IT-Planungsrat

Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur

- Version 1.0 vom 13. August 2021 -

08/2021

Impressum

Herausgeber

FITKO (Föderale IT-Kooperation)

Zum Gottschalkhof 3

60594 Frankfurt am Main

E-Mail: poststelle@fitko.de

Anstalt des öffentlichen Rechts | Präsidentin: Dr. Annette Schmidt

Ansprechpartner

Referat DG II 2 „Digitale Souveränität für die IT der öffentlichen Verwaltung“

Bundesministerium des Innern, für Bau und Heimat

Postanschrift: Alt-Moabit 140, 10557 Berlin

Hausanschrift: Salzufer 1 (Zugang Englische Straße), 10587 Berlin

E-Mail: DGII2@bmi.bund.de

www.cio.bund.de

Stand

August 2021

Inhaltsverzeichnis

1 Einführung

In der 33. Sitzung des IT-Planungsrates (IT-PLR) wurde das Konzeptpapier zur *Deutschen Verwaltungscloud-Strategie – Föderaler Ansatz* beschlossen (Entscheidung 2020/54)[1]. Die Maßnahme ist Teil der beschlossenen Strategie zur Stärkung der Digitalen Souveränität der IT der Öffentlichen Verwaltung (ÖV)[2] und ist dem definierten Lösungsansatz „*Herstellerunabhängige Modularität, (offene) Standards und Schnittstellen in der IT*“ zugeordnet. Digitale Souveränität wird hier definiert als „*die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“*[3].

Die im Oktober 2020 durch den IT-PLR beschlossene Deutsche Verwaltungscloud-Strategie (DVS) soll gemeinsame Standards und offene Schnittstellen für Cloud-Lösungen der ÖV schaffen, um übergreifend eine interoperable sowie modulare föderale Cloud-Infrastruktur zu etablieren.

Neben der anhaltenden Marktentwicklung eines zunehmenden Einsatzes von Cloud-Lösungen, existieren bereits eine Vielzahl von Cloud-Lösungen innerhalb der föderalen Verwaltungsebenen von Bund, Länder und Kommunen. Aufgrund fehlender Standardisierung in einzelnen Cloud-Architekturschichten sind die bestehenden föderalen Cloud-Lösungen jedoch, wenn überhaupt, nur eingeschränkt interoperabel und kompatibel. Primäres Ziel der DVS ist die Möglichkeit einer Cloud-übergreifenden und wechselseitigen Nutzung von Anwendungen (Softwarelösungen). Außerdem wird mit der DVS angestrebt, kritische Abhängigkeiten von Anbietern durch standardisierte, modulare IT-Architekturen zu reduzieren.

Mit dem Beschluss 2020/54 des IT-PLR wurde die Arbeitsgruppe *Cloud-Computing und Digitale Souveränität* (kurz: AG Cloud) beauftragt, die Zielarchitektur der DVS zu erarbeiten. Die AG Cloud hat auf Grundlage der Entscheidung des IT-PLR die technische Konzeption und

---

[1] Siehe Entscheidung 2020/54 – AG Cloud-Computing und Digitale Souveränität https://www.it-planungsrat.de/beschluesse/beschluss/ag-cloud-computing-und-digitale-souveraenitaet-1.

[2] Siehe Entscheidung 2021/09 – AG Cloud-Computing und Digitale Souveränität https://www.it-planungsrat.de/beschluesse/beschluss/ag-cloud-computing-und-digitale-souveraenitaet.

[3] Definition gem. Studie zum Thema „Digitale Souveränität“ der Kompetenzstelle Öffentliche IT (ÖFIT).

Operationalisierung an die Unterarbeitsgruppe (UAG) *Technik & Betrieb* übergeben. In dieser UAG sind insbesondere IT-Dienstleister der ÖV vertreten. Dies gewährleistet frühzeitig die technische Umsetzbarkeit.

Zur gezielten Bearbeitung des Arbeitsauftrages und entsprechend der Standardisierungsbereiche sowie Anforderungen im DVS-Konzeptpapier[4] gliedert sich die UAG, anhand von acht Handlungsfeldern, in folgende operative Teams:

- Handlungsfeld 1+4 „Infrastruktur und Schnittstellen“[5]
- Handlungsfeld 2 „Policies / Governance“
- Handlungsfeld 3 „Cloud-Service-Portal“
- Handlungsfeld 5 „Entwicklungsumgebung“
- Handlungsfeld 6 „Betriebsmodell“
- Handlungsfeld 7 „Code Repository“
- Handlungsfeld 8 „Proof-of-Concepts”

Ausgehend von dem DVS-Konzeptpapier wurden detailliertere, operative Ziele je Handlungsfeld formuliert. Anschließend wurden mithilfe von Anwendungsszenarien (sog. „Use Cases“) innerhalb der einzelnen Handlungsfelder Anforderungen an die Architektur erhoben. Basierend auf den ermittelten Anforderungen sowie den operativen Zielen wurde die erforderliche Systematik bzw. der grundsätzliche Aufbau der Deutschen Verwaltungscloud[6] abgeleitet, aus dem die vorliegende Zielarchitektur spezifiziert wurde.

---

[4] Als „DVS-Konzeptpapier“ wird im Folgenden das beschlossene Dokument aus der Entscheidung 2020/54 bezeichnet, siehe https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-54_Deutsche_Verwaltungscloud_Strategie.pdf.

[5] Handlungsfeld 1 und 4 wurden aufgrund thematischer Überschneidungen zusammengelegt.

[6] Als „Deutsche Verwaltungscloud“ wird im Folgenden die standardisierte, föderale Cloud-Infrastruktur von Bund, Länder und Kommunen im Rahmen der beschlossenen Deutschen Verwaltungscloud-Strategie bezeichnet.

2 Ziele und Rahmenbedingungen

In diesem Kapitel werden grundlegende Ziele und Rahmenbedingungen der vorliegenden Zielarchitektur dargestellt. Insbesondere erfolgt eine Beschreibung der Zielgruppe sowie die Abgrenzung zu nahestehenden Vorhaben und relevanten Vorgaben innerhalb der ÖV.

2.1 Zielsetzung und Aufbau des Konzeptes

Das vorliegende Dokument zur Zielarchitektur der DVS kommt dem Auftrag des IT-PLR nach:

> *„Der IT-Planungsrat beauftragt die Arbeitsgruppe Cloud-Computing und Digitale Souveränität auf Grundlage der definierten Standardisierungsbereiche und den Anforderungen eine Zielarchitektur zu erarbeiten und dem IT-Planungsrat in der 34. Sitzung über den Fortschritt zu berichten."* (IT-PLR Entscheidung 2020/54)

Ziel des Dokumentes ist es, gemeinsame Standards für die föderale Cloud-Infrastruktur der ÖV und deren Standorte zu definieren. Die Spezifizierung der DVS, als Fortführung des beschlossenen Konzeptpapiers, bildet die Basis zur Umsetzung erster Pilotierungsprojekte (siehe Kapitel 6). Die Vorgaben unterstützen die, mit dem Eckpunkte[7]- und Strategiepapier[8], angestrebte offene, modulare und interoperable Ausrichtung der IT-Architektur. Ebenso ist die Schaffung föderaler Cloud-Strukturen für Bund, Länder und Kommunen ein zentrales Element des 9-Punkte Plans des Beauftragten der Bundesregierung für Informationstechnik.[9]

Der initiale Fokus des vorliegenden Rahmenwerks der Zielarchitektur sowie den darauf basierenden Pilotierungsprojekten (vgl. Kapitel 6.1) liegt auf der Schaffung einer Grundlage, um zukünftige Softwarelösungen einheitlich betreiben zu können und damit untereinander austauschbar zu machen. Die Weiterentwicklung, bspw. die Konzeptionierung des Cloud-Service-Portals sowie der Koordinierungsstelle (*Arbeitstitel*) (vgl. Kapitel 6.2 und 6.3), erfolgt stufenweise.

---

[7] Siehe https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-19_Entscheidungsniederschrift_Umlaufverfahren_Eckpunktepapier.pdf.

[8] Siehe https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf.

[9] Siehe https://www.onlinezugangsgesetz.de/SharedDocs/downloads/Webs/OZG/DE/9-punkte-plan.pdf?__blob=publicationFile&v=4.

Anforderungen und Vorgaben für Softwarelösungen beim Beschaffungsprozess sind nicht Fokus des vorliegenden Dokumentes und werden von der UAG *Beschaffung* als Teil der AG Cloud gesondert adressiert (vgl. Kapitel 2.3.2). Die Bereitstellung von Software-as-a-Service (SaaS) ergibt sich analog dem Betrieb und der Bereitstellung von Softwarelösungen durch Softwarebetreiber (vgl. Kapitel 4.3).

Die Inhalte des vorliegenden Dokumentes sind neben dem einleitenden Kapitel 1 wie folgt gegliedert:

- **Kapitel 2** „Ziele und Rahmenbedingungen" beschreibt die Ziele der DVS-Architektur, den Geltungsbereich und die Zielgruppe, abzugrenzende Vorgaben und Vorhaben sowie die kontinuierliche Weiterentwicklung des vorliegenden Dokumentes.
- **Kapitel 3** „Mehrwerte für die Öffentliche Verwaltung und deren IT-Infrastruktur" zeigt auf, welche vielseitigen Mehrwerte durch die DVS geschaffen werden können.
- **Kapitel 4** „Systematik der Deutschen Verwaltungscloud" erläutert die grundsätzlichen Elemente der Deutschen Verwaltungscloud und die betrachteten Rollen.
- **Kapitel 5** „Wesentliche Standards für Cloud-Standorte" definiert obligatorische und optionale Standards für Cloud-Standorte und spezifiziert ausgewählte Standards mit weiterführenden Erläuterungen.
- **Kapitel 6** „Weiteres Vorgehen" beinhaltet die Beschreibung der nachfolgenden Handlungsempfehlungen zur Deutschen Verwaltungscloud, die Skizzierung weiterführender Dokumente für die fortlaufende Spezifizierung und die initiale Erläuterung zum Cloud-Service-Portal sowie zur Koordinierungsstelle der Deutschen Verwaltungscloud.

2.2 Geltungsbereich und Zielgruppe

Mit dem geplanten Beschluss des vorliegenden Dokumentes durch den IT-PLR sollen die Architektur der Deutschen Verwaltungscloud sowie die entsprechenden Standards übergreifend für Bund, Länder und Kommunen sowie für deren IT-Dienstleister gültig werden.

Die Vereinheitlichung im Rahmen der DVS richtet sich an die bestehende wie auch neu zu schaffende föderale Cloud-Infrastruktur der ÖV und dabei insbesondere an die beteiligten IT-Dienstleister. Bei Teilnahme an der Deutschen Verwaltungscloud ist die Umsetzung der Standards

seitens der ÖV und deren IT-Dienstleister verpflichtend für die vorab definierten Infrastrukturbereiche der Rechenzentren (siehe dazu Cloud-Standorte in Kapitel 4.2).

Eine Abweichung von den festgelegten Standards ist nur in Ausnahmefällen gestattet und bedarf einer dokumentierten Begründung. Die Genehmigung erfolgt durch das zu etablierende Architekturboard und die damit verbundene Koordinierungsstelle (siehe Kapitel 6.3)[10].

2.3 Abgrenzung

Die im Rahmen der Deutschen Verwaltungscloud festgelegten Standards betten sich in bereits bestehende Vorgaben/Richtlinien für IT-Lösungen auf unterschiedlichen förderalen Ebenen ein. Gleichzeitig muss das Vorhaben zur Umsetzung der DVS klar von anderen Initiativen im Bereich Cloud-Computing abgegrenzt und mögliche Schnittmengen identifiziert werden. Zu diesem Zweck sind nachfolgend Erläuterungen zu nahestehenden Vorhaben und zu relevanten Vorgaben der ÖV aufgeführt. Es wird jeweils dargestellt, inwiefern die Deutsche Verwaltungscloud sich von diesen abgrenzt, bzw. darauf aufbaut/zurückgreift.

Zusammenfassend setzt die Deutsche Verwaltungscloud die verwaltungsspezifischen Vorgaben (insbesondere im Hinblick auf bestehenden Standards und Sicherheits-, Datenschutz- sowie Geheimschutzanforderungen) um und beachtet bei der Modernisierung der IT-Infrastruktur der ÖV neueste Entwicklungen im Cloud-Bereich. Die Deutsche Verwaltungscloud setzt dabei Standards für föderale Cloud-Lösungen und ist komplementär zur laufenden Umsetzung des Onlinezugangsgesetzes (OZG).

2.3.1 Nahestehende Vorhaben

Folgende Vorhaben mit Bezug zur ÖV und Fokus auf Cloud-Computing wurden bei der Zielarchitektur berücksichtigt:

[10] Eine Nachnutzung bereits bestehender föderaler Strukturen wird im Rahmen der Feinkonzeptionierung geprüft. Beispielsweise wäre die Eingliederung in das bereits durch den IT-Planungsrat eingerichtete föderale IT-Architekturboard (siehe https://www.fitko.de/it-architektur) grundsätzlich denkbar.

- **Cloud-Lösungen von Bund, Ländern und Kommunen (z. B. Bundescloud)**: Wie in Kapitel 1 angedeutet, bestehen bereits verschiedene Cloud-Lösungen (Infrastrucuture-as-a-Service, IaaS; Container-as-a-Service, CaaS; Platform-as-a-Service, PaaS; Software-as-a-Service, SaaS[11]) auf den unterschiedlichen Verwaltungsebenen von Bund, Länder und Kommunen.
- **Gaia-X**[12]: Das Vorhaben Gaia-X zielt darauf ab, eine föderierte, europäische Dateninfrastruktur zu schaffen, indem ein Verbundsystem von bestehenden Cloud- und Service-Anbietern auf der Basis einheitlicher Schnittstellen und Standards, den sogenannten „Federation Services", etabliert wird. Im Vordergrund stehen dabei vor allem gemeinsame Werte bzgl. Datensouveränität, Offenheit und Interoperabilität. Zum Aufbau dieses Ökosystems in Europa wird ein stringenter Open-Source (OS)-Ansatz verfolgt.
- **Sovereign Cloud Stack**[13] (SCS): Das Projekt SCS entwickelt einen föderierbaren und vollständig offenen Software-Stack für Cloud-Betreiber, damit diese herstellerunabhängig Cloud-Infrastruktur bereitstellen und betreiben können. Bei der Entwicklung werden bewährte, modulare Standard-Softwarekomponenten (z. B. Kubernetes) verwendet und Werkzeuge und Prozesse für den automatisierten Betrieb solcher Umgebungen implementiert. SCS liefert somit eine Infrastrukturkomponente für Gaia-X, die als vollständig souveräner technischer Unterbau dienen kann.
- **OZG-Umsetzung**[14]: Mit dem „Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen" werden Bund und Länder (und damit auch die Kommunen) verpflichtet, ihre Verwaltungsleistungen bis Ende 2022 digital anzubieten. Ein zentraler

---

[11] Für grundlegende Erläuterungen des Themengebietes Cloud-Computing siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html.

[12] Siehe https://www.gaia-x.eu.

[13] Siehe https://scs.community/index.html.de.

[14] Siehe https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-ozg/info-ozg-node.html.

