Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

# "*Deutschland-Stack*"

## *Positionspapier*

2026

Kommentierung im Rahmen der 2. Konsultation des
Bundesministeriums für Digitales und Staatsmodernisierung

TeleTrusT-Arbeitsgruppe "Cyber-Nation" [https://www.teletrust.de/arbeitsgremien/cyber-nation/]

**Impressum**

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 310
E-Mail: info@teletrust.de
https://www.teletrust.de

# *Inhaltsverzeichnis*


**1 Zusammenfassung ..... 4**

**2 Einleitung ..... 5**

**3 Kriterien des Deutschland-Stack ..... 6**
3.1 Digitale Souveränität ..... 6
3.2 Interoperabilität ..... 8
3.3 Zukunftsfähigkeit ..... 8
3.4 Marktrelevanz ..... 8
3.5 Vertrauenswürdigkeit ..... 8
3.6 Nachhaltigkeit ..... 8

**4 Architekturprinzipien ..... 10**

**5 Technologiefelder und Standards ..... 12**
5.1 Virtualisierte softwarebasierte Infrastruktur ..... 12
5.2 Managed Services und Cloud ..... 14
5.3 IT-Sicherheit (besser Informations- und Cyber-Sicherheit) ..... 16
5.3.1 Begriffsdefinition ..... 16
5.3.2 Konkrete Anmerkungen ..... 16
5.3.3 Normen, Standards und regulatorische Anforderungen ..... 17
5.3.4 Allgemeines Fazit zu IT-Sicherheit und Fokusthemen ..... 18

**6 Tech-Stack-Landkarte als Orientierung ..... 22**

**7 Fazit und nächste Schritte ..... 23**

**8 Anhang: Leitfragen des BMDS ..... 24**

# 1 Zusammenfassung

Der Deutschland-Stack ist aus Sicht von TeleTrusT eine strategisch richtige und notwendige Initiative, um die digitale Handlungsfähigkeit des Staates langfristig zu sichern. Auch das gewählte Vorgehensmodell eines Konsultationsverfahrens wird ausdrücklich begrüßt. Gleichzeitig zeigt die Analyse: In der aktuellen Ausprägung ist der Deutschland-Stack noch zu stark als technische Bausteinliste gedacht. Für belastbare Wirkung im öffentlichen Sektor ist ein ein klar geführtes **Gesamtbetriebsmodell** aus Architektur, Governance, Sicherheit und Verantwortung erforderlich.

Der zentrale Hebel ist nicht die Auswahl einzelner Technologien, sondern die Fähigkeit, den Stack **sicher, kontrollierbar, resilient und austauschbar** zu betreiben - über Bund, Länder und Kommunen hinweg.

Damit verschiebt sich die Führungsfrage von "Welche Tools nutzen wir?" zu:

**"Wie stellen wir Souveränität, Sicherheit und Skalierung über den gesamten Lebenszyklus verbindlich sicher?"**

**Strategische Kernbotschaften:**

- **Souveränität ist eine Steuerungsleistung, kein Label.**
- **Sie erfordert wirksame Kontrolle über Daten, Zugriffe, Betriebsprozesse und Anbieterabhängigkeiten (inkl. Exit-/Wechselfähigkeit).**
- **Sicherheit muss als durchgängige Managementdisziplin verankert werden.**

Der Fokus sollte auf **Informations- und Cyber-Sicherheit** liegen (nicht nur IT-Sicherheit) - kontinuierlich von Spezifikation über Betrieb bis Weiterentwicklung.

- **Cloud und Managed Services sind Betriebsformen, keine Sicherheitsgarantie.**

Sicherheit und Souveränität entstehen durch Architektur und technische Kontrollpunkte, nicht durch Vertragsform oder Betriebsort.

- **Komplexität ist ein Top-Risiko.**

Ein "Flickenteppich" aus Einzellösungen erhöht Angriffsfläche, Betriebsaufwand und Ausfallrisiko. Priorität hat eine integrierte, standardisierte Infrastrukturarchitektur.

- **Resilienz ist Vorstands-/Leitungsthema.**

Wiederherstellungsfähigkeit, Redundanz, klare Verantwortlichkeiten und auditierbare Prozesse müssen verbindlich geplant und regelmäßig nachgewiesen werden.

**Risiken bei unveränderter Ausrichtung:**

- Zunehmende Hersteller- und Plattformabhängigkeiten im Widerspruch zum umfassend erhobenen Souveränitätsanspruch
- Höhere Sicherheits- und Compliance-Risiken durch inkonsistente Umsetzung
- Steigende Betriebs- und Migrationskosten durch Architekturbrüche
- Langsamere Skalierung und geringere Nachnutzbarkeit zwischen Verwaltungsebenen
- Vertrauensverlust bei kritischen Diensten im Krisenfall

Der Deutschland-Stack wird zum strategischen Rückgrat staatlicher Digitalisierung - **wenn er als Steuerungs- und Betriebsmodell geführt wird, nicht als Technologiekatalog.**

TeleTrusT signalisiert hierfür aktive Mitwirkung bei der weiteren inhaltlichen Ausgestaltung, Validierung und Umsetzungsbegleitung.

# 2 Einleitung

Das vorliegende Dokument enthält die Kommentare des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT), die dieser im Rahmen der zweiten Konsultationsphase des Bundesministeriums für Digitalisierung und Staatsmodernisierung (BMDS) erstellt hat. Maßgeblich war dabei die TeleTrusT-Arbeitsgruppe "Cyber-Nation" beteiligt.

Die Kommentare gliedern sich dabei im Wesentlichen in zwei Teile:

Zum einen wurden Kommentare zum generellen Vorgehensmodell ausgearbeitet, zum anderen zu Aspekten, die aufgrund der breiten Kompetenzen der Verbandsmitglieder im aktuellen Konzept des Deutschland-Stack vermisst werden.

Desweiteren nimmt TeleTrusT zu den jetzt vorliegenden Vorgaben und Ausführungen konstruktiv Stellung.

Diese Kommentierung geht daher im Folgenden auf die TeleTrusT-Sicht zu den grundlegenden Kriterien des Deutschland-Stack ein, kommentiert ausführlich die Architekturprinzipien und formuliert weitreichende Ergänzungen zum Themenfeld IT-Sicherheit bzw. besser Informations- und Cyber-Sicherheit beschrieben.

Abschließend beantwortet diese Kommentierung die drei Kernfragen des BMDS im Rahmen des 2. Konsultationsverfahrens.

# 3 Kriterien des Deutschland-Stack

**Zusammenfassung:**

Dieser Abschnitt erläutert die sechs BMDS-Kriterien für den Deutschland-Stack (Digitale Souveränität, Interoperabilität, Zukunftsfähigkeit, Marktrelevanz, Vertrauenswürdigkeit, Nachhaltigkeit) und ergänzt sie aus TeleTrusT-Sicht. Im Zentrum steht die **Digitale Souveränität**: staatliche Kontrolle über Daten, geringere Abhängigkeit von ausländischen Technologien, Vermeidung von Vendor-Lock-in, starke **Informations- und Cyber-Sicherheit** über alle Stack-Ebenen sowie rechtliche Handlungsfähigkeit. Open Source wird als wichtig bewertet, allerdings mit dem Hinweis, "Offenheit" differenziert (z.B. bei KI) zu definieren.

Zudem fordert TeleTrusT **Interoperabilität über offene, API-first-Schnittstellen**, kontinuierliche Modernisierung und Einbindung neuer Standards (inklusive Kryptoagilität), ausreichende Marktverfügbarkeit mit mehreren Anbietern, belastbare Vertrauens- und Sicherheitsmechanismen sowie ein langfristig tragfähiges, ökonomisch, ökologisch und sozial nachhaltiges Ökosystem. Insgesamt wird eine verbindliche, föderal umsetzbare Governance mit klaren rechtlichen Rahmenbedingungen angemahnt.

Gemäß des BMDS (https://deutschland-stack.gov.de/kriterien/) wurden aus dem Leitbild und dem politisch-strategischen Rahmen entsprechend der Zielsetzung und den Policies folgende Kriterien identifiziert:

- Digitale Souveränität
- Interoperabilität
- Zukunftsfähigkeit
- Marktrelevanz
- Vertrauenswürdigkeit
- Nachhaltigkeit

Nachfolgend einige Anmerkungen seitens TeleTrusT zu diesen Kriterien:

## 3.1 Digitale Souveränität

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

Digitale Souveränität bezieht sich beim Deutschland-Stack auf die Fähigkeit von Deutschland bzw. deren Verwaltung, die Kontrolle über die eigenen digitalen Ressourcen, Daten und Infrastrukturen zu erhalten. Sie umfasst dabei mehr Dimensionen als diejenigen, die hier dargestellt wurden. Diese werden daher hier nochmals dargestellt.

