IT-Planungsrat

Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur

- Version 2.0.1 vom 10. Oktober 2022 -

10/2022

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

Oktober 2022

Inhaltsverzeichnis

1 Einführung

In der 33. Sitzung des IT-Planungsrates (IT-PLR) wurde das Konzeptpapier zur *Deutschen Verwaltungscloud-Strategie – Föderaler Ansatz* beschlossen (Beschluss Nr. 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 dort 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, Ländern 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 es, eine Cloud- bzw. standortübergreifende und wechselseitige Nutzung von Cloud-Services und Softwarelösungen zu ermöglichen. Durch die standardisierten, modularen IT-Architekturen der DVS sollen außerdem kritische Abhängigkeiten von einzelnen Anbietern reduziert werden.

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 des Beschlusses des IT-PLR die technische Konzeption und Operationalisierung an die Unterarbeitsgruppe Technik und Betrieb (kurz: UAG Technik) übergeben. In dieser UAG

---

[1] Siehe IT-PLR Beschluss 2020/54 – AG Cloud-Computing und Digitale Souveränität https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-54_Deutsche_Verwaltungscloud_Strategie.pdf.

[2] Siehe IT-PLR Beschluss 2021/09 – AG Cloud-Computing und Digitale Souveränität https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf.

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

sind insbesondere IT-Dienstleister der ÖV vertreten. Durch die so hergestellte Nähe zur Praxis wird die fortlaufende technische Umsetzbarkeit parallel zur Konzeption gewährleistet.

Entsprechend den Standardisierungsbereichen und Anforderungen im DVS-Konzeptpapier[4] gliedert sich die UAG anhand von neun Handlungsfeldern in sieben operative Teams[5]:

- Handlungsfeld 1+4 „Infrastruktur und Schnittstellen“[6]
- Handlungsfeld 2 „Policies / Governance“
- Handlungsfeld 3 „Cloud-Service-Portal und Supportstrukturen“
- Handlungsfeld 5+7 „Entwicklungsumgebung und Code Repository“
- Handlungsfeld 6 „Betriebsmodell“
- Handlungsfeld 8 „Proofs-of-Concept”
- Handlungsfeld 9 „Einbindung externer Cloud-Anbieter“

Ausgehend vom 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[7] abgeleitet, aus dem die vorliegende Zielarchitektur spezifiziert wurde.

1.1 Anmerkungen zur ersten Fortschreibung

Das Rahmenwerk der Zielarchitektur wurde in der Version 1.0 in der 36. Sitzung des IT-PLR beschlossen (Beschluss Nr. 2021/46). Der IT-PLR beauftragte die AG Cloud zudem mit der Feinkonzeption von Cloud-Service-Portal und Koordinierungsstelle der DVS, mit der Evaluation der Nachnutzung bestehender Strukturen der ÖV für die Koordinierungsstelle, mit der

---

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

[5] Die Handlungsfelder 1 und 4 sowie 5 und 7 wurden aufgrund sich im Zeitverlauf entwickelnder wesentlicher thematischer Überschneidungen zusammengefasst.

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

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

Durchführung weiterer Machbarkeitsnachweise, mit der Weiterentwicklung der Standards der DVS und mit der regelmäßigen Fortschreibung des Rahmenwerks der Zielarchitektur.

Mit der ersten Fortschreibung des Rahmenwerks zur Version 2.0 wird dem letztgenannten Auftrag nachgekommen. Das Rahmenwerk wurde um zahlreiche Ausführungen gemäß des aktuellen Konzeptionsstands ergänzt und aktualisiert. Insbesondere finden sich substanzielle Änderungen in den folgenden Punkten:

- **Wesentliche Standards:** Bestehende Standards wurden ergänzt (s. Kapitel 5.3.4 Containerumgebung und Container-Cluster, Kapitel 5.3.5 Entwicklungsbereich) und neue Standards aufgenommen (s. Kapitel 5.3.3 Netzanbindung, Kapitel 5.3.6 Kommunikation zwischen Cloud-Standort, Softwarebetreiber und Cloud-Service-Portal).
- **Systematik der Deutschen Verwaltungscloud:** Die für die Deutsche Verwaltungscloud spezifizierten Rollen wurden anhand möglicher Nutzungsszenarien weiter detailliert (s. Kapitel 4).
- **Weiteres Vorgehen und Operationalisierung der Deutschen Verwaltungscloud:** Dieser Abschnitt wurde gemäß der zum Zeitpunkt der Fortschreibung aktuellen Entwicklungen zur Koordinierungsstelle und zur Pilotierung der Deutschen Verwaltungscloud umfassend aktualisiert.

Darüber hinaus wurde mit dem Start des produktiven Betriebs der OS-Plattform der ÖV, Open CoDE[8], ein wichtiger Baustein in der Systematik der Deutschen Verwaltungscloud integriert. Verweise auf Open CoDE wurden an den entsprechenden Stellen ergänzt.

[8] Siehe https://www.opencode.de.

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 Beschluss Nr. 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 fortlaufenden Umsetzung der Deutschen Verwaltungscloud (siehe Kapitel 5.4). Die in Kapitel 5 definierten Standards sowie die zu veröffentlichenden Detailstandards (s. Kapitel 2.4) unterstützen die in Eckpunkte[9]- und Strategiepapier[10] angestrebte offene, modulare und interoperable Ausrichtung der IT-Architektur der ÖV. 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[11].

Der Fokus des vorliegenden Rahmenwerks der Zielarchitektur sowie den darauf basierenden Pilotierungsprojekten (vgl. Kapitel 6.2) liegt auf der Schaffung einer Grundlage zum standardisierten Betrieb bestehender und zukünftiger Cloud-Dienste und Softwarelösungen, um Wechselmöglichkeiten sowohl im Hinblick auf Softwarelösungen als auch auf Anbieter bzw. Betriebsumgebungen herzustellen bzw. zu vereinfachen. Die Weiterentwicklung der Deutschen

---

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

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

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

Verwaltungscloud, bspw. die Konzeption der Koordinierungsstelle und die Entwicklung des Cloud-Service-Portals (vgl. Kapitel 6.1 und 5.4), erfolgt stufenweise.

Anforderungen und Vorgaben für Cloud-Dienste und 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) erfolgt analog dem Betrieb und der Bereitstellung von Individualsoftwarelösungen durch Softwarebetreiber (vgl. Kapitel 4.4).

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 sowie Nutzungsszenarien.
- **Kapitel 5** „Wesentliche Standards“ definiert obligatorische und optionale Standards für die Deutsche Verwaltungscloud und spezifiziert ausgewählte Standards mit weiterführenden Erläuterungen.
- **Kapitel 6** „Weiteres Vorgehen und Operationalisierung der Deutschen Verwaltungscloud“ beinhaltet Handlungsempfehlungen zum weiteren Aufbau der Deutschen Verwaltungscloud, die Skizzierung weiterführender Handlungsstränge für die fortlaufende Spezifizierung der Deutschen Verwaltungscloud und Erläuterungen zur Koordinierungsstelle der Deutschen Verwaltungscloud.

2.2 Geltungsbereich und Zielgruppe

Mit dem Beschluss Nr. 2021/46 des IT-PLR wurde die Architektur der Deutschen Verwaltungscloud sowie die entsprechenden Standards übergreifend für Bund, Länder und Kommunen sowie für deren IT-Dienstleister gültig.

Die Standardisierung im Rahmen der DVS richtet sich vor allem 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.

Eine Abweichung von den festgelegten Standards ist nur in begründeten Ausnahmefällen gestattet und bedarf einer dokumentierten Begründung und zeitlicher Einschränkung. Die Genehmigung erfolgt durch das zu etablierende Architekturboard und die Koordinierungsstelle (siehe Kapitel 6.1)[12].

2.3 Abgrenzung

Die im Rahmen der Deutschen Verwaltungscloud festgelegten Standards betten sich in bereits bestehende Vorgaben und 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 werden und es müssen mögliche Schnittmengen zu diesen 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 und zurückgreift.

Zusammenfassend setzt die Deutsche Verwaltungscloud die verwaltungsspezifischen Vorgaben (insbesondere im Hinblick auf etwaige bestehende Standards, z.B. Informationssicherheits-, Datenschutz- sowie Geheimschutzanforderungen) um und beachtet bei der Modernisierung der IT-Infrastruktur der ÖV neueste Entwicklungen im Cloud-Bereich.

2.3.1 Nahestehende Vorhaben

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

- **Cloud-Lösungen von Bund, Ländern und Kommunen (z. B. Bundescloud)**: Wie in Kapitel 1 angedeutet, bestehen bereits verschiedene Cloud-Lösungen (Bereitstellung der Servicemodelle Infrastrucuture-as-a-Service(IaaS); Platform-as-a-Service(PaaS) inkl.

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

Container-as-a-Service (CaaS); Software-as-a-Service(SaaS)[13]) auf den unterschiedlichen Verwaltungsebenen von Bund, Ländern und Kommunen.

- **Gaia-X**[14]: Das Vorhaben Gaia-X zielt darauf ab, eine föderierte, europäische Dateninfrastruktur nutzbar zu machen, 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**[15] (SCS): Das Projekt SCS entwickelt einen föderierbaren und vollständig offenen Software-Stack für Cloud-Dienstleister, damit diese Cloud-Infrastruktur herstellerunabhängig 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**[16]: 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 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[17].

---

[13] 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.

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

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

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

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

Bestehende Cloud-Lösungen der ÖV sowie die zugehörigen IT-Dienstleister müssen als Teilnehmer der Deutschen Verwaltungscloud die definierten Standards der DVS umsetzen. Durch die konsequente Umsetzung der DVS-Standards werden vielschichtige Mehrwerte geschaffen, die ebenfalls die OZG-Umsetzung und das EfA-Prinzip zukünftig unterstützen (siehe Kapitel 3). Perspektivisch sollen OZG und Deutsche Verwaltungscloud ineinandergreifen. Die OZG-Umsetzung ist nicht abhängig vom Aufbau der Deutschen Verwaltungscloud und wird als paralleler Handlungsstrang angesehen. Während OZG Verwaltungsleistungen digitalisiert, soll die DVS die IT-Infrastruktur der ÖV zukunftsfähig ausrichten. Dennoch kann die Deutsche Verwaltungscloud eine wesentliche unterstützende Wirkung auf die OZG-Umsetzung entfalten, wenn etwa EfA-Leistungen als DVS-konforme (Cloud-) Services entwickelt und angeboten werden, da sie so weitestgehend ohne individuellen Konfigurationsbedarf in allen Rechenzentren umgesetzt werden können, die den Standards der DVS entsprechen.

SCS ist für hohe Sicherheitsanforderungen konzipiert. Demnach ist im Projektplan des SCS vorgesehen, die Plattformbetreiber der ÖV für eine BSI[18]-Zertifizierung nach IT-Grundschutz durch entsprechende Architektur, Entwicklungsprozesse und die Bereitstellung entsprechenden Wissens zu unterstützen[19]. Die Kompatibilität der Deutschen Verwaltungscloud mit Gaia-X kann durch die Mitarbeit von SCS 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, sofern die Anforderungen an die Informationssicherheit und den Geheimschutz nachweislich erfüllt werden. Deshalb sind Vertreter des Projektes SCS im regelmäßigen Austausch mit der UAG Technik.

Während der vordergründige Fokus von Gaia-X auf der Etablierung einer den Zielen der Digitalen Souveränität entsprechenden vernetzten Dateninfrastruktur liegt, soll die Deutsche Verwaltungscloud vor allem die cloud-übergreifende Wiederverwendbarkeit von Cloud-Services und Softwarelösungen gewährleisten. Zukünftig könnten Lösungen des SCS bzw. Standards von Gaia-X übernommen und für die Deutsche Verwaltungscloud nachgenutzt werden. Die Standards

[18] Bundesamt für Sicherheit in der Informationstechnik.

[19] Nach derzeitigem Planungsstand erscheint die Bereitstellung der notwendigen Komponenten und die parallelen Vorbereitungen für eine Zertifizierung bis Anfang 2023 realistisch.

der Deutschen Verwaltungscloud werden dabei ihre Gültigkeit bewahren und lediglich entsprechend erweitert.

2.3.2 Relevante Vorgaben der ÖV

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

- **IT-Grundschutz**: Der IT-Grundschutz des BSI führt Methoden, Anleitungen und Empfehlungen auf, um das Niveau der Informationssicherheit in einer Institution aufrechtzuerhalten und anzuheben. Es wird dabei ein ganzheitlicher Ansatz verfolgt: Neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet. Der IT-Grundschutz wird durch das IT-Grundschutz-Kompendium und die BSI-Standards näher beschrieben. Mit dem IT-Grundschutz-Kompendium wird dem Anwendenden eine Handlungsanweisung bereitgestellt, um einen bestimmten Bereich abzusichern. Das Kompendium wird jährlich in einer neuen Version veröffentlicht. Durch die BSI-Standards werden bewährte Vorgehensweisen bereitgestellt, durch welche notwendige Sicherheitsmaßnahmen systematisch identifiziert und umgesetzt werden können[20].
- **Kriterienkatalog Cloud Computing des BSI (kurz: C5)**[21]: Der Katalog spezifiziert Mindestanforderungen an die Informationssicherheit für Cloud-Services. 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. Der C5 betrachtet auch explitzit die Mitwirkungspflicht von Cloud-Anbieter und Cloud-Kunde hinsichtlich der Informationssicherheit („shared responsibility“).

[20] S. BSI IT-Grundschutz, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

[21] 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.

- **Architekturrichtlinie für die IT des Bundes**[22]: Mit der Architekturrichtlinie für die IT des Bundes wird ein aktives Architekturmanagement für die IT der Bundesverwaltung verfolgt. Die von der IT-Konsolidierung Bund[23] betroffenen Bereiche sollen durch konkrete strategische Architekturvorgaben aktiv bei Entscheidungsprozessen unterstützt werden und die Vorgaben für die Weiterentwicklung der IT des Bundes einhalten. Außerdem unterstützen die Vorgaben eine Ausrichtung der laufenden IT-Projekte an den strategischen Anforderungen und politischen Aufgaben. Beispiele für Architekturvorgaben sind u. a. die Sicherstellung der Herstellerunabhängigkeit sowie die Sicherstellung von loser Kopplung und Modularität.
- **Weitere Bundes- und länderspezifische sowie kommunale Architekturrichtlinien/-vorgaben bzw. Mindestanforderungen für die IT**: Neben den Architekturrichtlinien des Bundes existieren weitere bundes-, sowie länderspezifische Architekturvorgaben und Mindestanforderungen für die IT. Dazu zählen die DSGVO, NdB-Dienstleisterpflichten sowie weitere Anforderungseinheiten des BSI in Cloud-Projekten, darunter bspw. die Mindeststandards des BSI[24], die Verschlussachenanweisung, Detektion und Zulassung.
- **Föderale Architekturrichtlinien für die IT**[25]: Um eine einheitliche Architektur über alle föderalen Ebenen hinweg sicherzustellen und aktiv zu steuern, wurden föderale Architekturrichtlinien definiert. Diese basieren auf den zuvor geschilderten Vorgaben des Bundes und der Länder.
- **Anforderungen an Technologieanbieter und -lösungen zur Stärkung der Digitalen Souveränität**[26]: Die AG Cloud und deren UAG Beschaffung definieren, als Teil der Strategie

---

[22] Siehe https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/architekturen-standard/ArchRL.pdf?__blob=publicationFile&v=7.

