral bereitgestellt, allerdings großflächig (von Bund, Ländern und Kommunen) nachgenutzt werden können.
Diese Funktionsbausteine der D-Architektur orientieren sich an den Funktionsbausteinen der OZG-Rahmenarchitektur und schreiben diese fort. Als weitere Inputs wurden auch die FIT-AB Referenzarchitektur, die Dienstelandkarte der Gemeinsamen IT des Bundes als auch die Betrachtungen zum Online-Dienst-Ökosystem der Stadt Hamburg genutzt.
Die ersten Funktionsbausteine werden im folgenden Unterkapitel beschrieben. Die Darstellung und Zuordnung der Funktionsbausteine in Schichten soll im weiteren Verlauf validiert und mit dem D-Stack abgestimmt werden.

Die Funktionsbausteine haben zwei Reifegrade:
Reifegrad hoch: Der Funktionsbaustein wurde im Vorprojekt Deutschland-Architektur konzipiert und abgestimmt.
Reifegrad niedrig: Der Funktionsbaustein wurde im Vorprojekt Deutschland-Architektur vorgeschlagen, im Projektteam jedoch nicht abschließend definiert. Eine Fortschreibung und Detaillierung wird anhand von weiteren Wertströmen empfohlen.

4.2 Überblick

Abbildung 4 Übersicht über Funktionsbausteine „Inanspruchnahme einer Verwaltungsleistung“

4.3 Beschreibung

Die in Abbildung 4 dargestellten Funktionsbausteine für den Wertstrom „Inanspruchnahme einer Verwaltungsleistung“ werden in der folgenden Tabelle beschrieben.

Funktionsbaustein	Beschreibung der Funktionalität
Zentrales Nutzenden-Frontend	Es wird ein zentraler Zugang für Verwaltungskunden eingerichtet, über den sie alle für sie relevanten Informationen und Funktionalitäten im Kontext der Verwaltungsinteraktion erreichen können (z. B. Antragsstellung, gestellte Anträge, erhaltene Bescheide, Status von Verwaltungsvorgängen, Pflege einer Vertreterregelung). Es bietet Zugriff auf alle wichtigen Funktionen, nutzt die Funktionalitäten selbst allerdings von separaten Funktionsbausteinen (z. B. Postfach, Statusmonitoring) nach.
Feedback und Nutzungsanalyse	Für adressaten-zentrierte Verwaltungsleistungen ist die Kenntnis des Nutzerverhaltens sowie deren Wahrnehmung der bereitgestellten Dienste essentiell. Daher werden statistische Nutzungsdaten bzgl. der digitalen Verwaltungsleistungen gesammelt und Mittel zu deren Auswertung bereitgestellt. Gleiches gilt für Feedback-Informationen zu den Nutzererfahrungen bei der Verwendung digitaler Verwaltungsleistungen.
Vorgangs- und Sachbearbeitung	[Reifegrad niedrig] Steht für jegliche Funktionalität, die für die Bearbeitung von Verwaltungsvorgängen auf der Seite der Verwaltung benötigt wird. Die Bearbeitung erfolgt im Normalfall automatisiert. Querschnittsfunktionalität kann hier im Rahmen von standardisierten Funktionalitäten und Mechanismen gesehen werden, die wiederkehrend benötigt werden und speziell die Vorgangs- und Sachbearbeitung effizient ermöglichen.