**Kontrolle über die Daten bzw. deren Verarbeitung**

Ein Aspekt der digitalen Souveränität ist die Kontrolle über die Daten, die dem Staat gehören. Deutschland als Staat muss weiterhin selbst gestalten können, wer Zugang zu den Daten hat, wie sie verarbeitet werden und wo sie gespeichert sind. Ziel dabei ist auch die Minimierung der Abhängigkeit von beteiligten Technologieunternehmen, als auch die Wahl von Anbietern, so dass der Staat sich Optionen bewahren kann und somit bei einem Ausfall eines Anbieters (zum Ausfall können auch politische Aspekte führen) auch weiterhin die volle Funktionalität als auch Kontrolle über die Daten und deren Verarbeitung erhalten kann.

**Unabhängigkeit von ausländischen Technologien**

Ein weiterer wichtiger Punkt ist die Unabhängigkeit von ausländischen digitalen Infrastrukturen, insbesondere aus den USA oder China. Mindestens ist eine Wechselfähigkeit zwischen Betreibern und Anbietern notwendig. Deutschland sollte danach streben, eigene Technologien, Softwarelösungen und Netze zu entwickeln oder auf solche aus vertrauenswürdigen Quellen inkl. Backdoor-Freiheit zurückzugreifen, etwa durch den Einkauf im nationalen Markt bzw. im europäischen Binnenmarkt. Auch die

Vermeidung von "Vendor-Lock-In" spielt eine entscheidende Rolle, um mehrere Optionen zu ermöglichen und nicht an einen Hersteller gebunden zu sein.

**IT-Sicherheit (besser: Informations- und Cyber-Sicherheit)**

Digitale Souveränität bedeutet auch, die eigene digitale Infrastruktur sicher zu gestalten und vor äußeren Bedrohungen, etwa Cyber-Angriffen oder fremd-staatlichen Überwachungsmaßnahmen, zu schützen. Ein umfassendes Sicherheitskonzept muss auf allen Layern des Stack technische und organisatorische Sicherheitsmaßnahmen bündeln, um eine umfassende Sicherheit hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu etablieren und zu erhalten. Eine technische Zertifizierbarkeit des Stack an sich sollte auch gegeben sein, so dass auch das BSI bzw. eine in Deutschland anerkannte Prüfstelle in den wesentlichen Funktionen Einblick in die Implementierung erhält und die Umsetzung verifizieren kann. Detaillierte Kommentare zum Element "IT-Sicherheit" (besser: Informations- und Cyber-Sicherheit) finden sich weiter unten.

**Zugang und Kontrolle über digitale Infrastrukturen**

Ein souveräner Umgang mit digitalen Infrastrukturen umfasst auch den Zugang zu grundlegenden Technologien wie Servern, Cloud-Diensten und Netzwerken. Staaten oder Organisationen, die digitale Souveränität anstreben, setzen oft auf eigene Rechenzentren oder öffentlich kontrollierte Infrastrukturen, um nicht von kommerziellen Anbietern abhängig zu sein.

**Rechtliche Autonomie und Regulierung**

Die rechtliche Dimension der digitalen Souveränität betrifft die Fähigkeit, eigene digitale Gesetze zu erlassen, die den Umgang mit Daten, Datenschutz und Cyber-Sicherheit regeln. Die Gesetze und Verordnungen sollen verhindern, dass fremde Staaten, Cyber-Kriminelle oder Unternehmen unkontrollierten Zugang zu sensiblen Daten erhalten oder diese ausnutzen. Hierbei ist auch der Aspekt der Geheimhaltung mit ihren entsprechenden Abstufungen adäquat zu berücksichtigen.

**Nutzung von Open Source**

Im Zusammenhang mit Digitaler Souveränität sollte auf Open-Source-Technologie gesetzt werden. Die OS-basierenden Produkte und Lösungen sind transparent, frei zugänglich und ermöglichen es den Nutzern, ihre digitale Infrastruktur nach eigenen Bedürfnissen weiter auszubauen, ohne von einem Unternehmen abhängig zu sein. Open Source fördert die Kontrolle und Anpassungsfähigkeit der Nutzer und reduziert die Machtkonzentration bei großen Tech-Firmen.

Allerdings wird dieser Aspekt im Deutschland-Stack derzeit zu pauschal betrachtet. Ausgeklammert wird insbesondere die Frage, was genau denn alles "Open" ist und wie "Open" es ist (insbesondere die unterschiedlichen möglichen Lizenztypen). Gerade im Kontext von KI (ein Themenfeld, das für den Deutschland-Stack von besonderer Relevanz ist) gibt es eine besonders große Spannbreite hinsichtlich dessen, was bei KI-Modellen und Technologien alles Open Source sein kann oder sein soll (etwa von Open Weights bis zu Open-Trainingsdaten). Diese Betrachtung ist insofern besonders relevant, da entsprechend unterschiedliche Formen von "Open Source" letztlich zu ganz unterschiedlichen Ausprägungen von Souveränität führen. Wünschenswert wäre hier zumindest eine stärkere Awareness für dieses Problem in der Definition des Deutschland-Stack und ggf. eine entsprechend formulierte Zielvorstellung, was ideal und was akzeptabel wäre. Damit wären dann zu mindestens Rahmenbedingungen geschaffen, die dann für die einzelnen Technologiefelder Anwendung finden könnten. Grundsätzlich sollten natürlich überall offene Standards verwendet werden, die in transparenten und anerkannten Vorgehensmethoden und Gremien diskutiert, festgelegt und fortgeschrieben werden.

Open Source und offene Schnittstellen können durch diese Transparenz einen erfolgskritischen Anteil zur Umsetzung von Digitaler Souveränität einnehmen.

**Kompetenzentwicklung**

Schließlich spielt auch die Entwicklung von digitalen Kompetenzen eine Rolle. Der Staat und der Betreiber als auch die Nutzer müssen in der Lage sein, technologische Entwicklungen zu verstehen, zu nutzen und mitzugestalten. Eine eigenständige Entwicklung muss ohne Abhängigkeiten von einzelnen juristischen Personen möglich sein.

## 3.2 Interoperabilität

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.

## 3.3 Zukunftsfähigkeit

Mit dem Deutschland-Stack sollen die Lösungen stets auf einem technologisch aktuellen Stand sein und es sollen mehr Innovationen genutzt werden. Als Mindestbedingung ist demnach zu fordern das Lösungen kontinuierlich aktualisiert werden. Erfolgskritisch ist aber auch die kontinuierliche Einbindung der IT- und Digitalwirtschaft sowie die rechtzeitige/zügige Einbringung aller benötigter neuester Standards einschließlich europäischer und deutscher Standards. Damit ist z.B. auch die Kryptoagilität über den Lebenszeitraum des Deutschland-Stack sicherzustellen. Hierbei ist in den letzten Jahren ersichtlich, dass es immer schwieriger wird, deutsche bzw. europäische Standards in Öko-Systeme insbesondere internationaler Anbieter einzubringen.

Insofern hat der Aspekt der Zukunftsfähigkeit also wesentliche Verbindungen auch zu einigen Aspekten, die oben im Kontext der digitalen Souveränität diskutiert wurden.

## 3.4 Marktrelevanz

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 aber auch eine Verteilung von Produktanbietern im Markt, so dass keine Abhängigkeiten von einzelnen Akteuren entstehen. Im Sinne der Souveränität spielt dabei auch die Verortung entsprechender Anbieter im nationalen, europäischen und internationalen Markt eine wesentliche Rolle.

## 3.5 Vertrauenswürdigkeit

Vertrauenswürdigkeit ist einerseits eine essenzielle Grundlage für die Akzeptanz durch die 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.

## 3.6 Nachhaltigkeit

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 dabei insbesondere auch die grundlegenden Wertevorstellungen von Deutschland und Europa berücksichtigen.

Je mehr Nutzer die Plattform nutzen, je besser kann die Nachhaltigkeit durch die finanziellen Einbringungen gesichert werden. Daher ist anzustreben, alle Bedarfsträger zu identifizieren und eine möglichst homogene und einheitliche Umsetzungs- und Einsatzstruktur zu erreichen.

Dabei ist auch zu prüfen, ob hier entsprechende Vorgaben im Format von Gesetzen und Verordnungen umsetzbar sind. Im Kontext des Zusammenspiels von Bund, Ländern und Kommunen spielen hierbei auch verfassungsrechtliche Fragen eine ganz wesentliche Rolle.

