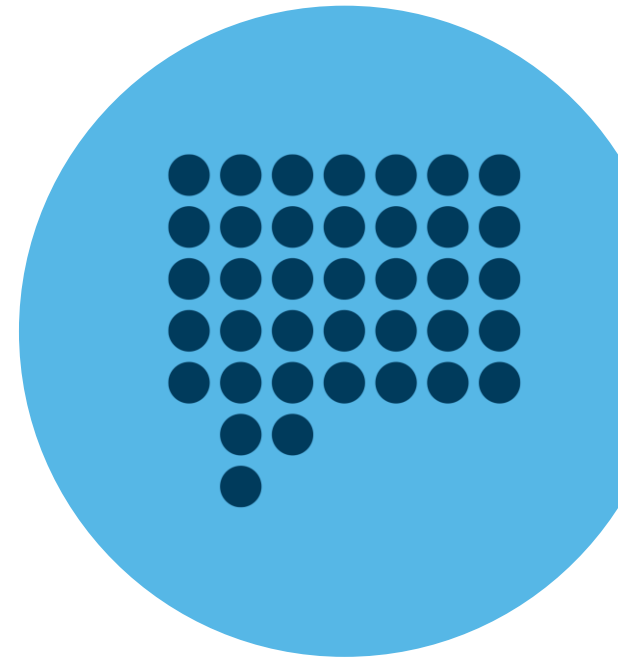


Unterlagen zur 12. Sitzung

23.04.2026

Agenda

- TOP 01 – Begrüßung und Feststellung der Beschlussfähigkeit
- TOP 02 – Mitteilungen des Vorsitz und der Geschäftsstelle
 - 02.1 – Allgemeine Mitteilungen des FIT-SB-Vorsitz
 - 02.2 – Allgemeine Mitteilungen der FIT-SB-Geschäftsstelle
- TOP 03 – Aktuelle IT-Standardisierungsvorhaben und – bedarfe – Deutschland-Architektur + Deutschland-Stack
 - 03.1 – Vorstellung des Ablaufs
 - 03.2 – Impulsvortrag des BMDS (*siehe Sitzungsunterlagen*) und kurzes Bild der Deutschland-Architektur
 - 03.3 – Impulsvortrag der FITKO (*siehe Sitzungsunterlagen*)
 - 03.4 – Workshop: Prozessmodellierung „Wie gestalten wir die Fortschreibung der Deutschland-Stack-Standards so, dass sie verbindlich bleibt - und lernfähig?“
- TOP 04 – Verschiedenes
- TOP 05 – Organisatorisches



Deutschland-Stack

Standards und Technologien

Thomas Bendig
Abteilung DS11
Bundesministerium für Digitales und
Staatsmodernisierung

23. April 2026



Agenda

Die Standards und Technologien des Deutschland-Stacks

01



Rückblick

03



Zukünftiger Prozess

02



Aktueller Stand

Rückblick



Rückblick

- 31.3.26 als Termin zur Veröffentlichung von D-Stack-Standards kurzfristig durch MPK vorgegeben
- Umfangreicher mehrstufiger Konsultationsprozess
- Workshops mit verschiedenen Stakeholder-Gruppen
- Sammlung der Vorschläge
- Auswahl und Eingrenzung durch Architekturprinzipien des D-Stacks
- Information von FIT-SB und FIT-AB
- Beschluss durch den IT-Planungsrat

Zum D-Stack gibt es ein gemeinsames politisches Commitment



Die MPK beschließt die föderale Modernisierungsagenda (TOP2.2 AG Staatsmodernisierung, Viertes Kapitel: Digitale Verfahren):

„Der Bund baut unter Einbeziehung der Länder einen D-Stack als nationale Technologieplattform zur Digitalisierung der deutschen Verwaltung.“



Die BReg vereinbart den D-Stack im Koalitionsvertrag und beschließt die Modernisierungsagenda Bund.

„Ländern und Kommunen wird die Nutzung folgender Lösungen ermöglicht, die prioritär umgesetzt werden: Ein interoperabler und europäisch anschlussfähiger souveräner Deutschland-Stack integriert KI, Cloud-Dienste sowie Basiskomponenten.“



Die DMK beschließt Aufträge an die Umsetzung des D-Stack.

- TOP 3.1 zu zentralem Cloud-Hosting-Angebot für mehr digitale Autonomie
- TOP 3.3 zur Bereitstellung einer gemeinsamen Plattform-Basis
- TOP 3.8 zu einer offenen und anschlussfähigen Ausgestaltung

MPK-Beschluss Föderale Modernisierungsagenda

Vom 4.12.2025

205: 1. Schaffung des D-Stack

Der Bund baut unter Einbeziehung der Länder einen D-Stack als nationale Technologieplattform zur Digitalisierung der deutschen Verwaltung. Er basiert auf Standards sowie auf Best-Practice-Ansätzen der föderalen Zusammenarbeit u.a. im Rahmen der deutschen Verwaltungscld, der GovStack-Initiative des Bundes, des europäischen Auslandes und der Wirtschaft. Er ist ein auf Kooperation ausgerichtetes Ökosystem mit Elementen der verbindlichen und fakultativen Nutzung von Komponenten durch Bund und Länder und Partizipationsmöglichkeiten für die Wirtschaft, Zivilgesellschaft und Wissenschaft („Einige für viele, offen für alle“). Vorrangig kommen dabei Open-Source Ansätze und Angebote digital-souveräner Anbieter zur Anwendung. Es wird eine Koordination des Aufbaus des digitalen Ökosystems etabliert.

Die entsprechenden Standards einschließlich ihrer Governance werden bis 31.03.2026 festgelegt.

Der D-Stack wird eine technisch sichere, europäisch anschlussfähige und souveräne Technologie-Plattform für Bund, Länder und Kommunen.

Ablauf

- Initiale Phase
 - Festlegung initialer Kriterien
 - Initiale Auswahl von Technologien und Standards angelehnt an CNCF-Landscape
- 1. Konsultation
 - 01.10.25-30.11.25
- 2. Konsultation
 - 15.01.26-14.02.26
- Beschluss IT-Planungsrat

Was wurde betrachtet

Essenziell war die Unterscheidung in

- Normen (formaler Normungsprozess)
- **Standards** (pragmatische Einigung zwischen Stakeholdern auf eine Vorgehensweise),
- **Technologie** (allgemeine Vorgehensweise, Potential) und
- Technologieprodukt (konkret einsetzbare Vorgehensweise mit Bezug zu einem Anbieter).