> Grundsatz bei der OZG-Umsetzung ist das „Einer für Alle“ (EfA)-Prinzip. Dies bedeutet, dass einmal entwickelte Lösungen eines Landes in anderen Ländern nachgenutzt werden können, um arbeitsteilig und zeitsparend bei der Digitalisierung vorzugehen[15].

Bestehende Cloud-Lösungen der ÖV sowie die zugehörigen IT-Dienstleister müssen als Teilnehmer der Deutschen Verwaltungscloud die dort definierten Standards umsetzen. Damit werden vielschichtige Mehrwerte geschaffen, die ebenfalls die OZG-Umsetzung und das EfA-Prinzip unterstützen (siehe Kapitel 3). Perspektivisch sollen OZG und Deutsche Verwaltungscloud ineinandergreifen. Die OZG-Umsetzung bis Ende 2022 ist dabei jedoch nicht abhängig von dem Aufbau der Deutschen Verwaltungscloud und wird als paralleler Handlungsstrang angesehen. Während OZG Verwaltungsleistungen digitalisiert, soll die DVS die IT-Infrastruktur der ÖV zukunftsfähig ausrichten.

SCS ist für hohe Sicherheitsanforderungen konzipiert. Demnach ist im Projektplan des SCS vorgesehen, die Plattformbetreiber der ÖV für eine BSI-Zertifizierung nach IT-Grundschutz durch entsprechende Architektur, Entwicklungsprozesse und die Bereitstellung entsprechenden Betriebswissens zu unterstützen[16]. Die Kompatibilität der Deutschen Verwaltungscloud mit Gaia-X kann durch die Mitarbeit von SCS als Open Work Package im Gaia-X-Verbund erreicht werden. Auf diese Weise kann die ÖV mit der bestehenden IT-Infrastruktur perspektivisch am Gaia-X-Ökosystem teilhaben. Die DVS unterstützt den Auf- und Ausbau von Gaia-X, indem Interoperabilität sichergestellt wird, sodass perspektivisch Gaia-X Cloud- und Service-Angebote in der ÖV eingesetzt werden können. Deshalb sind Vertreter des Projektes SCS im regelmäßigen Austausch mit der UAG *Technik & Betrieb*. Gaia-X und dem vordergründigen Fokus auf der Etablierung eines verbesserten Datenaustausches mit gemeinsamen Datenräumen stellen eine Ergänzung zur DVS dar. Die Deutsche Verwaltungscloud soll vor allem die cloud-übergreifende Wiederverwendbarkeit von Softwarelösungen gewährleisten. Zukünftig könnten nach Fertigstellung (Teil-)Gebiete des SCS bzw. Standards von Gaia-X übernommen und für die Deutsche Verwaltungscloud nachgenutzt werden. Die Standards der Deutschen Verwaltungscloud werden dabei ihre Gültigkeit bewahren und lediglich entsprechend erweitert.

---

[15] Für weitere Ausführungen siehe auch https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/nachnutzung/efa/efa-node.html.

[16] Nach derzeitigem Planungsstand erscheint die Bereitstellung der notwendigen Komponenten und die parallelen Vorbereitungen für eine Zertifizierung bis Mitte 2022 realistisch.

2.3.2 Relevante Vorgaben der ÖV

Die folgenden Vorgaben/Richtlinien der ÖV wurden bei der Zielarchitektur betrachtet:

- **IT-Grundschutz**: Das IT-Grundschutz-Kompendium des BSI führt Methoden, Anleitungen und Empfehlungen auf, um das Niveau der Informationssicherheit in einer Institution anzuheben und aufrechtzuerhalten. Es wird dabei ein ganzheitlicher Ansatz verfolgt: Neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet. Das Kompendium wird jährlich in einer neuen Version veröffentlicht.
- **Kriterienkatalog Cloud Computing des BSI (kurz: C5)**[17]: Der Katalog spezifiziert Mindestkriterien an die Informationssicherheit für Cloud-Services, die nicht unterschritten werden sollten. Ziel ist die transparente Darstellung der Erfüllung von Kriterien an die Informationssicherheit eines Cloud-Services auf Basis einer standardisierten Prüfung. Der Prüfbericht kann von Kunden im Rahmen einer eigenen Risikoanalyse verwendet werden. Der Kriterienkatalog wird von Cloud-Anbietern, Auditoren und Cloud-Kunden verwendet.
- **Architekturrichtlinie für die IT des Bundes**[18]: Mit der Architekturrichtlinie für die IT des Bundes wird ein aktives Architekturmanagement für die IT der Bundesverwaltung verfolgt. Die von der IT-Konsolidierung Bund[19] betroffenen Bereiche sollen durch konkrete strategische Architekturvorgaben aktiv bei Entscheidungsprozessen unterstützt werden und die Vorgaben für die Weiterentwicklung der IT des Bundes nutzen. Außerdem unterstützen die Vorgaben eine Ausrichtung der laufenden IT-Projekte an die

[17] C5 - Cloud Computing Compliance Criteria Catalogue, siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf?__blob=publicationFile&v=2.

[18] Siehe https://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/architekturrichtlinie_it_bund_2020.pdf?__blob=publicationFile.

[19] Siehe https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/it-konsolidierung/it-konsolidierung-node.html.

strategischen Anforderungen und politischen Aufgaben. Beispiele für Architekturvorgaben sind u. a. Sicherstellung der Herstellerunabhängigkeit und Sicherstellung von loser Kopplung/Modularität.

- **Länderspezifische und kommunale Architekturrichtlinien/-vorgaben bzw. Mindestanforderungen für die IT**: Neben den Richtlinien des Bundes, wie obenstehend beschrieben, existieren ebenso länderspezifische Architekturvorgaben und Mindestanforderungen für die IT.
- **Föderale Architekturrichtlinien für die IT**[20]: Um eine einheitliche Architektur über alle föderalen Ebenen hinweg sicherzustellen und aktiv zu steuern, wurden föderale Architekturrichtlinien verfasst. Diese basieren auf den zuvor geschilderten Vorgaben des Bundes und der Länder.
- **Anforderungen an Technologieanbieter und -lösungen zur Stärkung der Digitalen Souveränität**[21]: Die AG Cloud und deren UAG *Beschaffung* definieren, als Teil der Strategie zur Stärkung der Digitalen Souveränität der IT der ÖV[22], übergreifende Anforderungen an die Beschaffung von Informations- und Kommunikationstechnik durch bzw. für die ÖV. Diese Anforderungen sollen die Abhängigkeit von einzelnen Anbietern reduzieren, indem sie einen Rahmen für IT-Leistungen und deren Anbieter für die ÖV, bei der Entwicklung und Bereitstellung von Lösungen, vorgeben. Unter anderem soll ein Mindestmaß von Interoperabilität, Modularität und Transparenz eingefordert werden.

Bestehende Vorgaben, wie bspw. die des BSI in Form des C5 oder IT-Grundschutzes, wurden bei der Ausarbeitung der Zielarchitektur weitestgehend berücksichtigt und konkretisiert. Etwaige Widersprüche einzelner Vorgaben werden im Rahmen der Standardisierung aufgelöst. Als Ergänzung zum Anforderungskatalog für Technologieanbieter und -lösungen zur Stärkung der Digitalen Souveränität, der nach außen gerichtet bei der Beschaffung von IT-Lösungen perspektivisch herangezogen werden soll, richten sich die hier definierten Standards nach innen

[20] Siehe https://www.fitko.de/it-architektur.

[21] In Erarbeitung durch die *AG Cloud Computing und Digitale Souveränität* und deren UAG *Beschaffung*.

[22] Siehe Entscheidung 2021/09 – AG Cloud-Computing und Digitale Souveränität https://www.it-planungsrat.de/beschluesse/beschluss/ag-cloud-computing-und-digitale-souveraenitaet.

und sollen die bestehende Cloud-Infrastruktur der ÖV einheitlich und zukunftsorientiert ausrichten.

2.4 Weiterentwicklung des Dokumentes

Die in Kapitel 5 aufgeführten Standards werden anlassbezogen, jedoch mindestens jährlich iterativ weiterentwickelt und mit einem gemeinsamen Beschluss im Rahmen der einzurichtenden Koordinierungsstelle und dem dazugehörigen Architekturboard (siehe Kapitel 6.3) verabschiedet. Anschließend wird der IT-PLR informiert. Ein Beschluss durch den IT-PLR soll lediglich bei wesentlichen Änderungen des vorliegenden Rahmenwerks stattfinden. Vorerst liegt die Zuständigkeit der Fortführung des Dokumentes weiterhin bei der AG Cloud und deren UAG *Technik & Betrieb*.

Die kontinuierliche Weiterentwicklung gewährleistet eine stets zeitgemäße Ausrichtung der Deutschen Verwaltungscloud und erlaubt eine flexible Anpassung an sich ändernde Anforderungen und Rahmenbedingungen wie z. B. Technologieentwicklungen. Einige Standards, zu denen es detaillierterer Ausführungen für eine Umsetzung bedarf, werden in Kapitel 5.3 näher beschrieben. Außerdem werden basierend auf der Systematik und der Standards weiterführende Dokumente erarbeitet, welche einerseits die technischen Realisierungen verdeutlichen sollen und andererseits zusätzliche Elemente der Deutschen Verwaltungscloud spezifizieren (siehe Kapitel 6). Abbildung 1 stellt die geplante Dokumentenstruktur dar und ordnet das vorliegende Rahmenwerk ein.

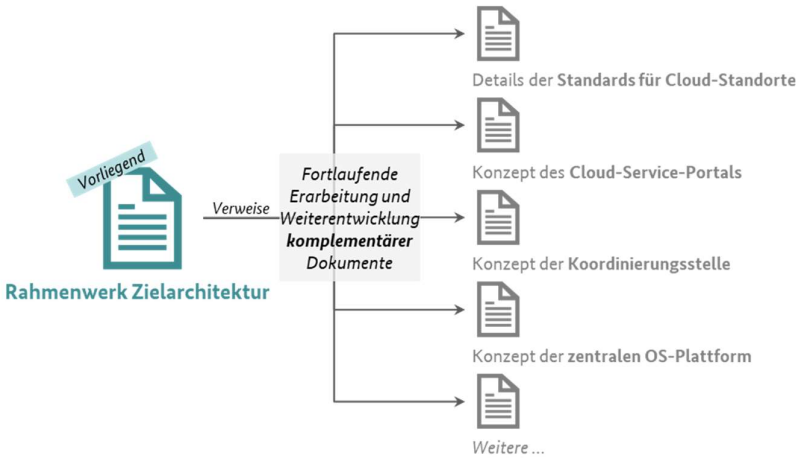

Abbildung 1: Dokumentenstruktur der DVS-Zielarchitektur

3 Mehrwerte für die Öffentliche Verwaltung und deren IT-Infrastruktur

Durch die im Rahmen der DVS angestrebten Vereinheitlichung von Betriebskonzepten, die Standardisierung der Infrastruktur- und Plattformbereitstellung sowie die Etablierung von einheitlichen Schnittstellen föderaler Cloud-Lösungen, werden zahlreiche Mehrwerte für die ÖV geschaffen (vgl. Abbildung 2). Diese Mehrwerte basieren auf den strategischen Zielen zur Stärkung der Digitalen Souveränität[23] sowie auf den definierten Zielen des DVS-Konzeptpapiers.

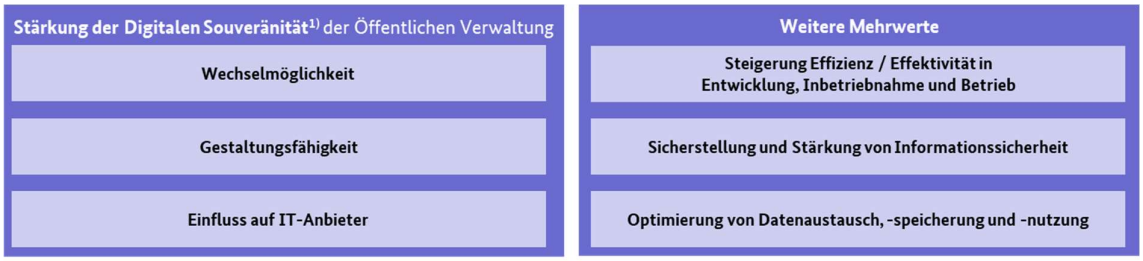

Abbildung 2: Mehrwehrte für die Öffentliche Verwaltung und deren IT-Infrastruktur (Auswahl)

Die Deutsche Verwaltungscloud stärkt die Digitale Souveränität der ÖV, indem **Wechselmöglichkeiten** geschaffen, die eigene **Gestaltungsfähigkeit** gefördert und der **Einfluss auf IT-Anbieter** gefestigt wird. Insbesondere tragen folgende Merkmale der DVS dazu bei:

- Die Vereinheitlichung von Anforderungen an den Betrieb in verschiedenen Cloud-Standorten schafft einen attraktiven Markt für Softwarelieferanten, was zu einer Erweiterung des Angebotes führt.
- Die Verhandlungsposition der ÖV gegenüber Softwarelieferanten wird gestärkt, da die Organisationen der unterschiedlichen Verwaltungsebenen mit gemeinsamen Standards einheitlich auftreten können.
- Die Mechanismen der Deutschen Verwaltungscloud fördern gezielt OS-Lösungen. Der Betriebsansatz etwa, bildet eine Grundlage für die gemeinsame Unterstützung von OS-Projekten – und damit der Förderung von Alternativlösungen – durch verschiedene Verwaltungsorganisationen.

[23] Siehe Entscheidung 2021/09 – AG Cloud-Computing und Digitale Souveränität https://www.it-planungsrat.de/beschluesse/beschluss/ag-cloud-computing-und-digitale-souveraenitaet.

- Die Einbeziehung von Lösungsansätzen aus anderen Initiativen, wie z. B. Gaia-X/SCS, berücksichtigt neueste Entwicklungen zur Übernahme in die Verwaltungsstrukturen.

Des Weiteren werden durch die Deutsche Verwaltungscloud die **Effizienz und Effektivität bei Entwicklung, Inbetriebnahme und Betrieb von Softwarelösungen** für die ÖV gesteigert und **die Informationssicherheit** übergreifend gestärkt. Ebenso wird eine **Optimierung von Datenaustausch, -speicherung und -nutzung** erzielt:

- Das Prinzip der EfA-Lösungen mit zentralem oder dezentralem Betrieb von Softwarelösungen im Rahmen der OZG-Umsetzung wird mit dem möglichen Austausch und der Nachnutzung von modularen Lösungsbausteinen anhand einheitlicher Standards perspektivisch gefördert.
- Die erweiterte Zusammenarbeit zwischen Betreibern von Cloud-Standorten schafft Synergieeffekte über den gesamten Software-Lebenszyklus hinweg.
- Die Plattformstandardisierung und der hohe Automatisierungsgrad unterstützen dabei, die IT-Infrastruktur der ÖV effizient und effektiv aufzustellen.
- Die Gestaltung und Ausrichtung der Deutschen Verwaltungscloud nach dem „privacy by design/security by design“-Prinzip berücksichtigt die Sicherheitsanforderungen über alle föderalen Ebenen hinweg.
- Die strenge Ausrichtung der definierten Standards an bestehenden Richtlinien/Vorgaben für IT-Sicherheit unterstützt dabei, die Informationssicherheit der Infrastruktur weiter zu stärken.