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

[24] Siehe https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mindeststandards_node.html

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

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

zur Stärkung der Digitalen Souveränität der IT der ÖV[27], 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 die Entwicklung und Bereitstellung von IT-Leistungen für die ÖV sowie deren Anbieter 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, sowie etwaige Verschlusssachenanweisungen des Bundes und der Länder, wurden bei der Ausarbeitung der Zielarchitektur berücksichtigt und konkretisiert. Etwaige Widersprüche einzelner Vorgaben werden im Rahmen der Standardisierung aufgelöst[28]. 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 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 und iterativ weiterentwickelt und mit einem gemeinsamen Beschluss im Rahmen der einzurichtenden Koordinierungsstelle und dem Architekturboard der DVS (siehe Kapitel 6.1) 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. Neben dem Rahmenwerk der Zielarchitektur gelten die Detailstandards der DVS, die regelmäßig auf der Internetseite des IT-PLR veröffentlicht werden, in der jeweils aktuellen Version. Die Detailstandards der DVS werden derzeit von der UAG Technik ausgearbeitet und stellen vertiefende Behandlungen einzelner Punkte der im Rahmenwerk gemachten Festlegungen

[27] Siehe IT-PLR Beschluss Nr. 2021/09 – AG Cloud-Computing und Digitale Souveränität https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf.

[28] Sollten die in der DVS festgelegten Standards sich mit Standards oder Anforderungen an die Informationssicherheit oder den Geheimschutz widersprechen oder gegensätzlich ausgelegt werden können, sind immer die vom BSI vorgegebenen Anforderungen maßgeblich und umzusetzen.

dar. Wie das Rahmenwerk liegt die Verantwortlichkeit für die Detailstandards bis zur Etablierung des Architekturboards der DVS ebenfalls bei der AG Cloud und der UAG Technik. Da es sich bei den Detailstandards um detaillierte Ausarbeitungen der im Rahmenwerk definierten Anforderungen (s. Kapitel 5) handelt, wird der IT-PLR über die Änderungen informiert, ohne dass ein Beschluss notwendig ist. Die Detailstandards werden als gesonderte Dokumente einzeln veröffentlicht.

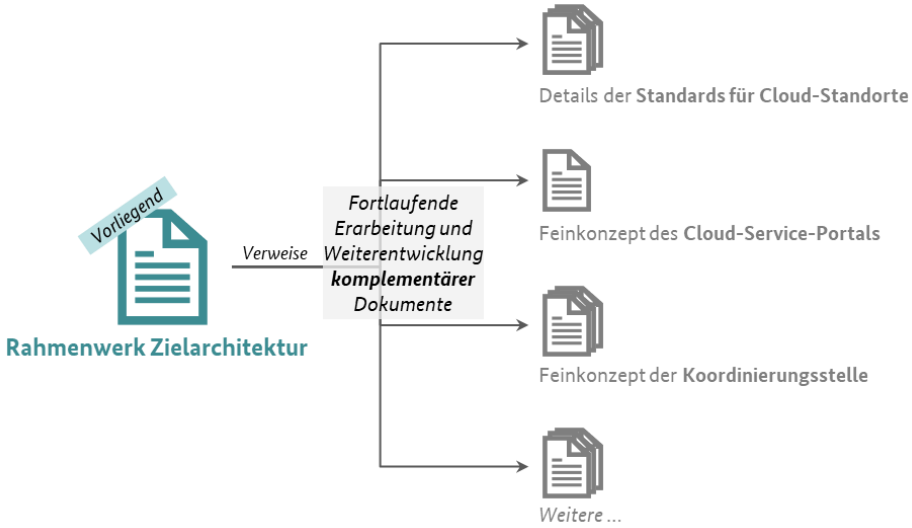

Abbildung 1: Dokumentenstruktur der DVS-Zielarchitektur

Die kontinuierliche Weiterentwicklung der Deutschen Verwaltungscloud und der Standards der DVS gewährleistet eine stets zeitgemäße Ausrichtung 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 den Standards weiterführende Dokumente erarbeitet, welche einerseits die technische Realisierungen verdeutlichen sollen und andererseits zusätzliche Elemente der Deutschen Verwaltungscloud spezifizieren (siehe Kapitel 5.4). Abbildung 1 stellt die geplante Dokumentenstruktur dar und ordnet das vorliegende Rahmenwerk ein.

3 Mehrwerte für die Öffentliche Verwaltung und deren IT-Infrastruktur

Durch die im Rahmen der DVS angestrebte Standardisierung von Betriebskonzepten, die Standardisierung der Infrastruktur- und Plattformbereitstellung sowie die Etablierung von standardisierten 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[29] (Wechselmöglichkeit, Gestaltungsfähigkeit und Einfluss auf IT-Anbieter) sowie auf den definierten Zielen des DVS-Konzeptpapiers.

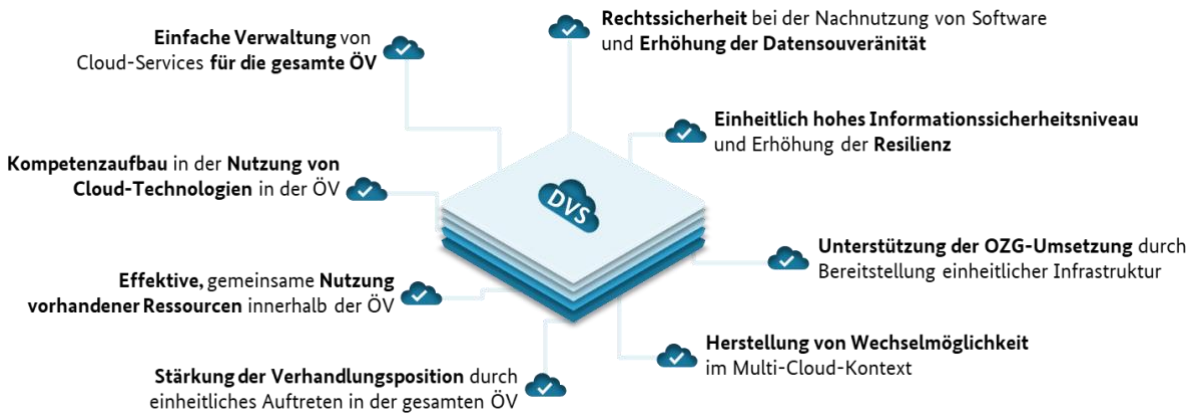

Abbildung 2: Mehrwehrte für die ÖV und deren IT-Infrastruktur (Auswahl)

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 Standardisierung 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.

[29] Siehe IT-PLR Beschluss Nr. 2021/09 – AG Cloud-Computing und Digitale Souveränität https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf.

- 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.
- Die Einbeziehung von Lösungsansätzen aus anderen Initiativen, wie z. B. Gaia-X oder 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 Cloud-Services und Softwarelösungen für die ÖV gesteigert und die Informationssicherheit übergreifend gestärkt. Ebenso wird eine Optimierung von Datenaustausch, -speicherung und -nutzung erzielt: Das Angebot von Cloud-Leistungen öffentlicher IT-Dienstleister an die gesamte ÖV über das Cloud-Service-Portal trägt zu einer effizienten und effektiven Nutzung verfügbarer Rechenzentrumsressourcen der ÖV und deren Dienstleister bei. Das Cloud-Service-Portal unterstützt hierbei durch das zentrale Angebot von Cloud-Services.
- Das Prinzip der EfA-Lösungen mit zentralem oder dezentralem Betrieb von Softwarelösungen im Rahmen der OZG-Umsetzung wird mittels einer standardisierten unterliegenden Infrastruktur mit dem möglichen Austausch und der Nachnutzung von modularen Lösungsbausteinen gefördert.
- Die erweiterte Zusammenarbeit zwischen Cloud-Service-Anbietern schafft Synergieeffekte über den gesamten Service-Lebenszyklus hinweg. Insbesondere trägt die Nutzung und Umsetzung der Deutschen Verwaltungscloud zum Kompetenzaufbau der öffentlichen IT-Dienstleister bei.
- Die Plattformstandardisierung und der hohe Automatisierungsgrad unterstützen dabei, die IT-Infrastruktur der ÖV effizient und effektiv aufzustellen. Durch die Möglichkeit des verteilten Betriebs von Cloud-Services und Softwarelösungen wird außerdem die Resilienz und Skalierbarkeit der Lösungen erhöht.

- Die Gestaltung und Ausrichtung der Deutschen Verwaltungscloud nach dem „privacy by design[30] / security by design[31]“-Prinzip berücksichtigt die Sicherheitsanforderungen über alle föderalen Ebenen hinweg.
- Die strenge Ausrichtung der definierten Standards an bestehenden Richtlinien und Vorgaben für Informationssicherheit unterstützt dabei, die Informationssicherheit der Infrastruktur weiter zu stärken.

[30] Siehe https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_de

[31] Siehe https://www.oeffentliche-it.de/-/security-by-design

4 Systematik der Deutschen Verwaltungscloud

In diesem Kapitel wird der Aufbau der Deutschen Verwaltungscloud im Zielzustand dargestellt. Zum einen werden grundsätzliche Eckpunkte festgehalten und die einzelnen Elemente des Aufbaus definiert. Zum anderen werden die relevanten Rollen innerhalb der Deutschen Verwaltungscloud beschrieben.

4.1 Grundsätzliche Eckpunkte

Im Rahmen der DVS 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 der Deutschen Verwaltungscloud in Rechenzentren von Bund, Ländern und Kommunen ermöglicht. Hierbei soll gewährleistet sein, dass Services oder Anwendungen, die innerhalb der Deutschen Verwaltungscloud bei verschiedenen Plattformanbietern des Bundes, der Länder und der Kommunen betrieben werden, ohne größeren Aufwand zwischen den verschiedenen Plattformanbietern den Betrieb wechseln können, um eine Multi-Cloud-Fähigkeit zu gewährleisten. Diese dezentrale, föderale Cloud-Infrastruktur soll durch die ÖV und deren IT-Dienstleister bereitgestellt und betrieben werden. Verwaltungsexterne Anbieter von Cloud-Leistungen werden auch einbezogen: Die Einbindung von Cloud-Services– die Standards der Deutschen Verwaltungscloud einhaltend – wird grundsätzlich unterstützt[32]. . Die Anwendung der DVS-Standards für verwaltungsexterne Anbieter von Cloud-Leistungen (z. B. Hyperscaler) sowie deren Services ist noch zu spezifizieren (vgl. Kapitel 4.2). Für den Aufbau der Deutschen Verwaltungscloud sollen hauptsächlich bereits existierende Cloudumgebungen in Bund, Ländern und Kommunen eingebunden werden. Bei diesen bzw. den betreibenden IT-Dienstleistern der ÖV ist das erforderliche Know-How bereits vorhanden. Durch die Herstellung von Kompatibilität unter den bestehenden

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

Cloudumgebungen können vorhandene Kapazitäten optimal genutzt und Synergien gehoben werden.

- **Allgemeine Verfügbarkeit von Cloud-Services**: Die angebotenen Cloud-Services (z.B. in den Servicemodellen IaaS, PaaS, SaaS) innerhalb der Deutschen Verwaltungscloud sollen für alle Organisationen der ÖV aus Bund, Ländern und Kommunen nutzbar sein. Entstehende Erweiterungen und Anpassungen eines Service bei einem Teilnehmenden der Deutschen Verwaltungscloud sollen in anderen Cloud-Standorten nachgenutzt werden können.
- **Einsatz von OS-Software (OSS)**: OSS wird für den Aufbau der Deutschen Verwaltungscloud priorisiert[33]. Kommerzielle Distributionen von OSS können eingesetzt werden[34]. Betriebene Cloud-Dienste und Softwarelösungen innerhalb der Deutschen Verwaltungscloud müssen nicht auf OSS basieren, Lock-in-Effekte[35] sollen jedoch verhindert, die Nachnutzung (z. B. durch OSS) ermöglicht und risikomindernde Maßnahmen[36] 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, das aus unterschiedlichen Netzen (z.B. Internet, Verwaltungsnetze) erreichbar ist und 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 des betriebenen Cloud-Diensts bzw. der betriebenen Softwarelösung) erfolgt direkt am Cloud-Standort ohne die Nutzung des

---

[33] 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 gemeinsamen Standards geschaffen werden.

[34] 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.

[35] „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.

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

Cloud-Service-Portals. Nähere Informationen zum Cloud-Service-Portal finden sich in Kapitel 5.4. Cloud-Services, die innerhalb der Deutschen Verwaltungscloud zur Verfügung stehen, sollen bereits vor dem Vollbetrieb des Cloud-Service-Portals bei den Cloud-Service-Anbietern bestellt und genutzt werden können.

- **Gemeinsame Weiterentwicklung:** Zur Kooperation an öffentlichen Entwicklungsprojekten und zur Weiterentwicklung wesentlicher Softwarekomponenten (z. B. Standard-Images oder Policies[37] für den Betrieb von Containern) wird eine verwaltungseigene Plattform eingerichtet, auf der Repositories für (OS-) Softwareprojekte wie z.B. Standard-(Applikations-) Images oder Policies für den Betrieb von Containern angelegt und gepflegt werden können. Es ist geplant, dieses Repository über den Continuous Integration- / Continuous Deployment-Prozess anzubinden. Bei der Plattform handelt es sich um die OS-Plattform der ÖV Open CoDE, die bereits jetzt einige dieser Funktionalitäten zur Verfügung stellt. Weitere Informationen zu Open CoDE finden sich auf der entsprechenden Website[38].

4.2 Übergreifende Struktur der Deutschen Verwaltungscloud

Grundsätzlich besteht die Deutsche Verwaltungscloud aus den folgenden zentralen Elementen:

1) **Cloud-Standorte, Plattformbetreiber, Softwarebetreiber und Cloud-Integratoren**
2) **Cloud-Service-Portal**
3) **Koordinierungsstelle**
4) **OS-Plattform der ÖV Open CoDE**

Spezifikationen der einzelnen Elemente finden sich in den folgenden Kapiteln.

[37] Vgl. u.a. Ergebnisdokument des 1. DVS Proof-of-Concept: https://www.it-planungsrat.de/fileadmin/it-planungsrat/foederale-zusammenarbeit/Gremien/AG_Cloud/220420_PoC-Ergebnisdokument_Langfassung_AG_Cloud_vf.pdf

[38] https://www.opencode.de.