Kriterien

- Nach der 1. Konsultation haben wir viel Feedback zur Zielsetzung erhalten und daher die strategischen Ausrichtung geschärft.
- Die Kriterien wurden auf die essenziellen Punkte konsolidiert.
Für die Kriterien besteht noch kein Ansatz zur automatisierten Erhebung und Nutzung in Compliance und Bewertungsprozessen, daher sind die Kriterien weiterhin nur Orientierung und nicht verbindlicher Mechanismus.

Kriterien und Reifegrade für Standards und Technologien in der 1. Konsultation

Kriterium	Stufe 0 (Mindestniveau)	und Stufe 1 (bis 20%)	und Stufe 2 (bis 40%)	und Stufe 3 (bis 60%)	und Stufe 4 (bis 80%)	und Stufe 5 (bis 100%)
Digitale Souveränität	Wechselfähigkeit	Betriebssteuerung	Anbielereinfluss	Gestaltungsfähigkeit	Technologieführerschaft	Volle Souveränität
Interoperabilität	Dokumentierte APIs	Kompatibilität	Offene APIs	Serviceorientierung	Erweiterbarkeit	Volle Interoperabilität
Zukunftsfähigkeit	Ablösung	Releasealter	Releasefrequenz	Forschungsinvest	StartUps	Volle Zukunftsfähigkeit
Marktrelevanz	Verfügbarkeit	Verbreitung	Kapitalisierung	Durchdringung	Standort	Volle Marktrelevanz
Vertrauenswürdigkeit	Sicherheitsdokumentation	Konformität	Audit	SecOps	Zero-Trust	Volle Vertrauenswürdigkeit
Nachhaltigkeit	Nachnutzbarkeit	Dokumentation	Offenheit	Wirtschaftlichkeit	Qualität	Volle Nachhaltigkeit

Kriterium: Digitale Souveränität

Beschreibung

Die Umsetzung von Digitaler Souveränität ist eine Kerneigenschaft im Deutschland-Stack. Welchen Umfang und welche Bedeutung digitale Souveränität einnimmt, entscheidet sich in der Umsetzung der einzelnen Stack-Elemente.

Mindestens ist eine Wechselfähigkeit zwischen Betreibern und Anbietern notwendig. Zudem sollte vorrangig im europäischen Binnenmarkt eingekauft werden. Open Source und offene Schnittstellen können durch die Transparenz einen erfolgskritischen Anteil zur Umsetzung von Digitaler Souveränität einnehmen.

Reifegrade 0-5

Es wird mindestens **Wechselfähigkeit** vorausgesetzt, also das es vergleichbare Alternativen gibt auf die mit überschaubarem Aufwand gewechselt werden kann.

Ergänzend zu Stufe 0 wird **Betriebssteuerung** bewertet, also die Möglichkeiten zum Einfluss auf die Verortung von Datenhaltung oder Rechenleistung.

Ergänzend zu Stufe 1 wird **Anbiereinfluss** bewertet, also die Möglichkeiten zum rechtlichen Einfluss auf den Anbieter oder zur aktiven Teilnahme an der Community.

Ergänzend zu Stufe 2 wird **Gestaltungsfähigkeit** bewertet, also die Möglichkeiten zur Nutzung eigener Kompetenzen und Aktivitäten in der Gestaltung.

Ergänzend zu Stufe 3 wird **Technologieführerschaft** bewertet, also die Möglichkeiten zum mehrheitlichen Einfluss auf die Entwicklung oder Förderung.

Ergänzend zu Stufe 4 wird **Volle Souveränität** bewertet, also die Möglichkeiten zum vollumfänglichen Einfluss.

Kriterium Interoperabilität

Beschreibung

Die Sicherstellung von Interoperabilität ist die zweite Kerneigenschaft im Deutschland-Stack. Grundlage ist Schnittstellen verfügbar zu machen (Zugang) und von Beginn an den Stack und seine Elemente nach API-First zu gestalten (Beschreibung).

Mit der Etablierung offener Schnittstellen wird die Schwelle zur Schaffung von Interoperabilität im Ökosystem gesenkt. Daher ist Offenheit ein begrüßenswerter Faktor in der Umsetzung der Integration und Anschlussfähigkeit.

Reifegrade 0-5

Es wird mindestens **Dokumentierte API** vorausgesetzt, also dass es eine Schnittstellendokumentation oder Spezifikation gibt.

Ergänzend zu Stufe 0 wird **Kompatibilität** bewertet, also die Möglichkeiten zum Austausch oder störungsfreien Betrieb.

Ergänzend zu Stufe 1 wird **Offene API** bewertet, also die öffentliche und freie Zugänglichkeit von Schnittstellen oder Spezifikationen.

Ergänzend zu Stufe 2 wird **Serviceorientierung** bewertet, also die Nutzbarkeit von serviceorientierten Produkten.

Ergänzend zu Stufe 3 wird **Erweiterbarkeit** bewertet, also die Möglichkeiten zur Erweiterung, Anpassung und Ausdifferenzierung.

Ergänzend zu Stufe 4 wird **Volle Interoperabilität** bewertet, also die Nutzbarkeit eines umfassenden Ökosystems.

Kriterium Zukunftsfähigkeit

Beschreibung

Mit dem Deutschland-Stack sollen die Lösungen stets auf einem technologisch aktuellen Stand sein und es sollen mehr Innovation genutzt werden. Als Mindestbedingung ist demnach zu fordern das Lösungen kontinuierlich aktualisiert werden. Erfolgskritisch ist aber auch die kontinuierliche Einbindung der IT- und Digitalwirtschaft.

Reifegrade 0-5

Es wird mindestens **Ablösung** vorausgesetzt, also das es keine relevanten Alternativen neueren Datums gibt.

Ergänzend zu Stufe 0 wird **Releasealter** bewertet, also wie lange das letzte Release her ist.

Ergänzend zu Stufe 1 wird **Releasefrequenz** bewertet, also in welchen Abständen ein Release erfolgt.

Ergänzend zu Stufe 2 wird **Forschungsinvest** bewertet, also die Menge an Investment in Forschung und Innovation oder an Contributern.

Ergänzend zu Stufe 3 wird **StartUp** bewertet, also die Menge an bestehenden StartUps.

Ergänzend zu Stufe 4 wird **Volle Zukunftsfähigkeit** bewertet, also ob eine immanente Abhängigkeit seitens Anderer besteht.

