



Stellungnahme zur

2. Konsultation des Deutschland-Stacks

Zusammenfassung

1. Rolle und Zielbild Deutschland-Stack vs. Tech-Stack

- Der Deutschland-Stack umfasst nicht nur Technik, sondern auch Governance, Steuerung und organisatorische Rahmenbedingungen; diese erweiterte Perspektive ist sachgerecht, wird in den aktuellen Webinhalten aber noch nicht hinreichend trennscharf vom „reinen“ Tech-Stack abgegrenzt.
- Unklar bleiben Zielversion, Arbeitsauftrag und Meilensteine des Deutschland-Stacks; hier fehlen ein konsistentes Zielbild, eine Roadmap bis 2028 und ein systematisches Monitoring mit klarer Output-/Outcome-Trennung.
- Angesichts zahlreicher paralleler Initiativen im Bund-Länder-Umfeld erscheint es sinnvoll, dass das BMDS diese gezielt bündelt, gute Ansätze integriert und allen Beteiligten Orientierung gibt.

2. Strategie und Nutzungs-Erlebnis

- Der adressierte Nutzerkreis des „Nutzungserlebnisses“ bleibt unscharf: Für den Stack sind primär professionelle Nutzer wie Anbieter, Integratoren und Architekten relevant, nicht Endnutzerinnen und Endnutzer von Verwaltungsleistungen.
- Es braucht eine klare Abgrenzung zwischen Endnutzer-UX und dem Nutzungserlebnis der Fach- und IT-Communities sowie eine jeweils zielgruppenspezifische Konkretisierung.
- Die geplante Plattform als Grundlage wird derzeit nicht ausreichend mit verbindlicher Interoperabilität verknüpft; erforderlich wären klare Festlegungen zu Datenformaten, Protokollen, Schnittstellen und wenigen zentralen Querschnittsdiensten, während Produkte grundsätzlich marktseitig bereitgestellt werden sollten.

3. KI, Governance und Architekturprinzipien

- Ohne explizite KI-Architektur bleibt der Deutschland-Stack reaktiv; mit einer durchdachten KI-Rolle kann KI als Orchestrator für Interoperabilität und Nutzungserlebnis wirken (Assistenz statt bloß neuer Oberflächen).
- Souveräne KI sollte als Infrastrukturprinzip verstanden werden: regelgebunden, auditierbar, menschenzentriert und geeignet, föderale Vielfalt mit Skalierung zu verbinden.
- Standardisierung ist Voraussetzung für Skalierung; KI kann deren operative Umsetzung unterstützen, ersetzt aber nicht verbindliche Standards als Grundlage.
- Bei den Architekturprinzipien schlagen Sie vor, keine neuen Grundsätze zu definieren, sondern konsequent auf bestehende nationale Architekturrichtlinien und OZG-Rahmenarchitektur zu



verweisen und diese strikt anzuwenden. Entscheidend wären Reduktion, Standardtreue und Durchgängigkeit, nicht eine zusätzliche Prinzipienebene.

4. Einzelprinzipien (Auswahl) und Beschaffung

- API-First, Serviceorientierung, Wiederverwendbarkeit, DevSecOps, Zero-Trust, technologischer Aktualitätsanspruch und Ende-zu-Ende-Digitalisierung lassen sich plausibel auf OZG-Rahmenarchitektur und nationale IT-Architekturenrichtlinie beziehen; hier schlagen Sie vor, die bestehenden Referenzen explizit nachzuzeichnen.
- „Made in EU first“ und „Prefer Buy over Make“ sind ambivalent: Sie können Marktrelevanz und digitale Souveränität stärken, bergen aber bei unklarer Ausgestaltung das Risiko neuer Abhängigkeiten (Marktdominanz großer Anbieter, unklare Rolle von Mittelstand und Dual-Strategien).
- „Managed Services only“ ist in der jetzigen Form unklar; es sollte besser im Kontext von DVC-Modellen und Betriebs-/Sourcing-Strategien geregelt werden statt als isoliertes Prinzip.