Funktionsbaustein	Beschreibung der Funktionalität
Postfach und Interaktion (G2C)	Für eine dynamische und historisierte (nachverfolgbare) Interaktion zwischen Verwaltung und Verwaltungskunden wird dieser Funktionsbaustein festgelegt. Er beschreibt jegliche Funktionalität, die hierbei benötigt wird - sowohl im Rahmen der Durchführung von Verwaltungsleistungen (z. B. Bereitstellung und Vorhalten von Bescheiden) als auch außerhalb davon (z. B. Nutzung eines zentralen Bürger-Postfachs im Kontext des privaten Online-Bankings). Verwaltungskunden können selbst festlegen über welchen Kanal sie Benachrichtigungen von der Verwaltung erhalten wollen.
Datenaustausch	Beschreibt eine möglichst homogene Datentransfer-Funktion, welche alle im Kontext der D-Architektur erforderlichen Datentransfers abdecken kann. Der Datenaustausch soll dabei nicht nur innerhalb der Verwaltung möglich sein, sondern auch mit verwaltungsexternen Akteuren.
Abruf und Bereitstellung von Daten und Nachweisen	Damit Verwaltungskunden notwendige Nachweise nicht explizit dem Antrag beifügen müssen, können diese im Rahmen der Antragsstellung automatisiert abgerufen und dem Antrag beigefügt werden.
Event-Verarbeitung für antragslose Verwaltung	[Reifegrad niedrig] Die Idee ist hierbei, dass ein Fachverfahren / EzE-Dienst eine relevante Datenänderung erkennt und diese bekannt macht, indem es einen entsprechenden Hinweis an diesen Funktionsbaustein sendet. Darauf „abonnierte“ Empfänger (z. B. andere EzE-Dienste) erhalten dann die Information, was sich geändert hat und können darauf basierend proaktiv Verwaltungsleistungen anstoßen. Dieses Vorgehen erfordert auch die Festlegung von Datenhoheit für solche Daten und entsprechende Datenformate, über die entsprechende Zustandsänderungen abgebildet werden können.
Elektronische Veraktung	Eine elektronische Veraktung von Informationen ist essenzieller Bestandteil einer digitalen Verwaltung, um Informationen, Beschlüsse und Nachweise rechtssicher zu verarbeiten und bereitzustellen.
Initiierung einer Verwaltungsleistung	Verwaltungskunden als Nutzende von Verwaltungsleistungen stellen einen digitalen Antrag und reichen dabei alle notwendigen Nachweise ein. Einige Nachweise können nach dem Once-Only-Prinzip vollautomatisch abgeholt werden. In einigen Fällen kann eine behördeninterne Antragsinitiierung erfolgen, nachdem bestimmte Ereignisse eintreten, wie z. B. nach der Geburt eines Kindes. Die Initiierung durch den Verwaltungskunden kann formularbasiert, interaktionsbasiert (z. B. Chat-basiert) oder API-basiert (z. B. durch eigene Unternehmensanwendungen) erfolgen.
Zuständigkeitsfindung [Zentrale Verzeichnisse]	Bietet Funktionen zur Pflege und Bereitstellung von föderalen Struktur- und Steuerungsdaten für die automatisierte Zuständigkeitsfindung von Verwaltungsleistungen. Es werden dabei sowohl Funktionen für die Redaktion der erforderlichen Daten, deren Speicherung als auch deren Abruf angeboten.
Parametrisierung [Zentrale Verzeichnisse]	Bietet Funktionen zur Pflege und Bereitstellung von föderalen Struktur- und Steuerungsdaten zur Parametrisierung von digitalen Verwaltungsleistungen, um eine bessere Nachnutzbarkeit

Funktionsbaustein	Beschreibung der Funktionalität
	herzustellen. Es werden dabei sowohl Funktionen für die Redaktion der erforderlichen Daten, deren Speicherung als auch deren Abruf angeboten.
Föderale Metadaten [Zentrale Verzeichnisse]	Bietet Funktionen zur Pflege und Bereitstellung von föderalen Metadaten zur Ermöglichung von antragslosen Verwaltungsleistungen sowie einheitlichem Fachlogik-Modell für EzE-Verwaltungsleistungen. Es werden dabei sowohl Funktionen für die Redaktion der erforderlichen Daten, deren Speicherung als auch deren Abruf angeboten.
Technisches Schnittstellenverzeichnis (API) [Zentrale Verzeichnisse]	Bereitstellung eines Verzeichnisses, in dem alle IT-Systeme für den Zugriff auf alle digitalen Angebote (z. B. Basisdienste, Antragsstellung, Endanwendungen) der Verwaltung gelistet sind, um einen Zugriff auf diese zu ermöglichen.
Design-System	Digitale staatliche Angebote müssen als solche erkennbar und an den Nutzenden ausgerichtet werden. Sie sollen daher leicht verständlich, übersichtlich und gleichartig in der Nutzung sein. Hierfür werden entsprechende Vorgaben und Vorlagen bereitgestellt, die in diesem Funktionsbaustein enthalten sind.
KI-Querschnittsdienste	Es handelt sich um KI-Basisfunktionalität, die für verschiedene fachliche Zwecke orchestriert werden kann (z. B. „Chatbasierte Antragsstellung“), u.a. durch Parametrierung der KI mit bestimmten Kontext-Informationen (z. B. fachlichen/juristischen Informationen, Zuständigkeitsfindung, Bezahlung).
Authentifizierung	Verwaltungskunden als Nutzende von Verwaltungsleistungen identifizieren und authentisieren sich bei Bedarf, um eine Verwaltungsleistung in Anspruch nehmen zu können. Zum Identitätsmanagement gehört zudem das Pflegen von Identitätsdaten und Personenstammdaten sowie das Hinterlegen von Vollmachten und Vertretungsregelungen.
Ein- und Auszahlung	Gebühren für Verwaltungsleistungen können online bezahlt werden. Es gibt sowohl Vorabentrichtung der Gebühren, als auch nachgelagerte Zahlungen, die erst im Rahmen der Sachbearbeitung bestimmt werden. Darüber hinaus umfasst dies auch die Auszahlung finanzieller Mittel durch die Verwaltung.
Siegeln und Signieren	Die elektronische Signatur ist eine Unterschrift, mit der natürliche Personen (Bürgerinnen und Bürger sowie Vertreterinnen und Vertreter von Behörden, Unternehmen und Organisationen) digitale Dokumente rechtsverbindlich elektronisch unterzeichnen können. Dies kann auch im Namen ihrer Mandantinnen und Mandanten geschehen. Behörden stellen durch elektronische Siegel die Echtheit digitaler Dokumente sicher. Die erforderliche Validierungs-/Prüflogik für Siegelung und Signatur ist hier ebenfalls enthalten.
Geokodierung	Dieser Funktionsbaustein bietet die Möglichkeit Geo-Koordinaten in Adressen und zu verwaltungspolitischer Gliederung umzurechnen.
Kartierung	Dieser Funktionsbaustein bietet die Möglichkeit (weltweite) Kartenansichten in Verwaltungsleistungen zu integrieren und wichtige Punkte zu markieren bzw. mit Zusatzinformationen auszustatten (z.B. Standorte von Behörden).