Kriterium Marktrelevanz

Beschreibung

Die Marktrelevanz ist ein essenzieller Faktor zur Verifikation der Umsetzbarkeit. Nur wenn es auch echte Technologie-/ Softwareprodukte am Markt gibt, werden wir in eine pragmatische und schnelle Umsetzung kommen. Das Mindestmaß liegt demnach in der Verfügbarkeit von Produkten am Markt. Erfolgskritisch ist dabei eine Verteilung von Produkthanbietern im Markt, so dass nicht Abhängigkeiten von einzelnen Akteuren entstehen.

Reifegrade 0-5

Es wird mindestens **Verfügbarkeit** vorausgesetzt, also das es einen relevanten Markt mit Produkten und Nutzenden gibt.

Ergänzend zu Stufe 0 wird **Verbreitung** bewertet, also ob ein führender Marktanteil bei Produkten, Anbietenden und Nutzenden besteht.

Ergänzend zu Stufe 1 wird **Kapitalisierung** bewertet, also ob es einen relevanten Geschäfts- und Finanzierungsanteil gibt.

Ergänzend zu Stufe 2 wird **Durchdringung** bewertet, also ob ein mehrheitlicher Marktanteil bei Produkten, Anbietenden und Nutzenden besteht.

Ergänzend zu Stufe 3 wird **Standort** bewertet, also ob der Wirtschaftsstandort oder das Wachstum gefördert wird.

Ergänzend zu Stufe 4 wird **Volle Marktrelevanz** bewertet, also ob es einen relevanten Einfluss auf den Wirtschaftsstandort gibt.

Kriterium Vertrauenswürdigkeit

Beschreibung

Vertrauenswürdigkeit ist einerseits eine essenzielle Grundlage für die Akzeptanz der Nutzenden und andererseits für die Bewältigung von gestiegenen Anforderungen der globalen Weltlage. Daher wird eine nutzbare Dokumentation zum Umgang mit Vertrauenswürdigkeit und Sicherheit als Ausdruck der Sensibilisierung benötigt.

Praktisch braucht es funktionierende Vertrauens- und Sicherheitsmechanismen, welche sich an den jeweiligen Bedarfslagen orientieren. Dabei ist ein Grundschutz für die allgemeine Funktionsfähigkeit sicherzustellen. Damit die Befassung mit Vertrauen und Sicherheit nicht erst im produktiven Betrieb entsteht, sollten die Kernfragen frühzeitig behandelt und kontinuierlich begleitet werden.

Reifegrade 0-5

Es wird mindestens **Sicherheitsdokumentation** vorausgesetzt, also das eine Dokumentation und Bewertung der Sicherheit besteht.

Ergänzend zu Stufe 0 wird **Konformität** bewertet, also ob eine Konformitätsprüfung oder Zertifizierung möglich ist.

Ergänzend zu Stufe 1 wird **Audit** bewertet, also ob eine Auditierung möglich ist.

Ergänzend zu Stufe 2 wird **SecOps** bewertet, also ob eine kontinuierliche Sicherstellung der Vertrauenswürdigkeit ermöglicht wird.

Ergänzend zu Stufe 3 wird **Zero-Trust** bewertet, also ob die Vertrauenswürdigkeit auf Einzelemente bezogen ist.

Ergänzend zu Stufe 4 wird **Volle Vertrauenswürdigkeit** bewertet, also ob es anerkannte, funktionierende und automatisierte Mechanismen zur Vertrauenswürdigkeit gibt.

Kriterium Nachhaltigkeit

Beschreibung

Der Deutschland-Stack muss perspektivisch ein sich selbst tragendes Ökosystem sein. Investments können nur verantwortet werden, wenn eine Nachnutzbarkeit gesichert ist. Zudem müssen die erbrachte Qualität und Leistung mit den laufenden Aufwänden einhergehen.

Neben der ökonomischen Bewertung sollten in diese Entwicklung auch ökologische und soziale Faktoren einfließen. Der Stack soll die grundlegenden Wertevorstellungen von Deutschland und Europa berücksichtigen.

Reifegrade 0-5

Es wird mindestens **Nachnutzbarkeit** vorausgesetzt, also das es die Möglichkeit zur Nachnutzung in verschiedenen Produkten und von verschiedenen Anbietern gibt.

Ergänzend zu Stufe 0 wird **Dokumentation** bewertet, also ob eine ausreichende Dokumentation von verschiedenen Anbietern oder eine Community gibt.

Ergänzend zu Stufe 1 wird **Offenheit** bewertet, also ob Dokumentation und Code (Open Content, Open Source) inklusive der Wirksamkeitsbewertung verfügbar ist.

Ergänzend zu Stufe 2 wird **Wirtschaftlichkeit** bewertet, also ob es funktionierende Geschäfts- und Finanzierungsmodelle gibt.

Ergänzend zu Stufe 3 wird **Quality** bewertet, also ob es Mechanismen zur Abrechnung, Leistungsmessung und Qualitätsbewertung gibt.

Ergänzend zu Stufe 4 wird **Volle Nachhaltigkeit** bewertet, also ob es ein selbsterhaltendes oder mehrwertgenerierendes Ökosystem gibt.

Aktueller Stand



Aktuelle Standards des Deutschland-Stacks

- Die Standards sollen eine **Orientierung und Sicherheit** für **Entwickler und Beschaffer** bieten.
- Die aktuelle Struktur ist das Ergebnis mehrerer Community-Prozesse und verschiedener Stakeholder-Workshops
- Die Standards sind nicht perfekt und werden es nie sein.
- Vollständigkeit und eindeutige Systematik können nicht erreicht werden.

Gemeinsam mit dem FIT-SB können sie systematisch ergänzt und weiterentwickelt werden.

Standards in 7 Technologie-Ebenen

- Künstliche Intelligenz
- Semantische Technologien
- Virtualisierte softwarebasierte Infrastruktur
- Integrierter Lebenszyklus (DevSecOps) und Schnittstellenmanagement
- Managed Services und Cloud
- IT-Sicherheit
- Workflowautomatisierung (LowCode)

Beschluss 49. IT-Planungsrat

Künstliche Intelligenz

- Agentische und generative Künstliche Intelligenz wird für die Automatisierung von Aufgaben, Abläufen und Regelwerken und das KI-basierte Entwickeln und Bereitstellen von Lösungen (AI Engineering) eingesetzt.
- Standards:
 - Model Context Protocol (MCP), Agent Network Protocol (ANP), Agent2Agent Protocol (A2A) und Agent-User Interaction Protocol (AG-UI)
- Festlegungsbedarfe:
 - Format zur Auswahl verschiedener Basis- und Fach-Sprachmodellen
 - Format zur Einbindung von fachspezifischen Quellen (Retrieval-Augmented Generation)
 - Format zur Nachvollziehbarkeit der Ergebnisse (Responsible AI)
 - Format zum Austausch von Sprachmodellen und Nachnutzung von Trainingsdaten