4 Systematik der Deutschen Verwaltungscloud

In diesem Kapitel wird der angestrebte, grundlegende Aufbau der Deutschen Verwaltungscloud dargestellt. Zum einen werden grundsätzliche Eckpunkte festgehalten und die einzelnen Elemente des Aufbaus definiert. Zum anderen werden die relevanten Rollen bei der Deutschen Verwaltungscloud beschrieben.

4.1 Grundsätzliche Eckpunkte

Im Rahmen des DVS-Konzeptpapiers haben Bund, Länder und Kommunen allgemeine Anforderungen an die Deutsche Verwaltungscloud und deren Standards festgelegt. Anhand dieser Anforderungen wurden die untenstehenden Eckpunkte für die Zielarchitektur sowie für die anschließende Umsetzung spezifiziert. Darüber hinaus werden bei der Definition der einzelnen Standards die Anforderungen beachtet (siehe Kapitel 5).

- **Verteilter IT-Betrieb**: Es wird ein verteilter Betrieb in Rechenzentren von Bund, Ländern und Kommunen ermöglicht. Diese dezentrale, föderale Cloud-Infrastruktur soll durch die ÖV und deren IT-Dienstleister bereitgestellt und betrieben werden. Private Anbieter und Drittanbieter sollen nicht ausgeschlossen werden, die Einbindung von externen Services (IaaS, PaaS, SaaS) – ausgerichtet an den Standards der Deutschen Verwaltungscloud – wird grundsätzlich unterstützt[24]. Die Anwendung der DVS-Standards für private Anbieter und Drittanbieter (z. B. Hyperscaler) sowie deren Services ist noch zu spezifizieren (vgl. Kapitel 4.2).
- **Allgemeine Verfügbarkeit von Softwarelösungen**: Die angebotenen Softwarelösungen innerhalb der föderalen Cloudstruktur sollen für alle Organisationen der ÖV aus Bund, Länder und Kommunen nutzbar sein. Entstehende Erweiterungen und Anpassungen einer Softwarelösung oder eines Services bei einem Teilnehmenden der Deutschen Verwaltungscloud sollen in anderen Cloud-Standorten nachgenutzt werden können.

[24] Eine Einbindung kann erst nach sorgfältiger Prüfung anhand diverser Kriterien (z. B. Gesichtspunkte der Daten- und Informationssicherheit) erfolgen.

- **Einsatz von OS-Software (OSS)**: OSS wird als ein geeignetes Mittel für den Aufbau der vernetzen Cloud-Infrastruktur angesehen und daher bei der Lösungserstellung priorisiert[25]. Kommerzielle Distributionen von OSS können eingesetzt werden[26]. Betriebene Softwarelösungen innerhalb der Deutschen Verwaltungscloud müssen nicht auf OSS basieren, Lock-in-Effekte[27] sollen jedoch verhindert, die Nachnutzung (z. B. durch OSS) ermöglicht und risikomindernde Maßnahmen[28] eingeplant und umgesetzt werden.
- **Zentrale Verwaltung von Services**: Die Suche, Beauftragung, Anpassung und Löschung von Services der Deutschen Verwaltungscloud erfolgt über ein zentrales Cloud-Service-Portal je Zugriffsnetz, das sich primär an Softwarebetreiber richtet. Die angebotenen Services werden in einem standardisierten Servicekatalog verwaltet. Der eigentliche Zugriff auf die bereitgestellten Services durch die Anwender (Nutzende der betriebenen Softwarelösung) erfolgt direkt am Cloud-Standort ohne die Nutzung des Cloud-Service-Portals.

4.2 Übergreifender Aufbau

Grundsätzlich besteht die Deutsche Verwaltungscloud aus verschiedenen Elementen:

1) **Cloud-Standorte**
2) **Cloud-Service-Portal**
3) **Koordinierungsstelle**

[25] Eine Priorisierung von OSS bedeutet nicht, dass proprietäre Lösungen grundsätzlich ausgeschlossen werden. Der Einsatz eines proprietären Software-Stacks ist innerhalb der Deutschen Verwaltungscloud möglich. Schnittstellen müssen jedoch entsprechend gemeinsamer Standards geschaffen werden.

[26] OS-Lösungen (u. a. auch im Cloud-Umfeld) werden oftmals von Unternehmen (weiter-)entwickelt, die kommerzielle Geschäftsmodelle (z. B. Support-Bereitstellungen, Enterprise-Funktionalitäten) verfolgen. Es kann sinnvoll sein, darauf zurückzugreifen, um Einführung und Betrieb der OS-Lösungen sicherzustellen und zu beschleunigen.

[27] „Lock-in-Effekt“ beschreibt die negativ empfundene Zwangsbindung, die es dem Kunden wegen entstehender Wechselkosten und sonstiger Wechselbarrieren erschwert, Produkt / Service oder Anbieter zu wechseln.

[28] Diese Maßnahmen sollen die Wahrscheinlichkeit und die negativen Auswirkungen eines „Lock-ins“ verringern.

Bei der Interaktion der Elemente sind stets die unterschiedlichen Arten des Zugriffes, d. h. aus dem Internet und den Verwaltungsnetzen, zu berücksichtigen (vgl. Abbildung 3). Spezifikationen der einzelnen Elemente finden sich in den folgenden Kapiteln.

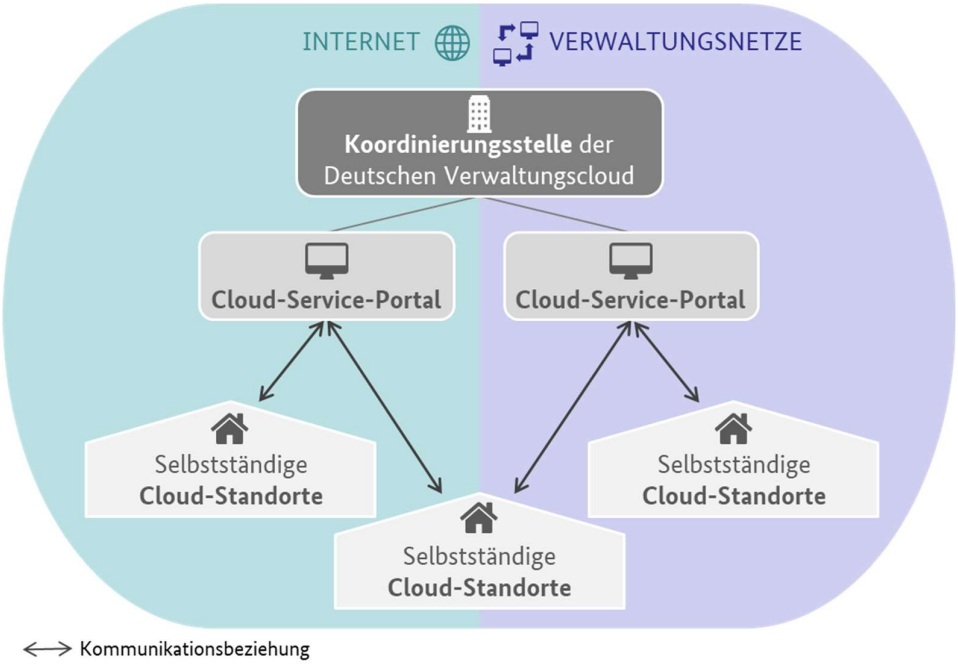

Abbildung 3: Elemente der Deutschen Verwaltungscloud und deren Interaktion (illustrative Darstellung)

Als **Cloud-Standorte** werden die Rechenzentren bei Bund, Ländern und Kommunen bezeichnet, die IT-Infrastruktur bereitstellen und bspw. Rechenkapazitäten innerhalb der Deutschen Verwaltungscloud verfügbar machen. Dabei muss nicht zwangsweise die gesamte Infrastruktur der Rechenzentren Teil der Deutschen Verwaltungscloud sein, es können auch Teilbereiche betrachtet werden. Cloud-Standorte können entweder nur aus dem Internet, nur innerhalb von Verwaltungsnetzen oder aus beiden Zugriffsnetzen erreichbar sein. Perspektivisch sollten die Services der Cloud-Standorte automatisiert über programmatische Schnittstellen (d. h. Application Programming Interfaces, APIs) steuerbar sein. Details zu den Cloud-Standorten finden sich in Kapitel 5.

Das **Cloud-Service-Portal** kommuniziert als zentrales Element mit den verschiedenen Cloud-Standorten. Es wird aus dem Internet und aus den Verwaltungsnetzen erreichbar sein. Den Zugriffsnetzen entsprechend wird es zwei separate Ausprägungen des Portals geben. Das Portal ermöglicht es, Services in einem Multi-Cloud Kontext zu suchen, zu beauftragen, anzupassen und

zu löschen. Verwaltet werden die Services mittels eines einheitlichen Kataloges als eine Art Verzeichnis. Die Angebote im Cloud-Service-Portal werden in Abhängigkeit des Zugriffsnetzes dargestellt. Beim Zugriff aus den Verwaltungsnetzen können alle Leistungen eines Cloud-Standortes mit Verbindung in die Verwaltungsnetze genutzt werden. Dieses schließt auch die Internetangebote ein. Beim Zugriff aus dem Internet können nur die Angebote aus dem Internet genutzt werden. Details zum Cloud-Service-Portal findet sich in Kapitel 6.2. Die Verknüpfung mit bereits bestehenden Service-Portalen auf den unterschiedlichen föderalen Ebenen wird geprüft.

Eine **Koordinierungsstelle** soll unter Berücksichtigung und ggf. Nachnutzung bestehender föderaler Strukturen eingerichtet werden, um zukünftig die Weiterentwicklung der Deutschen Verwaltungscloud zu koordinieren. Insbesondere soll diese Organisation für das Cloud-Service-Portal zuständig sein, dessen Entwicklung und Integration mit den Cloud-Standorten sicherstellen sowie den Servicekatalog, als Auflistung aller angebotenen Services innerhalb der Deutschen Verwaltungscloud, kontinuierlich pflegen. Darüber hinaus soll die Koordinierungsstelle die Einhaltung der definierten Standards prüfen. Die AG Cloud und deren UAG *Technik & Betrieb* wird diese operativen Tätigkeiten aufgrund der personellen Ressourcen nicht übernehmen können. Details zur Koordinierungsstelle der Deutschen Verwaltungscloud finden sich in Kapitel 6.3.

Die Wechselfähigkeit im Rahmen der DVS wird durch die Standardisierung bereitgestellter Ressourcen sowie die Vereinheitlichung der Anforderungen für Softwarelieferanten gewährleistet. Hierzu dient die DVS-Schicht (vgl. Abbildung 4), welche eine standardisierte Integration für möglichst viele Anbieter ermöglicht. Dadurch wird Unabhängigkeit von Herstellern sowie von OSS-Projekten im Sinne der Digitalen Souveränität gewährleistet. Die Integration von (Public) Cloud-Anbieter erfolgt über Cloud-Standorte der ÖV, den sogenannten „Public Cloud-Integratoren“. Softwarebetreiber sollen somit zukünftig auf einfache Art und Weise den Betriebsort für ihre Lösungen[29] auswählen können. Zielstellung ist, dass beim Betrieb einer Softwarelösung aus technischer Sicht kein Unterscheid zwischen einem Rechenzentrum der ÖV und dem Betrieb bei einem externen Cloud-Anbieter/Verbund besteht.

[29] Hinweis: SaaS-Lösungen entstehen über die Bereitstellung durch Softwarebetreiber und müssen nicht zwingend durch einen Cloud-Standort angeboten werden.

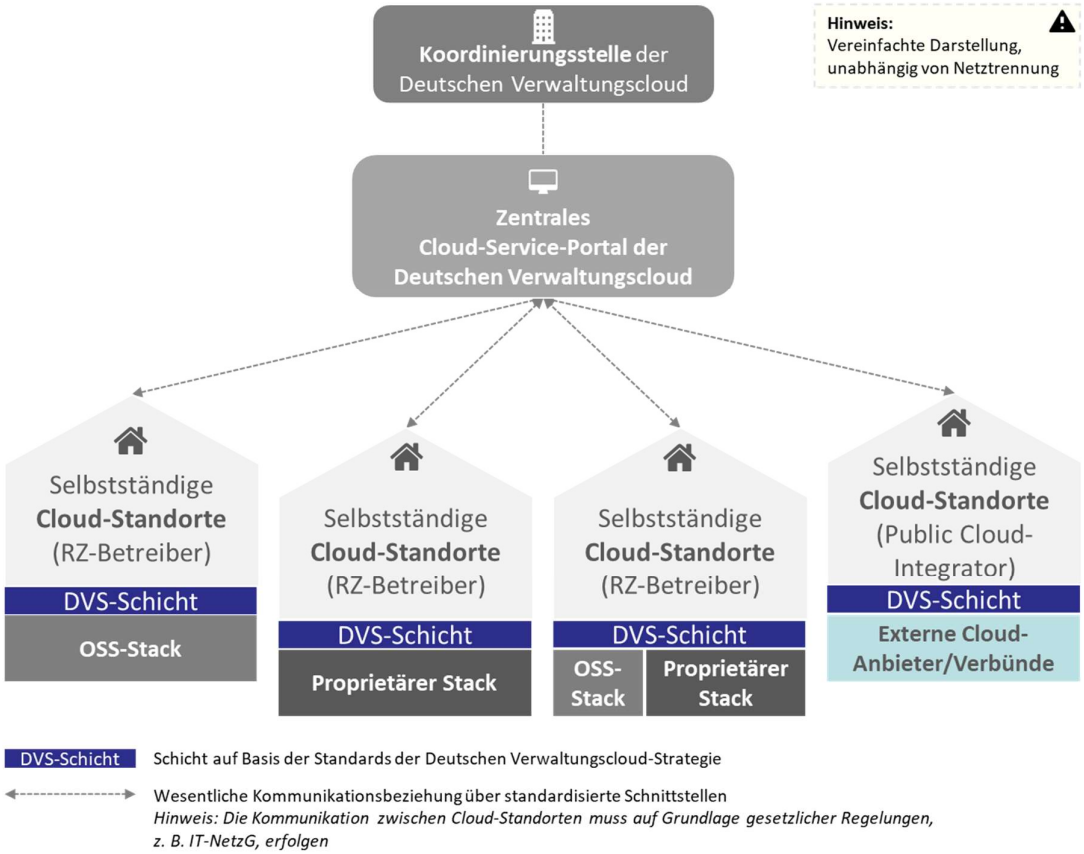

Abbildung 4: Aufbau der Cloud-Standorte, inkl. DVS-Schicht (illustrative Darstellung)

4.3 Definition der Rollen

Zur Festlegung eindeutiger Zuständigkeiten/Verantwortlichkeiten im Rahmen der Deutschen Verwaltungscloud werden folgende Rollen definiert:

a) **Auftraggeber (Bedarfsträger oder Kunde) einer Softwarelösung** – Der Auftraggeber (z. B. Verwaltungsorganisationen wie Ministerien) einer Softwarelösung beauftragt für den Betrieb den Softwarebetreiber anhand vertraglicher Verpflichtungen, um Softwarelösungen nutzbar zu machen.

b) **Softwarebetreiber** – Der Softwarebetreiber verantwortet als Auftragnehmer den Betrieb einer Softwarelösung entsprechend vertraglicher Verpflichtungen gegenüber dem Auftraggeber und managt die Service-Orchestrierung. Wenn möglich, stimmt er die Anforderungen an den Betrieb der Software mit dem Softwarelieferanten ab. Er ist das Bindeglied zwischen Plattformbetreiber und Softwarelieferant.

c) **Softwarelieferant** – Der Softwarelieferant ist eine Organisation (im Sinne einer juristischen Person) oder eine lose miteinander gekoppelte Community (Gruppe von Entwicklerinnen und Entwickler), welche dem Softwarebetreiber Software(-releases) bereitstellt.

d) **Plattformbetreiber** – Der Plattformbetreiber betreibt die IT-Infrastruktur am Cloud-Standort und stellt dem Softwarebetreiber Werkzeuge zur manuellen und/oder automatischen Orchestrierung bereit.

e) **Nutzende des Cloud-Service-Portals** – Das Cloud-Service-Portal ist der zentrale Einstiegspunkt für Mitarbeitende des Softwarebetreibers. Diese können in dem Cloud-Service-Portal mittels Self-Service verschiedene Services der Deutschen Verwaltungscloud suchen, anfordern, konfigurieren und administrieren. Bei SaaS-Angeboten im Portal können auch Auftraggeber einer Softwarelösung Nutzende des Cloud-Service-Portals sein.