Funktionsbaustein	Beschreibung der Funktionalität
Statusmonitoring	Dieser Funktionsbaustein bietet die Möglichkeit alle Status-bezogenen Informationen rund um Verwaltungsvorgänge für verschiedene Nutzendengruppen (Verwaltungs-interne und -externe) darzustellen.
Consent	[Reifegrad niedrig] Bietet Verwaltungskunden die Möglichkeit ihre Einwilligungen in Datenabrufe durch die Verwaltung (z. B. Nachweise, Statusänderungen) zu steuern und den aktuellen Status ihrer Einstellungen zu überprüfen/ändern. Ebenfalls können von der Verwaltung durchgeführte Datenabrufe / -zugriffe durch den Verwaltungskunden eingesehen werden.
Cloud-Infrastruktur	[Reifegrad niedrig] Jegliche IT-Infrastruktur (bis auf Netzwerke), über welche die gesamten Funktionsbausteine der D-Architektur bereitgestellt werden. Es ist davon auszugehen, dass nicht nur ein einzelner Cloud-Infrastruktur-Provider dafür genutzt wird, sondern es sich um eine Sammlung mehrerer D-Architektur-konformer Provider handelt. Dieser Funktionsbaustein wurde als relevant für den Betrieb erachtet, jedoch im Vorprojekt nicht näher betrachtet.
Netze	[Reifegrad niedrig] Eigentlich auch zur IT-Infrastruktur gehörig, aber hier in der Bedeutung herausgehoben. Hintergrund ist, dass im Rahmen der D-Architektur grundsätzlich über offene Netze kommuniziert werden soll, um allen relevanten Stakeholdern / Teilnehmern Zugang zu ermöglichen. Die Nutzung separater Netze für die öffentliche Verwaltung (z.B. Netze des Bundes, Landesnetze, Verbindungsnetze) soll jeweils hinterfragt werden, um deren Nutzung zu reduzieren. Absicherung der Kommunikation im Kontext der D-Architektur erfolgt über Zero-Trust Mechanismen und sollte andere Möglichkeiten für eine sichere Kommunikation ermöglichen als die Abschirmung über verschiedene Netzzonen. Wenn Netzzonen separiert werden, sollen diese über Software-definierte-Mechanismen konfigurierbar / steuerbar sein. Dieser Funktionsbaustein wurde als relevant für den Betrieb erachtet, jedoch im Vorprojekt nicht näher betrachtet.
Integrationsplattform	[Reifegrad niedrig] Hiermit ist ein Baustein gemeint, über den der Zugriff auf alle IT-Systeme im Rahmen des Ökosystems der D-Architektur ermöglicht und gesteuert wird.