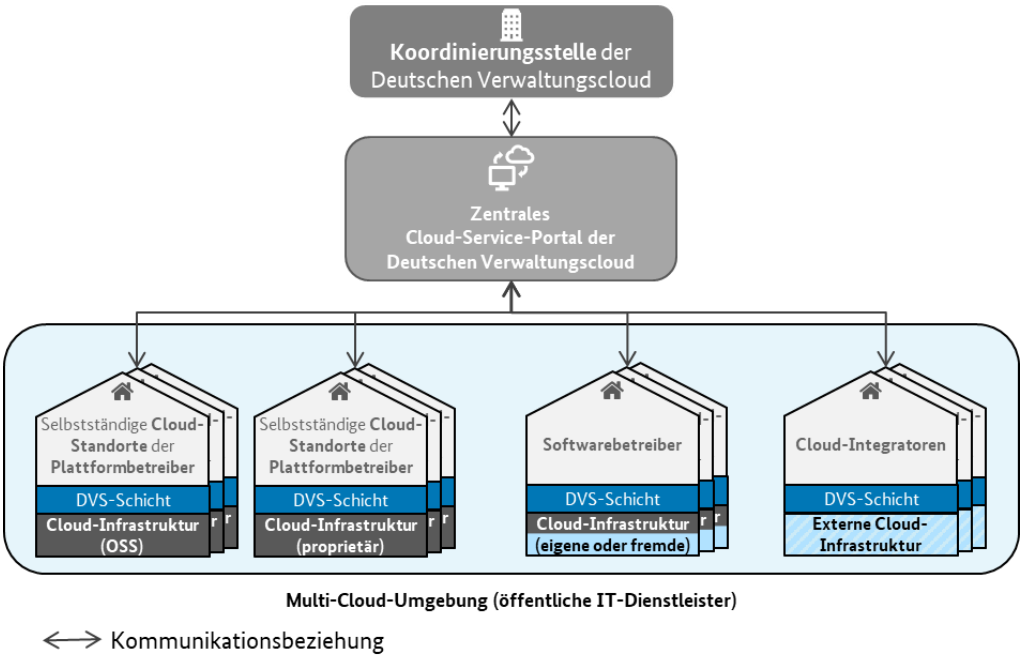

Abbildung 3: Elemente der Deutschen Verwaltungscloud (illustrative Darstellung)

Als **Cloud-Standorte** werden die Rechenzentren bei Bund, Ländern und Kommunen bzw. bei deren IT-Dienstleistern bezeichnet, die IT-Infrastruktur, also bspw. Rechenkapazitäten innerhalb der Deutschen Verwaltungscloud und damit insbesondere Services in den Servicemodellen IaaS und PaaS anbieten. 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 sollen die Services der Cloud-Standorte automatisiert über programmatische Schnittstellen (d. h. Application Programming Interfaces, APIs) steuerbar sein. Cloud-Standorte werden von den Plattformbetreibern bereitgestellt. Details zu den Standards für Plattformbetreiber und weitere Cloud-Service-Anbieter finden sich in Kapitel 5.

Neben den Plattformbetreibern, die in ihren Cloud-Standorten Cloud-Services verfügbar machen, bieten auch **Softwarebetreiber** Cloud-Services an, jedoch ausschließlich im Servicemodell SaaS. Dabei nutzen Softwarebetreiber die eigene oder fremde DVS-konforme Cloud-Infrastruktur zum Betrieb der SaaS-Angebote. Eine ausführliche Beschreibung entsprechender Nutzungsszenarien findet sich in Kapitel 4.3.

Bei **Cloud-Integratoren** handelt es sich um IT-Dienstleister der ÖV, die Angebote externer, d.h. verwaltungsfremder Cloud-Anbieter (z.B. Hyperscaler) gemäß den DVS-Standards konfigurieren und so rechtssicher für die Deutsche Verwaltungscloud verfügbar machen.

Das **Cloud-Service-Portal** ist der zentrale Einstiegspunkt für Bedarfsträger aus der ÖV zur Verwaltung von Cloud-Services in einem Multi-Cloud-Kontext[39]. Es wird aus dem Internet und aus den Verwaltungsnetzen erreichbar sein. Aufgrund der Trennungsanforderungen[40] an die Netzwerkstrukturen wird es entsprechend zwei separate Ausprägungen des Portals geben. Die Suche von Cloud-Services erfolgt mittels eines einheitlichen Cloud-Service-Katalogs. Die Angebote im Cloud-Service-Portal werden in Abhängigkeit des Zugriffsnetzes dargestellt. Beim Zugriff aus den Verwaltungsnetzen werden alle Cloud-Services mit Verbindung in die Verwaltungsnetze dargestellt und es kann dementsprechend auf sie zugegriffen werden. Dies schließt auch die Internetangebote ein. Beim Zugriff aus dem Internet werden nur die Angebote, die auch über das Internet verfügbar sind, zur Verwaltung angezeigt.

Zwischen Cloud-Service-Portal, Cloud-Service-Anbietern und den weiteren Nutzenden des Cloud-Service-Portals sind, unter Berücksichtigung der Anforderungen des BSI wie z.B. dem IT-Grundschutz, Kommunikationsmöglichkeiten zur Bereitstellung und zum Abruf von Serviceangeboten sowie zum weiteren Informationsaustausch umzusetzen (siehe Kapitel 5.3.6.).

Details zum Cloud-Service-Portal finden sich in Kapitel 5.4. Die Verknüpfung mit anderen Service-Portalen bei IT-Dienstleistern der ÖV 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 die Pflege des Servicekatalogs, als Auflistung aller angebotenen Services innerhalb der Deutschen Verwaltungscloud, durch die Cloud-Service-Anbieter koordinieren. Die Koordinierungsstelle verpflichtet die Cloud-Service-Anbieter zur Durchsetzung der Standards der

---

[39] Multi-Cloud bedeutet in diesem Fall, dass über das Cloud-Service-Portal auf Cloud-Services vieler verschiedener Cloud-Anbieter (insb. der IT-Dienstleister der ÖV) zurückgegriffen werden kann. Dies umfasst auch die Einbindung verwaltungsexterner Cloud-Angebote, s. a. „Cloud-Integratoren“ in Kapitel 4.2.

[40] S. Anschlussbedingungen NdB-VN.

DVS. Darüber hinaus soll die Koordinierungsstelle die Einhaltung der definierten Standards prüfen. Details zur Koordinierungsstelle der Deutschen Verwaltungscloud finden sich in Kapitel 6.1. und im Aufgabendokument der Koordinierungsstelle[41].

Die Wechselfähigkeit und Multi-Cloud-Fähigkeit im Rahmen der DVS wird durch die Standardisierung der Anforderungen für Dienstleister gewährleistet. Hierzu dienen die von der DVS gesetzten technischen und organisatorischen Standards (die sog. DVS-Schicht, vgl. Abbildung 3), welche eine standardisierte Integration für möglichst viele Dienstleister ermöglichen. Dadurch wird die Unabhängigkeit von Herstellern sowie von OSS-Projekten im Sinne der Digitalen Souveränität gewährleistet. Die Integration von externen Cloud-Anbietern erfolgt über die Cloud-Integratoren. Softwarebetreiber sollen somit zukünftig auf einfache Art und Weise den Cloud-Standort bzw. externe Anbieter für ihre Lösungen[42] auswählen können; sofern Daten der Endkunden bspw. Behörden betroffen sind, sind diese in den Entscheidungsprozess geeignet einzubinden. Zielstellung ist, dass beim Betrieb eines Cloud-Services bzw. einer Softwarelösung aus Sicht des Nutzenden kein technischer Unterschied zwischen dem Betrieb bei einem IT-Dienstleister der ÖV und dem Betrieb bei einem externen Cloud-Anbieter besteht.

Die zentrale **OS-Plattform der ÖV Open CoDE** ist die gemeinsame Plattform der ÖV für den Austausch von Open Source Software. Open CoDE beinhaltet als Zielbild ein zentrales Verzeichnis der verwaltungsrelevanten und verfügbaren OS-Software-Projekte/ -Lösungen, eine Webanwendung zur Versionsverwaltung und zur Ablage von offenem Quellcode bzw. Beteiligung an Projekten (Code Repository) sowie ein Diskussionsforum. Das Code Repository wurde bereits im Rahmen der Machbarkeitsstudien (Proof-of-Concepts, PoCs) zur DVS für die gemeinsame Projektarbeit, die Ablage von Quellcode und als externes Repository zum Abruf von Images und Softwareartefakten genutzt.

---

[41] Das Dokument „Deutsche Verwaltungscloud-Strategie: Feinkonzeption der Koordinierungsstelle, Aufgaben der Koordinierungsstelle“ beschreibt die wesentlichen Aufgaben der Koordinierungsstelle und ist zum Beschluss im 39. IT-PLR, parallel zum Beschluss des vorliegenden Rahmenwerks, geplant.

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

4.3 Definition der Rollen

Zur Festlegung eindeutiger Zuständigkeiten und Verantwortlichkeiten im Rahmen der Deutschen Verwaltungscloud werden folgende Rollen definiert. Diese Rollen werden in den nachstehenden Kapiteln gemäß den Definitionen verwendet. Organisationen oder Personen können mehrere Rollen innehaben:

a) **Cloud-Service-Kunde** – Der Cloud-Service-Kunde bezieht Services über einen Cloud-Service Vermittler oder direkt bei einem Cloud-Service-Anbieter aus der Deutschen Verwaltungscloud. Hierbei kann es sich sowohl um eine Behörde, eine Organisation der ÖV oder einen IT-Dienstleister der ÖV handeln.

b) **Cloud-Service Vermittler** – Der Cloud-Service-Vermittler beschafft einen Cloud-Service bei einem Cloud-Service-Anbieter der Deutschen Verwaltungscloud und verantwortet den Betrieb und die Leistungserbringung dieses Cloud-Services entsprechend vertraglichen Verpflichtungen gegenüber seinem Cloud Service-Kunden. Er kann als Bindeglied zwischen Cloud-Service-Anbieter und Cloud-Service-Kunden fungieren.

c) **Cloud-Service-Anbieter** – Der Cloud-Service-Anbieter bietet eine Leistung in der Deutschen Verwaltungscloud an und verantwortet die Leistungserbringung. Diese Rolle ist in der DVS ein Oberbegriff für Plattformbetreiber, Softwarebetreiber oder Cloud-Integrator.

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

   ii. **Softwarebetreiber** – Der Softwarebetreiber verantwortet den Betrieb und ggf. die Weiterentwicklung eines Cloud-Dienstes bzw. einer Softwarelösung entsprechend vertraglichen Verpflichtungen und managt die Service-Orchestrierung. Zudem stimmt er die Anforderungen an den Betrieb der Software mit dem Softwarelieferanten ab. Er ist das Bindeglied zwischen Plattformbetreiber und Softwarelieferant.

   iii. **Cloud-Integrator** – Der Cloud-Integrator handelt als Intermediär zwischen Cloud-Service-Kunden bzw. Softwarebetreibern und externen Cloud-Anbietern. Er macht Cloud-Services externer Anbieter DVS-konform verfügbar.

d) **Nutzende des Cloud-Service-Portals** – Das Cloud-Service-Portal ist der zentrale Einstiegspunkt für Mitarbeitende der Cloud-Service-Kunden. Diese können im Cloud-Service-Portal in der Deutschen Verwaltungscloud angebotene Cloud-Services suchen, bestellen, konfigurieren und administrieren.

e) **Koordinierungsstelle:** Die Koordinierungsstelle koordiniert die Weiterentwicklung der Deutschen Verwaltungscloud. Sie verantwortet das Cloud-Service-Portal und ist für dessen Entwicklung und Integration mit den Cloud-Standorten zuständig, sowie für den Servicekatalog, als Auflistung aller angebotenen Services innerhalb der Deutschen Verwaltungscloud. Die Koordinierungsstelle verpflichtet die an der Deutschen Verwaltungscloud teilnehmenden IT-Dienstleister zur Durchsetzung der Standards der DVS.

f) **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) gemäß den Standards der DVS bereitstellt.

4.4 Rollenverhältnisse und Nutzungsszenarien der Deutschen Verwaltungscloud

Zur Verdeutlichung der Interaktionen der zuvor definierten Rollen (Kapitel 4.3) sind im Folgenden typische Szenarien innerhalb der Deutschen Verwaltungscloud beispielhaft dargestellt. Anhand derer sollen die vielfältigen Rollen, die die IT-Dienstleister der ÖV innerhalb der Deutschen Verwaltungscloud einnehmen, beschrieben werden.

Szenario 1: Beschaffung über einen Cloud-Service-Vermittler

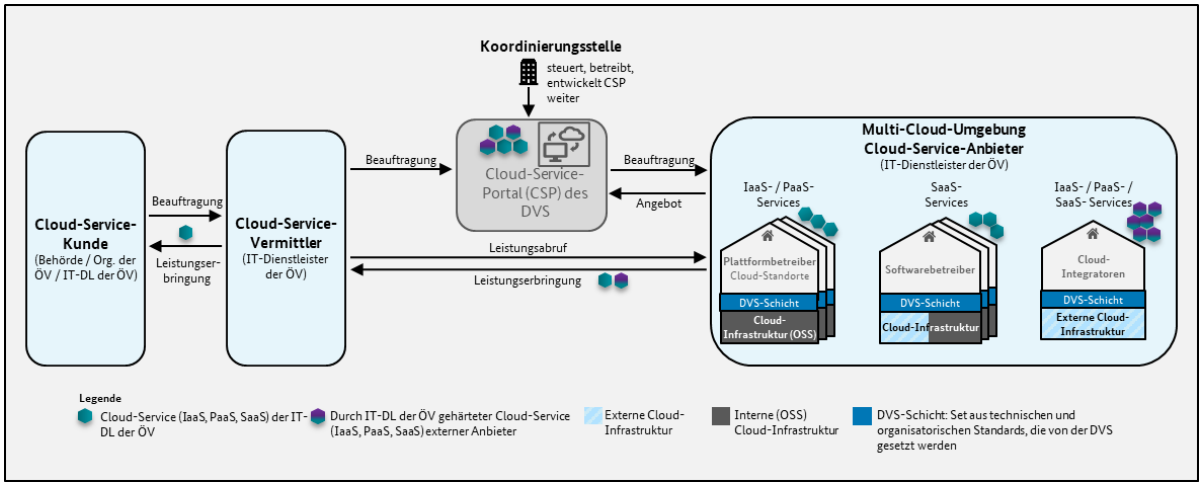

Abbildung 4: Szenario 1 – Beschaffung über einen Cloud-Service-Vermittler

Abbildung 4 beschreibt die Interaktionen in der Deutschen Verwaltungscloud für das Szenario 1, in dem ein Cloud-Service-Kunde über seinen Cloud-Service-Vermittler Leistungen aus der Deutschen Verwaltungscloud bezieht:

1) Ein **Cloud-Service-Kunde** (Behörde / Organisation der ÖV) beauftragt seinen **Cloud-Service-Vermittler** (IT-Dienstleiser der ÖV) mit der Bereitstellung einer Software bzw. eines Cloud-Services. Der **Cloud-Service-Vermittler** bestellt den angeforderten Cloud-Service im Cloud-Service-Portal bei einem **Cloud-Service-Anbieter.** Der **Cloud-Service-Vermittler** erbringt die Leistung gegenüber seinem **Cloud-Service-Kunden**.