Diese Rollen werden in den nachstehenden Kapiteln gemäß den Definitionen verwendet. Organisationen oder Individuen können mehrere Rollen innehaben.

4.4 Rollenverhältnisse und ausgewählte User Stories der Deutschen Verwaltungscloud

Zur Verdeutlichung der Interaktionen der zuvor definierten Rollen (Kapitel 4.3) ist im Folgenden ein typisches Szenario innerhalb der Deutschen Verwaltungscloud beispielhaft dargestellt. Dieses Szenario (siehe Abbildung 5) spiegelt wider, wie die Rollen mit den verschiedenen Elementen in Beziehung stehen und interagieren.

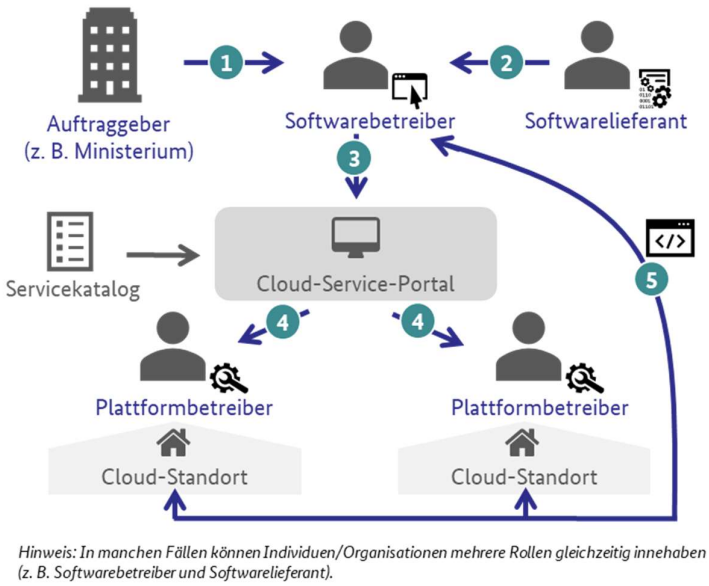

Abbildung 5: Verhältnis und wechselseitige Beziehung der Rollen (Beispielszenario)

Das abgebildete Szenario ist in fünf aufeinanderfolgende Schritte eingeteilt und zeigt die logische Abfolge bei der Beauftragung und der anschließenden Nutzung eines Services (Fokus: IaaS, CaaS und PaaS) der Deutschen Verwaltungscloud:

1) Ein **Auftraggeber** möchte eine bestimmte Softwarelösung nutzen und beauftragt dafür einen **Softwarebetreiber** als Auftragnehmer.
2) Der **Softwarebetreiber** bezieht die entsprechende Softwarelösung von einem **Softwarelieferanten**.
3) Zum Betreiben der Lösung nutzt der **Softwarebetreiber** das **Cloud-Service-Portal** und wählt im Servicekatalog einen passenden Service (IaaS, CaaS oder PaaS).
4) Der **Softwarebetreiber** bucht über das Cloud-Service-Portal die benötigten Services eines oder mehrerer **Plattformbetreiber bei definierten Cloud-Standorten**.
5) Der **Plattformbetreiber** stellt anschließend dem **Softwarebetreiber** die Cloud-Infrastruktur im ausgewählten Cloud-Standort zur Verfügung. Der **Softwarebetreiber** greift direkt auf den **Cloud-Standort** zu und ruft die Services ab.

Im Kontext des vorgestellten Szenarios, sowie darüber hinaus, lassen sich tiefergehende User Stories je Rolle beschreiben. Die nachstehende Beschreibung der User Stories folgt dabei dem einheitlichen Schema *„Als [Rolle] möchte ich [Anforderung/Ziel/Wunsch], um [Nutzen].*"

Die ausgewählten User Stories geben einen Einblick, was innerhalb der Deutschen Verwaltungscloud perspektivisch ermöglicht werden soll. Die User Stories dienen darüber hinaus als Grundlage, um den Umfang etwaiger Pilotierungsprojekte (siehe Kapitel 6.1) festzulegen. Die Liste wird fortlaufend erweitert.

ID	Beschreibung der User Story
U1	Als **Softwarebetreiber** möchte ich einheitliche Plattformen für den Softwarelieferanten bereitstellen, um weitestgehend herstellerunabhängige Entwicklungen an verschiedenen Cloud-Standorten zu ermöglichen.
U2	Als **Softwarebetreiber** möchte ich containerisierte Softwarelösungen in unterschiedlichen Cloud-Standorten betreiben, um Wiederverwendbarkeit zu erzielen.
U3	Als **Softwarebetreiber** möchte ich einheitliche/gleichartige Container-Cluster bereitgestellt bekommen, um das Deployment von Softwarelösungen zu erleichtern.
U4	Als **Softwarebetreiber** möchte ich die Kompatibilität des Cloud-Standortes für meine benötigten Ressourcen überprüfen, um den einwandfreien Betrieb zu gewährleisten.
U5	Als **Softwarebetreiber** möchte ich Anforderungen (insb. notwendige Infrastruktur, Netztopologien) an die Services des Plattformbetreibers definieren können, um den benötigten Zielzustand zu erhalten.
U6	Als **Plattformbetreiber** möchte ich ein einheitliches und gemeinsames Regelwerk für die Konfiguration von Container-Cluster benutzen, um standardisierte Services bereitstellen zu können.
U7	Als **Nutzende des Cloud-Service-Portals** möchte ich mittels Filterfunktion Services auswählen, um entsprechend meiner Kriterien passende Services zu finden.
U8	Als **Nutzende des Cloud-Service-Portals** möchte ich Services (SaaS, PaaS, CaaS und IaaS) beauftragen, um diese am ausgewählten Cloud-Standort zu nutzen.

4.5 Mögliche Softwarelösungen für den Betrieb in Cloud-Standorten

Bei der Ausgestaltung der beschriebenen Systematik sowie der abgeleiteten Standards für Cloud-Standorte wurden Lösungen betrachtet, deren Betrieb grundsätzlich in jedem Cloud-Standort möglich sein soll. Diese unterschiedlichen Anwendungsfälle für den Rechenzentrumsbetrieb wurden definiert, damit die Deutsche Verwaltungscloud den Anforderungen der einzelnen Softwarelösungen gerecht wird. Unter anderem wurden folgende Anwendungsfälle für zu betreibende Softwarelösungen berücksichtigt:

ID	Beschreibung des Anwendungsfalls
A1	**Fachverfahren mit Onlineantrag** Das Verfahren unterstützt die Sachbearbeiter einer oder mehrerer Dienststellen bei der Antragsbearbeitung, Bescheidung und Zahlbarmachung von Leistungen. Es bietet eine Schnittstelle zu Online-Anträgen und kann E-Akte-Systeme unterstützen.
A2	**TR-RESISCAN und TR-ESOR** Es wird eine Scan-Strecke nach TR-RESISCAN zum beweiswerterhaltenden Scannen von Dokumenten vor Ort betrieben. Die eingescannten Dokumente werden in die Ablage nach Standard TR-ESOR beweiswerterhaltend gespeichert. Aus dem jeweiligen Kontext ergeben sich auf jeden Fall erhöhte Anforderungen an den Schutzbedarf.
A3	**Künstliche-Intelligenz-gestützte Assistenzsysteme der Verwaltung** Persönliche (Sprach-)Assistenzsysteme unterstützen Bürgerinnen und Bürger als zentraler Zugangskanal zur Verwaltung (z. B. Chatbot im digitalen Raum). Ebenso nutzen Verwaltungsmitarbeitende „persönliche Assistenten“ als Entscheidungsunterstützung (z. B. Anomalie-Erkennung) zur effektiveren Fallbearbeitung.
A4	**E-Mail-Versand** Es wird ein Service zum Empfangen von E-Mails und zum Bereitstellen eines IMAP-Postfaches betrieben. E-Mails werden über einen SMTP-Server versendet. Der Zugang zum Service kann von einer Client-Anwendung oder einem Web-Frontend erfolgen.

ID	Beschreibung des Anwendungsfalls
A5	**Kollaborationsplattformen** Kollaborationsplattformen dienen zur Zusammenarbeit an Dokumenten, Listen und strukturierten Daten. Der Zugang zur Plattform kann von einer Client-Anwendung oder einem Web-Frontend erfolgen.
A6	**Videokonferenz- und Messagingsysteme** Es wird eine Kommunikationsplattform mit Messaging, Voice-over-IP, Videostreaming, Chat und Dateiübertragung bereitgestellt. Die Kommunikation erfolgt Ende-zu-Ende verschlüsselt in einem föderierten Ansatz. In der Regel wird ein Verbund aus Plattformen aufgebaut und ggf. werden Drittsysteme eingebunden.
A7	**Online Services Computer Interface (OSCI) und andere Datenübertragungsmechanismen** Im Cloud-Standort wird eine virtuelle Poststelle bereitgestellt, welche Daten entgegennehmen und verschlüsselt an einen anderen Cloud-Standort übertragen kann. Als ein Beispiel wird OSCI betrachtet.

5 Wesentliche Standards für Cloud-Standorte

Mit der Deutschen Verwaltungscloud sollen Standards für alle teilnehmenden Cloud-Standorte von Bund, Ländern und Kommunen eingeführt werden. Ziel dieses Kapitels ist die Beschreibung des Handlungsrahmens, der durch eine weiterführende Detaillierung konkretisiert wird.

Im DVS-Konzeptpapier hat man sich bereits gemeinsam auf fünf Standardisierungsbereiche verständigt:

1) *Entwicklung und Entwicklungsplattform,*
2) *Anwendungsbereitstellung und -management,*
3) *Code Repository,*
4) *Infrastruktur-Service und technologischer Stack* sowie
5) *Betriebsstandards und Betriebsmodell*

Diese Bereiche werden anhand der obligatorischen und optionalen Standards für Cloud-Standorte adressiert, die in den folgenden Unterkapiteln dargestellt sind.

Im Zusammenhang mit dem Standardisierungsbereich 3 (*Code Repository*) realisiert eine separate Projektgruppe[30] ein zentrales Code Repository Management System als Teil einer übergreifenden OS-Plattform. Eine dedizierte Betrachtung dessen ist in diesem Dokument nicht aufgeführt.

5.1 Vorlage zur Festlegung der Standards

Um die praktische Arbeit mit den Standards zu erleichtern, wird im Folgenden jeder Standard in einem einheitlichen Format dargestellt. Ein Standard wird dabei durch einen eindeutigen Titel, einen Verbindlichkeitsgrad sowie einer revisionssicheren Identifikationsnummer (ID) gekennzeichnet. Die untenstehende Formatvorlage ist an die der Architekturrichtlinie für die IT des Bundes angelehnt[31].

[30] Projektgruppe besteht aus Vertretern des BMI, Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie Nordrhein-Westfalen, Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg sowie dem baden-württembergischen IT-Dienstleister Komm.ONE.

[31] Siehe https://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/architekturrichtlinie_it_bund_2020.pdf?__blob=publicationFile.

Titel des Standards		**Verbindlichkeitsgrad**
ID: Revisionssichere Identifikationsnummer		
Beschreibung	Prägnante Darlegung des einzuhaltenden Standards	
Verweis	*Optional*: Verweis auf Kapitel 5.3 fortfolgend für Detaillierung des Standards und weiterführende (technische) Erläuterungen oder Verweis auf bestehende Festlegungen/Dokumente	

Tabelle 1: Vorlage zur Festlegung der Standards

Wie in Kapitel 2.4 erläutert, sollen die Standards regelmäßig, mindestens jährlich, aktualisiert und weiterentwickelt werden. Dies macht eine revisionssichere ID notwendig, damit die Nachvollziehbarkeit von Änderungen jederzeit gewährleistet ist. Die ID ist wie folgt aufgebaut:

DVS (*Präfix zur Kennzeichnung der Zugehörigkeit zur Deutschen Verwaltungscloud-Strategie*) –

XXX (*Fortlaufende, einmalige Nummerierung*) –

RXX (*Suffix zur Angabe des Revisionsstands des Standards, R01 kennzeichnet die initiale Version*)

Der Verbindlichkeitsgrad (MUSS, SOLL, KANN, DARF NICHT) entspricht ebenfalls einer standardisierten Form, um Interpretationsspielraum zu verringern und das gemeinsame Verständnis zu fördern. Die Begriffsdefinitionen der einzelnen Verbindlichkeitsgrade sind Kapitel 7.1 (Anhang) zu entnehmen[32].

5.2 Sammlung der Standards

Dieses Unterkapitel umfasst den aktuellen Stand der wesentlichen Standards für Cloud-Standorte. Weitere (technische) Detaillierungen zu einzelnen Standards sind in den nachfolgenden Kapiteln aufgeführt.

[32] Definitionen in Anlehnung an RFC 2119 (https://datatracker.ietf.org/doc/html/rfc2119).