Beschluss 49. IT-Planungsrat

Semantische Technologien

- Semantische Technologien werden für die Vernetzung, den Austausch und den Abruf von Daten eingesetzt.
- Standards:
 - Resource Description Framework (RDF), Web Ontology Language (OWL), SPARQL Protocol and RDF Query Language (SPARQL), Simple Knowledge Organization System (SKOS), Data Catalog Vocabulary (DCAT) und Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH)
 - JavaScript Object Notation (JSON), eXtensible Markup Language (XML), Comma-Separated Values (CSV), Open-Document Format (ODF), Portable Document Format Universal Accessibility (PDF/UA)
 - Structured Query Language (SQL), Open und Java Database Connectivity (ODBC und JDBC)
- Festlegungsbedarfe:
 - Format für vektor-, graphen-, dokumenten- und objektorientierte Datenhaltung
 - Format für Datenmodellierung, Datenintegration, Datenauswertung und Datenvisualisierung
- Formate für Fachdatenaustausch (Fachdatenstandards, harmonisierte Fachdatenräume)



Beschluss 49. IT-Planungsrat

Virtualisierte softwarebasierte Infrastruktur

- Virtualisierte softwarebasierte Infrastruktur wird für die effiziente, flexible und skalierbare Ressourcenallokation eingesetzt.
- Standards:
 - Metro Ethernet Forum 70 (MEF) für Software-Defined Wide Area Networks (SD-WAN), Network Function Virtualization (NFV)
- Festlegungsbedarfe:
 - Format für Software-Defined Storage (SDS)
 - Format für Verwaltung von virtuellen Maschinen und Ressourcen



Beschluss 49. IT-Planungsrat

Integrierter Lebenszyklus (DevSecOps) und Schnittstellenmanagement

- Ein integrierter Lebenszyklus von Entwicklung bis Betrieb inklusive Sicherheit (DevSecOps) sowie ein zentrales Schnittstellenmanagement werden für die Automatisierung der Bereitstellung und Integration von Lösungen eingesetzt.
- Standards:
 - GIT, Pipelines für Continuous Integration und Delivery (CI/CD), Infrastructure und Policies as Code (IaC, PaC), Software Bill of Materials (SBOM), Open Web Application Security Project (OWASP)
 - Kubernetes, Representational State Transfer (REST), gRPC Remote Procedure Calls (gRPC), GraphQL, Message Queuing Telemetry Transport (MQTT), openAPI
 - Vorausgesetzt werden international anerkannte Transport- und Kommunikationsprotokolle wie beispielsweise IPv6, HTTPS, FTPS, SMTPS, QUIC
- Festlegungsbedarfe:
 - Formate für Scan, Test, Analyse, Logs, Observability, Security (u.a. SIEM, IDS, EDR, SAST, DAST, CS)
 - Formate für Package Management, Distribution, Load Balancing, Proxies, Gateways, Service Mesh und Service



Beschluss 49. IT-Planungsrat

Managed Services und Cloud

- Managed Services und Cloud werden für den effizienten und skalierbaren Zugriff auf betriebliche Angebote eingesetzt.
- Standards:
 - Standards der Deutschen Verwaltungscld (DVC), OpenStack, Sovereign Cloud Stack (SCS)
 - Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT)
- Festlegungsbedarfe:
 - Formate für standardisierte, bedarfsorientierte Service Levels, Berichtsmechanismen und Geschäftsbedingungen zu Leistungen in insbesondere Compute, Storage, Communication, Logging, Observability, Backup, Support, Cost Calculation, License und Performance Management



Beschluss 49. IT-Planungsrat

IT-Sicherheit

- IT-Sicherheit wird für die Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit eingesetzt.
- Standards:
 - BSI IT-Grundschutz, technische Richtlinien BSI, C5 Katalog
 - Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), Elliptic Curve Cryptography (ECC)
 - Module-Lattice-based Key Encapsulation Mechanism (ML-KEM) für Post-Quanten-Kryptografie (PQK)
 - Open Authorization (OAuth), OpenID Connect (OIDC), JSON Web Token (JWT), One-Time Password (OTP) für Multi-Faktor-Authentifizierung (MFA)
- Festlegungsbedarfe:
 - Format zu Sensibilisierung von Nutzenden
 - Format für Krypto-Agilität



Beschluss 49. IT-Planungsrat

Workflowautomatisierung (LowCode)

- Workflowautomatisierung (LowCode) wird für die einfache Modellierung von Verfahrens- und Arbeitsabläufen eingesetzt.
- Standards:
 - ./.
- Festlegungsbedarfe:
 - Format zur Integration oder Anbindung von externen Lösungen
 - Format für Export und Import von Modellen
 - Format für die Ausführung auf verschiedenen Betriebs- und Infrastrukturmgebungen



Weiterentwicklung der Kriterien



Weiterentwicklung der Kriterien

1. **Digitale Souveränität – Unabhängigkeit:**
2. **Digitale Souveränität – Wechselfähigkeit:**
3. **Digitale Souveränität – Kontrollfähigkeit:**
4. **Transparenz:**
5. **Interoperabilität & Erweiterbarkeit:**
6. **Datensicherheit & -compliance / Daten- & Informationssouveränität:**
7. **Nutzerzentrierung & Zweckmäßigkeit:**
8. **Reifegrad:**
9. **Innovationskraft & Zukunftsfähigkeit:**

Weiterentwicklung der 9 Kriterien

Zur besseren Operationalisierung der Bewertung wurde eine 2. Ebene von Unterkriterien definiert, die eine konkretere Bewertung und (Self-)Assessments ermöglichen.

Digitale Souveränität – Unabhängigkeit:

- Die Unabhängigkeit beschreibt die politische und räumliche Unabhängigkeit von Technologie und Standard. Damit werden die rechtliche Sicherheit und das Vertrauen in die öffentliche Hand gestärkt.
- **Offener Standard / Open-Source-Verfügbarkeit:** Bewertet, ob der Standard offen verfügbar ist und unter einer freien Lizenz steht bzw. durch ein offenes Gremium gesteuert wird.
- **Multiple Anbieter/ Implementierungen:** Bewertet, ob mehrere voneinander unabhängige unterschiedliche Implementierungen vorliegen.
- **Aufwandsarmer Vendorwechsel:** Bewertet, wie leicht ein Wechsel des Anbieters oder der Implementierung möglich ist.