5. Technologiefelder und Standards

- Bei agentischer und generativer KI sollten Standards zur Überwachung von Agenten, Qualitätssicherung und Compliance von Beginn an verbindlich mitgedacht werden, nicht erst „zukünftig“.
- Die Anforderung zur Auswahl verschiedener Basis- und Fach-Sprachmodelle sollte kontextsensitiv formuliert werden („solange im Anwendungskontext sinnvoll“) und stets mit Nachvollziehbarkeit der Antworten, Quellen, Lizenzen und Verarbeitung verknüpft werden (Responsible AI).
- Bei „Semantische Technologien und Echtzeitanalytik“ ist wichtig, dass Semantik nicht aus der bloßen Nennung von Formaten wie JSON, XML, CSV entsteht, sondern aus einheitlichen Schemata und Geschäftsregeln; außerdem erscheint ein stärkerer Bezug zu EU-Ansätzen (z.B. SEMIC, Interoperable Europe Act) sachgerecht.
- Technologiebeispiele wie Kafka, Git, ODBC/JDBC oder konkrete Kryptoverfahren sollten eher als Prinzipien (Streaming, Versionskontrolle, relationale Abfrage, krypto-agile Verschlüsselung) formuliert werden, um Produktneutralität und Zukunftssicherheit zu wahren; stattdessen sollte auf BSI-Empfehlungen und offene Standards verwiesen werden.
- Bei Cloud und Managed Services sollten bestehende Modelle (DVC, govdigital, Reifegradmodelle) explizit berücksichtigt werden; zudem wäre ein klarer Verweis, dass der Deutschland-Stack vorhandene Angebote und Vorarbeiten nutzt, sinnvoll.



Detaillierte Kommentierung

Deutschland-Stack / Tech-Stack

In den aktuell zur Verfügung gestellten Informationen (Stand 24.01.26) auf der Webseite <https://deutschland-stack.gov.de/gesamtbild/#strategie> sind positive Fortschritte erkennbar. Das Bild konkretisiert sich, was wir als DATABUND begrüßen. Es scheint aber weiterhin einiges im Fluss zu sein, da sich die Seiteninhalte in den vergangenen Tagen offenbar noch mehrfach geändert haben. Allerdings bleiben weiterhin Unklarheiten bei der Zielversion und dem Arbeitsauftrag des Deutschland-Stack / Tech-Stack. Eine umfassende Definition von Meilensteinen und Monitoring, sowie eine Unterscheidung zwischen Output und Outcome (was soll erreicht werden?) erscheint uns sinnvoll.

Weiterhin gibt es derzeit parallele Entwicklungen und Initiativen. Es ist sinnvoll, wenn das Bundesministerium für Digitales und Staatsmodernisierung diese einsammeln würde, um ggf. gute Ansätze zu integrieren und um allgemein allen beteiligten Akteuren die Orientierung zu erleichtern.

Anmerkungen zur Strategie

(Quelle: <https://deutschland-stack.gov.de/gesamtbild/>)

Der Deutschland-Stack (gegenüber reinem Tech-Stack) umfasst auch den Bereich Governance. Wir sehen allerdings Schwierigkeiten zwischen Tech-Stack und Deutschland-Stack trennscharf zu unterscheiden. Z. B: die Überlegungen zur Plattform müssen sich unseres Ermessens auf den Deutschland-Stack beziehen, beim Tech-Stack passt diese Thematik nicht rein.

Stichwort	Kommentar/Fragen/Anmerkungen
Nutzungs- Erlebnis	Der Adressatenkreis des "Nutzungserlebnisses" bleibt unscharf. Für den Stack sind dies primäre professionelle Nutzergruppen (Anbieter, Integratoren, Architekten). Eine klare Abgrenzung zur Endnutzer-UX sowie eine zielgruppenspezifische Konkretisierung sind erforderlich.
Plattform als Grundlage und für Interoperabilität	Wie aus der Bereitstellung über „Plattform als Grundlage“ auf Interoperabilität geschlossen werden soll, wird nicht deutlich. Verbindlich sollten Festlegungen auf Datenformate, Protokolle, Schnittstellen und einige wenige zentrale Querschnittsdienste getroffen werden. Die Umsetzung sollte grundsätzlich durch die Wirtschaft erfolgen und Anforderungen technologie-offen und -technik-neutral sein. Die staatlichen Stellen definieren nur den Ordnungsrahmen – nicht die Produkte. Die Föderale Strategie, in Summe ein vernetztes, modulares Ökosystem anzubieten, ist vielfältiger als es hier skizziert wird.
Künstliche Intelligenz, Daten und Standardisierung als Enabler	Der Deutschland-Stack bleibt ohne KI Architektur - mit KI wird er handlungsfähig. KI ist kein Produkt im Stack, sondern dessen Orchestrator. Interoperabilität wird