Das Szenario 1 umfasst dabei die Beauftragung von Services in den Servicemodellen IaaS, PaaS, als auch SaaS. Diese können ebenfalls über einen Cloud-Integrator von einem externen Cloud-Anbieter bezogen werden. Durch das Szenario 1 wird der Fall abgebildet, dass der Cloud-Service-Kunde eine Organisation der ÖV ist, welche entweder selbst kein Mitglied der Deutschen Verwaltungscloud ist oder über einen zentralen IT-Dienstleister der ÖV verfügt, über welchen sie alle IT-Beschaffungen abdeckt. Dieser IT-Dienstleister der ÖV würde somit in der Rolle als Cloud-Service-Vermittler agieren. Während der Regelfall für dieses Szenario die Beauftragung zur Bereitstellung von SaaS-Angeboten sein wird, ist auch denkbar, dass bei einem Cloud-Service-Kunden auch eigene Entwicklungsabteilungen bestehen und er für diese über seinen Cloud-Service-Vermittler Infrastruktur- und Plattformservices beschafft.

Szenario 2: Direkte Beschaffung in der Deutschen Verwaltungscloud

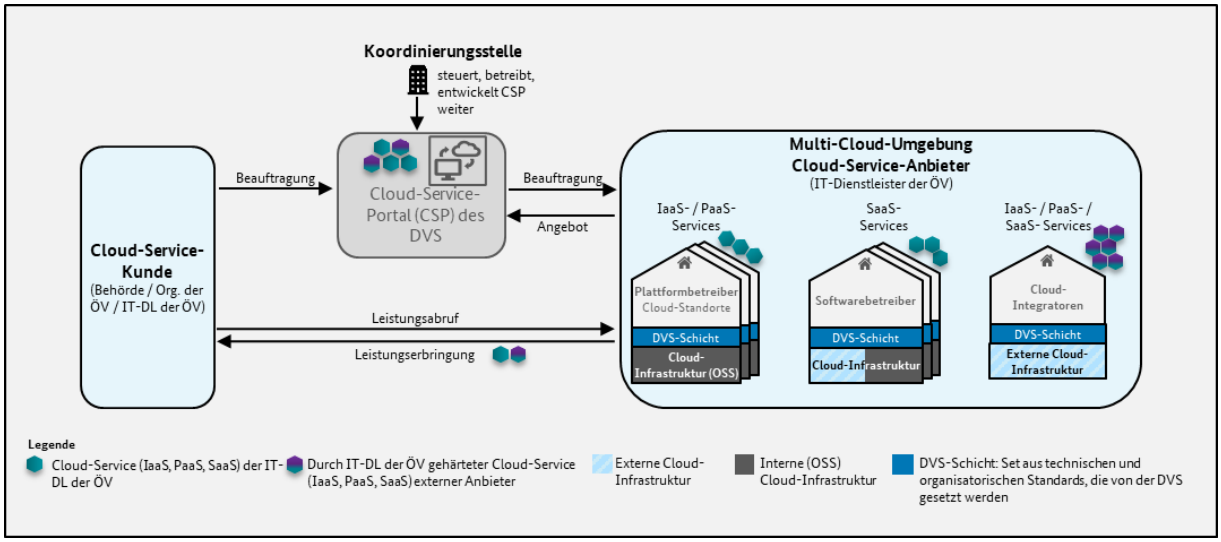

Abbildung 5: Szenario 2 – Direkte Beschaffung in der Deutschen Verwaltungscloud

Abbildung 5 beschreibt das Szenario 2, in dem ein Cloud-Service-Kunde direkt auf die Leistungen der Deutschen Verwaltungscloud zugreift:

2) Ein **Cloud-Service-Kunde** (Behörde / Organisation der ÖV) ruft einen im Cloud-Service-Portal verfügbaren Cloud-Service zur Bereitstellung bei einem **Cloud-Service-Anbieter** (je nach Serviceart **Softwarebetreiber**, **Plattformbetreiber** oder **Cloud-Integrator**) ab. Der **Cloud-Service-Anbieter** stellt den Cloud-Service bereit. Der **Cloud-Service-Kunde** ruft die Leistungserbringung beim **Cloud-Service-Anbieter** ab.

Aus Szenario 2 lassen sich zwei Spezialfälle ableiten:

a. Ein **Cloud-Service-Kunde** ruft einen oder mehrere Cloud-Services zur Bereitstellung nicht für den eigenen Konsum bei einen **Cloud-Service-Anbieter** ab, sondern nutzt diesen, um ein neues, eigenes Cloud-Service-Angebot herzustellen.
b. Ein **Cloud-Service-Kunde** ruft einen im Cloud-Service-Portal verfügbaren Infrastruktur- oder Plattformservice bei einen **Cloud-Service-Anbieter** (**Plattformbetreiber** oder **Cloud-Integrator**) ab, um damit in der Rolle als Softwarebetreiber eine (ggf. von einem **Softwarelieferanten** bereitgestellte) Anwendung zu betreiben.

Das Szenario 2 und dessen Spezialfälle bilden sowohl den Fall ab, dass eine Behörde oder eine Organisation der ÖV als Cloud-Service-Nutzer direkt Cloud-Services aus der Deutschen

Verwaltungscloud bezieht, als auch die Fälle, in denen IT-Dienstleister der ÖV als Cloud-Service-Nutzer die Deutsche Verwaltungscloud für die Beschaffung von Cloud-Services für den eigenen Bedarf oder zur Erstellung eines eigenen Leistungsangebots nutzen.

Szenario 3: Angebot von Cloud-Services in der Deutschen Verwaltungscloud

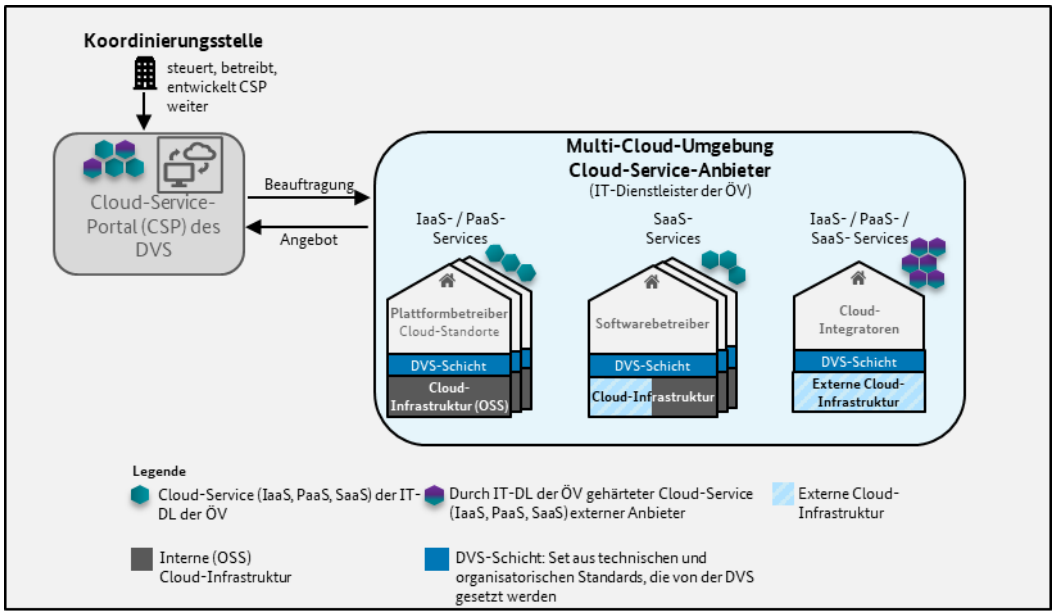

Abbildung 6: Szenario 3 - Angebot von Cloud-Services in der Deutschen Verwaltungscloud

Abbildung 6 beschreibt das Szenario 3, in dem Cloud-Service-Anbieter, also Plattformbetreiber, Cloud-Integratoren und Softwarebetreiber, ihre Cloud-Services in der DVS anbieten.

3) Ein **Cloud-Service-Anbieter** (je nach Serviceart Softwarebetreiber, Plattformbetreiber oder Cloud-Integrator) stellt eigene Cloud-Services in den Servicemodellen IaaS, PaaS oder SaaS über das Cloud-Service-Portal zur Bestellung und nachfolgenden Nutzung bereit.

Für das Szenario 3 lässt sich noch ein Spezialfall für die Rolle des Cloud-Integrators ableiten:

a. Ein **Cloud-Integrator** kauft einen Cloud-Service von einem externen Cloud-Anbieter außerhalb der Deutschen Verwaltungscloud ein, konfiguriert ihn gemäß den DVS-Standards und macht ihn DVS-konform über das Cloud-Service-Portal verfügbar.

Im Kontext der vorgestellten Szenarien, 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 6.2) festzulegen. Die Liste wird fortlaufend erweitert.

ID	Beschreibung der User Story
U1	Als **Softwarebetreiber** möchte ich standardisierte 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 standardisierte bzw. gleichartige Container-Cluster bereitgestellt bekommen, um das Deployment von Softwarelösungen zu erleichtern.
U4	Als **Softwarebetreiber** möchte ich Instrumente zum Management der Containerumgebungen bereitgestellt bekommen
U5	Als **Softwarebetreiber** möchte ich den Status (inkl. z.B. Zugriff auf Monitoring-Informationen) meiner Services in den Cloudumgebungen aller Plattformbetreiber und Cloud-Integratoren jederzeit einsehen können.
U6	Als **Softwarebetreiber** möchte ich die Kompatibilität meiner benötigten Ressourcen aus dem Cloud-Standort mit dem DVS-Standard überprüfen, um den einwandfreien Betrieb zu gewährleisten.
U7	Als **Plattformbetreiber** möchte ich ein einheitliches und gemeinsames Regelwerk für die Konfiguration von Container-Clustern benutzen, um standardisierte Services bereitstellen zu können.
U8	Als **Nutzende des Cloud-Service-Portals** möchte ich mittels Filterfunktion Services auswählen, um entsprechend meiner Kriterien passende Services zu finden.

ID	Beschreibung der User Story
U9	Als **Nutzende des Cloud-Service-Portals** möchte ich Cloud-Services (z.B. in den Servicemodellen SaaS, PaaS inkl. CaaS-Angebote 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 IT-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	Benennung 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 in einem Behördenstandort betrieben. Die eingescannten Dokumente werden in einem nach Standard TR-ESOR definiertem Speichersystem beweiswerterhaltend gespeichert.
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.

ID	Benennung des Anwendungsfalls
A4	**E-Mail-Kommunikation** Es wird ein Service zum Empfangen und Versenden von E-Mails sowie 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.
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.
A8	**Souveräner Arbeitsplatz für die ÖV** Für die ÖV wird eine Alternative im Bereich Arbeitsplatz entwickelt und bereitgestellt (Arbeitstitel: Souveräner Arbeitsplatz). Der Souveräne Arbeitsplatz wird auf existierende OSS-Lösungen zurückgreifen und soll sämtliche von der ÖV benötigte Basisfunktionen abdecken. Dies betrifft insb. die Bereiche Produktivität (Textverarbeitung, Tabellenkalkulation, Fileablage, Drucken etc.), Kollaboration (gemeinsames Bearbeiten von geteilten Dateien) und Kommunikation (Video- und Audiokonferenzen, E-Mails, Kurznachrichten etc.).

5 Wesentliche Standards

Mit der Deutschen Verwaltungscloud sollen Standards für alle teilnehmenden Softwarebetreiber, Plattformbetreiber bzw. deren Cloud-Standorte und Cloud-Integratoren von Bund, Ländern und Kommunen eingeführt werden. Ziel dieses Kapitels ist die Beschreibung und Konkretisierung des Handlungsrahmens.

Im DVS-Konzeptpapier wurden sechs Standardisierungsbereiche definiert:

1) *Entwicklung und Entwicklungsplattform,*
2) *Anwendungsbereitstellung und -management,*
3) *Code Repository,*
4) *Infrastruktur-Service und technologischer Stack*,
5) *Betriebsstandards und Betriebsmodell sowie*
6) *Einbindung von externen Cloud-Anbietern.*

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

Im Zusammenhang mit Standardisierungsbereich 3 (*Code Repository*) hat eine separate Projektgruppe[43] ein zentrales Code Repository Management System als Teil einer übergreifenden OS-Plattform (OS-Plattform der ÖV Open CoDE) realisiert. Dieses Plattform befindet sich im Betrieb und wird kontinuierlich weiterentwickelt. Eine dedizierte Betrachtung der Plattform ist kein Bestandteil des vorliegenden Dokuments.

5.1 Vorlage zur Festlegung der Standards

Für die Beschreibung der Standards wurde ein einheitliches Format gewählt. Ein Standard wird dabei durch einen eindeutigen Titel, einen Verbindlichkeitsgrad sowie eine revisionssichere

[43] Die Projektgruppe besteht aus Vertretern des BMI, des Ministeriums für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen, des Ministeriums für Inneres, Digitalisierung und Migration Baden-Württemberg sowie des baden-württembergischen IT-Dienstleister Komm.ONE.

Identifikationsnummer (ID) gekennzeichnet. Die untenstehende Formatvorlage ist an die der Architekturrichtlinie für die IT des Bundes angelehnt[44].

Titel: Titel des Standards	**Verbindlichkeitsgrad: MUSS / SOLLTE / KANN / DARF NICHT**
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: Formatvorlage zur Festlegung der Standards

Wie in Kapitel 2.4 erläutert, sollen die Standards regelmäßig, mindestens jährlich, aktualisiert und weiterentwickelt werden. Eine revisionssichere ID sorgt dafür, dass die Nachvollziehbarkeit von Änderungen zu jeder Zeit 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, SOLLTE, 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[45].

[44] Siehe https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/architekturen-standard/ArchRL.pdf?__blob=publicationFile&v=7.

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

5.2 Sammlung der Standards

Dieses Unterkapitel umfasst den aktuellen Stand der wesentlichen Standards der Deutschen Verwaltungscloud. Weitere (technische) Detaillierungen zu einzelnen Standards sind in den nachfolgenden Kapiteln aufgeführt.

Titel: Anwendbares Recht		**Verbindlichkeitsgrad: 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.	