# 4 Architekturprinzipien

TeleTrusT empfiehlt, den Deutschland-Stack um weitere zentrale Architekturprinzipien zu ergänzen: **Skalierbarkeit, hohe Verfügbarkeit, Fehlertoleranz, Automatisierung, Performance, Portabilität, Resilienz und Beherrschbarkeit** ("so komplex wie nötig"). Kernaussage ist, dass Sicherheit, Souveränität und Betriebsfähigkeit nur im Zusammenspiel von **Technologie, Governance und Infrastruktur** entstehen.

Statt eines "Flickenteppichs" aus Einzellösungen wird eine **ganzheitliche, virtualisierte Infrastruktur** gefordert (Compute, Storage, Netzwerk, Security, Backup/Recovery, Container/Cloud plus kontrollierte Hardware). Das reduziert Komplexität und Angriffsflächen und ermöglicht die konsequente Umsetzung von **Security-by-Design**-Vorgehensmodellen über den gesamten Lebenszyklus.

**Managed Services und Cloud** werden als **Betriebsmodelle** eingeordnet, nicht als Sicherheitskonzepte. Sicherheit muss architektonisch erzwungen werden (u.a. Zugriffskontrolle, Segmentierung, Protokollierung, Wiederherstellung) und gilt unabhängig vom Betriebsort.

Zudem fordert TeleTrusT eine durchgängige **Informations- und Cyber-Sicherheitsmethodik** (statt enger IT-Sicherheits-Sicht), kontinuierliche Risiko- und Compliance-Steuerung nach relevanten Normen/Regelwerken (z.B. ISO 27001, BSI-Grundschutz, C5, DSGVO, NIS2, eIDAS) sowie stärkere Orientierung an aktuellen BSI-Richtlinien (inkl. TR-02102 für Kryptografie).

Im operativen Fokus stehen **Zero-Trust-Zugriff, Defense-in-Depth, ressourcenzentrierte Freigaben** und eine **mehrstufige, getrennte Backup-/Recovery-Architektur** zur resilienten Wiederherstellung.

Bei den Architekturprinzipien empfiehlt TeleTrusT zusätzlich den bereits betrachteten Feldern noch die folgenden Aspekte, die ebenfalls beachtet werden sollten:

**Skalierbarkeit**
Der Deutschland-Stack sollte so entworfen sein, dass er horizontal und/oder vertikal skalierbar ist. Sowohl Instanzen (horizontal) als auch Ressourcen (vertikal) sollten dynamisch hinzugefügt bzw. reduziert werden können - je nach Bedarf der Nutzung.

**Hohe Verfügbarkeit**
Der Deutschland-Stack muss so gestaltet werden, dass sie auch bei Ausfällen einzelner Komponenten oder Ressourcen kontinuierlich verfügbar sind. Redundanz-Systeme (einschließlich Geo-Redundanz) und Failover-Mechanismen sind zu nutzen und bereitzustellen.

**Fehlertoleranz**
Der Deutschland-Stack sollte Fehler selbständig erkennen und die Auswirkungen der Fehler minimieren, ohne dass es zu Systemausfällen kommt.

**Automatisierung**
Automatisierung ist ein wesentlicher Bestandteil im Deutschland-Stack, um manuelle Eingriffe, die Kosten verursachen, zu langsam wirken und fehleranfällig sein können, zu minimieren.

**Performanceoptimierung**
Der Deutschland-Stack sollten für die bestmögliche Performance optimiert werden. Dies kann durch unterschiedlichste Maßnahmen erreicht werden, etwa den Einsatz von CDNs (Content Delivery Networks), Caching-Mechanismen oder durch die Optimierung von Datenbankabfragen und Lastverteilung erreicht werden.

**Portabilität**
Anwendungen und Daten sollten zwischen verschiedenen Betreibern/verschiedenen Instanzen verschoben werden können, ohne größere Änderungen vorzunehmen.

**Resilienz**
Die einzelnen Komponenten im Deutschland-Stack müssen so entworfen werden, dass sie auch unter Stress oder bei Fehlern stabil bleiben. Auto-Healing-Mechanismen, robuste Backup- und Wiederherstellungsprozesse sind notwendig, um auch bei größeren Fehlern eine schnelle Wiederherstellbarkeit zu garantieren.

**Beherrschbarkeit**
Souveränität bedeutet nicht nur die theoretische Möglichkeit zu haben, eine spezifische Technologie zu nutzen und weiterzuentwickeln, sondern auch über die dafür erforderlichen Ressourcen und Kompetenzen zu verfügen. Neben der bereits beschriebenen Kompetenzentwicklung ist hierbei aber auch der Aspekt der Komplexität des Stack und der eingesetzten Technologien wesentlich. Eine hohe Komplexität dieser führt zu einer abnehmenden Beherrschbarkeit und damit im Übrigen auch zu einer abnehmenden Cyber-Sicherheit. Daher sollte dieser Aspekt als weitere Rahmenbedingung für die Auswahl und Nutzung von Technologien explizit benannt werden.

Damit wären komplementäre Anforderungen ergänzend zu "Die Nutzung ist intuitiv und aufwandsarm" im Kontext des Nutzungserlebnis formuliert - nur mit dem expliziten Fokus auf hohe technologische Beherrschbarkeit und den positiven Auswirkungen auf Informations- und Cyber-Sicherheit und Souveränität. Ergänzend konnte dieses Entscheidungsprinzip auch als "nur so komplex wie notwendig" und als "funktional nur so umfangreich wie nötig" bei den Architekturprinzipien eingeordnet werden.

Generell ist festzustellen, dass wesentliche Funktionalitäten des Deutschland-Stack nur im konsequenten Zusammenspiel von Technologie, Governance und Infrastruktur entstehen können. Insofern gibt es enge Abhängigkeiten zwischen Schutzzielen im Sinne der Sicherheit und daraus abgeleiteten architekturellen Vorgaben.

# 5 Technologiefelder und Standards

## 5.1 Virtualisierte Softwarebasierte Infrastruktur

Eine virtualisierte, softwarebasierte Infrastruktur ist heute die zentrale Grundlage moderner staatlicher und kritischer IT. Sie ermöglicht die softwaredefinierte Steuerung und Virtualisierung von Rechenleistung, Speicher, Netzwerk und Plattformdiensten und schafft damit Standardisierung, Automatisierung, Mandantenfähigkeit und Prüfbarkeit.

**Für sich allein betrachtet ist diese Sicht jedoch nicht ausreichend, um die Anforderungen an Sicherheit, Resilienz und digitale Souveränität nachhaltig zu erfüllen.**

In der Praxis zeigen rein softwarezentrierte Infrastrukturlösungen klare Grenzen. Die physischen Abhängigkeiten, Fehlerdomänen, Wiederherstellbarkeit, Performance und Kontrollfähigkeit lassen sich nicht ausschließlich auf der Softwareebene beherrschen.

**Wird Infrastruktur lediglich als abstrahierte Software-Schicht verstanden, entstehen häufig komplexe, fragmentierte Systemlandschaften, die Sicherheit durch nachträgliche Zusatzlösungen erzwingen müssen.**

Der Deutschland-Stack verfolgt daher einen erweiterten Infrastrukturbegriff:

**Virtualisierte softwarebasierte Infrastruktur wird als Teil einer ganzheitlichen IT-Infrastruktur verstanden.**

Im idealtypischen Fall bildet die Infrastruktur eine funktionale Einheit, bestehend aus:

- virtualisierten Server- und Client-Umgebungen (inkl. VDI)
- softwaredefiniertem Storage (Block, File, Objekt)
- integrierten Netzwerk-, Routing-, Load Balancing- und Firewall-Funktionen
- mandantenfähigen Infrastruktur-Services (IaaS, Network as a Service)
- Zero-Trust-Mechanismen pro Mandanten- und Infrastrukturdomain
- Backup- und Wiederherstellungsfunktionen als Infrastruktur-Service
- Container- und Cloud-Plattformen (z.B. Kubernetes)
- sowie einer dafür ausgelegten, kontrollierten Hardware als Fundament

**Diese Elemente sind architektonisch miteinander verzahnt und werden nicht als lose Einzelkomponenten betrieben und können nach Bedarf entsprechend der Bedürfnisse der einzelnen Mandanten aktiviert oder deaktiviert werden.**

Ein zentrales Ergebnis dieser ganzheitlichen Infrastrukturarchitektur ist die **Reduktion von Komplexität**. Durch die Bündelung von Infrastruktur- und Sicherheitsfunktionen in einer konsistenten Plattform werden:

- Angriffsflächen und Schnittstellen reduziert
- Schwachstellen und Fehlkonfigurationen minimiert
- Administrationsaufwände gesenkt
- Betriebsqualität, Stabilität und Wiederherstellbarkeit erhöht

Sicherheit entsteht damit nicht durch einen Flickenteppich aus Produkten, sondern durch die Infrastruktur selbst - Security by Design.