Digitale Souveränität – Wechselfähigkeit

Die Wechselfähigkeit als zweite Souveränitätskategorie beschreibt, wie leicht Technologie und Standard ausgetauscht und durch andere, äquivalente Lösungen ersetzt werden können. Eine hohe Wechselfähigkeit ermöglicht es Bund, Ländern und Kommunen, auf technologische oder regulatorische Änderungen flexibel zu reagieren.

- **Politische (Nur EU-rechtliche Anbieter):** Bewertet, ob Bereitstellung und Betrieb durch Anbieter erfolgen, die dem EU-Rechtsraum unterliegen.
- **Räumliche (Möglichkeit zum Selbstbetrieb):** Bewertet, ob Standard bzw. Technologien nur in einer vorgegebenen Cloud oder durch den Nutzer selbst betrieben werden können.

Digitale Souveränität – Kontrollfähigkeit:

Die Kontrollfähigkeit bewertet als dritte und letzte Souveränitätskategorie, in welchem Maße öffentliche Stellen die eingesetzte Technologie steuern können. Bund, Länder und Kommunen können ihre Aufgaben nur dauerhaft souverän erledigen, wenn sie die volle Herrschaft über eingesetzte Technologien und Standards haben.

- **Rollen- & Berechtigungen steuerbar:** Bewertet, ob ein Rollen- und Berechtigungskonzept vorhanden ist, das sich an organisations- und verwaltungsspezifische Anforderungen anpassen lässt
- **Möglichkeit zum nutzerseitigen Patching/Updating ohne Dritte:** Bewertet, ob Nutzer sicherheitsrelevante oder funktionale Patches selbst einspielen können, ohne auf die Hilfe von Dritten angewiesen zu sein.

Transparenz

Transparenz ist eine grundlegende Voraussetzung für die Nachvollziehbarkeit von Funktionsweise, Architektur und Weiterentwicklung einer Technologie. Sie bedingt die Vertrauenswürdigkeit in den Staat und bildet die Grundlage für den Großteil der weiteren Kriterienkategorien.

- **Verfügbarkeit offizieller Dokumentationen:** Bewertet, ob hinreichende Dokumentationen (gut dokumentierten APIs, SDKs oder Konnektoren) vorliegen, um eine Implementierung eines Standards zu unterstützen.
- **Code Transparenz:** Bewertet, ob Quellcode oder vollumfängliche Spezifikationen offen einsehbar sind.
- **Auditierbarkeit durch Dritte:** Bewertet, ob ein Standard derart hinreichend dokumentiert ist, dass es einem fachkundigen Dritten möglich ist diesen zu analysieren und zu bewerten.

Interoperabilität & Erweiterbarkeit:

Diese Kategorie bewertet, wie gut eine Technologie mit anderen Systemen zusammenarbeitet und wie flexibel sie sich funktional erweitern lässt. Dadurch wird zum einen gewährleistet, dass die Vielzahl an föderaler Fachverfahren und Diensten interoperabel sind und zum anderen, dass die Gestaltungsfähigkeit von Bund, Ländern und Kommunen in Bezug auf ihre IT gestärkt wird.

- **Standardisierte Schnittstellen:** Bewertet, ob der Standard bzw. die Technologie klar definierte, auf offenen Standards basierende Schnittstellen bereitstellt, die eine herstellerübergreifende Integration ermöglichen.
- **Generische Möglichkeiten zur Konfigurierbarkeit:** Es existieren Erweiterungspunkte, um den Funktionsumfang auszubauen oder standardisierte Mechanismen zur Anpassung/Erweiterung des Quellcode und damit individuellen Bedürfnissen besser gerecht zu werden. Dies umfasst sowohl Erweiterungen, die selbst oder durch Dritte konzipiert wurden, als auch standardmäßig angeboten werden.
- **Nicht-generische Möglichkeit zur Konfigurierbarkeit:** Die bereits gegebene Erweiterbarkeit kann durch zusätzlichen Aufwand erhöht werden. Entscheidend ist, dass die Systematik auch dann erweitert werden kann, wenn dies ursprünglich nicht vorgesehen war. Berücksichtigt werden dabei ausschließlich Erweiterungen, die auch plausibel sind.
- **Verwendung für Aufbau & Betrieb von Microservice Architekturen:** Es bedarf der Förderung von losen Kopplungen in Anwendungen, individueller Deploybarkeit der Services und Bereitstellung von Applikationen durch Services.

Datensicherheit & -compliance / Daten- & Informationssouveränität:

Diese Kategorie fasst alle Anforderungen an Sicherheit, Datenschutz und regulatorische Konformität zusammen. Das ist aufgrund des Umgangs mit hochsensiblen Daten in der öffentlichen Verwaltung von höchster Priorität.

- **Richtlinien- & Normenkonformität:** Bewertet, inwieweit rechtliche Vorgaben (z.B. DSGVO, BSI-Grundschutz, Barrierefreiheitsanforderungen) unterstützt werden.
- **Datenschutz by Design:** Bewertet, ob der Standard bzw. die Technologie Prinzipien des „Privacy by Design“ (z.B. Datenminimierung, Zweckbindung) berücksichtigt.
- **Security by Design :** Bewertet, ob Sicherheitsmechanismen (z.B. IAM) von Beginn an integrierter Bestandteil der Implementierung sind oder nachträglich ergänzt werden können.
- **Zertifizierte Compliance:** Bewertet, ob formale Sicherheits-Zertifizierungen (z.B. ISO 27001) vorliegen.
- Berücksichtigung von Zerotrust-Prinzipien

Nutzerzentrierung & Zweckmäßigkeit:

Hier wird beschrieben, wie gut eine Technologie auf die Bedürfnisse ihrer Zielgruppen ausgerichtet ist und wie praxistauglich sie im Alltag eingesetzt werden kann. Denn Technologien entfalten ihren Wert nur, wenn sie von ihren Nutzern und Anwendern akzeptiert und bedient werden können.

- **Passfähigkeit:** Bewertet, wie gut Technologie oder Standard zu fachlichen Anforderungen, bestehenden Prozessen, IT-Rahmenbedingungen der öffentlichen Verwaltung passt.
- **Nutzerzentriertes Design:** Bewertet, ob ein nutzerzentriertes Design (z.B. UX-Design, Usability-Tests) berücksichtigt wird.
- **Einfachheit & Verständlichkeit in Betrieb & Anwendung:** Bewertet, wie leicht sich die Lösung installieren, betreiben und tatsächlich nutzen lässt.
- **Schulungsangebote:** Bewertet, ob Schulungsangebote verfügbar sind, die eine kompetente Nutzung und den Betrieb unterstützen.
- **Nutzung in nationalen Initiativen und öffentlicher Verwaltung:** Bewertet, ob bereits ein gezielter Einsatz der Technologie oder des Standards im Öffentlichen Sektor stattfindet, geplant ist oder empfohlen wird.