5 Governance-Eckpunkte

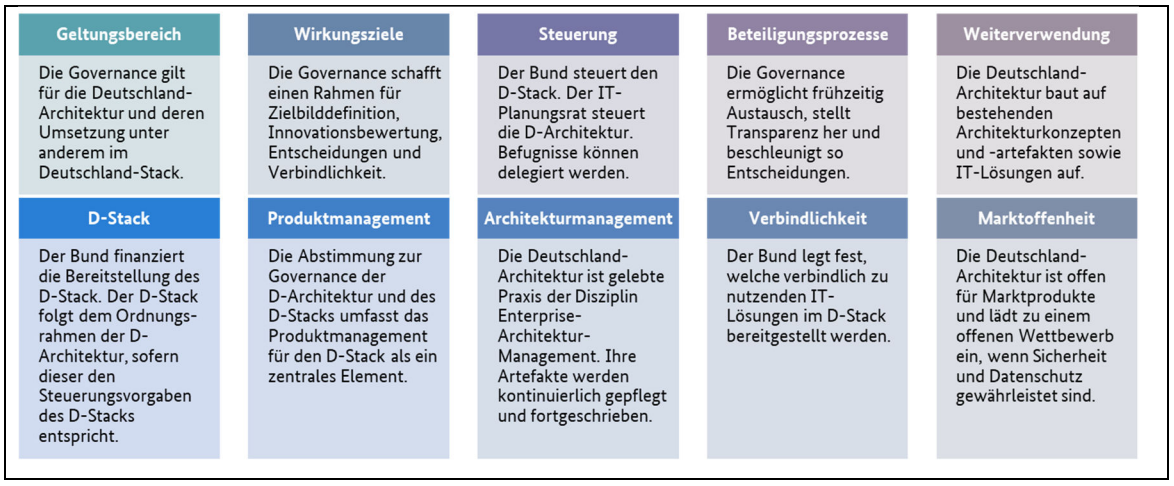

Abbildung 5 Governance-Eckpunkte Zusammenfassung

Basierend auf den folgenden Eckpunkten sollen konkrete Inhalte spezifiziert und zu einem Governance-Konzept ausgebaut werden.

1. **Geltungsbereich**: Die Governance definiert, wie die Deutschland-Architektur geprüft, geändert und unter anderem im Deutschland-Stack (D-Stack) umgesetzt wird. Sie ist Ordnungsrahmen und Arbeitsgrundlage aus verbindlichen Regeln und standardisierten Abläufen. Zentrale Entscheidungsobjekte für die Governance sind die Aufnahme, Änderung und Herausnahme von Architekturartefakten; dazu zählen auch Funktionsbausteine für die Deutschland-Architektur. Funktionsbausteine der Deutschland-Architektur sind Grundlage für die Abstimmung des BMDS mit Bund und Ländern. Lösungen des D-Stack werden entlang der Standards und Vorgaben der Deutschland-Architektur, des Tech-Stacks und der föderalen Architekturrichtlinie realisiert.
2. **Wirkungsziele**: Die Governance schafft einen Rahmen, 1) mit dem ein akzeptiertes, widerspruchsfreies und aktuelles Zielbild der Deutschland-Architektur definiert wird, 2) der die frühzeitige Bewertung von Innovationen und deren architektonische Einordnung begünstigt, 3) der schnelle und wirksame Entscheidungen ermöglicht und 4) der die Verbindlichkeit der Architekturvorgaben bei der Planung und Umsetzung sicherstellt.
3. **Architekturmanagement**: Die Deutschland-Architektur ist kein fertiges Artefakt, sondern eine gelebte Praxis der methodischen Disziplin des EAMs folgend. Diese befasst sich mit der Dokumentation, Analyse, Planung und Umsetzung der Architektur der IT der öffentlichen Verwaltung und ist ein strategisches und operatives Instrument des IT-Planungsrates. Im Architekturmanagement werden die Artefakte der Deutschland-Architektur kontinuierlich gepflegt und fortgeschrieben.
4. **Steuerung**: Die Steuerung der Deutschland-Architektur erfolgt durch den IT-Planungsrat. Die Steuerung des D-Stack erfolgt durch den Bund. ITPLR und Bund können Steuerungs- und Entscheidungsbefugnisse delegieren. Die Etablierung eines Clearing-Boards zur Auflösung eventuell auftretender Konflikte soll für das Governance-Konzept bewertet werden. Außerdem werden operative Aufgaben bei Bedarf an das jeweilige IT-Architekturmanagement delegiert. Das föderale IT-Architekturmanagement ist durch den IT-Planungsrat im Rahmenkonzept Föderales IT-Architekturmanagement geregelt ([1] B-2024/28-IT). Artefakte, Arbeitsweisen, Methoden, Arbeitsräume & Tools werden im

Governance-Konzept weiter definiert, genauso wie klare Kommunikations- und Eskalationsstufen. Voraussetzung dafür ist eine leistungsfähige Architekturorganisation, die mit den dafür erforderlichen Ressourcen ausgestattet ist.