	<p>nicht programmiert, sondern durch KI operationalisiert. Nutzungserlebnis entsteht durch intelligente Assistenz, nicht durch neue Oberflächen. Souveräne KI ist Infrastruktur- regelgebunden, auditierbar und menschenzentriert. KI verbindet föderale Vielfalt mit Skalierungsfähigkeit.</p> <p>Standardisierung ist die Voraussetzung für Skalierung, KI unterstützt deren operative Umsetzung. Ohne verbindliche Standards bleibt Interoperabilität Absicht - erst mit KI ist sie wirksam nutzbar.</p> <p>Weitere Details entnehmen Sie bitte der „Anlage 2 Bewertung und Empfehlungen zum Themenbereich Künstliche Intelligenz im Deutschland-Stack“.</p>
--	---

Anmerkungen zu den Architekturprinzipien

(Quelle: <https://deutschland-stack.gov.de/gesamtbild/>)

Der DATABUND schlägt vor, dass der Deutschland-Stack keine neuen Architektur-Prinzipien formuliert, sondern auf die bereits vorhandenen Prinzipien der Nationalen Architektur-Richtlinie verweist. Genau hier fehlt die aktuelle Herleitung. Nicht neue Prinzipien, sondern stringente Reduzierung, Standardtreue und Durchgängigkeit werden gebraucht. Hierzu nachfolgend eine gegenüberstellende Zuordnung und punktuelle Anmerkungen:

Stichwort	Kommentar/Fragen/Anmerkungen
API-First – Stack-Elemente setzen auf offene, gut dokumentierte Schnittstellen	maschinenlesbar (z.B. OpenAPI, ...) lässt sich auf OZG-Rahmen Architektur beziehen (UE4; F10 03; F12 04) lässt sich auf die Nationale Architekturrichtlinie beziehen (TV-02; AV-02; FV-02)
Serviceorientierung und lose Kopplung – Stack-Elemente sind modular, unabhängig austauschbar und klar abgegrenzt.	lässt sich auf OZG-Rahmen Architektur beziehen (F12 05) lässt sich auf die Nationale IT-Architekturrichtlinie beziehen (FV-09; AV-09)
Wiederverwendbarkeit – Stack-Elemente sind qualitätsgesichert nachnutzbar.	lässt sich auf OZG-Rahmen Architektur beziehen (F10 04) lässt sich auf die Nationale IT-Architekturrichtlinie beziehen (AV-10; TV-05)
DevSecOps only – Stack-Elemente werden durch einen integrierten automatisierten Prozess von Entwicklung, Sicherheit und Betrieb gesteuert.	lässt sich auf die Nationale IT-Architekturrichtlinie beziehen (TV-01; TV-05) kein Bezug zu OZG Rahmen Architektur
Zero-Trust – Stack-Elemente werden flexibel mit vertrauensbildenden Maßnahmen ausgestattet.	lässt sich auf die Nationale IT-Architekturrichtlinie beziehen (FV-08) kein Bezug zu OZG Rahmen Architektur



Technologisch aktuell – Stack-Elemente sind auf dem neuesten Stand der Technik	lässt sich auf OZG-Rahmen Architektur beziehen (UE5) lässt sich auf die Nationale IT-Architekturrichtlinie beziehen (TV-08)
Made in EU first – Stack-Elemente werden prioritär durch Produkte aus EU-Ländern umgesetzt.	Lösungen sollen offenbar primär am europäischen Markt eingekauft werden, allerdings bleibt auch der außereuropäische Einkauf möglich. Dies ist in Bezug auf die Digitalen Souveränität klar einzugrenzen. lässt sich auf OZG-Rahmen Architektur beziehen (F13 02) lässt sich auf die Nationale IT-Architekturrichtlinie beziehen (AV-09)
Prefer Buy over Make – Stack-Elemente werden primär als Standard-Produkte am Markt beschafft.	lässt sich weder auf OZG-Rahmenarchitektur noch auf Nationale Architekturrichtlinie direkt beziehen kann sich positiv auf „Marktrelevanz“ und „Digitale Souveränität“ auswirken; je nach operativer Umsetzung dem aber auch entgegenwirken; bspw. bleibt unklar, ob bei einzelnen Stack-Elementen eine „Dual-Strategie“ gefahren wird oder hier starke Abhängigkeiten (Marktdominanz) entstehen. Es bleibt auch unklar, ob Beschaffungen primär bei Telekom und Co stattfinden oder im Mittelstand.
Ende-Zu-Ende-Digitalisierung – Stack-Elemente müssen Ende-zu-Ende digitalisiert und in anschlussfähigen Prozessen verwendet werden.	lässt sich auf OZG-Rahmen Architektur beziehen (UE3) lässt sich auf die Nationale IT-Architekturrichtlinie beziehen (AV-04; AV-05; AV-06) HINWEIS: der Bezug von Stack-Elementen zu E2E-Prozessen muss aus einer Fähigkeiten-Landkarte abgeleitet werden, nicht umgekehrt.
Managed Services only – Stack-Elemente werden durch professionelle Betriebs-(Dienst)leistungen angereichert	Bei Managed Services only – ist unklar wie dies genau gedacht ist. Es lässt sich weder auf OZG-Rahmenarchitektur noch auf Nationale Architekturrichtlinie direkt beziehen Muss dieses Prinzip nicht als Teil der DVC gesehen werden?