Reifegrad

Der Reifegrad bewertet den aktuellen Entwicklungs- und Verbreitungsstand einer Technologie, da der Deutschland-Stack tragfähige, langfristig nutzbare Grundbausteine bereitstellen soll. Technologien mit hohem Reifegrad sind erprobt und verfügen über stabilen Support. Gleichzeitig erlaubt es die systematische Bewertung des Reifegrads aber auch, junge, innovative Lösungen zu pilotieren.

- **Größe der Nutzer-/Anwenderbasis:** Bewertet, wie weit verbreitet der Standard bzw. die Technologie aktuell ist.
- **Größe der Support-Community:** Bewertet, wie viele nicht Hersteller-spezifische Communities den Standard betreuen.
- **Standard von Gremien formal anerkannt:** Bewertet, ob der technische Standard von renommierten Gremien standardisiert wurde.
- **Existenz von Konformitäts-Tests und Zertifizierungen:** Bewertet, ob standardisierte Zertifizierungsprogramme vorliegen, mit denen die Implementierung des Standards gemessen und validiert werden kann.

Innovationskraft & Zukunftsfähigkeit:

Diese Kategorie beschreibt, in welchem Maße Technologien und Standards zukünftige Anforderungen adressieren und Innovation im öffentlichen Sektor ermöglichen. Das ist nötig, damit der Tech-Stack anschlussfähig bleibt und eine nachhaltige Digitalisierung von Staat und Verwaltung unterstützt.

- **Veröffentlichungsjahr/ Generation:** Bewertet, in welcher technologischen Generation sich der Standard bzw. die Technologie befindet.
- **Release-Frequenz & Inhalt des letzten Releases:** Bewertet, wie häufig und in welchem Umfang Releases erscheinen.
- **Umfang & Aktivität von Community Beiträgen:** Bewertet die Stärke, mit der sich Communities einbringen.
- **Möglichkeit zur Performance Messung:** Bewertet, ob Überwachung der Performance mittels KPIs möglich ist, ob also z.B. der Erfolg der Implementierung oder die Einhaltung von SLAs kontinuierlich verfolgbar und quantifizierbar ist.
- **Forschungs-/Entwicklungstätigkeit:** Bewertet die Auswirkungen auf den laufenden Wissenschaftlichen Diskurs.

Zukünftiger Prozess

Vorschlag



Vorschlag zum weiteren Vorgehen

Der Deutschland-Stack wünscht sich eine enge Zusammenarbeit mit dem FIT-SB bei der zukünftigen Weiterentwicklung der Standards und Technologien des D-Stacks.

Das FIT-SB kann:

- Der Haupt-Partner des D-Stacks für Standardisierungsfragen werden
- Die Kriterien zur Bewertung von Standards weiterentwickeln und schärfen
- Einen regelmäßigen Prozess zur Bewertung eingehender Vorschläge etablieren
- In einem Standard-TOP in jeder Sitzung, Empfehlungen für die Aufnahme neuer Standards in den D-Stack, an das BMDS aussprechen

Das BMDS würde in Zukunft alle Standards des D-Stacks zuvor durch das FIT-SB bewerten lassen.



Bundesministerium
für Digitales und
Staatsmodernisierung



**Vielen Dank für Ihre
Aufmerksamkeit.**

#WirMachen

www.bmds.bund.de

Weitere Kriterien: D-Stack - Architekturprinzipien

Prinzip	Erläuterung
API-first	Programmierschnittstellen (APIs) werden von Anfang an als zentrale Elemente der Lösungsarchitekturen konzipiert und spezifiziert sowie im Betrieb laufend dokumentiert.
Serviceorientierung & lose Kopplung	Dienste (Services) sind zentrale Architekturbausteine, die Funktionen bündeln. Sie und ihre IT-Lösungen sind modular konzipiert, weitgehend unabhängig austauschbar und klar abgegrenzt.
Wiederverwendbarkeit & Portierbarkeit	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.
Zero-Trust	Dienste müssen Zero-Trust-Prinzipien berücksichtigen.
Technologisch aktuell	Der aktuelle Stand der Technik ist bestimmend für Technologieauswahl und Architekturentscheidungen.
Made in Germany or EU first	Zur längerfristigen Stärkung der Souveränität setzt der D-Stack auf Produkte aus Deutschland und 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 wird 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.
Managed Services only	Die Nutzung bestehender, zentral gemanagter IT-Dienste ist stets zu bevorzugen, um Effizienz, Sicherheit, Verfügbarkeit und Skalierbarkeit zu erhöhen.





IT-Standards in der Verwaltung

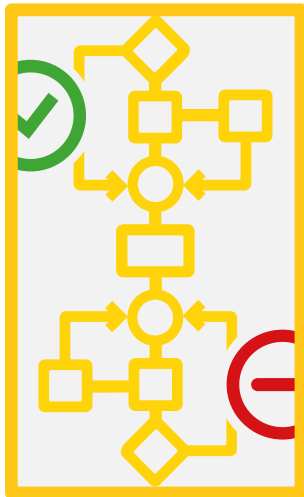
Konformitätskriterien

23. April 2026 | FIT-SB | Conny Diebel

Prüfung von IT-Standards

- › Auf der Grundlage des §2 des IT-Staatsvertrags legt der IT-Planungsrat gemeinsame IT-Standards fest.
- › Die Prüfung und Bewertung von IT-Standards ist eine der Hauptaufgaben des Föderalen Standardisierungsboards (FIT-SB).