Im Deutschland-Stack- und Europa-Stack-Kontext ermöglicht dieser Ansatz:

- die Gestaltung digitaler Souveränität aus eigener Infrastruktur heraus
- Unabhängigkeit von externen Plattform- und Ökosystemzwängen
- vollständige Kontrolle über Architektur, Betrieb und Sicherheitslogik

und die Umsetzung von Sicherheits- und Resilienz-Anforderungen unabhängig vom Betriebsort.

**Virtualisierte softwarebasierte Infrastruktur ist notwendig. Erst als ganzheitliche Infrastruktur-Einheit aus Software und Hardware wird sie sicher, resilient, beherrschbar und souverän.**

**Deutschland-Stack - Gegenüberstellung**

Flickenteppich-Ansatz vs. ganzheitliche virtualisierte Infrastruktur

| Aspekt | Flickenteppich aus Einzellösungen | Deutschland-Stack - Ganzheitliche virtualisierte Infrastruktur |
|---|---|---|
| **Grundverständnis** | Infrastruktur als Summe einzelner Produkte und Tools | Infrastruktur als einheitliche, softwaredefinierte Architektur |
| **Virtualisierung** | Punktuell (Server, ggf. Storage), isoliert betrachtet | Durchgängig: Compute, Storage, Netzwerk, Sicherheit, Plattform |
| **Sicherheitslogik** | Nachträglich ergänzt, oft kompensierend | Infrastrukturell verankert, technisch erzwungen |
| **Komplexität** | Hoch: viele Schnittstellen, Sonderfälle, Ausnahmen | Reduziert durch Bündelung und Standardisierung |
| **Angriffsflächen** | Groß durch Produktvielfalt und Integrationen | Minimiert durch konsistente Architektur |
| **Administration** | Heterogen, wissensabhängig, fehleranfällig | Zentral, standardisiert, reproduzierbar |
| **Betrieb** | Stark personen- und herstellerabhängig | Architekturgetrieben, auditierbar |
| **Netzwerk & Security** | Separate Appliance, manuelle Kopplung | Integrierte Services (Routing, Firewall, Segmentierung) |
| **Zero Trust** | Zusatzlösung am Rand, nicht durchgängig | Mandantenfähig in der Infrastruktur verankert |
| **Backup & Recovery** | Extern, oft nachgelagert | Backup als Infrastruktur-Service je Mandant |
| **Resilienz** | Reaktiv, abhängig von Einzelkomponenten | Infrastrukturelle Eigenschaft (Design + Betrieb) |
| **Fehlerdomänen** | Unklar, schwer kontrollierbar | Physisch und logisch definiert |
| **Skalierung** | Aufwändig, migrationsintensiv | Linear, integriert, ohne Architekturbruch |
| **Cloud-/Hybridfähigkeit** | Fragmentiert, inkonsistente Logik | Betriebsort-neutral, gleiche Sicherheitslogik |
| **Souveränität** | Abhängigkeiten von Produkten & Ökosystemen | Kontrolle aus eigener Infrastruktur heraus |
| **Zukunftsfähigkeit** | Steigende Komplexität über Zeit | Stabil durch architektonische Klarheit |

## *5.2 Managed Services und Cloud*

Managed Services und Cloud werden häufig mit Auslagerung, Effizienz oder Kostenreduktion gleichgesetzt. Für staatliche und kritische IT-Infrastrukturen greift diese Sichtweise zu kurz. Im Deutschland-Stack-Verständnis sind Managed Services und Cloud keine Technologien, sondern Betriebsmodelle. Grundsätzlich ersetzen Managed Services und Cloud keine Architektur. Sie wirken ausschließlich innerhalb einer definierten Architektur. Ohne eine tragfähige Infrastruktur- und Sicherheitsarchitektur bleiben Managed Services und Cloud wirkungslos oder risikobehaftet.

**1. Betriebsmodell ist nicht Sicherheitsmodell**

Ein zentrales strukturelles Risiko besteht darin, Betriebsmodelle mit Sicherheits- oder Souveränitätsgarantien gleichzusetzen.

Es steht fest, dass

- Cloud kein Sicherheitskonzept ist,
- Managed Services kein Nachweis von Souveränität darstellen und
- Verträge keine technische Kontrolle ersetzen.

Sicherheits- und Souveränitätseigenschaften entstehen ausschließlich durch die Architektur, Zugriffskontrolle, technische Segmentierung, Resilienz- und Wiederherstellungsmechanismen. Managed Services und Cloud können diese Eigenschaften unterstützen, sie können sie nicht erzeugen.

Anforderungen aus Sicht des BSI und kritischer Infrastrukturen ergeben sich klare Anforderungen an Betriebsmodelle und sind unabhängig vom Betriebsort. Sie umfassen:

- dauerhafte Wirksamkeit von Sicherheitsmaßnahmen
- klare Trennung von Rollen, Rechten und Verantwortlichkeiten
- Nachvollziehbarkeit und Prüfbarkeit aller Änderungen
- technische Durchsetzung von Zugriffsbeschränkungen
- gesicherte und überprüfbare Wiederherstellungsfähigkeit

Diese Anforderungen gelten gleichermaßen für Eigenbetrieb, extern gemanagte Umgebungen und Cloud-basierte Betriebsformen. Der Betriebsort ändert nichts an der Verantwortung.

**2. Managed Services als standardisierte, kontrollierte Betriebsform**

Im Deutschland-Stack werden Managed Services als standardisierte und kontrollierte Betriebsform auf Basis einer vorab definierten Infrastruktur- und Sicherheitsarchitektur verstanden. Sie bietet:

- klar abgegrenzte Services
- definierte Betriebsgrenzen
- technisch erzwungene Policies
- eingeschränkte manuelle Eingriffe
- dokumentierte und reproduzierbare Betriebszustände

Managed Services reduzieren operative Risiken, indem sie Sonderkonfigurationen vermeiden, menschliche Fehlerquellen begrenzen, Betriebsprozesse vereinheitlichen. Sie vereinfachen Betrieb, ohne Kontrolle abzugeben.

**3. Architekturgetriebene Services statt isolierter Betriebsleistungen**

Ein zentrales Prinzip des Deutschland-Stack ist die Architekturgebundenheit von Betriebsleistungen. In einer virtualisierten, softwarebasierten Infrastruktur können zentrale Funktionen als architekturkonforme Services bereitgestellt werden, wie:

- Netzwerk- und Routingfunktionen
- Sicherheits- und Segmentierungsfunktionen
- gesicherte Kommunikationspfade
- Backup- und Wiederherstellungsprozesse

- Protokollierung, Monitoring und Lastverteilung
- Server- und Client-Virtualisierung
- Speicher- und Plattformdienste (Objekt-, Block-, File-Storage, Container-Plattformen)

Diese Services sind technisch integriert, nicht frei kombinierbar, nicht individuell modifizierbar. Teil einer konsistenten Gesamtarchitektur. Betrieb folgt der Architektur - nicht umgekehrt.

### 4. Cloud: Betriebsort, kein Kontrollmodell

Im Deutschland-Stack wird Cloud nicht als Sicherheits- oder Kontrollmodell verstanden, sondern als Betriebsort. Dabei ist entscheidend, ob die Architektur Cloud-fähig ist, die Sicherheitsmechanismen ortsunabhängig wirken und der Betrieb und Wiederherstellung kontrollierbar bleiben.

Cloud-Nutzung ist dann geeignet, wenn keine Architekturbrüche entstehen und keine zusätzlichen Abhängigkeiten aufgebaut werden. Es müssen die gleichen Sicherheits- und Betriebsregeln gelten wie im On-Prem-Betrieb. Betriebsort-Neutralität ohne Architekturbruch ist ein wesentliches Ziel virtualisierter Infrastrukturen.

Die gleiche Architektur kann betrieben werden:

- On-Premise
- in privaten oder souveränen Cloud-Umgebungen
- in hybriden Szenarien

ohne Anpassung der Sicherheitslogik, Änderung der Zugriffskontrollen und Verlust der Wiederherstellungsfähigkeit. Souveränität entsteht durch Architektur und Kontrolle, nicht durch den Ort des Betriebs.

### 5. Verantwortung und Kontrollpunkte im Betrieb

Auch bei Managed Services gilt uneingeschränkt:

- Sicherheitsverantwortung bleibt beim Auftraggeber
- Kontrollpunkte müssen technisch verankert sein
- Betriebszugriffe sind zu beschränken und zu protokollieren
- privilegierte Zugriffe sind streng zu regulieren

Managed Services dürfen den Betrieb standardisieren, Fachbereiche entlasten, Verfügbarkeit erhöhen. Managed Services dürfen nicht die Verantwortung verwischen, Kontrollmechanismen umgehen und Wiederherstellungsfähigkeit schwächen.