Anwendbares Recht	**MUSS**
ID: DVS-001-R01	
Beschreibung	Für die gesamte Leistungserbringung im Rahmen der Deutschen Verwaltungscloud muss deutsches Recht uneingeschränkt anwendbar sein.
Verweis	Sicherstellung rechtlicher Anforderungen an korrektes Verwaltungshandeln

Vorgaben für Produktion, Service und Subunternehmer	**MUSS**
ID: DVS-002-R01	
Beschreibung	Für den Betrieb von Softwarelösungen mit Anforderungen hinsichtlich Vertraulichkeit, Sicherheit und Rechtssicherheit müssen folgende Rahmenbedingungen eingehalten werden: - Point of Production ist Deutschland - Point of Service ist Deutschland Jeder Software- oder Plattformbetreiber muss eine Liste der Subunternehmen in der gesamten Lieferkette dokumentieren und Sicherheitsüberprüfungen für die Mitarbeiter mit Zugriff auf die Systeme sicherstellen können.
Verweis	Strategie zur Stärkung der Digitalen Souveränität der IT der Öffentlichen Verwaltung Sicherstellung rechtlicher Anforderungen an korrektes Verwaltungshandeln

Hoheit über Hard- und Software	**MUSS**
ID: DVS-003-R01	
Beschreibung	Die eingesetzte Hard- und Software muss so gewählt und betrieben werden, dass die Handlungsfähigkeit der Auftraggeber und Softwarebetreiber durch Entscheidungen des Softwarelieferanten oder eines Anbieters nicht gefährdet wird. Für wichtige Verfahren muss die Hoheit[33] der eingesetzten Hard- und Software in der ÖV liegen. Entsprechend der beschlossenen Strategie zur Stärkung der Digitalen Souveränität der IT der ÖV muss die Gestaltungsfähigkeit gewahrt werden.
Verweis	Strategie zur Stärkung der Digitalen Souveränität der IT der Öffentlichen Verwaltung

Standards für Softwarekomponenten	**MUSS**
ID: DVS-004-R01	
Beschreibung	Jeder Cloud-Standort muss Softwarekomponenten auf Basis der Standards der DVS verwenden. Dies betrifft insbesondere den Containerbetrieb. Auf den Komponenten aufbauende Produkte können sich unterscheiden.
Verweis	Siehe Kapitel 5.3.1

[33] Von „Hoheit“ wird in diesem Zusammenhang gesprochen, wenn die ÖV in ausreichendem Maße über die Systeme bestimmen kann, um die notwendige Verfügbarkeit, die IT-Sicherheit und den Datenschutz zu gewährleisten.

Zertifizierung nach IT-Grundschutz des BSI	**MUSS**
ID: DVS-005-R01	
Beschreibung	Jeder Cloud-Standort muss einen passenden Informationsverbund definieren und diesen nach ISO 27001 auf der Grundlage von IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zertifiziert haben.
Verweis	*Ohne Verweis*

Erfüllung des Kriterienkatalogs C5	**SOLL**
ID: DVS-006-R01	
Beschreibung	Jeder Cloud-Standort sowie deren Cloud-Services sollen die Kriterien aus dem Kriterienkatalog C5 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfüllen.
Verweis	*Ohne Verweis*

Hoheit über Krypto-Module und Schlüssel	**MUSS**
ID: DVS-007-R01	
Beschreibung	Die Kryptomodule / Schlüssel müssen in Hoheit der ÖV sein, um den Zugriff auf die gespeicherten Daten selbstbestimmt zu kontrollieren. Technologien zur Verschlüsselung müssen durch die Cloud-Standorte anpassbar sein, um jederzeit die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umsetzen zu können.
Verweis	Strategie zur Stärkung der Digitalen Souveränität der IT der Öffentlichen Verwaltung Anforderungen aus dem IT-Grundschutz zur Verschlüsselung der Daten

Bereitstellung von Containerumgebung (CaaS) und Container-Cluster	**MUSS**
ID: DVS-008-R01	
Beschreibung	Jeder Cloud-Standort muss eine Containerumgebung (Container-as-a-Service, CaaS) zum Betrieb von Lösungen bereitstellen. Die Umgebung beinhaltet die benötigten IaaS- und PaaS-Komponenten für den Containerbetrieb. Jeder Cloud-Standort muss außerdem Containerorchestrierungsumgebungen bereitstellen.
Verweis	Siehe Kapitel 5.3.3

Anlieferung von Containerlösungen	**MUSS**
ID: DVS-009-R01	
Beschreibung	Jeder Cloud-Standort muss ein System zur Anlieferung von Containerlösungen (Container-Registry) für die Softwarebetreiber bereitstellen. Das System muss die Beschreibung von Zielzuständen für das Ausrollen oder die Aktualisierung der betriebenen Softwarelösungen unterstützen. Für die Softwarelösungen muss die Systematik zum Schwachstellenscan unterstützt werden.
Verweis	Siehe Kapitel 5.3.1 und 5.3.3

Angebot von Erweiterungen zur Containerumgebung	**KANN**
ID: DVS-010-R01	
Beschreibung	Jeder Cloud-Standort kann Erweiterungen zur oder mit Anbindung an die Containerumgebung anbieten. Denkbar sind bspw. spezifische Basis-Images, Frameworks oder Datenbankmanagementsysteme (DBMS).
Verweis	Siehe Kapitel 5.3.3

Erreichbarkeit der Standorte	MUSS
ID: DVS-011-R01	
Beschreibung	Jeder Cloud-Standort muss aus den Verwaltungsnetzen, für die er Cloud-Services anbietet, z. B. Netze des Bundes, oder aus dem Internet erreichbar sein. Die Kommunikation zwischen Cloud-Standorten muss auf Grundlage gesetzlicher Regelungen, z. B. IT-NetzG, erfolgen. Die Berücksichtigung der Netzstrategie 2030 mit der Schaffung eines Informationsverbundes der ÖV (kurz: IVÖV) muss erfolgen[34].
Verweis	Siehe Kapitel 5.3.2

Umsetzung des Zonenmodells	SOLL
ID: DVS-012-R01	
Beschreibung	Jeder Cloud-Standort soll die Blaupause des Zonenmodells für einheitliche Zugangswege umsetzen. Standort-spezifische Abweichungen sind möglich, solang diese konform mit den Vorgaben des BSI sind.
Verweis	Siehe Kapitel 5.3.2

[34] Siehe https://www.bdbos.bund.de/DE/NdB/Ziele/ziele_node.html.

Einrichtung einer Schnittstelle zum Cloud-Service-Portal	MUSS
ID: DVS-013-R01	
Beschreibung	Jeder Cloud-Standort muss Anforderungen zur Bereitstellung, Änderung oder Löschung von Services durch das Cloud-Service-Portal über eine standardisierte (technische) Schnittstelle entgegennehmen können. Weiterhin muss das Incident[35]- und Change[36]-Management über diese Schnittstelle unterstützt werden. Zudem müssen Informationen zum Servicekatalog, zur Bereitstellung von Services und Abrechnungsdaten an das Cloud-Service-Portals mittels der Schnittstelle übermittelt werden können.
Verweis	Siehe Kapitel 6.2

[35] Als „Incident“ wird in diesem Zusammenhang ein Sicherheitsvorfall oder eine Betriebsstörung einer IT-Lösung bezeichnet.

[36] Als „Change“ wird in diesem Zusammenhang das Modifizieren oder Aktualisieren einer IT-Lösung bezeichnet.

Betreiberwechsel	**MUSS**
ID: DVS-014-R01	
Beschreibung	Jeder Cloud-Standort muss in der Rolle als Plattformbetreiber dem Softwarebetreiber geeignete Möglichkeiten für einen Betreiberwechsel innerhalb der Deutschen Verwaltungscloud bieten. Gespeicherte Daten müssen dem Softwarebetreiber in der Form bereitgestellt werden, sodass der Datenexport an einem anderen Cloud-Standort wiederhergestellt werden kann. Bei SaaS-Angeboten müssen durch den Softwarebetreiber Funktionen zum Datenexport in einem offenen und standardisierten Format bereitgestellt werden.
Verweis	*Ohne Verweis*

Bereitstellung notwendiger Dokumentationen	**MUSS**
ID: DVS-015-R01	
Beschreibung	Jeder Cloud-Standort muss in der Rolle als Plattformbetreiber dem Softwarebetreiber notwendige Unterlagen zu den bereitgestellten Services verfügbar machen.
Verweis	*Ohne Verweis*

Bereitstellung von Entwicklungsbereichen	**KANN**
ID: DVS-016-R01	
Beschreibung	Jeder Cloud-Standort kann Entwicklungsbereiche bereitstellen.
Verweis	Siehe Kapitel 5.3.4

Anbindung an die zentrale OS-Plattform	**MUSS**
ID: DVS-017-R01	
Beschreibung	Jeder Cloud-Standort muss bei Bereitstellung von Entwicklungsbereichen die Anbindung an die zentrale OS-Plattform inkl. Code Repository[37] ermöglichen.
Verweis	Siehe Kapitel 5.3.4

Unterstützung von DevOps-Ansätzen	**MUSS**
ID: DVS-018-R01	
Beschreibung	Jeder Cloud-Standort muss mit den bereitgestellten Entwicklungsbereichen die DevOps-Ansätze Continuous Integration und Continuous Deployment unterstützen.
Verweis	Siehe Kapitel 5.3.4

[37] Die zentrale OS-Plattform wird derzeit von einer dedizierten Projektgruppe in Abstimmung mit der UAG *Technik & Betrieb* aufgebaut, siehe https://www.cio.bund.de/SharedDocs/Kurzmeldungen/DE/2021/pm_os_plattform.html.

Angebot von Software-as-a-Service (SaaS)	**KANN**
ID: DVS-019-R01	
Beschreibung	Jeder Cloud-Standort kann SaaS-Lösungen im Cloud-Service-Portal anbieten.
Verweis	*Ohne Verweis*

Funktion eines Ausweichrechenzentrums	**KANN**
ID: DVS-020-R01	
Beschreibung	Jeder Cloud-Standort kann die Funktion eines Ausweichrechenzentrums für den Betrieb von Fachapplikationen in besonderen Situationen anbieten (bspw. Georedundanz).
Verweis	*Ohne Verweis*

5.3 Details einzelner Standards

Ausgehend von den zuvor festgelegten Standards für Cloud-Standorte werden diese nachfolgend zum Teil weiter präzisiert. Die Präzisierung stellt jedoch keine abschließende technische Spezifizierung dar. Mit weiterführenden Dokumenten (vgl. Kapitel 6.1) sollen den Betreibern der Cloud-Standorte zukünftig **technische Handreichungen** zur zielgerichteten Umsetzung bereitgestellt werden.

Eine zusammenfassende Übersicht wie ein Cloud-Standort auf Basis der Standards aus Kapitel 5.2 gestaltet ist, kann der Abbildung 6 entnommen werden. Details dazu finden sich nachfolgend.

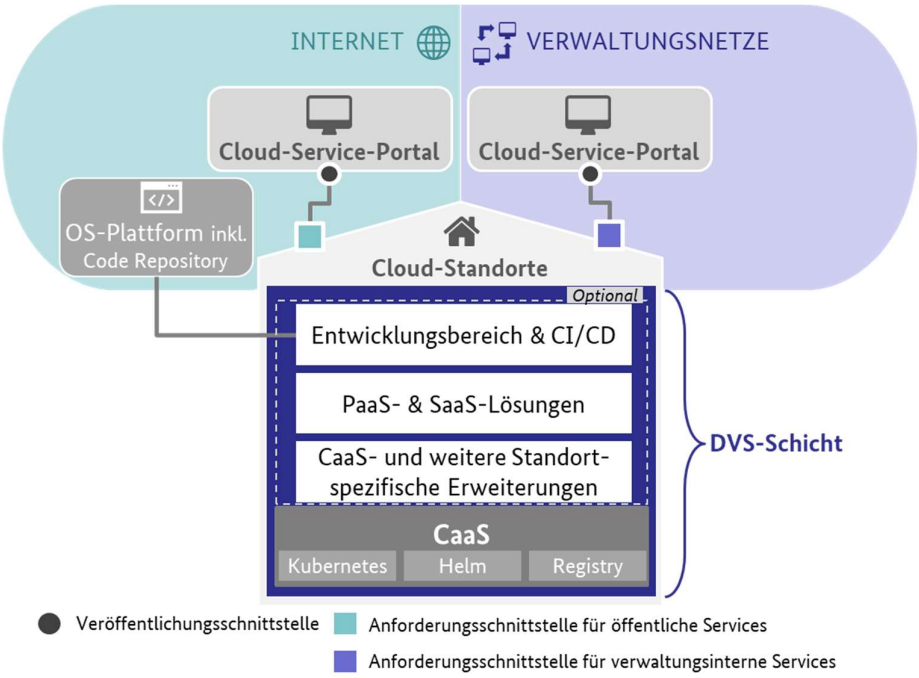

Abbildung 6: Obligatorische und optionale Standards der Cloud-Standorte (illustrative Darstellung)

5.3.1 Festgelegte Softwarekomponenten

Wie in den grundsätzlichen Eckpunkten der Deutschen Verwaltungscloud (siehe Kapitel 4.1) erläutert, wird der Einsatz von OS-Lösungen priorisiert. Aus diesem Grund müssen einheitliche, skalierbare, OS-basierte Softwarekomponenten zur Bereitstellung von Containerumgebungen in den jeweiligen Cloud-Standorten genutzt werden:

Kubernetes – Software zur automatisierten Orchestrierung und Verwaltung von Container-Anwendungen (bspw. Skalieren, Betreiben und Warten) auf verteilten Hosts.

Helm – Software, die als Paketmanager für Kubernetes fungiert und das Deployment von containerisierten Softwarelösungen sowie die Versionsverwaltung mit Hilfe sogenannter Helm-Charts erleichtert.

Container-Registry (z. B. Harbor) – Softwaretyp zur Verwaltung von Repositories für Softwareartefakte und Images (Speicherabbild eines Containers) mit Zusatzfunktionen wie Schwachstellenscannern.

Auf den Softwarekomponenten aufbauende Produkte können sich unterscheiden. So sind kommerzielle Distributionen (siehe Kapitel 4.1) von OSS oder proprietäre Produkte auf Basis der Softwarekomponenten grundsätzlich möglich. Der Einsatz von OSS wird bevorzugt.

5.3.2 Zonenmodell

Ein, am IT-Grundschutz[38] ausgerichtetes, einheitliches Zonenmodell wurde als Blaupause zur Umsetzung in allen Cloud-Standorten definiert (vgl. Abbildung 7). Standort-spezifische und mit den Vorgaben des BSI konforme Abweichungen sind möglich.

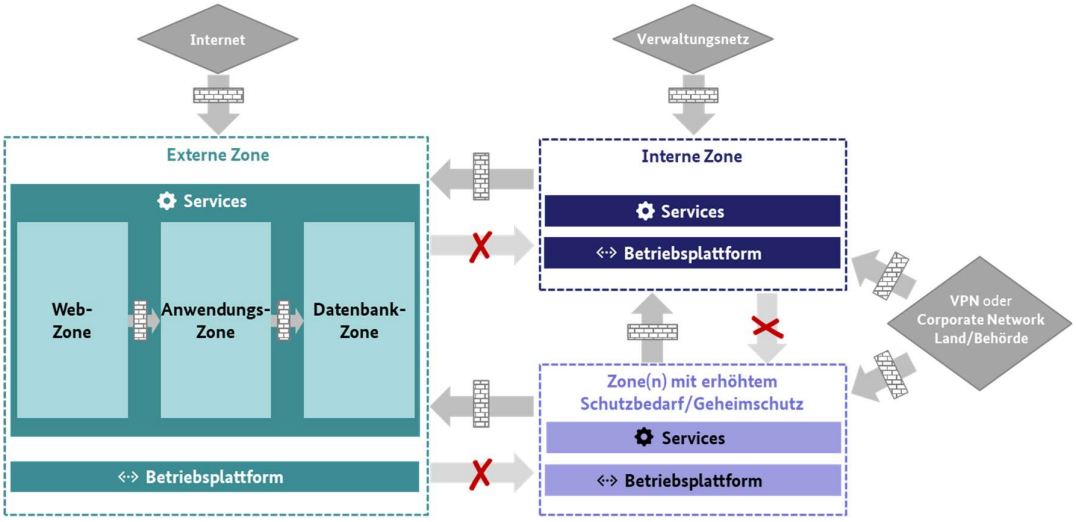

Abbildung 7: Blaupause des einheitlichen Zonenmodells der Cloud-Standorte

Die drei Zonen 1) Externe Zone, 2) Interne Zone und 3) Zone mit erhöhtem Schutzbedarf oder Geheimschutzanforderungen (z. B. VS-NfD) sind voneinander getrennt. Die Trennung kann BSI-konform sowohl physisch als auch virtuell erfolgen, wenn dies sicherheitstechnisch auf gleichwertigem Niveau erreichbar ist. Die Zonen werden entsprechend den Möglichkeiten der Cloud-Standorte in Betrieb genommen. Es besteht keine Verpflichtung alle Zonen anzubieten.