Drei Aspekte bei der Prüfung von IT-Standards



Prüfung des Bedarfs



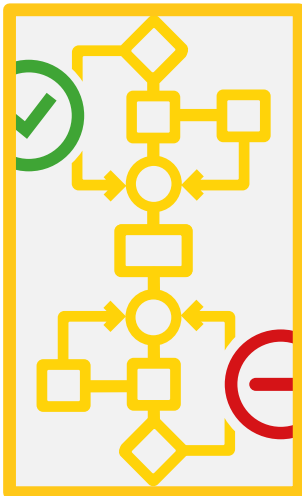
Prüfung, ob ein vorhandener Marktstandard den Bedarf decken kann



Prüfung der Qualität eines IT-Standards

Prüfung von IT-Standards

Durchführung der Bewertung



bei der Entscheidung zur Aufnahme eines IT-Standards auf die Standardisierungsagenda



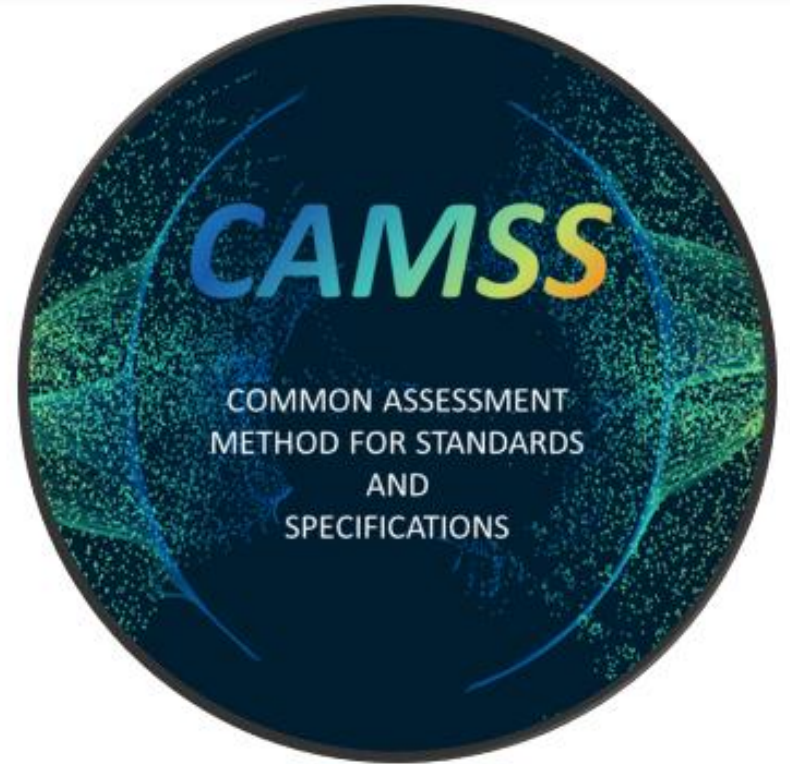
vor einer Empfehlung an den IT-Planungsrat für einen Beschluss gemäß §2 IT-Staatsvertrag

CAMSS-Methode

CAMSS-Profile zur Bewertung von IT-Standards

CAMSS ist als Methode generisch. Konkrete Anforderungen werden im wesentlichen mit Profilen („Szenarien“) abgebildet

- „Multi-Stakeholder Platform“
Szenario zur Nutzung für Standardsoftware oder marktübliche Software
- „EIF-Szenario“
bildet Kriterien aus dem European Interoperable Framework (EIF) ab



Quelle: <https://interoperable-europe.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss>

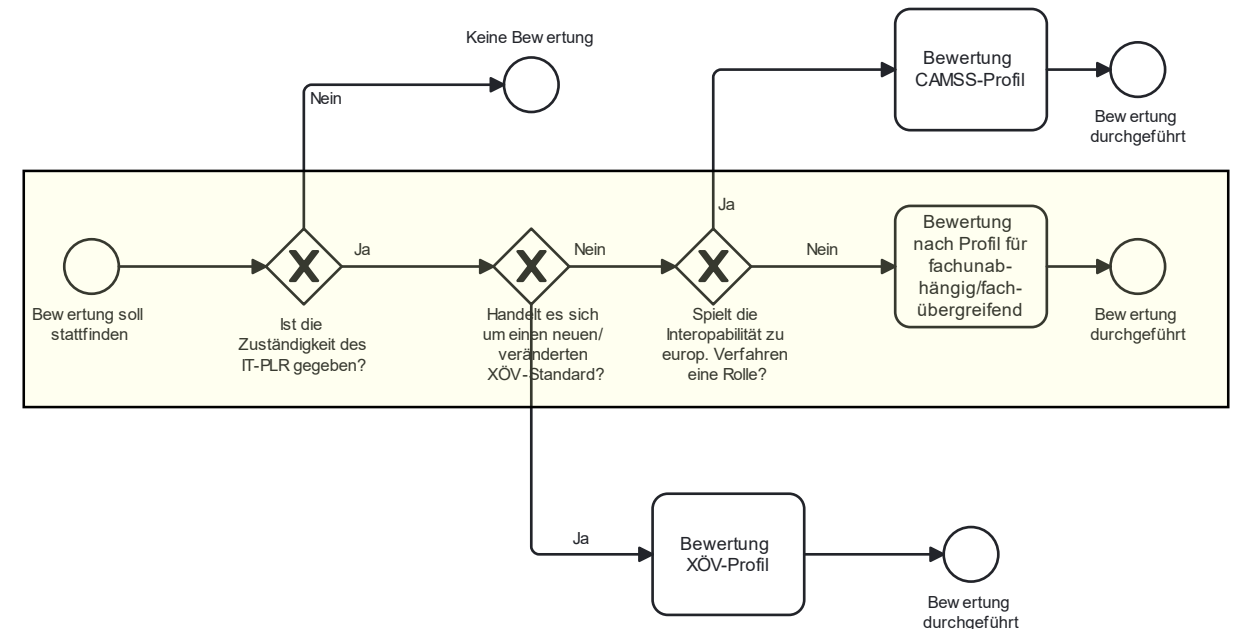
Profil für fachunabhängige und fachübergreifende IT Standards

CAMSS-Kriterien abgeleitet

Aus den vorliegenden CAMSS-Kriterien wurden Kriterien für ein nationales Bewertungsschema für fachunabhängige und fachübergreifende Standards abgeleitet und am 17.09.2025 vom FIT-SB verabschiedet.

Es soll zum Einsatz kommen, wenn:

- die Zuständigkeit des IT-Planungsrats gegeben ist
- kein XÖV-Bezug gegeben ist (aktueller Stand)
- die Interoperabilität zu europäischen IT-Verfahren nicht im Fokus ist



Profil für fachunabhängige und fachübergreifende IT Standards

CAMSS-Kriterien abgeleitet

Subsidiarität und Verhältnismäßigkeit	Offenheit	Transparenz
Wiederverwendung	Technologieneutralität	Sicherheit und Privatsphäre
Mehrsprachigkeit	Verwaltungsvereinfachung	Informationsbewahrung
Qualität, Effektivität und Effizienz	Digitale Souveränität	Marktakzeptanz

Subsidiarität und Verhältnismäßigkeit

Es handelt sich um einen fachunabhängigen oder fachübergreifenden IT Standard

Es gibt in der öffentlichen Verwaltung keinen anderen, bereits beschlossenen IT-Standard mit gleichem oder ähnlichem Standardisierungsgegenstand

Der Bedarf an einem IT-Standard ist nachgewiesen

Der Bedarf an der verbindlichen Vorgabe eines IT-Standardisierungs-bedarfs ist nachgewiesen

Die Möglichkeit der Vorgabe eines Marktstandards im Sinne des § 2 Abs 1 Satz 2 IT-Staatsvertrag wurde geprüft

Offenheit

Alle Interessensträger können sich diskriminierungsfrei an der Entwicklung und Weiterentwicklung des IT-Standards beteiligen.