Anmerkungen zu Technologiefeldern und Standards

(Quelle: <https://deutschland-stack.gov.de/gesamtbild/>)

Agentische und generative KI markieren einen Paradigmenwechsel in der digitalen Wertschöpfung. Je autonomer die KI-Systeme werden, desto mehr steigen die Anforderung an die Transparenz, Steuerbarkeit und die Verantwortung. Deshalb braucht es zwingend verbindliche Standards der Überwachung von KI-Agenten zur Qualitätssicherung und zur Einhaltung der Compliance. Entscheidend ist, dass Nutzenden kontextabhängig passende Basis- und Fachmodelle auswählen können, damit die Nachvollziehbarkeit der generierten Antworten jederzeit gewährleistet wird (inklusive Angabe von Lizenzen, Quellen und Verarbeitung).

Die anderen unten genannten Technologiefelder und Standards folgen keiner stringenten Kategorisierung. Hier wurde punktuell aufgezeigt, in welche Richtung Standards und Anforderungen geschaffen und formuliert werden müssen, wie Technologie angewendet werden soll. Die Definition einer entsprechenden Basis hat Vorrang vor der Vorgabe einzelner Techniken.

<u>Stichwort</u>	<u>Kommentar/Fragen/Anmerkungen</u>
Agentische und Generative KI	
Zitat: „Künftig benötigt werden auch Standards zur Überwachung von Agenten und bei der Unterstützung der Qualitätssicherung.“	Anmerkung: zur Vermeidung von Risiken sollten diese von Anfang an Teil sein.
Zu Generativer KI wird ausgeführt, dass Zitat: „Nutzenden die Option zur Auswahl von verschiedenen Basis- und Fach-Sprachmodellen gegeben werden muss“	Dies sollte situativer formuliert sein, i.S.v. „solange dies im Kontext der Anwendung sinnvoll ist“
Sehr hohe Relevanz hat die Anforderung, Zitat: dass „Nutzenden eine Nachvollziehbarkeit der generierten Antwort und Einhaltung der Compliance gegeben werden muss (im Sinne Responsible AI, u.a. Nachweise zu Quellen, Lizenzen, Verarbeitung)“	Im oben genannten Absatz behandelt.
Semantische Technologien und Echtzeitanalytik	
Als Zitat: „technische Standards für die Umsetzung von semantischer Technologie“ werden u.a. festgelegt: (...) JSON, XML und CSV als Datenformate (...)"	Hier ist wichtig, sicherzustellen, dass ein einheitliches Datenformat notwendig ist, dass erst Schema und Geschäftsregeln einem Datenformat Semantik verleihen.
Zitat: „ODF und PDF/UA als Dokumentenformate“	Welche Korrelation zu Semantik hat dies? Dies müsste konkretisiert werden.
Zitat: „SQL, ODBC und JDBC für die Abfrage von relationalen Daten“	Hier sollte nur Bezug zu SQL genommen werden, da ODBC und JDBC spezielle Implementierungen sind.
Zitat: „Ebenfalls benötigt werden stärker harmonisierte Semantiken und Taxonomien zur Etablierung von Fachdatenstandards (u.a. XÖV, HL7, SWIFT) für die Verbesserung der semantischen Interoperabilität.“	Ausgehend vom Grundprinzip „EU first“ erscheint eine Einbettung in / Bezugnahme zu SEMIC und EU InteropAct sinnhafter.
Zitat: „Festgelegt wird aber, dass (...) bestehende Management- und Integrations-Ansätze aus Business Intelligence (u.a. ETL, OLAP), Streamanalytik (u.a.	Die explizite Nennung von Kafka ist nicht nachvollziehbar.