### 6. Wiederherstellungsfähigkeit als verbindliche Betriebsanforderung

Ein zentrales Bewertungskriterium für Managed-Service- und Cloud-Modelle ist die Wiederherstellungsfähigkeit. Diese muss technisch abgesichert sein, unabhängig vom Betriebsort funktionieren und regelmäßig überprüfbar sein.

Wiederherstellung ist damit kein Zusatzservice, sondern integraler Bestandteil des Betriebsmodells.

### 7. Deutschland-Stack Kontext

Im Deutschland-Stack ergibt sich eine klare, nicht verhandelbare Struktur:

- Sicherheit definiert Zugriff, Kontrolle und Schutzbedarf
- Virtualisierte softwarebasierte Infrastruktur setzt diese Anforderungen technisch um
- Managed Services & Cloud sind die kontrollierte Betriebsform dieser Architektur
- Resilienz und Wiederherstellung sind integraler Bestandteil des Betriebs
- Managed Services und Cloud sind Mittel zum Zweck - nicht das Ziel.

## 5.3 IT-Sicherheit (besser Informations- und Cyber-Sicherheit)

### 5.3.1 Begriffsdefinition

Grundsätzlich stellt sich die Frage, warum in den Dokumenten zum Deutschland-Stack durchgehend von "IT-Sicherheit" die Rede ist. Mit den aktuellen Gesetzgebungen (wie etwa NIS2) wird durchgehend der standardisierte Begriff "Informationssicherheit" genutzt, der "IT-Sicherheit" umfasst. IT-Sicherheit ist in der heute üblichen Sprechweise etwa des BSI lediglich die Sicherheit von informationstechnischen Komponenten.

Informationssicherheit umfasst dabei auch die kryptographische Sicherheit (siehe dazu auch weiter unten). Nicht umfasst sind allerdings die Aspekte der modernen Cyber-Sicherheit, soweit sie z.B. die Sicherheit von Netzwerkinfrastrukturen im Großen, die internationale Cyber-Sicherheitslage und Ähnliches betreffen.

Es wird daher empfohlen, durchgehend die Begrifflichkeit "Informations- und Cyber-Sicherheit" zu nutzen.

### 5.3.2 Konkrete Anmerkungen

Informations- und Cyber-Sicherheit ist angesichts der massiven Bedrohungslage durch fremde Mächte und organisierte Kriminalität eine essentielle Querschnittstechnologie, die in allen Standards und Technologien des Deutschland-Stack Anwendung finden muss.

Dazu bedarf es nicht nur einer Benennung einzelner IT-Sicherheitsstandards (AES, RSA, ML-KEM) und Protokolle (OAuth, OICD, JWT) sondern vielmehr einer alle Ebenen des Deutschland-Stack durchdringenden Informationssicherheitsmethodik, die den zukünftigen Nutzern des Deutschland-Stack unmittelbar zur Verfügung steht, beziehungsweise bei der Entwicklung und dem Betrieb der Technologiebausteine Berücksichtigung findet.

All dies ist in der derzeitigen Version des Deutschland-Stack nicht gegeben und fällt massiv hinter die Vorgehensweise zurück, die bereits in vergangenen Jahren im Rahmen der IT-Konsolidierung Bund sowie der IT-Sicherheitsstandards des IT-Planungsrat für die öffentliche Verwaltung beschlossen wurde.

Um ein angemessenes Sicherheitsniveau des Deutschland-Stack nachhaltig zu gewährleisten, müssen daher auf allen Ebenen des Stack Sicherheitsmaßnahmen umgesetzt werden, die die jeweils einwirkenden Sicherheitsrisiken mitigieren können.

Dazu gehören auch die in der Strategie benannten Umsetzungsvorschläge, jedoch werden wesentlich mehr Maßnahmen umzusetzen sein, damit der Deutschland-Stack nach Stand der Technik abgesichert wird und auch abgesichert bleibt, denn die Bewertung von Technologien und Services hinsichtlich Informationssicherheit kann immer sich immer nur auf einen gegebenen Zeitpunkt und Stand beziehen und muss daher grundsätzlich als kontinuierlicher Prozess verstanden und umgesetzt werden.

Um den jeweils gültigen Stand der Technik zu erreichen, ist eine Fülle von Standards, Normen, Gesetze und Verordnungen zu beachten. Aus diesen ergeben sich dann technische und organisatorische Maßnahmen, die umgesetzt werden sollten oder müssen, um das der aktuellen Gefährdungslage entsprechende und ausreichende Sicherheitsniveau zu garantieren und damit die Vertraulichkeit, die Integrität und die Verfügbarkeit zu sichern.

### *5.3.3 Normen, Standards und regulatorische Anforderungen*

Im Folgenden werden einzelne Normen, Standards und regulatorische Anforderungen genannt:

**ISO/IEC 27001 (Informationssicherheits-Managementsysteme)**
Cloud-Anbieter und Unternehmen, die Cloud-Dienste nutzen, können durch die Zertifizierung nach ISO/IEC 27001 nachweisen, dass sie ein ISMS implementiert haben, welches auch Cloud-spezifische Sicherheitsanforderungen berücksichtigt.

**ISO/IEC 27017 (Cloud-Sicherheit)**
Diese Norm bietet spezifische Empfehlungen für die Informationssicherheit im Cloud-Computing-Umfeld. Sie ergänzt ISO/IEC 27001 und enthält Cloud-spezifische Sicherheitsmaßnahmen und Best Practices.

**IT-Grundschutz (BSI)**
Der BSI IT-Grundschutz ist ein umfassendes Rahmenwerk zur Informationssicherheit, das vom Bundesamt für Sicherheit in der Informationstechnik entwickelt wurde. Es bietet konkrete Maßnahmen zur Absicherung von IT-Systemen und ist damit auch eine Umsetzungsvariante für die ISO 27001-Umsetzung.

**C5 - Cloud Computing Compliance Criteria Catalogue (BSI)**
Der C5-Katalog wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt und dient als Compliance-Katalog für Cloud-Anbieter, um die Anforderungen an die IT-Sicherheit in Cloud-Umgebungen zu erfüllen. Dabei enthält der C5-Katalog detaillierte Sicherheitsvorgaben, die Cloud-Anbieter befolgen müssen, wenn sie Dienstleistungen in Deutschland anbieten oder für deutsche Unternehmen tätig sind. Er orientiert sich auch an den o.g. internationalen Standards wie ISO/IEC 27001 und dem IT-Grundschutz des BSI.

**ISO/IEC 27018 (Schutz personenbezogener Daten in der Cloud)**
Diese Norm fokussiert sich auf den Schutz personenbezogener Daten in Cloud-Umgebungen, insbesondere in Bezug auf den Umgang mit personenbezogenen Daten. Datenschutzanforderungen gemäß der Datenschutz-Grundverordnung (DSGVO) und anderen regulatorischen Anforderungen können auf Basis dieser Norm umgesetzt werden.

**PCI DSS (Payment Card Industry Data Security Standard)**
Da auch Payment als Bestandteil des Deutschland-Stack umgesetzt werden soll, müssen die Standards der Kreditwirtschaft beachtet werden. Ein relevanter Standard ist PCI DSS. Es ist der Standard zur Sicherheit von Zahlungskarteninformationen, der Anforderungen für die sichere Speicherung, Verarbeitung und Übertragung von Kreditkartendaten. Sollten weitere Payment-Varianten angewandt werden müssen die jeweiligen Anforderungen für die genutzten Payment-Verfahren beachtet werden.

**Bundesdatenschutzgesetz (BDSG) und Datenschutz-Grundverordnung (DSGVO)**
Die DSGVO hat unmittelbaren Rechtscharakter in allen EU-Mitgliedsländern und regelt den Datenschutz für alle Bürger in der Europäischen Union. Cloud-Anbieter müssen sicherstellen, dass sie die Anforderungen der DSGVO erfüllen, insbesondere hinsichtlich der Datenverarbeitung, Speicherung und des Zugriffs auf personenbezogene Daten. Für Cloud-Dienste, die personenbezogene Daten aus der EU speichern oder verarbeiten, ist die DSGVO unverzichtbar.

Das BDSG regelt in Deutschland den Datenschutz auf nationaler Ebene und ergänzt die europäische DSGVO hinsichtlich der Umsetzung. Es behandelt die Rechte von Einzelpersonen bezüglich der Erhebung, Verarbeitung und Speicherung personenbezogener Daten.

**NIS 2.0-Richtlinie und zugehörige nationale Umsetzungs-Gesetze und weitere Verordnungen**
Die NIS 2.0-Richtlinie hat ebenfalls Auswirkungen auf Cloud-Dienste, insbesondere für diejenigen, die kritische Infrastrukturen oder wichtige digitale Dienste wie auch die Bundesverwaltungen bereitstellen. Die Hauptforderungen beinhalten auch strengere Sicherheitsvorgaben, und ein stark fokussiertes Risikomanagement. Im Deutschland-Stack müssen die entsprechenden Anforderungen in Form von Sicherheitsarchitekturen und Compliance-Strategien berücksichtigt werden.