Titel: Vorgaben für Produktion, Service und Subunternehmer	Verbindlichkeitsgrad: MUSS
ID: DVS-002-R01	
Beschreibung	Für den Betrieb von Cloud-Services und Softwarelösungen mit Anforderungen hinsichtlich Vertraulichkeit, Sicherheit und Rechtssicherheit MÜSSEN folgende Rahmenbedingungen eingehalten werden: - Point of Production ist Deutschland - Point of Service ist Deutschland Jeder Cloud-Service-Anbieter MUSS eine Liste aller 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

Titel: Hoheit über Hard- und Software		Verbindlichkeitsgrad: MUSS
ID: DVS-003-R02		
Beschreibung	Die eingesetzte Hard- und Software MUSS so gewählt und betrieben werden, dass die Handlungsfähigkeit der Cloud-Service-Kunden durch Entscheidungen des Softwarelieferanten oder eines Cloud-Service-Anbieters nicht gefährdet wird. Für wichtige Verfahren MUSS die Hoheit[46] 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	

Titel: Standards für Softwarekomponenten		Verbindlichkeitsgrad: MUSS
ID: DVS-004-R01		
Beschreibung	Jeder Cloud-Service-Anbieter 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	

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

Titel: Zertifizierung nach IT-Grundschutz des BSI		Verbindlichkeitsgrad: MUSS
ID: DVS-005-R01		
Beschreibung	Jeder Cloud-Service-Anbieter MUSS einen passenden Informationsverbund definieren und diesen nach ISO 27001 auf der Basis von IT-Grundschutz des BSI zertifiziert haben.	
Verweis	*Ohne Verweis*	

Titel: Erfüllung des Kriterienkatalogs C5		Verbindlichkeitsgrad: SOLLTE
ID: DVS-006-R01		
Beschreibung	Jeder im Rahmen der Deutschen Verwaltungscloud erbrachte Cloud-Service SOLLTE[47] die Kriterien aus dem Kriterienkatalog C5 des BSI erfüllen.	
Verweis	*Ohne Verweis*	

[47] Der Verbindlichkeitsgrad für diesen Standard ist ab dem 01.01.2024 als MUSS geplant. Dies hat den Hintergrund, dass der Kriterienkatalog C5 des BSI für Containertechnologie noch nicht hinreichend verbreitet ist.

Titel: Hoheit über Krypto-Module und –Schlüssel		Verbindlichkeitsgrad: MUSS
ID: DVS-007-R01		
Beschreibung	Die Kryptomodule und -Schlüssel MÜSSEN in der Hoheit der ÖV liegen, um den Zugriff auf die gespeicherten Daten selbstbestimmt zu kontrollieren. Technologien zur Verschlüsselung MÜSSEN durch die Dienstleister / Serviceerbringer anpassbar sein, um jederzeit die Vorgaben des 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	

Titel: Bereitstellung von Containerumgebung (CaaS) und Container-Cluster		Verbindlichkeitsgrad: MUSS
ID: DVS-008-R01		
Beschreibung	Jeder Plattformbetreiber MUSS eine Containerumgebung (Container-as-a-Service, CaaS) zum Betrieb von Softwarelösungen bereitstellen. Die Umgebung beinhaltet die erforderlichen IaaS- und PaaS-Komponenten für den Containerbetrieb und die Container-Services.	
Verweis	Siehe Kapitel 5.3.4	

Titel: Anlieferung von Containerlösungen		Verbindlichkeitsgrad: 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 5.3.4	

Titel: Angebot von Erweiterungen zur Containerumgebung		Verbindlichkeitsgrad: KANN
ID: DVS-010-R01		
Beschreibung	Jeder Plattformbetreiber KANN Erweiterungen zur oder mit Anbindung an die Containerumgebung anbieten. Denkbar sind bspw. spezifische Standard-Images, Frameworks oder Datenbankmanagementsysteme (DBMS).	
Verweis	Siehe Kapitel 5.3.4	

Titel: Erreichbarkeit der Standorte		Verbindlichkeitsgrad: MUSS
ID: DVS-011-R02		
Beschreibung	Jeder Cloud-Standort MUSS aus den Verwaltungsnetzen, für die er Cloud-Services anbietet, z. B. Netze des Bundes (NdB-VN), oder aus dem Internet erreichbar sein. Die Kommunikation zwischen Cloud-Standorten MUSS auf Grundlage gesetzlicher Regelungen, z. B. IT-NetzG, erfolgen. Die Anforderungen der DVS sind bei der Umsetzung des Informationsverbunds der Öffentlichen Verwaltung (IVÖV) im Rahmen der Netzstrategie 2030 zu berücksichtigen[48].	
Verweis	Siehe Kapitel 5.3.2	

Titel: Umsetzung des Zonenmodells		Verbindlichkeitsgrad: MUSS
ID: DVS-012-R02		
Beschreibung	Jeder Cloud-Standort MUSS die Blaupause des Zonenmodells für einheitliche Zugangswege umsetzen. Standort-spezifische Abweichungen sind möglich, solange diese konform mit den Vorgaben des BSI (IT-Grundschutz) sind.	
Verweis	• Siehe Kapitel 5.3.2 • BSI IT-Grundschutz	

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

Titel: Einrichtung einer Schnittstelle zum Cloud-Service-Portal		Verbindlichkeitsgrad: MUSS
ID: DVS-013-R01		
Beschreibung	Jeder Cloud-Service-Anbieter 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[49]- und Change[50]-Management über diese Schnittstelle unterstützt werden. Zudem MÜSSEN Informationen zum Servicekatalog, zur Bereitstellung von Services und Abrechnungsdaten an das Cloud-Service-Portal mittels der Schnittstelle übermittelt werden können.	
Verweis	Siehe Kapitel 5.3.6 und 5.4	

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

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

Titel: Betreiberwechsel		Verbindlichkeitsgrad: MUSS
ID: DVS-014-R02		
Beschreibung	Jeder Cloud-Service-Anbieter MUSS dem Cloud-Service-Kunden geeignete Möglichkeiten für einen Betreiberwechsel innerhalb der Deutschen Verwaltungscloud bieten. Gespeicherte Daten MÜSSEN exportierbar sein und dem Cloud-Service-Kunden so bereitgestellt werden, dass ein Import oder eine Wiederherstellung bei einem anderen Cloud-Service-Anbieter umsetzbar ist. Für alle Angebote MÜSSEN durch den Software- oder Plattformbetreiber notwendige Funktionen zum Datenexport in einem offenen und standardisierten Format bereitgestellt werden. Dabei sind sowohl internationale Technologie-Standards (z.B. Dateiformat-Standards) als auch die XÖV-Standards der ÖV (z.B. XProzess, XDatenfelder, XDomea) zu berücksichtigen.	
Verweis	*Ohne Verweis*	

Titel: Bereitstellung notwendiger Dokumentationen		Verbindlichkeitsgrad: MUSS
ID: DVS-015-R01		
Beschreibung	Jeder Plattformbetreiber MUSS dem Softwarebetreiber notwendige Dokumentationen zu den bereitgestellten Services verfügbar machen.	
Verweis	*Ohne Verweis*	

Titel: Bereitstellung von Entwicklungsbereichen		Verbindlichkeitsgrad: KANN
ID: DVS-016-R01		
Beschreibung	Jeder Plattformbetreiber KANN Entwicklungsbereiche bereitstellen.	
Verweis	Siehe Kapitel 5.3.5	

Titel: Anbindung an die zentrale OS-Plattform der ÖV Open CoDE		Verbindlichkeitsgrad: MUSS
ID: DVS-017-R01		
Beschreibung	Jeder Plattformbetreiber MUSS bei Bereitstellung von Entwicklungsbereichen den Zugriff auf die OS-Plattform der ÖV Open CoDE ermöglichen.	
Verweis	Siehe Kapitel 5.3.5 und https://www.opencode.de	

Titel: Unterstützung von DevOps-Ansätzen		Verbindlichkeitsgrad: MUSS
ID: DVS-018-R01		
Beschreibung	Jeder Plattformbetreiber MUSS mit den bereitgestellten Entwicklungsbereichen die in Kapitel 5.3.5 genannten DevOps-Ansätze Continuous Integration und Continuous Deployment unterstützen.	
Verweis	Siehe Kapitel 5.3.5	

Titel: Angebot von Software-as-a-Service (SaaS)	Verbindlichkeitsgrad: KANN
ID: DVS-019-R01	
Beschreibung	Jeder Softwarebetreiber KANN Services im Servicemodell SaaS im Cloud-Service-Portal anbieten.
Verweis	*Ohne Verweis*

Titel: Funktion eines Ausweichrechenzentrums	Verbindlichkeitsgrad: KANN
ID: DVS-020-R01	
Beschreibung	Jeder Cloud-Standort KANN die Funktion eines Ausweichrechenzentrums für den Betrieb von Fachanwendungen mit besonderen Anforderungen anbieten (bspw. mit dem Ziel der Georedundanz).
Verweis	*Ohne Verweis*

Titel: Cloud-Service-Portal	Verbindlichkeitsgrad: MUSS
ID: DVS-020-R01	
Beschreibung	Es wird ein Self-Service-Portal für Cloud-Services für die ÖV eingerichtet, über das sich Cloud-Services in verschiedenen Servicemodellen (z.B. IaaS, PaaS, SaaS) verwalten lassen.
Verweis	Siehe Kapitel 5.4 und Feinkonzept des Cloud-Service-Portals

5.3 Details einzelner Standards

Ausgehend von den zuvor festgelegten Standards werden diese nachfolgend zum Teil weiter präzisiert. Die Präzisierung stellt jedoch keine abschließende technische Spezifizierung dar. Teilweise werden für die jeweiligen Standards besonders wichtige Anforderungen aus dem IT-Grundschutz-Kompendium hervorgehoben, hierbei ist jedoch zu beachten, dass der IT-Grundschutz grundsätzlich durch die teilnehmenden Cloud-Service-Anbieter umzusetzen ist. Mit weiterführenden Dokumenten (vgl. Kapitel 6) sollen insbesondere den Cloud-Service-Anbietern zukünftig **technische Handreichungen** zur zielgerichteten Umsetzung bereitgestellt werden.

Eine Übersicht, wie ein Cloud-Standort auf Basis der Standards aus Kapitel 5.2 gestaltet ist, kann der Abbildung 7 entnommen werden. Details dazu finden sich nachfolgend.

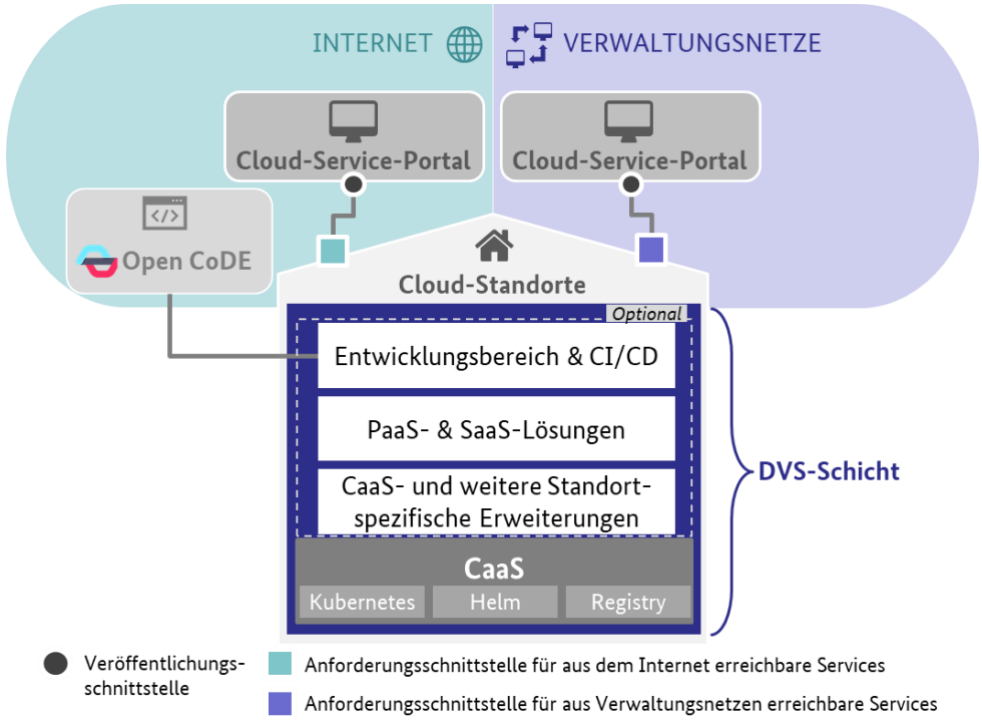

Abbildung 7: Obligatorische und optionale Standards der Cloud-Standorte (illustrative Darstellung)

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

standardisierte, skalierbare, OS-basierte Softwarekomponenten zur Bereitstellung von Containerumgebungen in den jeweiligen Cloud-Standorten genutzt werden. Die nachfolgende Auflistung ist nicht abschließend, im Laufe der weiteren Konzeption können weitere Komponenten hinzukommen oder es können genannte Komponenten durch alternative (z.B. aktuellere, zweckadäquatere) ersetzt werden (in diesen Fällen sind Übergangszeiträume für Migrationen erforderlich):

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 mithilfe 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[51] ausgerichtetes, einheitliches Zonenmodell wurde als Blaupause zur Umsetzung in allen Cloud-Standorten definiert (vgl. Abbildung 8). Standort-spezifische und mit den Vorgaben des BSI konforme Abweichungen sind möglich.

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.

---

[51] 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.

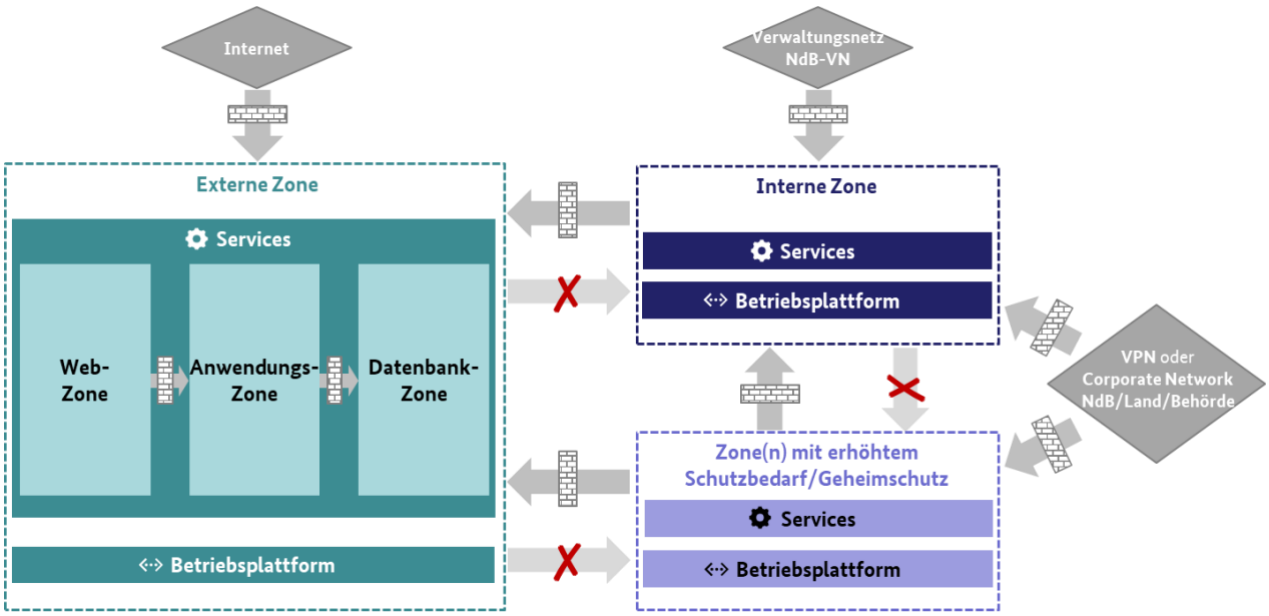

Abbildung 8: Blaupause des einheitlichen Zonenmodells der Cloud-Standorte

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 unterschiedliche Zwecke: Die Web-Zone wird zur Bereitstellung von Application-Level-Gateway bzw. Web-Proxy, die Anwendungs-Zone wird zur Bereitstellung von Applikationsservern und die Datenbank-Zone wird zur Bereitstellung von DBMS genutzt. Die Eingrenzung der Demilitarisierten Zone (DMZ) innerhalb der Externen Zone erfolgt in Kapitel 5.3.4, da diese eng mit der Containercluster-Bereitstellung verknüpft ist.