Die Externe Zone ist für die Nutzung aus dem Internet vorgesehen und hat eine weitere Unterteilung in Web-, Anwendungs- und Datenbank-Zone. Diese drei Zonen erfüllen jeweils

[38] Siehe u. a. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_1_1_Netzarchitektur_und_design_Edition_2021.pdf?__blob=publicationFile&v=23.

unterschiedliche Zwecke: Die Web-Zone wird zur Bereitstellung von Application-Level-Gateway bzw. Web-Proxy, die Anwendungs-Zone wird zur Bereitstellung von Front- und Backend und die Datenbank-Zone wird zur Bereitstellung von DBMS genutzt. Zur Eingrenzung einer Demilitarisierten Zone (DMZ) innerhalb der Externen Zone werden zwei Optionen in Kapitel 5.3.3 aufgezeigt, da dies eng mit der Containercluster-Bereitstellung verknüpft ist.

Die Kommunikation zwischen den Zonen sowie der Zugriff von außen (z. B. aus dem Internet oder den Netzen des Bundes, NdB) erfolgt gefiltert mittels Sicherheitsgateways[39] (P-A-P-Struktur gemäß Empfehlung des BSI[40] oder vergleichbar). Die Netztrennung muss mittels performanter Firewalls mindestens auf Layer 4 des OSI-Modells (Transport-Layer) erfolgen.

In diesem Zuge werden bestimmte Zugangswege von einer Zone in eine andere nicht gewährt. Demnach ist der Zugriff aus dem Internet über die Externe Zone zur Internen Zone nicht gestattet. Je Zone soll eine unabhängige Betriebsplattform etabliert werden, auf der die Services orchestriert und gesteuert werden.[41]

Aus dem dargestellten Zonenmodell lassen sich speziellere Anforderungen für den Plattformbetreiber ableiten:

- Der Plattformbetreiber MUSS Netze für die Administration der Hosts und des Container-Services von den Anwendungsnetzen logisch oder physisch trennen, z. B. auf Basis eines Virtual Local Area Networks (VLANs).
- Der Plattformbetreiber MUSS die verschiedenen Management-Interfaces der IT-Systeme nach ihrem Einsatzzweck und ihrer Netzplatzierung über einen zustandsbehafteten Paketfilter oder vergleichbar trennen.
- Der Plattformbetreiber MUSS sicherstellen, dass die Segmentierung nach Zonen nicht durch die Management-Kommunikation unterlaufen werden kann. Eine Überbrückung von Segmenten MUSS ausgeschlossen werden.

---

[39] Siehe Glossar für eine Definition des BSI.

[40] „Paketfilter – Application-Level-Gateway – Paketfilter“ (P-A-P)-Struktur sollte eingesetzt werden, siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2021.pdf?__blob=publicationFile&v=2.

[41] In Anlehnung an IT-Grundschutz Baustein NET: Netze und Kommunikation - NET.1.1 Netzarchitektur und -design, NET.1.2 Netzmanagement, NET.3.1 Router und Switches, NET.3.2 Firewall.

- Der Plattformbetreiber MUSS eine BSI-konforme Verwaltung der Administrationskonten und der technischen Accounts sicherstellen.
- Der Plattformbetreiber MUSS die Anbindung von Protokollierungssystemen entsprechend einer BSI-konformen Systematik sicherstellen.
- Der Plattformbetreiber MUSS ein Auditsystem[42] für Systembereiche etablieren. Hierzu zählen Konfigurationsdateien, Registry und Softwarebetriebsprozess.

5.3.3 Containerumgebung und Container-Cluster

Ein elementarer Aspekt bei der Bereitstellung einer Containerumgebung ist der Aufbau der Cluster zur Ausführung von containerisierten Softwarelösungen. Kubernetes bietet für eine weitere Untergliederung einzelner Cluster die Funktion zum Erstellen sog. „Namespaces". *Namespaces* können als virtuelle Cluster innerhalb eines Kubernetes-Clusters angesehen werden.

Die Ausgestaltung der Cluster hängt u. a. von Technik- und Sicherheitsanforderungen ab, wie die des definierten Zonenmodells in Kapitel 5.3.2. Basierend auf dem Modell wurden Schemata zur Bereitstellung von Container-Cluster für Webanwendungen innerhalb der Externen Zone entwickelt. Dabei werden zwei Umsetzungsoptionen aufgezeigt:

- **Option 1: Strenge Trennung** (siehe Abbildung 8)
  Die Web-Zone wird als DMZ angesehen. Dementsprechend werden die Web-Zone und die Anwendungs-Zone mit Clustern nach P-A-P-Struktur getrennt. Jede Kommunikationsbeziehung benötigt eine explizite Freigabe.

[42] Siehe Glossar für eine Begriffsdefinition.

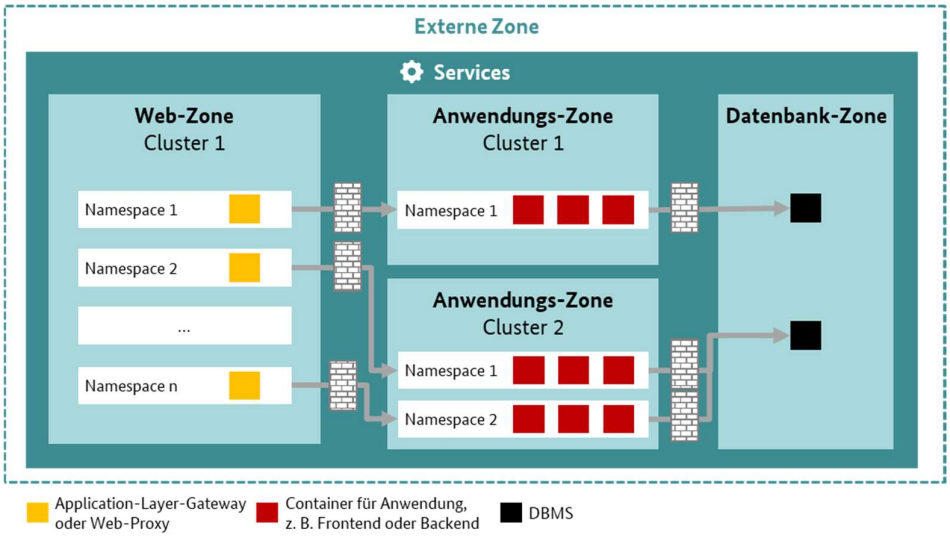

Abbildung 8: Strenge Trennung der Container-Cluster in Externer Zone (illustrative Darstellung)

- **Option 2: Weiche Trennung** (siehe Abbildung 9)

  Die komplette Externe Zone wird als DMZ angesehen. Die Trennung der Web-Zone und der Anwendungs-Zone findet innerhalb des Clusters statt. Vorgesehen sind separate Worker für Web- und Anwendungs-Zone. Eine Netztrennung zwischen den Zonen findet durch Virtualisierung und Policies statt. Jede Kommunikationsbeziehung benötigt ebenso eine explizite Freigabe.

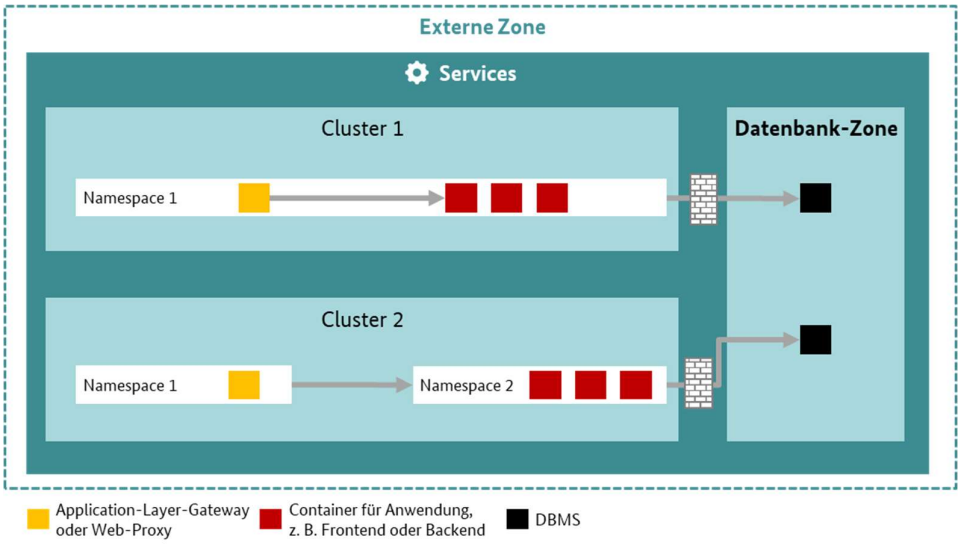

Abbildung 9: Weiche Trennung der Container-Cluster in Externer Zone (illustrative Darstellung)

Ergänzend zu der dargestellten Aufteilung der Container-Cluster wurden weitere Anforderungen für den Plattformbetreiber entwickelt. Hierzu wurden verschiedene IT-Grundschutz-Bausteine (inkl. *SYS.1.6: Container* (Community Draft aktuell in Überarbeitung)[43]) herangezogen:

- Der Plattformbetreiber SOLL für jeden nach außen exponierten Service eine eigene IP-Adresse bereitstellen. Verschiedene, nach außen exponierte Services sollten sich über die IP-Adressierung unterscheiden lassen, um Schutzmaßnahmen außerhalb der Kubernetes-Umgebung zu vereinfachen.
- Der Plattformbetreiber MUSS für die Kommunikation zwischen den Nodes des Kubernetes-Clusters sichere Tunnelprotokolle nutzen.
- Der Plattformbetreiber MUSS die Kommunikation auf die erforderlichen Kommunikationsverbindungen inklusive Nodes, Kommunikationsprotokolle und Ports einschränken, die für Inbetriebnahme und Betrieb des Clusters und seiner Nodes erforderlich sind.
- Der Plattformbetreiber MUSS sicherstellen, dass Nutzer-Workloads grundsätzlich keine (System-)Namespaces mit dem Host teilen können.
- Der Plattformbetreiber MUSS die Isolation der Container durch geeignete Berechtigungen auf Ressourcen und Kernel-Funktionen sicherstellen.
- Der Plattformbetreiber MUSS sicherstellen, dass Master-Nodes keine Nutzer-Workloads ausführen dürfen.
- Der Plattformbetreiber MUSS die Entwicklungsumgebung und die Produktivumgebung in verschiedenen Kubernetes-Clustern betreiben.
- Der Plattformbetreiber MUSS die Control-Plane von den Worker-Nodes trennen.
- Der Plattformbetreiber MUSS Fachverfahren mit verschiedenen Schutzbedarfen in getrennten Container-Clustern betreiben.

[43] Dieser Draft wird zeitnah ersetzt, siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Drafts/Community_Draft/SYS_1_6_Container_CD.pdf;jsessionid=7314F64FFE5E792081A11F73B35E52E5.internet482?__blob=publicationFile&v=1.

Die Anlieferung von Softwarelösungen für die bereitgestellten Container-Cluster stellt eine wichtige Schnittstelle im Zusammenwirken von Softwarebetreiber und Plattformbetreiber dar. Sie ist elementar für die sichere Betriebsdurchführung und die Maßnahmen-Umsetzung zur Gewährleistung der IT-Sicherheit. Aus diesem Grund werden folgende Mindestanforderungen in diesem Bereich gestellt:

- Der Plattformbetreiber MUSS eine Container-Registry zur Bereitstellung der Softwarelösungen für die Inbetriebnahme in der Containerumgebung bereitstellen.
- Der Softwarebetreiber MUSS einen Zielzustand definieren, der durch den Plattformbetreiber automatisiert ausgerollt werden kann.
- Der Plattformbetreiber MUSS gewährleisten, dass ein automatisierter Schwachstellenscan ausgeführt werden kann und dessen Ergebnisse für den Softwarebetreiber einsehbar sind. Der Plattformbetreiber MUSS dem Softwarebetreiber im Zuge dessen kritische Schwachstellen unverzüglich melden.
- Der Plattformbetreiber MUSS die Bereitstellung der zugesicherten Ressourcen und das Ausrollen der übergebenen Zielzustände sicherstellen, sofern die Integrität der Umgebung nicht gefährdet wird.
- Der Plattformbetreiber MUSS zur Fehlerbehebung, gemäß den vereinbarten Service-Level-Agreements (SLAs), und zur Skalierung automatisch Container ausrollen. Der Plattformbetreiber MUSS bei Einschränkung der Container-Laufzeit den Incident an den Softwarebetreiber zur Fehlerbehebung übergeben.
- Der Plattformbetreiber MUSS sicherstellen, dass die Planung eines Deployments im Rahmen eines Changes gesteuert und dokumentiert werden kann. Der Plattformbetreiber MUSS außerdem gewährleisten, dass der Change mindestens über das Cloud-Service-Portal mittels Schnittstellen initiiert werden kann, dabei KANN die Initiierung automatisiert über eine Pipeline unterstützt werden.

5.3.4 Entwicklungsbereich

Zur Unterstützung der dezentralen Softwareentwicklung kann ein Cloud-Standort optional verschiedene Erweiterungen getrennt von der produktiven Umgebung bereitstellen. Aufgrund der Vielzahl von Werkzeugen und der hohen Innovationsrate werden in diesem Bereich keine

verpflichtenden Standards vorgeschrieben (vgl. Kapitel 5.2). Bei der Bereitstellung muss jedoch die Kompatibilität zur Deutschen Verwaltungscloud gewahrt, die Vorgaben zur Einhaltung von Informationssicherheit und Datenschutz[44] sowie die dabei geltenden Architekturrichtlinien (vgl. Kapitel 2.3.2) eingehalten sowie ein ausreichendes Rollen- und Rechte-Management unterstützt werden. Insbesondere müssen Entwicklungsbereiche die Anbindung an die zentrale OS-Plattform inkl. Code Repository ermöglichen.

Ein hoher Automatisierungsgrad im Rahmen der Entwicklung von Softwarelösungen ist ein wichtiger Aspekt für eine moderne IT-Infrastruktur. Demnach wurden für das Angebot einer Pipeline für den Continuous Integration-Prozess (CI-Pipeline) folgende Anforderungen definiert:

- Der Plattformbetreiber MUSS sicherstellen, dass bei der Trennung der CI-Pipeline von der Pipeline für das Continuous Delivery die Anforderungen aus Kapitel 5.3.3 eingehalten werden.
- Der Plattformbetreiber MUSS sicherstellen, dass die Übergabe der Artefakte und Images über gesonderte Repositories erfolgt, um eine strikte Trennung zwischen Entwicklung und Produktivbetrieb zu realisieren. Der Plattformbetreiber SOLLTE getrennte Registries für Entwicklung und Produktivbetrieb einsetzen.
- Der Plattformbetreiber MUSS gewährleisten, dass die Pipeline mindestens die Nutzung von Systemen zur Sourcecode-Verwaltung auf Basis von Git sowie den Zugang zu Systemen für die Build-Erstellung unterstützt.
- Der Plattformbetreiber KANN die Pipeline so einrichten, dass die Bereitstellung der erstellten Artefakte und Images für ein Repository zum Ausrollen in einer Testumgebung unterstützt wird.
- Der Plattformbetreiber KANN ein Ticketsystem für die Softwareentwicklung zur Unterstützung bereitstellen.
- Der Plattformbetreiber KANN Werkzeuge zur Prüfung der Codequalität und zum Sicherheitstest bereitstellen.