**eIDAS-Verordnung**
Da u.a. auch die EUDI-Wallet verwendet werden soll, gilt auch die eIDAS-Verordnung, die die elektronische Identifikation und (qualifizierten) Vertrauensdienste in der EU reguliert und Anforderungen an die Nutzung der jeweiligen Dienste definiert. Die Cloud-Anbieter, die elektronische Signaturen oder andere

vertrauenswürdige Dienste anbieten und nutzen, müssen sicherstellen, dass sie den Anforderungen der eIDAS-Verordnung entsprechen.

**Weitere einschlägige Technische Richtlinien des BSI**
Das BSI erarbeitet seit Jahren Technische Richtlinien und gibt über diese Rahmenwerke / Leitplanken für die Umsetzung von Sicherheitsmaßnahmen vor. Dazu zählen u.a. Verfahren, Algorithmen, technische Schnittstellenbeschreibungen, Prozessvorgaben usw.

Für die im Strategie-Papier definierten technischen Maßnahmen sind zahlreiche Richtlinien des BSI relevant und auch maßgeblich. In besonderem Maße gilt dies etwa für die Vorgaben zur Kryptographie (siehe unten). Als generelle Vorgehensweise und Methodik wird insbesondere vorgeschlagen, für einschlägige Technikfelder, für die bereits dedizierte und maßgebliche Vorgaben des BSI existieren, diese nicht in den Vorgaben zum Deutschland-Stack zu duplizieren, sondern hier jeweils konsequent die entsprechenden technischen Richtlinien des BSI zu referenzieren - nur so kann sichergestellt werden, dass stets der aktuell gültige Stand herangezogen wird und damit auch stets die aktuell gültige Sicht des BSI auf den Stand der Technik Berücksichtigung findet.

**Kryptographische Festlegungen**
Die hier getroffenen Festlegungen sind im Wesentlichen nicht kompatibel mit den derzeit vorliegenden Festlegungen und Vorgaben seitens des BSI in der Technischen Richtlinie TR-02102. Darüber hinaus sind Aussagen wie "AES und RSA für die Verschlüsselung von Kommunikation" technisch nicht korrekt, hier sind weitere Details festzulegen, da bei etwa falsch parametrisierter Nutzung dieser Mechanismen auch Schwachstellen entstehen können. Es wird daher empfohlen, hier lediglich auf die BSI-Vorgaben in Form der TR-02102 in aktuell gültiger Form zu referenzieren.

## *5.3.4 Allgemeines Fazit zu IT-Sicherheit und Fokusthemen*

Generell empfiehlt TeleTrusT, den Stand der Technik in Bezug auf IT-Sicherheit für den Deutschland-Stack dediziert anzupassen und in einem Projekt während der Phasen Spezifikation, Umsetzung, Test und Betrieb begleitend zu definieren und an gegebene Bedrohungen anzupassen. Hierzu ist ein vollständiges Sicherheitskonzept zu realisieren und insbesondere auch fortzuschreiben und eine umfassende Risikoanalyse umzusetzen, aber auch Sicherheitsanalysen der Umsetzungen usw. vorzunehmen.

Die folgenden Schwerpunkte geben einen ersten Überblick über die zu behandelnden Themen:

- Risikomanagement
- Datenklassifizierung und Datenschutz
- Zugriffs- und Identitätsmanagement (IAM)
- Netzwerksicherheit
- Technologische Sicherheit
- Verfügbarkeitsmanagement und Notfallwiederherstellung
- Sicherheitsvorfälle und Reaktion
- Compliance und rechtliche Anforderungen
- Verwaltung von Drittanbietern und Cloud-Partnern /-Lieferanten
- Überwachung und Auditing einschließlich Sicherheitsbewertung und -weiterentwicklung (Audits, Penetrationstests bzw. Schwachstellenanalysen)

Im Folgenden wird nochmals eine Brücke zwischen aufgeführten Elementen eines Sicherheitskonzepts und konkreten architektonischen Ableitungen geschlagen, um zu belegen, dass zahlreiche gewünschte Funktionalitäten des Deutschland-Stack nur im Zusammenspiel von Technologie, Governance und Infrastruktur entstehen können.

#### 5.3.4.1 Zugriffssicherheit als zentrale Sicherheitsmaßnahme

Die Zugriffskontrolle stellt die erste und zentrale Sicherheitslinie dar. Ziel ist es sicherzustellen, dass

- ausschließlich berechtigte Identitäten
- unter definierten Rahmenbedingungen
- auf klar abgegrenzte Ressourcen

zugreifen können. Grundlegende Prinzipien sind hierbei:

- kein implizites Vertrauen (Zero-Trust)
- kein pauschaler Netzwerkzugang
- keine System- oder Netzwerksichtbarkeit ohne explizite Autorisierung

Zugriffsentscheidungen erfolgen dabei stets

- identitätsbasiert
- gerätebezogen
- kontextabhängig
- zeitlich und funktional begrenzt.

Der Deutschland-Stack verfolgt keinen klassischen netzwerkzentrierten Sicherheitsansatz. Stattdessen wird ein ressourcen- und anwendungszentriertes Zugriffsmodell umgesetzt. Der Zugriff beschränkt sich ausschließlich auf

- explizit definierte Anwendungen
- klar abgegrenzte Dienste
- konkret freigegebene Daten oder Dokumente,

Für Nicht-autorisierte sind Netzsegmente, Systeme und Dienste sind nicht sichtbar und nicht erreichbar.

Dieser Ansatz reduziert die Angriffsfläche signifikant und begrenzt die Auswirkungen von Sicherheitsvorfällen strukturell.

**Mehrstufiges Kontrollmodell (Defense in Depth)**

Die Zugriffssicherheit folgt einem mehrstufigen Kontrollmodell im Sinne von Defense in Depth:

**Stufe 1 - Identitäts- und Kontextprüfung**
- eindeutige Identitätsfeststellung
- Prüfung des Gerätezustands
- Bewertung des Zugriffskontexts
- richtlinienbasierte Freigabe oder Ablehnung

**Stufe 2 - Kontrolle vor der Verbindungsherstellung**
- Entscheidung über den Aufbau einer Verbindung
- Definition zulässiger Zielressourcen
- Vermeidung unnötiger Kommunikationspfade

**Stufe 3 - Kontrolle innerhalb der Zielumgebung**
- kein freier Netzwerkzugang
- Zugriff ausschließlich auf freigegebene Ressourcen
- konsequente Durchsetzung des Least-Privilege-Prinzips
- Whitelist-basierte Zugriffskontrolle

**Dieses Kontrollmodell wirkt sowohl auf Seiten des zugreifenden Systems als auch innerhalb der Zielumgebung.**

#### 5.3.4.2 Rolle der Verschlüsselung innerhalb der Sicherheitsarchitektur

Verschlüsselung spielt zur Sicherstellung der Vertraulichkeit von Daten eine wesentliche Rolle und wird daher im Deutschland-Stack als ergänzende Schutzschicht eingesetzt, insbesondere

- bei der Datenhaltung
- beim Dateizugriff
- zum Schutz bei physischem Zugriff oder Datenabfluss.

Sie ersetzt jedoch ausdrücklich nicht

- Zugriffskontrollen
- Segmentierungsmechanismen
- Überwachungs-, Detektions- und Wiederherstellungsmechanismen.

#### 5.3.4.3 Resilienz und Wiederherstellungsfähigkeit

Für kritische Infrastrukturen ist neben der Prävention insbesondere die Wiederherstellungsfähigkeit sicherzustellen. Ein ausschließlich storage-basierendes Backup ist nicht ausreichend, da

- Produktiv- und Sicherungssysteme häufig denselben Angriffsraum nutzen
- identische Administrations- und Vertrauensdomänen bestehen
- Schadsoftware beide Ebenen gleichzeitig kompromittieren kann.

**Mehrstufige Backup-Architektur mit Trennprinzipien**

Eine resiliente Backup-Architektur im Sinne des Deutschland-Stack berücksichtigt folgende Grundsätze:

- klare Trennung von Produktiv- und Sicherungssystemen
- zeitlich begrenzte Erreichbarkeit von Sicherungsmedien
- logische und physische Trennung
- kontrollierte Auslagerung

Wesentliche Merkmale:

- großer lokaler Sicherungsbereich
- Sicherungsmedien, die nur für definierte Zeiträume aktiv sind
- vollständige Trennung nach Abschluss der Sicherung
- Möglichkeit der physischen Auslagerung

**Diese Architektur reduziert das Risiko flächendeckender Kompromittierungen und ermöglicht Wiederherstellung auch nach schweren Sicherheitsvorfällen.**

**Leistungsfähigkeit als Voraussetzung für Resilienz**

Eine ausreichende Leistungsfähigkeit der Sicherungssysteme ist zwingende Voraussetzung, um

- regelmäßige Sicherungen großer Datenmengen durchzuführen
- Backup-Fenster kurz zu halten
- zeitnahe Wiederherstellungen zu ermöglichen.