Der Zugriff von außen (z. B. aus dem Internet oder via NdB-VN) erfolgt gefiltert mittels Sicherheitsgateways[52] (Paketfilter – Application-Level-Gateway – Paketfilter- (P-A-P) -Struktur gemäß Empfehlung des BSI[53] oder vergleichbar), siehe Kapitel 5.3.3. Bei der Netzanbindung müssen die Anschlussbedingungen der jeweiligen Netzbetreiber erfüllt werden. Die konkrete technische Ausstattung muss entsprechend gewählt werden und die notwendigen Zulassungen aufweisen, z. B. für VS-NfD. Zukünftig kann auch der Informationsverbund der öffentlichen

[52] Siehe Glossar für eine Definition des BSI.

[53] „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.

Verwaltung (IVÖV), welcher in der Netzstrategie 2030 definiert ist, unterstützt werden. Die Kommunikation zwischen den Zonen erfolgt gefiltert mittels Paketfilter. Die Netztrennung muss mittels performanter Firewalls mindestens auf Layer 4 des OSI-Modells (Transport-Layer) erfolgen.In diesem Zuge dürfen bestimmte Zugangswege von einer Zone in eine andere nicht gewährt werden. Demnach ist der Zugriff aus dem Internet über die Externe Zone zur Internen Zone nicht gestattet. Je Zone sollte eine unabhängige Betriebsplattform etabliert werden, auf der die Services aus den jeweiligen Administrationsnetzen orchestriert und gesteuert werden[54].

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.
- Der Plattformbetreiber MUSS eine BSI-konforme Verwaltung der Administrationskonten und der technischen Accounts sicherstellen.
- Der Plattformbetreiber MUSS die Anbindung von Monitoring- und Protokollierungssystemen entsprechend einer BSI-konformen Systematik (vgl. IT-Grundschutz-Bausteine) sicherstellen.
- Der Plattformbetreiber MUSS ein Audit-System[55] für Systembereiche etablieren. Hierzu zählen Konfigurationsdateien, Registry und Softwarebetriebsprozess.

[54] 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.

[55] Siehe Glossar für eine Begriffsdefinition.

5.3.3 Netzanbindung

Ergänzend zum Zonenmodell in Kapitel 5.3.2 werden in diesem Standard Festlegungen zur Netzanbindung bzw. zu Netzübergängen getroffen. Gegenstand der Betrachtung ist der Übergang vom Internet in die Webzone der externen Zone sowie der von dort ausgehenden Paketfilter (Firewalls) vor der Anwendungszone (vgl. Abbildung 8).

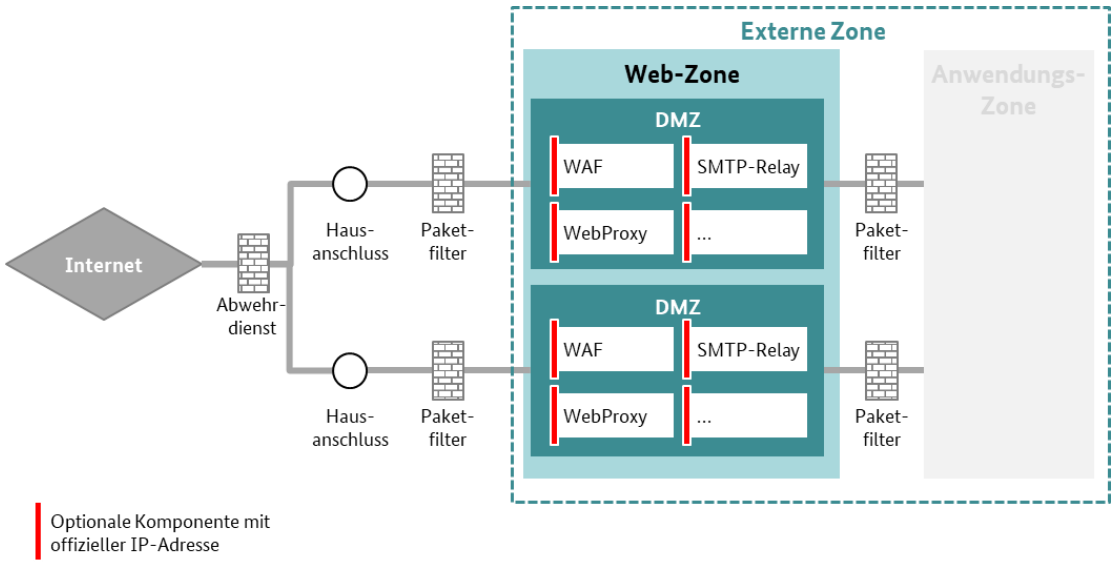

Abbildung 9: P-A-P-Struktur gemäß IT-Grundschutz des BSI

Gemäß IT-Grundschutz des BSI ist eine P-A-P-Struktur abzubilden (vgl. Abbildung 9). Der P-A-P-Struktur vorgelagert sollte durch den Internet-Provider ein Dienst zur Angriffserkennung und -abwehr, wie bspw. ein DDoS-Abwehrdienst, bereitgestellt werden. Der Cloud-Standort selbst ist durch eine redundante Netzanbindung mit mindestens zwei physischen Leitungen an das Internet angebunden. Die beiden Paketfilter dienen auch als Firewalls. Das Application Level Gateway (Webzone in Abbildung 9) enthält Komponenten wie beispielsweise eine Web Application Firewall (WAF), einen Web-Proxy, ein SMTP-Relay, o. ä. In dieser Zone und an diesen Komponenten terminieren die öffentlichen IP-Adressen, d.h. in allen nachgelagerten Strukturen werden nur interne IP-Adressen vergeben. Zudem ist in der Webzone keine Anwendungslogik zulässig, d.h. es dürfen dort keine Application Server o. ä. betrieben werden.

Entsprechend gelten die folgenden Anforderungen an die Netzanbindung:

- Der Cloud-Standort MUSS eine redundante Netzanbindung mit getrennten Leitungswegen sicherstellen.
- Der Cloud-Standort MUSS eine knoten- und kantendisjunkte Netzanbindung sicherstellen.
- Der Cloud-Standort SOLLTE beim Internetzugang einen vorgeschalteten Dienst zur Angriffserkennung und -abwehr nutzen.
- Sämtliche Netzzugänge MÜSSEN Bestandteil eines Informationsverbundes sein, für den der IT-Grundschutz umgesetzt wurde.
- IPv4 MUSS unterstützt werden.
- IPv6 SOLLTE unterstützt werden.
- Der Ausbau auf IPv6 MUSS angestrebt werden.

Insbesondere gelten die folgenden Anforderungen, die sich aus dem IT-Grundschutz-Baustein NET.1.1 ergeben:

- Bei der Anbindung des Internets MUSS eine P-A-P-Struktur genutzt werden.
- Sämtliche Datenströme MÜSSEN durch die Firewall-Struktur auf die notwendigen Protokolle und Kommunikationsbeziehungen eingeschränkt und dokumentiert werden.
- Eine revisionssichere Protokollierung MUSS an der Firewall möglich sein.
- Ein Security Information and Event Management (SIEM) MUSS eingesetzt werden.

Darüber hinaus gelten folgende Einstufungen hinsichtlich der IT-Grundschutz-Anforderung NET.1.1.A9[56]:

- Das Internet wird als unsicheres Netz eingestuft.
- Das NdB-VN[57] wird als vertrauenswürdig eingestuft. Es erreicht jedoch nicht das gleiche Vertrauensniveau wie die Netze des Cloud-Standorts.

Die hier beschriebene P-A-P-Struktur ist für die Anbindung an das Internet vorgegeben. Der Zugriff aus Verwaltungsnetzen kann analog erfolgen, es ist jedoch ein vereinfachter Aufbau der

[56] Auszug aus BSI-Grundschutz-Baustein NET.1.1.A9 *Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen*: „Für jedes Netz MUSS festgelegt werden, inwieweit es als vertrauenswürdig einzustufen ist. Netze, die nicht vertrauenswürdig sind, MÜSSEN wie das Internet behandelt und entsprechend abgesichert werden."

[57] Netze des Bundes-Verbindungsnetz.

Absicherung der ein- und ausgehenden Kommunikation möglich – mit der Grundannahme, dass es sich um einen Kommunikationspartner aus einem sicheren Netz handelt.

5.3.4 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.

Die Web-Zone wird als DMZ angesehen. Dementsprechend ist die Anwendungs-Zone gegenüber außen mit einer P-A-P-Struktur getrennt (für Details s. Kapitel 5.3.3). Diese stellt somit die Absicherung zum Internet dar. Jede Kommunikationsbeziehung zwischen Container-Clustern und Namespaces benötigt eine explizite Freigabe. Abbildung 10 veranschaulicht die Containerumgebung.

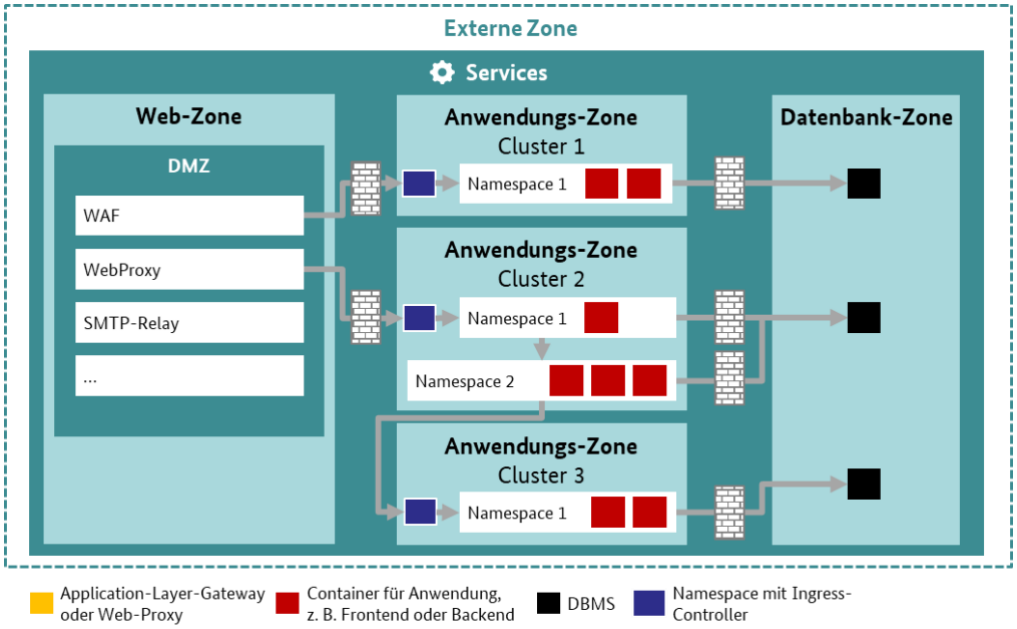

Abbildung 10: Anordnung der Container-Cluster hinter einer klassischen P-A-P-Struktur (illustrative Darstellung)

Die Trennung von Anwendungen innerhalb eines Clusters erfolgt über Namespaces. Ingress-Controller werden dabei in separaten Namespaces betrieben. Innerhalb der Cluster müssen alle Anwendungen jeweils das gleiche Schutzniveau erreichen. Ansonsten wird die Verteilung von Anwendungscontainern im Cluster nicht reglementiert; diese ist dann entsprechend den Sicherheitskonzepten der jeweiligen Anwendungen zu planen.

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:* Containerisierung[58] und *APP.4.4:* Kubernetes[59]) herangezogen:

- Der Plattformbetreiber SOLLTE für jeden nach extern exponierten Service eine eigene IP-Adresse am Ingress bereitstellen. Verschiedene, nach extern exponierte Services sollten sich über die IP-Adressierung unterscheiden lassen, um Schutzmaßnahmen außerhalb der Kubernetes-Umgebung zu vereinfachen.
- Wenn über den Ingress mehrere Anwendungen veröffentlicht werden, SOLLTE jede Anwendung über eine eigene IP-Adresse verfügen.
- Auf die Anwendungen MUSS über DNS zugegriffen werden können.
- Der Ingress MUSS von anderen Funktionalitäten getrennt werden.
- 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.

---

[58] Siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/07_SYS_IT_Systeme/SYS_1_6_Containerisierung_Edition_2022.html.

[59] Siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/06_APP_Anwendungen/APP_4_4_Kubernetes_Edition_2022.pdf?__blob=publicationFile&v=3.

- 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.

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.
- Der Softwarebetreiber KANN eine eigene CI/CD-Pipeline nutzen. In diesem Fall stellt der Plattformbetreiber geeignete Übergabepunkte bereit.

5.3.5 Entwicklungsbereich

Zur Unterstützung der dezentralen Softwareentwicklung kann ein Cloud-Standort 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[60] 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 der ÖV Open CoDE ermöglichen.