5. **Beteiligungsprozesse**: Die Governance verbindet Beteiligung und Geschwindigkeit, indem sie den Austausch frühzeitig ermöglicht, die Entscheidungen jedoch in fristgebundenen Takten und klar umrissenen Instanzen und Formaten trifft. Die Prozesse der Deutschland-Architektur sind schnell und transparent und es werden klar definierte Zielgruppen kontinuierlich und frühzeitig beteiligt. Dabei ist jederzeit bekannt, welche Themen, wo, wie und warum entschieden werden und wer darüber entscheidet. Für Anwendungsfälle, in denen die Anforderungen der Deutschland-Architektur noch nicht erfüllt werden, werden ALLE; die Migrationspfade geboten.
6. **Weiterverwendung**: Die Deutschland-Architektur baut auf bestehenden Architektur- und Lösungsartefakten sowie Architekturkonzepten auf. Bestehende Lösungen, Produkte, Standards, Rahmenarchitekturen und Dienste sollen in die Deutschland-Architektur integriert oder die Interoperabilität zur Deutschland-Architektur sichergestellt werden.
7. **D-Stack**: Der Bund finanziert noch zu bestimmende Komponenten des D-Stack. Die Finanzierung der Komponenten des D-Stack ist im Einzelfall zu klären. Dabei folgt der D-Stack dem Ordnungsrahmen der Deutschland-Architektur, es sei denn, dieser Rahmen widerspricht den internen Steuerungsvorgaben des D-Stacks. Daraus ergibt sich, dass das BMDS die Verantwortung übernimmt für die Kuratierung und Bereitstellung der Lösungsbausteine im Rahmen des D-Stack und die Empfehlungen der Länder mit einbezieht. Lösungen können dabei auch von Dritten bereitgestellt werden, die der Bund dann zu D-Stack-Lösungen erklären kann.
8. **Produktmanagement**: Deutschland-Architektur soll die architektonische Grundlage sein für das Produkt- und Portfoliomanagement der FITKO ebenso wie des BMDS. Das Governance-Konzept der Deutschland-Architektur soll die Zusammenarbeit mit dem Produktportfolio- sowie Produktmanagement beschreiben; die Ausarbeitung erfolgt unter Berücksichtigung des Produktmanagement-Modell für die Produkte des IT-Planungsrats ([2] B-2023/25-IT).
9. **Verbindlichkeit**: In der Deutschland-Architektur sollen die Funktionsbausteine gemäß der folgenden vier Kategorien bewertet werden; daraus lassen sich Empfehlungen für die Auswahl von konkreten Produkten/IT-Lösungen ableiten: Zentral betriebene, verbindliche Lösungen (z. B. EUDI-Wallet) sowie zentral betriebene, freiwillige Lösungen (individuell auf Länderwunsch z. B. im Bundesportal betrieben), dezentral betriebene, verbindliche (z. B. verbindliche Nutzung von quelloffenem Code, der auf allgemein zugänglichen Plattformen wie Open Code bereitgestellt wird) sowie dezentral betriebene, freiwillige Lösungen (z. B. freiwillige Nutzung von quelloffenem Code). Die Durchsetzung und Sanktionierung der Verbindlichkeit muss im Governance-Konzept dargelegt werden. Das BMDS legt fest, für welche Funktionsbausteine das BMDS im D-Stack verbindlich zu nutzende IT-Lösungen bereitstellt.
10. **Marktoffenheit**: Die Governance gewährleistet, dass die Umsetzung der Deutschland-Architektur mit Marktprodukten erfolgen kann, indem die Anforderungen der Deutschland-Architektur entsprechend formuliert werden. Die Deutschland-Architektur lädt dabei zu einem offenen Wettbewerb ein, der jedoch nicht auf Kosten von Sicherheit, Datenschutz und

Souveränität stattfinden soll. Die Governance schafft einen Rahmen, in dem das sichergestellt ist.

Quellen:

[1] https://www.it-planungsrat.de/fileadmin/beschluesse/2024/Beschluss2024-28_Postfach-und_Kommunikationsl%C3%B6sungen_Architektur%C3%BCberblick.pdf
[2] https://www.it-planungsrat.de/fileadmin/beschluesse/2023/Beschluss2023_25_AL_Anlage_1_Produktmanagement-Modell.pdf

6 Verzeichnisse

Impressum

Ein Projekt des IT-Planungsrats
http://www.it-planungsrat.de/