**Hohe Sicherungs- und Wiederherstellungsleistungen tragen damit direkt zur Aufrechterhaltung der Betriebsfähigkeit bei.**

#### 5.3.4.4 Infrastruktur als Sicherheitsgrundlage

Die zugrunde liegende Infrastruktur bildet die technische Basis für Sicherheit, Verfügbarkeit und Resilienz.

Moderne, integrierte Infrastrukturen ermöglichen

- Weiterbetrieb bei Ausfall einzelner Komponenten
- system- und datenbasierte Redundanz
- stabile Betriebsbedingungen für sicherheitskritische Anwendungen.

Mechanismen zur verteilten Datenhaltung und -kodierung reduzieren das Risiko von Datenverlusten und erhöhen die Fehlertoleranz.

Auch Aspekte wie Virenschutz, Endpunktsicherheit und Netzwerksicherheit im Allgemeinen zahlen auf die Infrastruktursicherheit ein.

# 6 Tech-Stack-Landkarte als Orientierung

Im Kontext der Tech-Stack-Landkarte wären aus TeleTrusT-Sicht die folgenden Ergänzungen sinnvoll:

- Keycloak
- SAML (zur Verwendung existierender Authentifizierungsdienste)

Des Weiteren werden auch Systeme für folgende Funktionalitäten benötigt SIEM, IDS/IPS, Firewalls, Backup, Key Management. Diese sind noch nicht berücksichtigt.

Weitere Protokolle sind sinnvoll zu nutzen:

- NTP/NTS
- Syslog

HTTP sollte zu grundsätzlich zu HTTPS geändert werden, auch wenn TLS extra dargestellt wurde. Unsichere Protokolle wie http sollten nur in begründeten Ausnahmefällen verwendet, generell aber vermieden werden.

Hinsichtlich des Monitoring Stack gibt es weitere Komponenten, die betrachtet werden sollten:

1. Metriken (Sammlung & Speicherung)

- Prometheus → der De-facto-Standard für Metriken-Sammlung im Cloud-Native-Umfeld, Pull-basiert mit PromQL als Abfragesprache
- Alternative: VictoriaMetrics → Prometheus-kompatibel, aber ressourcenschonender bei großen Datenmengen

2. Visualisierung

- Grafana → der Platzhirsch, unterstützt praktisch alle Datenquellen (Prometheus, InfluxDB, usw.)
- Alternative: Kibana → primär für OpenSearch-Daten

3. Logs (Sammlung & Auswertung)

- Loki → von Grafana Labs, "Prometheus für Logs", "lightweight" und gut integriert mit Grafana
- Alternative: OpenSearch
- Alternative: Fluentd / Fluent Bit Log-Shipper, sammelt Logs von verschiedenen Quellen ein
- Alternative: Logstash → Teil des klassischen ELK-Stack, transformiert und routet Logs

4. Alerting

- Alert Manager → gehört zum Prometheus-Ökosystem, Deduplizierung, Gruppierung, Routing zu verschiedenen Kanälen
- Alternative: Grafana Alerting → direkt in Grafana integriert; Alerting über verschiedene Datenquellen

Eine häufige Kombination wäre also Prometheus + Loki + Grafana + Alertmanager oder alternativ OpenSearch, Logstash, Kibana (ELK).

**Authentifizierungsfunktionen**
Um eine schnelle Integration der Authentifizierung von Nutzern im Deutschland-Stack zu realisieren, sollten die Anwender die Möglichkeit haben, vorhandene Authentisierungsdienste über "Mein Unternehmenskonto", Elster-Anmelde-Funktionen via Zertifikate, ElsterSecure usw. als auch BundID oder eID-Funktion des Personalausweises und perspektivisch die European Digital Identity Wallet (EUDIW) zu verwenden.

# 7 Fazit und nächste Schritte

Aus Sicht von TeleTrusT stellt der Deutschland-Stack eine wesentliche Initiative dar, um die digitale Infrastruktur insbesondere im Public Sector resilient, skalierbar und zukunftsfähig aufzustellen.

Insofern begrüßt TeleTrusT sowohl das Vorhaben selbst als auch den gewählten Weg der Konsultation mit einer breiten Einbeziehung aller relevanten Stakeholder ausdrücklich.

In dem vorliegenden Kommentierungs- und Positionspapier wird neben zahlreichen inhaltlichen Kommentierungen, Ergänzungen und Anmerkungen aber auch dargestellt, dass der Deutschland-Stack mehr sein muss als eine reine "Ansammlung" technischer Standards, Module und Services.

TeleTrusT ist aus Erfahrung überzeugt, dass die gewünschten Anforderungen an den Deutschland-Stack nur dann erfüllt werden können, wenn neben den erforderlichen technischen Festlegungen auch ein Betriebs-, Governance- und Infrastrukturmodell entwickelt wird, das die unterschiedlichen technischen Elemente verbindet.

Dies gilt insbesondere für den Bereich der Informations- und Cyber-Sicherheit, genauso aber auch für notwendige Elemente wie Skalierbarkeit, Verfügbarkeit und Resilienz. All dies sind Eigenschaften, die sich nicht allein durch das Zusammenfügen geeigneter Technologien und Standards ergeben, sondern sie erfordern ein geeignetes Zusammenspiel und Zusammenwirken von Technologie, Infrastruktur und Governance. Dies kann nur erreicht werden, wenn all das bereits von Anfang an konsequent in den Architekturzielen und -prinzipien mitgedacht wird. Eine konsequente Ende-zu-Ende Betrachtung unterstützt dies.

TeleTrusT regt weiterhin eine Klärung der Verbindlichkeit der Umsetzung der Vorgaben des Deutschland-Stack für die verschiedenen Stakeholder an (insbesondere Bund, Länder und Kommunen). Dabei ist aus Sicht von TeleTrusT die Verbindlichkeit der Vorgaben des Deutschland-Stack zur Informations- und Cyber-Sicherheit von besonderer Relevanz.

TeleTrusT begrüßt die Einführung des Deutschland-Stack durch das BMDS nachdrücklich und bietet für den weiteren Prozess aktive und intensive Mitwirkung insbesondere zu den folgenden Punkten an:

- **Weitere inhaltliche Zuarbeit, insbesondere zu den Themenfeldern Informations- und Cyber-Sicherheit, Architekturprinzipien, Infrastruktur und Governance**
- **Kontinuierliche Mitwirkung im Prozess der Weiterentwicklung und Pflege des Deutschland-Stack**
- **Durchführung eines Workshops mit dem BMDS zur Detaillierung der Kommentare und Ausarbeitung weiterer Konzepte und Details**

# 8 Anhang: Leitfragen des BMDS

**Frage 1: Gibt es pragmatische Umsetzungsbedingungen, die ergänzt werden müssen?**

**Antwort: Ja, es gibt mehrere pragmatische Umsetzungsbedingungen, die ergänzt bzw. verbindlich gemacht werden müssen.**

**Zentrale Ergänzungsbedarfe (pragmatisch)**

1. Verbindliches Target Operating Model (TOM)
   - Einheitliches Zielbild für Technologie, Governance, Betrieb und Sicherheitsverantwortung über Bund, Länder, Kommunen.
   - Ohne dieses Modell bleibt der Stack eine technische Liste statt ein betreibbares System.

2. Verbindliche Sicherheits-Governance über den Lebenszyklus
   - Durchgängige Methodik für Informations- und Cyber-Sicherheit von Spezifikation bis Betrieb/Weiterentwicklung.
   - Inklusive Risikoanalyse, Audits, kontinuierlicher Verbesserungszyklus, Sicherheitsanalysen.

3. Architekturprinzipien als verpflichtende Entscheidungskriterien
   - Nicht nur "wünschenswert", sondern verbindlich:
     Skalierbarkeit, Verfügbarkeit, Fehlertoleranz, Automatisierung, Portabilität, Resilienz, Beherrschbarkeit.
   - Leitprinzip: "nur so komplex wie nötig".

4. Konsolidierte Standards- und Compliance-Referenz
   - Klare, einheitliche Referenzierung relevanter Rahmenwerke (u. a. ISO 27001/27017/27018, IT-Grundschutz, C5, DSGVO, NIS2, eIDAS).
   - Bei Kryptografie pragmatisch: nicht eigene Detailregeln duplizieren, sondern auf aktuelle BSI-Richtlinien (insb. TR-02102) referenzieren.