[44] Bspw. durch eine strikte Trennung von Entwicklungs- und Produktionsumgebungen.

Für die Anlieferung von Artefakten und Images in den Entwicklungsbereich sollte am Cloud-Standort eine separate Registry bereitgestellt werden. In diesem Zusammenhang müssen folgende Anforderungen beachtet werden:

- Der Plattformbetreiber MUSS sicherstellen, dass Images und Beschreibungsdateien für Zielzustände an der Registry angeliefert werden können.
- Der Plattformbetreiber MUSS dem Softwarebetreiber ermöglichen, Veränderungen an seinen Images und Dateien nachvollziehen zu können.

6 Weiteres Vorgehen

Dieses Kapitel beschreibt die nächsten Schritte bei der Ausgestaltung der Deutschen Verwaltungscloud. Außerdem werden die bereits erarbeiteten Inhalte zum Cloud-Service-Portal und zur Koordinierungsstelle dargelegt.

6.1 Handlungsstränge zur Operationalisierung der Deutschen Verwaltungscloud

Das weitere Vorgehen zur Umsetzung der Deutschen Verwaltungscloud teilt sich in drei Handlungsstränge, die parallel durch die UAG *Technik & Betrieb* sowie weiteren, nahestehenden Organisationen oder (Arbeits-)Gruppen bearbeitet werden:

1) **Durchführung von Pilotierungsprojekten zur Umsetzung der Standards für Cloud-Standorte:**
   Ausgehend von den in Kapitel 5 definierten Standards für Cloud-Standorte der Deutschen Verwaltungscloud sollte eine Pilotierungsphase erfolgen, in der wesentliche Standards in der Praxis erprobt werden. Dies ist vor allem für den Containerbetrieb maßgeblich und stellt die Machbarkeit sicher. Ergebnisse dieser Phase können anschließend bei der kontinuierlichen Weiterentwicklung und Detaillierung der Standards berücksichtigt werden. Zudem können sich die verschiedenen IT-Dienstleister der ÖV aktiv einbringen, Erfahrungen austauschen und Good-Practice-Ansätze teilen und ggf. einsteuern.

2) **Fortführung der (Fein-)Konzeptionierung des Cloud-Service-Portals und der Koordinierungsstelle:**
   Wesentliche Elemente der Deutschen Verwaltungscloud sind, neben den Cloud-Standorten, das Cloud-Service-Portal und die Koordinierungsstelle (vgl. Kapitel 4.2). Aufgrund der hohen Komplexität und der Vielzahl an Fragestellungen, müssen jeweils gesonderte Konzepte für diese beiden Elemente (Cloud-Service-Portal und Koordinierungsstelle) erstellt werden. Die Konzepte werden basierend auf den bereits erarbeiteten Inhalten der UAG *Technik & Betrieb* fortgeführt und verfeinert. Wesentliche Merkmale des Cloud-Service Portals sind in Kapitel 6.2, der Koordinierungsstelle in Kapitel 6.3 beschrieben.

3) **Kontinuierliche Weiterentwicklung und Detaillierung der Standards für Cloud-Standorte**:

Wie in Kapitel 2.4 geschildert, soll das vorliegende Dokument – insbesondere die Standards für Cloud-Standorte – stetig weiterentwickelt werden. Dies ermöglicht die flexible Anpassung und Ergänzung von Standards. Die parallellaufende Verprobung im Rahmen der Pilotierung (vgl. Handlungsstrang 1) gewährleistet einen fortlaufend engen Praxisbezug. Darüber hinaus sollen auf Basis der Standards technische Handreichungen spezifiziert werden, die den IT-Dienstleistern der ÖV die Umsetzung erleichtern soll.

Über den Fortschritt der einzelnen Handlungsstränge und der damit verbundenen Operationalisierung der Deutschen Verwaltungscloud wird der IT-PLR weiterhin regelmäßig informiert. Die Aktualisierung der Standards als Ergebnis aus Handlungsstrang 3 soll in einem regelmäßigen Intervall an den IT-PLR berichtet werden (siehe Kapitel 2.4). Eine umfassende Zeitplanung je Handlungsstrang ist derzeit noch in Erarbeitung.

6.2 Konzeptionierung Cloud-Service-Portal und Servicekatalog

Mit der Deutschen Verwaltungscloud soll ein zentrales Portal für die gesamte ÖV als webbasierte Lösung eingerichtet werden, welche es erlaubt Services (IaaS, CaaS, PaaS und SaaS) in einem Multi-Cloud Kontext zu registrieren, zu suchen, zu beauftragen, anzupassen und zu löschen. Die föderalen Cloud-Standorte werden mittels einheitlicher, technischer Schnittstellen an das Cloud-Service-Portal angebunden. Die Einrichtung dieser Schnittstellen ist obligatorisch für jeden Cloud-Standort.

Das Portal fungiert als zentraler Einstiegspunkt für Mitarbeitende des Softwarebetreibers und muss über die Verwaltungsnetze, wie z. B. die NdB oder NdB-VN, und aus dem Internet erreichbar sein. Anbieter der Services (Plattform- oder Softwarebetreiber) können jeweils festlegen, ob das Angebot aus dem Internet oder den Verwaltungsnetzen erreichbar sein darf. Entwicklungsbereiche können bspw. aus dem Internet erreichbar sein, während Fachverfahren nur innerhalb der Verwaltungsnetze angeboten werden.

Zur Beschreibung und Auflistung der Services wird ein navigierbarer Servicekatalog für Nutzende des Cloud-Service-Portals angelegt. Der Katalog enthält für jeden Service eindeutig definierte Attribute, die nähere Informationen bereitstellen. Die Kompatibilität mit Gaia-X und dem

föderierten Katalog[45] wird sichergestellt. Angebotene Services müssen einen Mindeststandard bei der Beschreibung erfüllen. Folgende wesentlichen Merkmale wurden als Attribute im Servicekatalog festgelegt:

- Name und Kurzbeschreibung des Service
- Informationen des Anbieters (u. a. Anzahl und Standorte der Rechenzentren, Referenzen und Zertifizierungen/Testierungen)
- Version des Service (u. a. Gültigkeitszeitraum/Supportzeitraum, Versionshistorie)
- Enthaltene Leistungen
- Preis je Einheit
- Abhängigkeiten zu anderen Services
- Angebotener Schutzbedarf und Vertraulichkeitsstufen[46] aus Sicht des Betreibers
- Zone für die Bereitstellung (Externe Zone, Interne Zone, Zone mit erhöhtem Schutzbedarf oder Geheimschutzanforderungen)
- Aufzählung aller an der Erbringung des Service beteiligter Sub-Dienstleister und Nachunternehmer
- Abrechnungsmodalitäten und Abnahmemengen
- SLA (u. a. Betriebs-, Reaktions- und Wiederherstellungszeiten)
- *[Weitere Ergänzungen im Rahmen der Feinkonzeptionierung möglich]*

Den Nutzenden des Cloud-Service-Portals werden vielfältige Funktionen zur Verfügung gestellt, die das Administrieren und Verwalten von verschiedenen Services bei ggf. unterschiedlichen Anbietern vereinfachen. Folgende erforderliche Funktionalitäten wurden definiert:

[45] Der föderierte Katalog standardisiert im Rahmen von Gaia-X die Beschreibung von Services mittels einheitlicher Attribute. Eine möglichst hohe Deckungsgleichheit zum Servicekatalog der Deutschen Verwaltungscloud wird deshalb angestrebt.

[46] Jeder Servicekatalog-Eintrag wird mit Schutzbedarf normal eingestuft. Bei Unterstützung des Schutzbedarf hoch, sind die Eigenschaften zu beschreiben, wie z. B. verschlüsselte Datenhaltung bei persistentem Speicher.

- Registrierung einer Organisation und deren Mitarbeiterinnen und Mitarbeiter zur Nutzung des Cloud-Service-Portals
- Suchen innerhalb des Servicekatalogs entsprechend verschiedener Gruppierungskriterien
- Beauftragung eines Service (insbesondere IaaS- und PaaS-Umgebungen)
- Kündigung eines Service
- Anpassung/Konfiguration eines Service und Veranlassung eines Changes für Softwarelösungen in einer IaaS-/CaaS-/PaaS-Umgebung
- Auslösung eines Incidents zu einem Service
- Auflistung aller genutzten Services der jeweiligen Organisation
- Öffnen einer bereitgestellten SaaS-Lösung mittels Link
- Zugriff auf Abrechnungsdaten mit einmaligen und nutzungsabhängigen Kosten
- Anzeigen eines individuell konfigurierbaren Dashboards zur Auswertung von Informationen zu gebuchten Services
- *[Weitere Ergänzungen im Rahmen der Feinkonzeptionierung möglich]*

Zu diversen Funktionalitäten wurden nähere Anforderungen erfasst. So muss bspw. der Cloud-Standort in der Rolle als Plattformbetreiber bei der Beauftragung eines Changes für das Ausrollen einer neuen oder initialen Version einer Softwarelösung den Ausführungszustand an das Cloud-Service-Portal übermitteln. Ebenso muss die Angabe von Abhängigkeiten zu anderen Changes abbildbar sein, wie die zwingende Reihenfolge oder ein zeitlicher Ablauf von Changes. Incidents müssen über das Cloud-Service-Portal von autorisierten Nutzenden (Mitarbeitende eines Softwarebetreibers) ausgelöst werden können. Der Plattformbetreiber meldet anschließend den Eingang des Incidents und bestätigt die Einstufung der Kritikalität. Verbundene Kosten werden dem Softwarebetreiber zeitnah mitgeteilt.

Des Weiteren ist der Softwarebetreiber verantwortlich für die Lizenzierung in Abstimmung mit dem Plattformbetreiber. Der Plattformbetreiber benötigt jedoch ein Veto-Recht, falls der Softwarebetreiber Lizenzen einsetzen möchte, die die Lizenzkonformität seines Cloud-Standortes gefährden. Demnach sollte der Plattformbetreiber die Lizenzierung seiner angebotenen Services sicherstellen und im Servicekatalog die genutzten Lizenzen entsprechend dokumentieren sowie

Nutzungsvoraussetzungen vermerken. Der Softwarebetreiber ist dann für die Lizenzierung der genutzten Komponenten der Softwarelösung, welche die Services des Plattformbetreibers nutzt, zuständig. Zur weiteren Ausführung der Zuständigkeiten und Verfahrensweisen des Lizenzmanagements ist die Erstellung eines eigenen Dokumentes geplant.

Die weitere Ausgestaltung und Erhebung zusätzlicher funktionaler und nicht funktionaler Anforderungen wird fortgeführt und in einem gesonderten Konzept mit den Grundlagen der Betriebsführung dokumentiert.

6.3 Konzeptionierung Koordinierungsstelle der Deutschen Verwaltungscloud

In Zukunft soll die stetige Weiterentwicklung der Deutschen Verwaltungscloud (inkl. Erstellung/Fortführung von Konzepten) von der UAG *Technik & Betrieb* an eine zu spezifizierende Koordinierungsstelle übergeben werden. Diese Koordinierungsstelle der Deutschen Verwaltungscloud soll für das Cloud-Service-Portal verantwortlich sein und u. a. den Finanzierungsbedarf für dessen Entwicklung und Betrieb sicherstellen. Die Organisation ist zudem dafür zuständig, den Servicekatalog zu aktualisieren und koordiniert deshalb die kontinuierliche Pflege des Katalogs durch die Cloud-Standorte. Als weitere Aufgabe soll die Koordinierungsstelle die Einhaltung der Standards prüfen. Der dazugehörige Prozess wird im Feinkonzept erarbeitet.

Grundsätzlich soll die Koordinierungsstelle als Vermittler zwischen Cloud-Standorten (Plattformbetreiber) und Nutzerorganisationen (Softwarebetreiber) auftreten. Außerdem soll sie die Teilnahme der beiden Parteien regeln und die Befugnis haben, bei Bedarf einzelne Organisationen (z. B. bei potenzieller Kompromittierung der Informationssicherheit) von der Deutschen Verwaltungscloud auszuschließen.

Daneben soll ein Architekturboard eingerichtet werden, das in Zukunft die Standards der Deutschen Verwaltungscloud anhand rechtlicher Änderungen und technologischer Trends/Weiterentwicklungen regelmäßig adaptiert. Teilnehmende des Architekturboards sollen bspw. Interessenvertreter der ÖV, IT-Dienstleister der ÖV, Softwarebetreiber sowie Vertreterinnen und Vertreter aus den Bereichen Datenschutz, Informationssicherheit sowie Compliance sein. Bestehende Strukturen innerhalb der ÖV sind bei der weiteren Prüfung und Ausgestaltung der Koordinierungsstelle sowie des Architekturboards zwingend zu berücksichtigen und sollten ggf.

nachgenutzt werden. Damit soll die Schnittstellenkomplexität minimiert werden. So muss die Eingliederung des geplanten Architekturboards in das bereits durch den IT-Planungsrat eingerichtete föderale IT-Architekturboard[47] geprüft werden.

Zur skizzierten Koordinierungsstelle der Deutschen Verwaltungscloud wird ein separates Dokument erstellt.

[47] Siehe https://www.fitko.de/it-architektur.

7 Anhang

7.1 Definition der Verbindlichkeitsgrade der Standards

Jeder Standard für Cloud-Standorte hat einen Verbindlichkeitsgrad in Form von Modalverben angegeben, der eine Richtlinie für die Umsetzung darstellt. Untenstehende Definitionen werden, entlang des RFC 2119[48] (Key words for use in RFCs to Indicate Requirement Levels), festgelegt. Die Anlehnung an den RFC 2119 findet ebenso Anwendung im IT-Grundschutz-Kompendium des BSI[49] und der Architekturrichtlinie für die IT des Bundes[50].

MUSS – Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss (uneingeschränkte Anforderung/verbindliche Festlegung).

SOLL – Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss sorgfältig abgewogen und stichhaltig begründet werden.

KANN – Dieser Ausdruck kennzeichnet eine Aussage mit dem Charakter einer gestatteten Option.

DARF NICHT – Dieser Ausdruck bedeutet, dass etwas in keinem Fall getan werden darf (uneingeschränktes Verbot).

---

[48] Request for Comments, siehe https://datatracker.ietf.org/doc/html/rfc2119.

[49] Siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6.

[50] Siehe https://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/architekturrichtlinie_it_bund_2020.pdf?__blob=publicationFile.