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

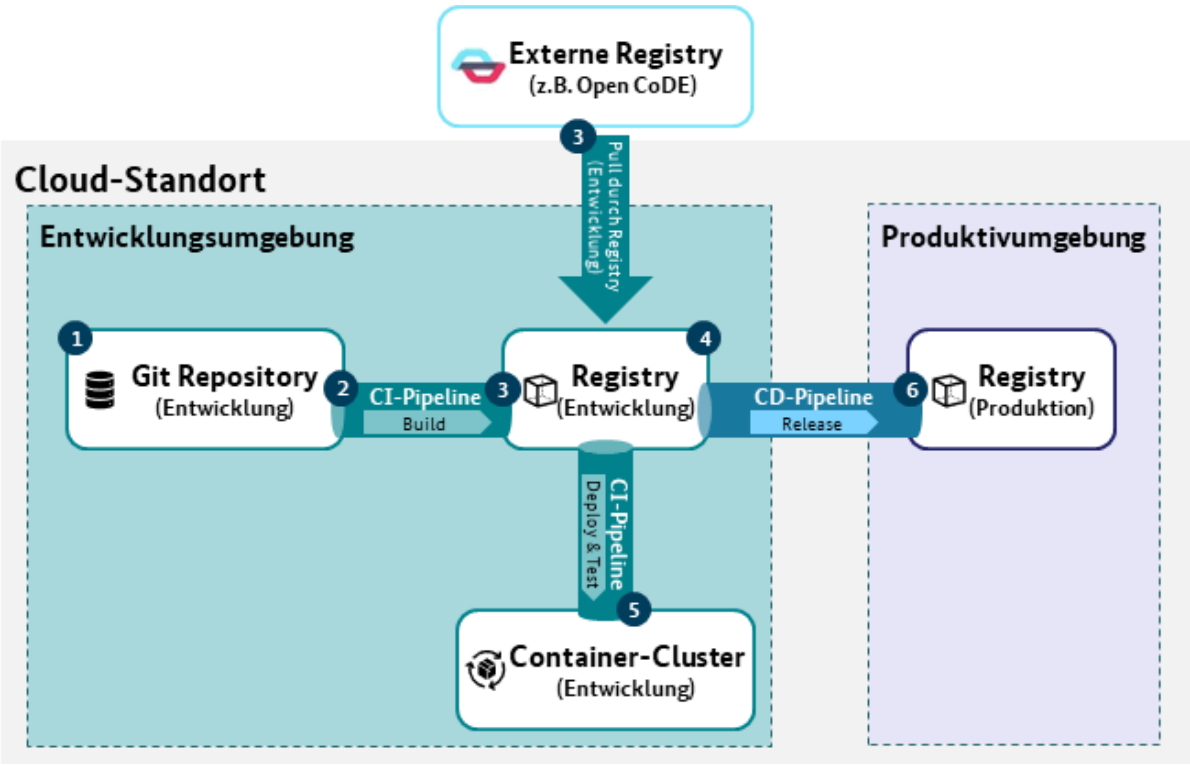

Abbildung 11: Entwicklungsbereich und CI-/CD-Pipeline

Ein hoher Automatisierungsgrad im Rahmen der Entwicklung von Cloud-Services und Softwarelösungen ist ein wichtiger Aspekt für eine moderne IT-Infrastruktur. Entsprechend wurde für den Continuous Integration- bzw. Continuous Deployment-Prozess (CI-/CD-Pipeline) ein standardisierter Workflow entwickelt, der in Abbildung 11 skizziert ist und wie folgt abläuft:

1. Einchecken des Quellcodes im Git-Repository in der im Cloud-Standort bereitgestellten Entwicklungsumgebung.
2. Automatische (zeitgesteuerte) bzw. manuelle Auslösung des Build-Prozesses zum Bau des neuen Artefakts bzw. Images.
3. Einchecken bzw. Push des neuen Artefakts bzw. Images in der Registry der Entwicklungsumgebung. In dem Fall, dass ein Artefakt bzw. Image von einer externen Registry (z.B. von der OS-Plattform der ÖV Open CoDE oder von einem anderen Hersteller) zur Verfügung gestellt wird, wird die neue Version durch einen Pull durch die Registry der Entwicklungsumgebung abgerufen. Sollte die externe Registry diesen Vorgang nicht unterstützen, kann alternativ das neue Artefakt bzw. Image von der externen Registry in die Registry der Entwicklungsumgebung gepusht werden. Genauere

Ausführungen zu diesem Vorgang werden in dem zugehörigen Detailstandard beschrieben.

4. Schwachstellenscan des neuen Artefakts bzw. Images in der Registry der Entwicklungsumgebung.
5. Deployment und Test des neuen Artefakts bzw. Images aus der Registry im Cluster der Entwicklungsumgebung.
6. Nach erfolgreichem Deployment und Test: Erzeugung eines Changes durch den Softwarebetreiber an den Plattformbetreiber und anschließende automatische oder manuelle Auslösung des Rollouts des Releases des neuen Artefakts bzw. Images und Übergabe des Artefakts bzw. Images an die Registries der Produktionsumgebungen.

Der oben genannte Change zur Auslösung des Releases kann manuell oder automatisch bestätigt werden und löst somit die Ausführung der CD-Pipeline aus. Automatische Bestätigungen sind jedoch nur bei Standard-Changes (s. Glossar) möglich. Abweichend von Abbildung 11 können die Registries der Entwicklungs- und Produktionsumgebung auch in nur einem System betrieben werden. Dies setzt entsprechende Vorkehrungen zur logischen Trennung zwischen Entwicklungs- und Produktionsumgebung voraus. Näheres hierzu wird in einem entsprechenden Detailstandard geregelt.

Für den CI-/CD-Prozess werden folgende Anforderungen definiert:

- Der Plattformbetreiber MUSS ein Git-Repository am Cloud-Standort bereitstellen. Hierbei kann es sich auch um ein externes Repository handeln.
- 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.
- Für die Anlieferung von Artefakten und Images in den Entwicklungsbereich MUSS am Cloud-Standort eine Registry bereitgestellt werden. Es SOLLTE eine zusätzliche Registry zur Ablage der produktiven Deployments eingerichtet 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.

- Die vom Plattformbetreiber bereitgestellte Registry der Entwicklungsumgebung MUSS externe Registries über Pull-Anforderungen spiegeln können. Eine nähere Betrachtung dieser Anforderung wird in dem zugehörigen Detailstandard vorgenommen.
- Die vom Plattformbetreiber bereitgestellte Registry der Entwicklungsumgebung KANN Push-Anforderungen von externen Registries unterstützen.
- Die vom Plattformbetreiber bereitgestellte Registry MUSS die Speicherung von Images, Konfigurationsdateien, Helm Charts und weiteren Deployment-Dateien unterstützen können. Es MUSS die Ablage eines kompletten Deployments ermöglicht werden.
- Die vom Plattformbetreiber bereitgestellte Registry MUSS die Prüfung der Signatur von Artefakten und Images ermöglichen.
- Bei Versionsaktualisierungen MÜSSEN Schwachstellenscans in der Entwicklungsumgebung ausgeführt werden können. Der Schwachstellenscan MUSS durch die Registry getriggert werden. Zyklische, mindestens tägliche Schwachstellenscans MÜSSEN unterstützt werden. Über gefundene Schwachstellen MÜSSEN verantwortliche Personen des Softwarebetreibers per E-Mail informiert werden können. Der Schwachstellenscan wird in dem zugehörigen Detailstandard näher definiert.
- Versionsstände von Artefakten und Images MÜSSEN eindeutig getaggt werden können.
- Die CI- / CD-Pipeline MUSS so konfiguriert werden können, dass die Bereitstellung der erstellten Artefakte und Images für ein Repository zum Ausrollen in einer Testumgebung unterstützt wird.
- Der Plattformbetreiber KANN an seinem Cloud-Standort Schnittstellen für Webhooks usw. bereitstellen, damit die Pipeline von externen Entwicklungsumgebungen angesteuert werden kann.
- Die Freigabe eines Artefakts oder Images für die Produktionsumgebung MUSS mit einem Change dokumentiert 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 sicherstellen, dass bei der Trennung der CI-Pipeline von der Pipeline für die Continuous Delivery die Anforderungen aus Kapitel 5.3.3 eingehalten werden.
- Der Plattformbetreiber KANN Werkzeuge zur Prüfung der Codequalität und zum Sicherheitstest bereitstellen.
- Der Plattformbetreiber KANN zur Unterstützung der Softwareentwicklung ein Ticketsystembereitstellen.

In der gesamten CI- / CD-Pipeline ist eine technisch und organisatorisch sichere Gestaltung der Prozesse einzuhalten. Näheres ist in den entsprechenden Detailstandards ausgeführt.

5.3.6 Kommunikation zwischen Cloud-Standort, Softwarebetreiber und Cloud-Service-Portal

Zwischen Cloud-Service-Portal (Kapitel 5.4) und den Cloud-Service-Anbietern ist ein regelmäßiger direkter Datenaustausch notwendig. Entsprechende APIs müssen dafür auf allen Seiten bereitgestellt werden. Die Daten zur Kommunikation zwischen den Beteiligten umfassen u.a.:

- Informationen zu Beauftragung, Änderung und Kündigung von Cloud-Services,
- Informationen zur Erstellung bzw. Statusänderung von Incidents und Changes,
- Abrechnungsdaten und
- Verfügbarkeitsberichte der Cloud-Services für das Monitoring.

Das Cloud-Service-Portal wird kein vollständiges Ticketsystem bereitstellen, jedoch eine Schnittstelle zu Ticketsystemen bei den Cloud-Service-Anbietern, Cloud-Service-Vermittlern und Cloud-Service-Kunden anbieten, um den Empfang und die Verwaltung von Tickets zu ermöglichen. Dabei muss die Durchgängigkeit des Supportprozesses erhalten bleiben, d. h., die jeweiligen Beteiligten sollten ihre Ticketsysteme anbinden und weiternutzen können. Hierbei und bei den o. g. Daten ist die Transparenz des aktuellen Status zwischen Cloud-Service-Portal und Cloud-Standort bzw. Softwarebetreiber immer aufrechtzuerhalten, d. h., allen Parteien müssen stets die gleichen Informationen vorliegen.

Nähere Kommunikationsbeziehungen zwischen Cloud-Service-Portal und Plattform- bzw. Softwarebetreibern, Cloud-Integratoren und Cloud-Standort sowie technische Details sind Gegenstand der entsprechenden Detailstandards.

5.4 Standards für das Cloud-Service-Portal

Im Rahmen der Deutschen Verwaltungscloud soll ein zentrales Self-Service-Portal für die gesamte ÖV als webbasierte Lösung eingerichtet werden, welche es erlaubt, Cloud-Services (z.B. in den Servicemodellen IaaS, PaaS inkl. CaaS-Angebote, SaaS) in einem Multi-Cloud-Kontext anzukündigen, zu registrieren, zu suchen, zu beauftragen, anzupassen und zu löschen. Die Cloud-Service-Anbieter werden mittels standardisierter technischer Schnittstellen an das Cloud-Service-Portal angebunden, um eine durchgehend hohe Automatisierung zu ermöglichen. Die Einrichtung dieser Schnittstellen ist obligatorisch für jeden Cloud-Standort.

Das Portal fungiert als zentraler Einstiegspunkt für Mitarbeitende des Auftraggebers bzw. Softwarebetreibers und muss über das Verwaltungsnetz zwischen Bund und Ländern (NdB-VN) und aus dem Internet erreichbar sein. Cloud-Service-Anbieter können jeweils festlegen, ob das Angebot aus dem Internet oder den Verwaltungsnetzen sichtbar und erreichbar ist. 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[61] soll langfristig sichergestellt werden. Angebotene Services müssen einen Mindeststandard bei der Beschreibung erfüllen. Folgende wesentliche 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),

[61] 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.

- Version des Service (u. a. Gültigkeitszeitraum/Supportzeitraum, Versionshistorie),
- Enthaltene Leistungen,
- Preis je Einheit,
- Abhängigkeiten zu anderen Services,
- Unterstützter Schutzbedarf und unterstützte Vertraulichkeitsstufen[62] aus Sicht des Betreibers,
- Zone für die Bereitstellung (Externe Zone, Interne Zone, Zone mit erhöhtem Schutzbedarf (z.B. VS-Zone, für Geheimschutzanforderungen),
- Aufzählung aller an der Erbringung des Service beteiligter Sub-Dienstleister und Nachunternehmer,
- Abrechnungsmodalitäten und Abnahmemengen,
- SLA (u. a. Betriebs-, Reaktions- und Wiederherstellungszeiten, Serviceklassen und Servicezeiten des Service),
- Modalitäten für Change Requests und für den Service Desk, und
- Reporting.

Weitere Ergänzungen im Rahmen der Feinkonzeptionierung sind möglich.

Den Nutzenden des Cloud-Service-Portals werden vielfältige Funktionen zur Verfügung gestellt, die das Verwalten von verschiedenen Services vereinfachen. Zur Nutzendenverwaltung im Cloud-Service-Portal sollen sowohl Organisationen und Unterorganisationen als auch Nutzende nach einem Registrierungsverfahren mit unterschiedlichen Berechtigungen angelegt werden können. Außerdem sollen im Cloud-Service-Portal beispielsweise Informationen zur Abrechnung und Verweise auf Service-Monitoring-Tools über das Cloud-Service-Portal abrufbar sein. Sämtliche funktionale und nicht-funktionale Anforderungen werden in der zukünftigen Feinkonzeptionierung des Cloud-Service-Portals behandelt. Diese umfassen ebenfalls das Vorgehen bei der Erfassung und Bearbeitung von Incidents, bei Change Requests sowie der

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

Durchführung von Service Changes, wie etwa beim Ausrollen einer neuen Softwareversion oder eines geänderten Service durch einen Cloud-Service-Anbieter.

Des Weiteren ist der Softwarebetreiber in Abstimmung mit dem Plattformbetreiber für die Lizenzierung verantwortlich. Der Plattformbetreiber benötigt jedoch ein Veto-Recht, falls der Softwarebetreiber Lizenzen einsetzen möchte, die die Lizenzkonformität seines Cloud-Standortes gefährden. Demnach muss 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.

Das Feinkonzept für das Cloud-Service-Portal befindet sich zum Zeitpunkt der Fortschreibung des vorliegenden Rahmenwerks in Erstellung. Nach Fertigstellung sollen die Entwicklung bzw. Beschaffung des Cloud-Service-Portals angestoßen werden. Im Rahmen der kontinuierlichen Weiterentwicklung der Deutschen Verwaltungscloud soll auch das Cloud-Service-Portal regelmäßig weiterentwickelt werden. Die hiermit verbundene Erhebung neuer funktionaler und nicht-funktionaler Anforderungen obliegt der einzurichtenden Koordinierungsstelle (s. Aufgabendokument der Koordinierungsstelle und Kapitel 6.1).

6 Weiteres Vorgehen und Operationalisierung der Deutschen Verwaltungscloud

Dieses Kapitel beschreibt die nächsten Schritte bei der Ausgestaltung der Deutschen Verwaltungscloud. Zudem werden weitere, bereits erarbeitete Inhalte zur Konzeption und Umsetzung der Deutschen Verwaltungscloud dargelegt.

Das weitere Vorgehen zur Umsetzung der Deutschen Verwaltungscloud teilt sich in drei Handlungsstränge, die parallel durch die UAG Technik sowie weiteren, nahestehenden Organisationen oder (Arbeits-) Gruppen bearbeitet werden. Dazu gehören 1) die Fortführung der Konzeption und des Aufbaus der Koordinierungsstelle inkl. Cloud-Service-Portal (Kapitel 6.1), 2) die kontinuierliche Weiterentwicklung und Detaillierung der Standards der DVS inkl. der Entwicklung der Supportstrukturen und -prozesse für die DVS und 3) die Durchführung von Pilotierungsprojekten zur Umsetzung und Evaluation der Standards für Cloud-Service-Anbieter sowie Softwarelieferanten (Kapitel 6.2). Die genannten Standards sollen (z.B. aufgrund technologischer oder rechtlicher Änderungen) flexibel angepasst und ergänzt werden können (Kapitel 2.4). Die parallellaufende Erprobung im Rahmen der Pilotierung 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 sollen.

Über den Fortschritt der einzelnen Handlungsstränge und der damit verbundenen Operationalisierung der Deutschen Verwaltungscloud, insbesondere hinsichtlich der Aktualisierung der Standards, wird der IT-PLR weiterhin regelmäßig informiert.