Kafka), Big Data und InMemory Datenhaltung zur standardisierten Datenhaltung von hohen Mengen an Echtzeitinformationen und automatisierten Auswertungsmechanismen kombiniert werden“	
Virtualisierte Softwarebasierte Infrastruktur	Sind die hier genannten Aspekte wirklich Themen für den D-Stack?? Dies sind unseres Erachtens nach eher network basics der technischen Infrastrukturen.
DevSecOps und APIs	
Als technische Standards werden festgelegt: <u>Zitat:</u> „GIT für die Versionskontrolle von Code“	GIT ist ein Beispiel für eine Technologie zur Versionskontrolle. Hier sollte stattdessen das Prinzip der Versionskontrolle mit den zu erreichenden Zielen definiert werden, ohne genau eine Technologie/Software/Produkt vorzuschreiben. Im Kern sollte es um die Code-Versionskontrolle unter Nutzung quelloffener Lösungen gehen.
<u>Zitat:</u> „Als technische Standards für die Umsetzung von Integration, Orchestrierung und APIs werden u.a. festgelegt: REST, gRPC, GraphQL und MQTT für den Austausch...“ zusätzlich wird ausgeführt, Zitat: „Als Grundlage vorausgesetzt werden aktuelle sichere Transport- und Kommunikationsprotokolle (u.a. IPv6, HTTPS, FTPS, SMTPS, QUIC)“	Ziel dieser „Austausch“ primär auf die Interaktion innerhalb Kubernetes ab? Es scheint dabei auch um Interaktion mit den Services der Plattform / des Plattform-Ökosystems zu gehen .. Was ist dann mit den EU Building Blocks (bspw. eDelivery und eIDAS Vertrauensdienste)? Im Sinne von "EU first" und Europ. Interoperabilität ist dies absolut essentiell! Auch ein Verweis auf nationale Übertragungsprotokolle (OSCI/XTA) wäre sinnvoll, da diese in einigen Gesetzen und Ausführungsverordnungen gesetzt sind. Grundsätzlich ist hier anzumerken, dass bestehende und etablierte dem Datenaustausch dienende Transport-Infrastrukturen und Protokolle berücksichtigt werden müssen, da es Migrationspfade geben müssen u.a.: SOAP, WS*
Managed Services und Cloud	
Zitat: „Cloud wird insbesondere für die Art des Bezuges von betrieblichen Leistungen als Liefer- und Finanzierungsmodell genutzt. Für Cloud in diesem Sinne gibt es aktuell keine spezifischen Standards. Festgelegt wird aber, dass ...“	Hier erscheint uns die über DVC und govdigital angestoßenen und bereits realisierten Modelle und Rahmensetzungen nicht ausreichend berücksichtigt bzw. benannt. So gibt es bspw. für den Abruf von Leistungen ein Reifegrad-Modell im Kontext der DVC. Hier wäre der grundlegende Verweis (im Abschnitt „Zusammenhang mit weiteren Aktivitäten“) „Der Deutschland-Stack nutzt die Angebote und Vorarbeiten der DVC nach.“ besser, deutlicher und expliziter formuliert.
IT-Sicherheit	
Als technische Standards für IT-Sicherheit werden u.a. festgelegt. Zitat: „AES und RSA für die Verschlüsselung von Kommunikation“	Warum explizit diese konkrete Nennung und warum fehlt hier ECC? Besser sollte auf aktuelle Empfehlungen des BSI referenziert und Krypto-Agilität als Prinzip gestärkt werden. Besser sollte formuliert werden: „... aktuell sicherere Algorithmen, wie z.B. AES“
Workflowautomatisierung (LowCode)	Der Begriff LowCode ist als Prinzip nicht standardisiert, sondern wird je nach Produkt unterschiedlich interpretiert. Hier sollte nur das unterliegende Prinzip einfacher Bedienbarkeit (Beispielsweise auch durch Codeschnipsel) festgeschrieben und detailliert werden.