7.2 Zuordnung von Begrifflichkeiten im Kontext der Norm DIN ISO/IEC 17788:2016-04

Die Norm DIN ISO/IEC 17788:2016-04 regelt Begrifflichkeiten im Kontext von Cloud-Umgebungen. Im Rahmen der DVS wurde sich bewusst auf abweichende Bezeichnungen geeinigt, um das Rollenspiel zwischen klassischer Welt und neuer Welt einfacher abzubilden. Durch die Verkettung der Beziehungen nehmen die Rollen der DVS bei Bedarf mehrere Rollen nach der DIN ISO/IEC 17788:2016-04 ein[51]. Grundsätzlich werden die Begrifflichkeiten wie folgt zugeordnet:

Ein **Auftraggeber** (Bedarfsträger oder Kunde) einer Softwarelösung wird als **Cloud-Dienstleistungskunde** (engl. *cloud service customer*) verstanden, der zum Zwecke der Nutzung von Cloud-Services in einer Geschäftsbeziehung zum Softwarebetreiber steht.

Der **Softwarebetreiber** wird gegenüber dem Auftraggeber als **Cloud-Dienstleister** (engl. *cloud service provider*) betrachtet und steht mit diesem zum Zwecke der Bereitstellung von Cloud-Services in einer Geschäftsbeziehung. Der Softwarebetreiber stellt vorrangig aber nicht zwingend ausschließlich Softwarelösungen bereit, die durch den Auftraggeber genutzt werden. Der Softwarebetreiber steht gleichzeitig als **Cloud-Dienstleistungskunde** zum Zwecke der Nutzung von Cloud-Services in einer Geschäftsbeziehung mit dem Plattformbetreiber.

Ein **Plattformbetreiber** wird gegenüber dem Softwarebetreiber als **Cloud-Dienstleister** angesehen und steht mit diesem zum Zwecke der Bereitstellung von Cloud-Services in einer Geschäftsbeziehung. Der Plattformbetreiber stellt vorrangig aber nicht zwingend ausschließlich Plattformdienste bereit, auf deren Basis Softwarelösungen von Softwarebetreibern betrieben werden.

Der **Softwarelieferant** wird als **Cloud-Dienstleistungspartner** (engl. *cloud service partner*) verstanden, der dem Softwarebetreiber Software zur Verfügung stellt, aber selbst keinen Cloud-Service erbringt. Der Softwarelieferant kann in geschäftlicher Beziehung mit dem Auftraggeber und / oder dem Softwarebetreiber stehen.

Die **Nutzende des Cloud-Service-Portals** sind Mitarbeiter des Auftraggebers oder des Softwarebetreibers. Sie nutzen die Funktionen des Cloud-Service-Portals unter anderem zur

[51] Die Definitionen nach DIN ISO/IEC 17788:2016-04 sind im Glossar aufgeführt.

Beauftragung, Verwaltung und Kündigung von Services.

7.3 Glossar

Zur Unterstützung der einheitlichen Verwendung der wichtigsten Begriffe wird ein Glossar geführt. Folgende Begriffe sind wesentlich für dieses Dokument:

- **Application-Level-Gateway** – Sicherheitskomponente, die die Kommunikation zwischen Clients und Applikationsservern kontrolliert.
- **Auditsystem** – Ein Audit untersucht, ob Prozesse, Anforderungen und Richtlinien die geforderten Standards erfüllen. Das Auditsystem stellt die möglichst automatisierte Durchführung von Audits sicher.
- **Auftraggeber einer Softwarelösung** – Der Auftraggeber (z. B. Verwaltungsorganisationen wie Ministerien) einer Softwarelösung beauftragt für den Betrieb den Softwarebetreiber anhand vertraglicher Verpflichtungen, um Softwarelösungen nutzbar zu machen.
- **Basis-Image** – Basis-Images sind Container-Images, welche als Grundlage zur Erstellung von Container für Softwarelösungen genutzt werden. Sie enthalten Komponenten des Betriebssystems und gegebenenfalls standardisierte Erweiterungen.
- **Change** – Modifizieren oder Aktualisieren einer IT-Lösung.
- **Cloud Computing** – Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite, der im Rahmen von Cloud Computing angebotenen Dienstleistungen, umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software (*Definition gemäß BSI: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html*).
- **Cloud Native Computing** – Cloud Native Computing ist ein Ansatz in der Softwareentwicklung, der Cloud Computing verwendet, um skalierbare Anwendungen (Softwarelösungen) in modernen, dynamischen Umgebungen wie öffentlichen, privaten

und hybriden Clouds zu erstellen und auszuführen (*Definition gemäß Cloud Native Computing Foundation: https://github.com/cncf/foundation/blob/master/charter.md*).

- **Cloud-Dienstleister** – Eine Partei, die Cloud-Dienste zur Verfügung stellt. Der Cloud-Dienstleister konzentriert sich auf Aktivitäten zur Bereitstellung und Sicherstellung von Cloud-Diensten für den Cloud-Dienstleistungskunden sowie auf die Wartung von Cloud-Dienstleistungen. Die Rolle des Cloud-Dienstleisters umfasst eine große Menge von Aktivitäten (z. B. Anbieten von Diensten, Bereitstellen und Überwachen von Diensten, Verwalten von Geschäftsplänen, Bereitstellen von Auditdaten usw.) sowie zahlreiche Unterrollen (z. B. Geschäftsmanager, Dienstmanager, Netzanbieter, Sicherheits- und Risikomanager usw.) (*Definition gemäß DIN ISO/IEC 17788:2016-04*).
- **Cloud-Dienstleistungskunde** – Eine Partei, die in einer Geschäftsbeziehung zum Zweck der Nutzung von Cloud-Diensten steht. Die Geschäftsbeziehung besteht zu einem Cloud-Dienstleister oder einem Cloud-Dienstleistungspartner. Schlüsselaktivitäten für einen Cloud-Dienstleistungskunden sind unter anderem die Nutzung von Cloud-Diensten, die geschäftliche Administration und die Administration der Nutzung von Cloud-Diensten (*Definition gemäß DIN ISO/IEC 17788:2016-04*).
- **Cloud-Dienstleistungspartner** – Eine Partei, die in Unterstützung oder Ergänzung der Aktivitäten des Cloud-Dienstleisters und/oder des Cloud-Dienstleistungskunden handelt. Die Aktivitäten eines Cloud-Dienstleistungspartners variieren je nach Art des Partners und dessen Beziehung zum Cloud-Dienstleister oder zum Cloud-Dienstleistungskunden. Beispiele für Cloud-Dienstleistungspartner sind der Cloud-Auditor und Cloud-Dienstleistungsvermittler (*Definition gemäß DIN ISO/IEC 17788:2016-04*).
- **Cloud-Standort** – Cloud-Standorte bezeichnen die Rechenzentren bei Bund, Ländern und Kommunen, die IT-Infrastruktur bereitstellen und bspw. Rechenkapazitäten innerhalb der Deutschen Verwaltungscloud verfügbar machen. Dabei muss nicht zwangsweise die gesamte Infrastruktur der Rechenzentren Teil der Deutschen Verwaltungscloud sein, es können auch Teilbereiche betrachtet werden.
- **Compliance** – Compliance ist die Umschreibung für die Gewährleistung von regelkonformem Handeln in Bezug auf die Einhaltung von Gesetzen und Richtlinien.

- **Container-as-a-Service** – Cloud-Computing-Modell, das Virtualisierungsleistungen in Form eines Container-basierten Services bereitstellt. Angesiedelt ist es zwischen den Modellen IaaS und PaaS.
- **Container-Cluster** – Cluster in Kubernetes sind ein Rechner-Verbund, der für den Betrieb von containerisierten Softwarelösungen zuständig ist.
- **Continuous Deployment** – Ansatz in der Softwareentwicklung, bei dem Änderungen an der Software automatisiert und nach festen Kriterien in die aktuelle Software beziehungsweise in die Produktion überführt werden. Auf diese Weise wird eine kontinuierliche Auslieferung der Software ermöglicht.
- **Continuous Integration** – Ansatz in der Softwareentwicklung, bei dem neue Programmteile sofort getestet und zusammengeführt werden, statt dies bspw. nur einmal täglich zu tun.
- **Demilitarisierte Zone** – Speziell kontrolliertes Netzwerk, das sich zwischen dem externen Netzwerk (Internet) und dem internen Netz befindet. Es stellt eine Art Pufferzone dar, die die Netze durch strenge Kommunikationsregeln und Firewalls voneinander trennt.
- **Deployment** – Bereitstellung von Software mit halb- oder vollautomatisierten Prozessen zur Installation und Konfiguration auf PCs und Servern.
- **Deutsche Verwaltungscloud** – Standardisierte, föderale Cloud-Infrastruktur von Bund, Länder und Kommunen im Rahmen der beschlossenen Deutschen Verwaltungscloud-Strategie.
- **DevOps-Ansatz** – Zusammenwachsen von Entwicklung und Betrieb von IT-Systemen und -Lösungen.
- **Digitale Souveränität** – Die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können (*Definition gemäß ÖFIT:* *https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souveränität*).
- **Firewall** – System aus soft- und hardwaretechnischen Komponenten, das dazu eingesetzt wird, IP-basierte Datennetze sicher zu koppeln (*Definition gemäß BSI:* *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einz*

el_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2021.pdf?__blob=publicationFile&v=2).

- **Incident** – Sicherheitsvorfall oder eine Betriebsstörung einer IT-Lösung.
- **Kryptomodul** – Mit einem Kryptomodul ist ein Produkt gemeint, das die im Kryptokonzept dargelegte Sicherheitsfunktion bietet. Ein solches Produkt kann dabei aus Hardware, Software, Firmware oder aus einer Kombination daraus bestehen. Hinzu kommen noch notwendige Bauteile wie Speicher, Prozessoren, Busse und die Stromversorgung, um die Kryptoprozesse umzusetzen. Ein Kryptomodul kann in unterschiedlichen IT- ode Telekommunikationssystemen verwendet werden, um sensible Daten bzw. Informationen zu schützen (*Definition gemäß BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_1_Kryptokonzept_Edition_2021.pdf?__blob=publicationFile&v=2*).
- **Master** – Ein Kubernetes-Cluster basiert auf einem Satz von Maschinen. Diese werden in Master und Worker aufgeteilt. Der Kubernetes Master besteht aus drei Prozessen, die auf einem einzelnen Node in Ihrem Cluster ausgeführt werden, der als Master-Node bezeichnet wird.
- **Messaging** – Software, die text- oder zeichenbasierte Kommunikation in Echtzeit ermöglicht.
- **Multi-Cloud** – Parallele Nutzung von Cloud-Services und -Plattformen mehrerer Anbieter.
- **P-A-P-Struktur** – "Paketfilter – Application-Level-Gateway – Paketfilter" als Empfehlung des BSI für ein dreistufiges Firewall- bzw. Sicherheitsgateway-System.
- **Pipeline** – CI/CD-Pipeline dient zur Ausführung von Automatisierungsschritten für die Bereitstellung von neuen Softwareversionen.
- **Plattformbetreiber** – Der Plattformbetreiber betreibt die IT-Infrastruktur im Cloud-Standort und stellt dem Softwarebetreiber Werkzeuge zur manuellen und/oder automatischen Orchestrierung bereit.

- **Service-Level-Agreement** – Vereinbarung zwischen Anbieter und Kunde und dient der Qualitätssicherung. In dieser Vereinbarung werden die genauen Leistungseigenschaften und Gütestufen (*Service Levels*) des Produktes bzw. der Dienstleistung festgelegt.
- **Service-Orchestrierung** – Unter Orchestrierung versteht man die automatisierte Konfiguration, Verwaltung und Koordinierung von Computersystemen, Softwarelösungen und Services. In Verbindung mit Containerumgebungen bezeichnet Orchestrierung vor allem die Steuerung, wann Container starten und stoppen, die Gruppierung von Containern in Clustern und Koordinierung aller Prozesse, aus denen sich eine Softwarelösung zusammensetzt.
- **Sicherheitsgateway** – Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardware-technischen Komponenten. Es gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer Sicherheitsrichtlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden (*Definition gemäß BSI: https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/S/Sicherheitsgateway.html).*
- **Softwarebetreiber** – Der Softwarebetreiber verantwortet als Auftragnehmer den Betrieb einer Softwarelösung entsprechend vertraglicher Verpflichtungen gegenüber dem Auftraggeber und managt die Service-Orchestrierung. Wenn möglich, stimmt er die Anforderungen an den Betrieb der Software mit dem Softwarelieferanten ab. Er ist das Bindeglied zwischen Plattformbetreiber und Softwarelieferant.
- **Softwarelieferant** – Der Softwarelieferant ist eine Organisation (im Sinne einer juristischen Person) oder eine lose miteinander gekoppelte Community (Gruppe von Entwicklerinnen und Entwickler), welche dem Softwarebetreiber Software(-releases) bereitstellt.
- **Softwarelösung** – Eine Softwarelösung ist eine Anwendungssoftware für eine bestimmte, konkrete Aufgabenstellung, die also der Lösung eines konkreten Problems eines Auftraggebers dient.

- **Virtual Local Area Network** – Logisches Netz, das auf einem physischen LAN aufsetzt.
- **Voice-over-IP** – Es wird nicht mehr klassisch über einen analogen Telefonanschluss, sondern über einen Breitband-Internetanschluss telefoniert. Dazu werden Sprachsignale umgewandelt und als Datenpakete über ein IP-Netzwerk übertragen.
- **Web-Proxy** – Der Web-Proxy fungiert als ein Gateway zwischen einem Client, z. B. Web-Browser, und dem Applikationsserver. Neben Sicherheitsfunktionen übernehmen diese Proxy-Server oft auch Funktionen zur Verbesserung des I/O-Verhaltens der Webanwendung.
- **Worker** – Ein Kubernetes-Cluster basiert auf einem Satz von Maschinen. Diese werden in Master und Worker aufgeteilt. Die Worker stellen die Ressourcen zur Ausführung der Container-Anwendungen bereit. Jedes Cluster muss mindestens einen Worker beinhalten.
- **Workload** – Ein Workload ist im Computerumfeld ein einzelner Arbeitsauftrag, der an physische oder virtuelle Systeme zur Bearbeitung vergeben wird.

7.4 Abkürzungsverzeichnis

Abkürzung	Bedeutung
AG	Arbeitsgruppe
API	Application Programming Interfaces
BSI	Bundesamt für Sicherheit in der Informationstechnik
CaaS	Container-as-a-Service
CI/CD	Continuous Integration/Continuous Delivery
DBMS	Datenbankmanagementsystem
DVS	Deutsche Verwaltungscloud-Strategie
EfA	Einer-für-Alle
IaaS	Infrastructure-as-a-Service
IP	Internet Protocol
IT	Informationstechnologie
IT-PLR	IT-Planungsrat
IVÖV	Informationsverbundes der Öffentlichen Verwaltung
NdB	Netze des Bundes
ÖFIT	Kompetenzstelle Öffentliche IT
OS	Open-Source
OSCI	Online Services Computer Interface
OSS	Open-Source-Software
ÖV	Öffentliche Verwaltung
OZG	Onlinezugangsgesetz
PaaS	Platform-as-a-Service

Abkürzung	Bedeutung
SaaS	Software-as-a-Service
SCS	Sovereign Cloud Stack
SLA	Service-Level-Agreement
UAG	Unterarbeitsgruppe
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VS-NfD	Verschlusssachen – Nur für den Dienstgebrauch