5. Nachweisbare Resilienz-/Recovery-Anforderungen
   - Wiederherstellung als verbindliche Betriebsanforderung, nicht als Zusatz-Feature.
   - Getrennte Backup-Domänen, regelmäßige Tests, technische Nachweise (RTO/RPO-orientiert), Protokollierung.

6. Klare Rollen, Verantwortlichkeiten und Kontrollpunkte
   - Auch bei Managed Services/Cloud bleibt Verantwortung beim Auftraggeber.
   - Technische Durchsetzung von Zugriffen, privilegierten Rechten, Protokollierung und Prüfbarkeit.

7. Umsetzungsreife durch Referenzimplementierungen/PoCs
   - Gemeinsame PoCs mit messbaren Erfolgskriterien:
     Sicherheit, Betriebsfähigkeit, Interoperabilität, Wiederherstellbarkeit, Skalierung.
   - Damit wird aus Strategie eine belastbare Umsetzung.

8. Vollständigere technische Basis in der Stack-Landkarte
   - Ergänzung fehlender Praxisbausteine (z.B. SIEM, IDS/IPS, Key Management, Backup, Firewalls, Monitoring-Stack, sichere Protokolle wie HTTPS/NTS/Syslog).

9. Kompetenz- und Betriebsfähigkeit sichern
   - Nicht nur Technologieauswahl, sondern ausreichende personelle/organisatorische Fähigkeiten für Betrieb, Sicherheit, Migration und Wechselfähigkeit.

10. Verbindlichkeit im Föderalmodell klären
    - Der Text fordert ausdrücklich Klärung, wie verpflichtend Vorgaben für Bund/Länder/Kommunen sind (inkl. rechtlich tragfähiger Rahmenbedingungen).

**Fazit:**

Ja, zusätzliche pragmatische Umsetzungsbedingungen sind notwendig, vor allem Verbindlichkeit, Governance, klare Verantwortlichkeiten, operationalisierte Sicherheits- und Recovery-Nachweise sowie föderal belastbare Standardisierung. Ohne diese Ergänzungen drohen die benannten Risiken wie höhere Komplexität, mehr Abhängigkeiten, steigende Kosten und geringere Krisenfestigkeit.

**Frage 2: Passt die Ausrichtung der Standards und Technologien zu den strategischen Zielen?**

**Antwort: Ja - aber nur teilweise und nur unter klaren Bedingungen.**

Die Ausrichtung von Standards und Technologien passt grundsätzlich zu den strategischen Zielen (Souveränität, Sicherheit, Interoperabilität, Zukunftsfähigkeit, Resilienz), wenn sie nicht als reine Tool-/Bausteinliste verstanden wird, sondern als verbindlich gesteuertes Gesamtmodell.

**Warum es grundsätzlich passt**

Die Kommentare zeigen eine klare strategische Linie:

- **Souveränität als Steuerungsfähigkeit** statt Label (Kontrolle über Daten, Zugriffe, Betriebsprozesse, Exit-/Wechselfähigkeit).
- **Interoperabilität** über offene Schnittstellen und API-First.
- **Zukunftsfähigkeit** durch kontinuierliche Modernisierung, Einbindung neuer Standards und Kryptoagilität.
- **Sicherheit** als durchgängige Informations- und Cyber-Sicherheitsmethodik (nicht punktuelle IT-Sicherheitsmaßnahmen).
- **Resilienz/Verfügbarkeit** als Architekturziel (Redundanz, Wiederherstellbarkeit, Fehlertoleranz).
- **Nachhaltigkeit/Marktrelevanz** durch mehrere Anbieter, Nachnutzbarkeit und föderale Umsetzbarkeit.

Damit sind die strategischen Ziele und die gewünschte Technologieausrichtung **inhaltlich konsistent**.

**Wo die Passung aktuell noch nicht vollständig ist**

Es bestehen an den folgenden Stellen Lücken in der aktuellen Ausprägung:

1. **Zu starke Technologiekatalog-Logik**
   Es fehlt ein verbindliches Target Operating Model aus Architektur, Governance, Betrieb und Verantwortung.
2. **Sicherheitsrahmen nicht durchgängig genug**
   Einzelstandards (z.B. AES/RSA, OAuth/OIDC/JWT) reichen nicht; nötig ist ein lifecycle-basiertes Sicherheitsmanagement mit Risiko-, Audit- und Verbesserungszyklus.
3. **Teilweise unklare/inkonsistente Standardreferenzen**
   Insbesondere bei Kryptografie wird auf bessere Anbindung an aktuelle BSI-Vorgaben (TR-02102) hingewiesen.
4. **Komplexitätsrisiko**
   Ohne ganzheitliche Infrastruktur droht ein "Flickenteppich", der Sicherheit, Betrieb und Skalierung verschlechtert.
5. **Cloud/Managed Services missverstanden**
   Der Text betont: Das sind Betriebsmodelle, keine Sicherheitsgarantie. Sicherheit entsteht durch Architektur und technische Kontrollpunkte.

**Fazit:**

Die Ausrichtung passt **strategisch in der Zielrichtung**, aber die **operative Passung** ist noch **unvollständig**. Sie wird erst dann wirklich stimmig, wenn:

- Architekturprinzipien verbindlich gemacht werden (Resilienz, Portabilität, Beherrschbarkeit, "nur so komplex wie nötig"),
- Sicherheits- und Compliance-Governance durchgängig umgesetzt wird,
- Standards konsolidiert und aktuell referenziert werden,
- und skalierbare Referenzimplementierungen den Ansatz praktisch validieren.

Wenn diese Punkte umgesetzt werden, ist die Ausrichtung von Standards und Technologien **klar kompatibel** mit den strategischen Zielen des Deutschland-Stack.

**Frage 3: Sind die priorisierten Technologiefelder mit den relevanten Technologien und Standards für den Deutschland-Stack unterlegt?**

**Antwort: Nur teilweise. Die priorisierten Technologiefelder sind zwar benannt und inhaltlich gut beschrieben, aber in der aktuellen Ausprägung noch nicht durchgängig und konsistent mit den notwendigen Technologien/Standards unterlegt.**

**Was bereits unterlegt ist**

- **Virtualisierte softwarebasierte Infrastruktur** ist als Kernfeld konkretisiert (Compute/Storage/Netzwerk/Firewall/Load-Balancing, Containerplattformen wie Kubernetes, Zero-Trust-Mechanismen, Backup/Recovery als Infrastruktur-Service, kontrollierte Hardware).
- **Managed Services und Cloud** werden als Betriebsmodelle klar eingeordnet und mit Anforderungen hinterlegt (Rollen-/Rechtetrennung, Protokollierung, technische Durchsetzung von Policies, Wiederherstellbarkeit - unabhängig vom Betriebsort).
- Informations- und Cyber-Sicherheit wird umfassend strukturiert (Risikomanagement, IAM, Netzwerksicherheit, Incident Response, Audits/Pentests, Compliance).

**Wo die Unterlegung noch fehlt oder unzureichend ist**

- TeleTrusT kritisiert, dass der Stack derzeit **zu sehr wie eine Bausteinliste wirkt** und eine **durchgängige Methodik** fehlt (v. a. für Informations- und Cyber-Sicherheit über den gesamten Lebenszyklus).
- Bei **Kryptografie** wird explizit bemängelt, dass die bisherigen Festlegungen **nicht kompatibel bzw. zu unpräzise** sind und stattdessen **konsequent auf BSI TR-02102** (aktueller Stand) referenziert werden sollte.
- In der **Tech-Stack-Landkarte** fehlen aus TeleTrusT-Sicht wichtige Komponenten, z.B**. SIEM, IDS/IPS, Firewalls, Backup, Key Management**, außerdem Ergänzungen wie **Keycloak** und **SAML** sowie Protokolle wie **NTP/NTS**, **Syslog** und die klare Vorgabe **HTTPS** statt **HTTP**.
- Für Interoperabilität wird zwar **API-first** gefordert, aber es wird impliziert, dass die verbindliche, föderal umsetzbare **Standardisierung/Governance** noch nicht ausreichend konkret ist.

**Fazit:**

Die priorisierten Technologiefelder sind **in Teilen** mit relevanten Technologien und Standards unterlegt (vor allem Infrastruktur, Betriebsmodelle, Sicherheitsprinzipien), aber **noch nicht vollständig**: Es fehlen **zentrale Security- und Betriebsbausteine**, eine **konsolidierte Standardreferenz** (insbesondere Kryptografie nach BSI) und eine **durchgängige, verbindliche Methodik** statt punktueller Nennungen.

**Bundesverband IT-Sicherheit e.V. (TeleTrusT)**

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.