Eine öffentliche Überprüfung ist Teil des Releasezyklus

Die Lizenzierung der geistigen Eigentumsrechte an dem IT-Standard erfolgt zu FRAND-Bedingungen

Der IT-Standard unterstützt die Bereitstellung offener Verwaltungsdaten

Transparenz

Inwieweit geht der IT-Standard nachvollziehbar auf Abläufe, Bestimmungen, Daten und Dienstleistungen der Verwaltung ein?

Mehrsprachigkeit

Wird die DIN 91379 für die Schreibweise von Namen angemessen berücksichtigt?

Wiederverwendung

Werden verbindlich beschlossene Kerndatenmodelle angemessen berücksichtigt?

Werden bewährte Datenobjekte, Codelisten und Prozessmuster in angemessenem Umfang wiederverwendet?

Technologieneutralität

Ist der IT-Standard technologieneutral?

Sicherheit und Privatsphäre

Inwieweit ermöglicht der IT-Standard einen sicheren Datenaustausch?

Inwieweit gewährleistet der IT-Standard die Authentizität und Authentifizierung der an einem Datenaustausch beteiligten Akteure?

Verwaltungsvereinfachung

Trägt der IT-Standard zur Umsetzung des Once Only Prinzips bei?

Informationsbewahrung

Inwieweit ermöglicht der IT-Standard die langfristige Bewahrung von Daten/Informationen/Wissen?

Qualität, Effektivität und Effizienz

Ist der IT-Standard geeignet, den gemeldeten Bedarf zu decken?

Ist der IT-Standard detailliert genug, konsistent und vollständig für die Verwendung und Entwicklung von Produkten und Dienstleistungen

Basiert der IT-Standard auf Normen oder Marktstandards im Sinne des § 2 Abs. 1 Satz 2 IT-Staatsvertrag

Basiert der IT-Standard auf einem Fachmodell, welches etablierte Modellierungsmethoden nutzt?

Hat der IT-Standard die notwendige Reife?

Digitale Souveränität

Die öffentliche Verwaltung muss die Entwicklung und Weiterentwicklung des IT-Standards ausreichend kontrollieren und steuern können

Ist der dauerhafte Betrieb des IT-Standards gewährleistet?

Entspricht der IT-Standard den einschlägigen Vorgaben der föderalen Architekturrichtlinie?

Marktakzeptanz

Wird der IT-Standard von verschiedenen Anbietern/Lieferanten für unterschiedliche Implementierungen verwendet?

Es handelt sich um einen fachunabhängigen oder fachübergreifenden IT Standard	Inwieweit geht der IT-Standard nachvollziehbar auf Abläufe, Bestimmungen, Daten und Dienstleistungen der Verwaltung ein?	Ist der IT-Standard geeignet, den gemeldeten Bedarf zu decken?
Es gibt in der öffentlichen Verwaltung keinen anderen, bereits beschlossenen IT-Standard mit gleichem oder ähnlichem Standardisierungsgegenstand	Werden verbindlich beschlossene Kerndatenmodelle angemessen berücksichtigt?	Ist der IT-Standard detailliert genug, konsistent und vollständig für die Verwendung und Entwicklung von Produkten und Dienstleistungen
Der Bedarf an einem IT-Standard ist nachgewiesen	Werden bewährte Datenobjekte, Codelisten und Prozessmuster in angemessenem Umfang wiederverwendet?	Basiert der IT-Standard auf Normen oder Marktstandards im Sinne des § 2 Abs. 1 Satz 2 IT-Staatsvertrag
Der Bedarf an der verbindlichen Vorgabe eines IT-Standardisierungsbedarfs ist nachgewiesen	Ist der IT-Standard technologieneutral?	Basiert der IT-Standard auf einem Fachmodell, welches etablierte Modellierungsmethoden nutzt?
Die Möglichkeit der Vorgabe eines Marktstandards im Sinne des § 2 Abs 1 Satz 2 IT-Staatsvertrag wurde geprüft	Inwieweit ermöglicht der IT-Standard einen sicheren Datenaustausch?	Hat der IT-Standard die notwendige Reife?
Alle Interessensträger können sich diskriminierungsfrei an der Entwicklung und Weiterentwicklung des IT-Standards beteiligen.	Inwieweit gewährleistet der IT-Standard die Authentizität und Authentifizierung der an einem Datenaustausch beteiligten Akteure?	Die öffentliche Verwaltung muss die Entwicklung und Weiterentwicklung des IT-Standards ausreichend kontrollieren und steuern können
Eine öffentliche Überprüfung ist Teil des Releasezyklus	Wird die DIN 91379 für die Schreibweise von Namen angemessen berücksichtigt?	Ist der dauerhafte Betrieb des IT-Standards gewährleistet?
Die Lizenzierung der geistigen Eigentumsrechte an dem IT-Standard erfolgt zu FRAND-Bedingungen	Trägt der IT-Standard zur Umsetzung des Once Only Prinzips bei?	Entspricht der IT-Standard den einschlägigen Vorgaben der föderalen Architekturrichtlinie?
Der IT-Standard unterstützt die Bereitstellung offener Verwaltungsdaten	Inwieweit ermöglicht der IT-Standard die langfristige Bewahrung von Daten/Informationen/Wissen?	Wird der IT-Standard von verschiedenen Anbietern/Lieferanten für unterschiedliche Implementierungen verwendet?

Profil für fachunabhängige und fachübergreifende IT Standards

CAMSS-Kriterien abgeleitet

Subsidiarität und Verhältnismäßigkeit	Offenheit	Transparenz
Wiederverwendung	Technologieneutralität	Sicherheit und Privatsphäre
Mehrsprachigkeit	Verwaltungsvereinfachung	Informationsbewahrung
Qualität, Effektivität und Effizienz	Digitale Souveränität	Marktakzeptanz