6.1 Konzeption der Koordinierungsstelle der Deutschen Verwaltungscloud

In Zukunft soll die inhaltliche Verantwortlichkeit für die Deutsche Verwaltungscloud (inkl. der Erstellung und Fortführung von Konzepten) von der UAG Technik an eine zu spezifizierende Koordinierungsstelle übergeben werden. Diese Koordinierungsstelle der Deutschen Verwaltungscloud soll für das Cloud-Service-Portal verantwortlich sein und u. a. die Finanzierung für dessen Entwicklung und Betrieb sicherstellen. Die Organisation ist zudem dafür zuständig, den Servicekatalog zu aktualisieren, und sie koordiniert die kontinuierliche Pflege des Katalogs durch

die Plattform- und Softwarebetreiber. Als weitere Aufgabe soll die Koordinierungsstelle die Einhaltung der Standards prüfen und durchsetzen.

Grundsätzlich soll die Koordinierungsstelle als Vermittlerin zwischen Cloud-Service-Anbietern und Cloud-Service-Vermittlern bzw. Cloud-Service-Kunden auftreten sowie deren Teilnahme an der DVS regeln und koordinieren. Sie soll außerdem die Befugnis haben, bei Bedarf einzelne Organisationen (z. B. bei potenzieller Kompromittierung der Informationssicherheit) von der Deutschen Verwaltungscloud auszuschließen. Eine detaillierte Beschreibung der Aufgaben liefert das Aufgabendokument der Koordinierungsstelle.

Der IT-PLR beauftragte die AG Cloud in seiner 36. Sitzung mit der Evaluation der Nachnutzung bestehender Strukturen der ÖV (IT-PLR Beschluss Nr. 2021/46). Diesem Auftrag wird aktuell nachgekommen, indem die Kompatibilität diverser bereits etablierter Organisationen in der ÖV mit den Aufgaben der Koordinierungsstelle und dem Zielbild der Deutschen Verwaltungscloud ermittelt wird. Parallel wird im Sinne der iterativen Weiterentwicklung der Deutschen Verwaltungscloud eine „Minimal Viable Product“ (MVP)-Version der Koordinierungsstelle inkl. Cloud-Service-Portal konzipiert. In diesem Rahmen sollen die teilnehmenden IT-Dienstleister als Cloud-Service-Anbieter und Cloud-Service-Kunden bereits erste Cloud-Services nach den Standards der DVS anbieten und nutzen können. Die Erfahrungen mit dieser Minimalversion der zentralen Elemente der Deutschen Verwaltungscloud sollen in die stetige Weiterentwicklung eingebracht und das MVP so kontinuierlich ergänzt und verfeinert werden, bis schließlich alle definierten Aufgaben der Koordinierungsstelle und die Anforderungen an das Cloud-Service-Portal erfüllt werden.

Neben der Koordinierungsstelle soll ein Architekturboard eingerichtet werden, das in Zukunft die Standards der Deutschen Verwaltungscloud anhand rechtlicher Änderungen und technologischer Trends und 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 und 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

beispielsweise die Eingliederung des geplanten Architekturboards in das bereits durch den IT-PLR eingerichtete föderale IT-Architekturboard[63] geprüft werden.

6.2 Durchführung von Pilotierungsprojekten

Ausgehend von den in Kapitel 5 definierten Standards der Deutschen Verwaltungscloud wurde zur Pilotierung der Umsetzung ein Proof-of-Concept (PoC, dt.: Machbarkeitsstudie) durchgeführt, in dessen Rahmen wesentliche Standards der DVS in der Praxis erprobt wurden. Die Durchführung des 1. DVS PoC erfolgte zwischen dem 1. Juli 2021 und dem 14. Januar 2022. Ein Ziel war der Nachweis des Grundprinzips der DVS – der standardisierte Betrieb von Software-Containern in unterschiedlichen Cloud-Standorten in ganz Deutschland. Dieses Ziel wurde erreicht; es wurden bereits bestehende definierte Standards der DVS in maschinenlesbare Richtlinien („Policies“) überführt und auf Container-Cluster in acht verschiedenen Datenzentralen aus Deutschland und Österreich angewendet. Die Einhaltung der Policies wurde mittels Konformitätstests überprüft und es wurden mehrere OS-Anwendungen unter Einhaltung der Policies an den verschiedenen Cloud-Standorten bereitgestellt. Zusätzlich sind weitere Ergebnisse bei der kontinuierlichen Weiterentwicklung und Detaillierung der Standards der DVS berücksichtigt worden und in die erste Fortschreibung des vorliegenden Rahmenwerks eingeflossen[64].

Im Rahmen des ersten PoCs hat sich ein neues Zusammenarbeitsmodell zwischen den teilnehmenden IT-Dienstleistern der ÖV etabliert, das insbesondere auch die gemeinsame Arbeit an Projekten auf der OS-Plattform der ÖV Open CoDE beinhaltet. Basierend auf dieser Zusammenarbeit und den Ergebnissen des 1. DVS PoC schreitet die kontinuierliche Umsetzung der DVS im Rahmen des DVS PoC 2.0 voran. Die wesentlichen Ziele des im Jahr 2022 stattfindenden DVS PoC 2.0 sind:

- die Fertigstellung der Definition der technologischen Grundlagen für die Bereitstellung von Entwicklungs- und Containerumgebungen innerhalb der DVS,

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

[64] Ein ausführliches Ergebnisdokument des 1. DVS PoC ist verfügbar unter https://www.it-planungsrat.de/fileadmin/it-planungsrat/foederale-zusammenarbeit/Gremien/AG_Cloud/220420_PoC-Ergebnisdokument_Langfassung_AG_Cloud_vf.pdf.

- die Befähigung der IT-Dienstleister der ÖV zum Angebot erster Leistungen gemäß DVS-Standards,
- die weitere Etablierung einer aktiven Zusammenarbeit zwischen IT-Dienstleistern der ÖV in OS-Projekten und
- die Definition standardisierter Anforderungen an Softwarelieferanten zur Lieferung von Containerlösungen.

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[65] (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[66] und der Architekturrichtlinie für die IT des Bundes[67].

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

SOLLTE – 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).

---

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

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

[67] Siehe https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/architekturen-standard/ArchRL.pdf?__blob=publicationFile&v=7.

7.2 Glossar

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

- **Application-Level-Gateway** – Die Funktionen eines Sicherheitsgateways auf Anwendungsebene werden von den so genannten Application-Level-Gateways (ALG) übernommen. Implizit nehmen ALGs auch Funktionen auf den ISO-/OSI-Schichten 1 bis 3 wahr. ALGs, auch Sicherheitsproxies genannt, unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über einen Proxy hinweg nimmt der Proxy die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt der Proxy analog. Sämtliche Kommunikationsbeziehungen zwischen den beiden Rechnern verlaufen in diesem Fall also mittelbar über den Proxy. Diese Kommunikationsform ermöglicht es einem Proxy beispielsweise bestimmte Protokollbefehle zu filtern (Definition gemäß BSI[68])..
- **Architekturboard** – (Zukünftiges) Gremium, das vorrangig für die (Weiter-) Entwicklung bestehender und neuer Standards der DVS zuständig ist und unabhängig von der Koordinierungsstelle besteht.
- **Audit-System** – Ein Audit untersucht, ob Prozesse, Anforderungen und Richtlinien die geforderten Standards erfüllen. Das Audit-System stellt die möglichst automatisierte Durchführung von Audits sicher.
- **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

[68] Siehe https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/Functions/glossar.html?nn=520190&cms_lv2=132780.

Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software (Definition gemäß BSI[69]).

- **Cloud-Integratoren** - IT-Dienstleister der ÖV, die Angebote verwaltungsexterner Cloud-Anbieter gemäß den DVS-Standards konfigurieren und so rechtssicher für die Deutsche Verwaltungscloud verfügbar machen.
- **Cloud-Service-Portal** – Zukünftiger zentraler Anlaufpunkt für die ÖV und deren IT-Dienstleister zur Verwaltung von Cloud-Services. Es soll seinen Nutzenden ermöglichen, Cloud-Services, bspw. IaaS- oder SaaS-Dienste, zu bestellen, zu stornieren und Informationen über bereitgestellte Cloud-Services zu erhalten. Ein Feinkonzept für das Cloud-Service-Portal befindet sich derzeit in Erstellung.
- **Cloud-Standort** – Cloud-Standorte bezeichnen die Rechenzentren bei Bund, Ländern, Kommunen und deren IT-Dienstleistern, 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.
- **Code Repository** - Zentrale Verwaltungsumgebung in der Softwareentwicklung zur Versionierung von Quellcode inkl. Dokumentationsfunktion.
- **Compliance** – Compliance ist die Umschreibung für die Gewährleistung von regelkonformem Handeln in Bezug auf die Einhaltung von Gesetzen und Richtlinien.
- **Containerisierung** - Verpacken von Softwarecode in Pakete, die alle erforderlichen Komponenten wie Libraries, Frameworks und andere Abhängigkeiten enthalten und in ihrem eigenen Container isoliert sind.
- **Containerumgebung** - Technische Plattform zum Betrieb und zur Verwaltung von Container-Clustern (Beispiele entsprechender Technologien sind OpenShift und Rancher). Die in diesem Kontext betrachteten Containerumgebungen basieren auf dem Kubernetes-Standard.
- **Container-as-a-Service** – Container-as-a-Service (CaaS) ist eine Form containerbasierter Virtualisierung, bei der die Laufzeitumgebung, Orchestrierungstools und die

[69] Siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html.

zugrundeliegenden Infrastruktur-Ressourcen über einen Cloud-Computing-Provider zur Verfügung gestellt werden (Definition gemäß IONOS[70]).

- **Container-Cluster** – Cluster in Kubernetes sind ein Rechner-Verbund, der für den Betrieb von containerisierten Softwarelösungen zuständig ist.
- **(Container-) Image** –Datei mit ausführbarem Code, der einen Container erzeugen kann. Es handelt sich um eine paketierte Applikation, die weiterhin die für die Applikation notwendigen Softwarebausteine enthält. Container-Images sind unveränderbar und können in jeder Container- bzw. Systemumgebung deployed werden.
- **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, Qualitätssicherung und Betrieb von IT-Systemen und -Lösungen.

[70] Siehe https://www.ionos.de/digitalguide/server/knowhow/caas-container-as-a-service-anbieter-im-vergleich/.

- **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[71]).
- **Fachverfahren** - Ein Fachverfahren ist die konkrete technische Umsetzung eines Verwaltungsprozesses in einem oder mehreren Informationssystemen. Es kann von einer oder mehreren Behörden intern genutzt werden, aber auch die Beteiligung der Bürgerinnen und Bürger, z.B. in einem Antragsverfahren, erlauben.
- **Firewall** – System aus soft- und hardwaretechnischen Komponenten, das dazu eingesetzt wird, IP-basierte Datennetze sicher zu koppeln (Definition gemäß BSI[72]).
- **Helm Charts** – Packaging-Format des Paketmanagers bestehend aus einer Sammlung von Daten und Anweisungen, mit denen die Kubernetes-Ressourcen und Abhängigkeiten der spezifischen Kubernetes-Anwendungen beschrieben sind[73].
- **Incident** – Sicherheitsvorfall oder eine Betriebsstörung einer IT-Lösung.
- **IVÖV** – Informationsverbund der öffentlichen Verwaltung - der Netzverbund soll zwischen den Einrichtungen der Bundes-, der Länder- und der Kommunen sowie den Anbietern von IT-Fachverfahren etabliert werden. Für den Informationsverbund übernimmt die BDBOS die Rolle der zentralen Netzbetreiberin sowie die Bereitstellung der netznahen Dienste.
- **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

---

[71] Siehe https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souveränität.

[72] 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.

[73] Siehe https://www.cloudcomputing-insider.de/was-ist-helm-a-921110/.

unterschiedlichen IT- oder Telekommunikationssystemen verwendet werden, um sensible Daten bzw. Informationen zu schützen (Definition gemäß BSI[74]).

- **Kubernetes Master** – Ein Kubernetes-Cluster basiert auf einem Satz von Maschinen. Diese werden in Master-Nodes und Worker-Nodes 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** – Die Nutzung mehrerer Cloud-Services verschiedener Cloud-Service-Anbieter in einer einzigen heterogenen Architektur durch einen Cloud-Service-Kunden.
- **Namespace** – Virtueller Cluster innerhalb eines Kubernetes-Clusters. Namespaces stellen im Kontext von Kubernetes einen Mechanismus zum Isolieren von Ressourcengruppen innerhalb eines Clusters bereit. Im Allgemeinen dienen Namespaces in der Informatik der Gruppierung bzw. Strukturierung.
- **Normal Changes** – Alle Änderungen, die keine Standard-Changes oder Notfall-Changes darstellen (Definition gemäß ITIL[75]).
- **Notfall-Changes (Emergency Changes)** – Änderungen, die sofort implementiert werden müssen, zum Beispiel um einen Major Incident zu beheben (Definition gemäß ITIL[76]).
- **OS Plattform der ÖV (Open CoDE)** – (Internet-) Plattform der ÖV, die aus einem zentralen und durchsuchbaren Verzeichnis an verwaltungsrelevanten Open Source Projekten, einem Code Repository zur Ablage von offenen Quellcodes bzw. Beteiligung an Projekten sowie einem Diskussionsforum besteht. Das Code Repository ist ein Standardisierungsbereich der DVS und soll die zentrale Ablage bzw. Spiegelung sowie Wiederverwendung von Quellcodes mit deren Dokumentation ermöglichen.

---

[74] Siehe 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.

[75] Siehe https://wiki.de.it-processmaps.com/index.php/Change_Management.

[76] Siehe https://wiki.de.it-processmaps.com/index.php/Change_Management.

- **Paketfilter** – Softwareprogramme für einfachere Firewallkonzepte zur Selektion von digitalen Signalen[77].
- **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.
- **Quellcode / Quelltext** – für den Menschen lesbarer, in einer Programmiersprache verfasste Beschreibungstext einer Software. Dieser Text beschreibt die Software exakt und vollständig, so dass dieser vollständig automatisch von einem Computer in Maschinensprache übersetzt werden kann.
- **Security Information and Event Management (SIEM)** – Echtzeitüberwachung und -analyse von Ereignissen sowie Verfolgung und Protokollierung von Sicherheitsdaten für Compliance- oder Prüfungszwecke[78].
- **Service-Level-Agreement** – Vereinbarung zwischen Anbieter und Kunde, welche der Qualitätssicherung dient. 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.

---

[77] Siehe https://www.itwissen.info/Paketfilter-packet-filter-PF.html.

[78] Siehe https://www.ibm.com/de-de/topics/siem.

- **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[79]*).*
- **Simple Mail Transfer Protocol (SMTP)-Relay –** Standardnetzwerkprotokoll zur Einspeisung und Weiterleitung von E-Mails im Internet[80].
- **Softwarebetreiber** – Der Softwarebetreiber verantwortet als Auftragnehmer den Betrieb einer Softwarelösung entsprechend vertraglichen 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.
- **Standard-Change:** Vorautorisierte Änderungen mit geringem Risiko, die einer erprobten Prozedur folgen (Definition gemäß ITIL[81]).
- **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.

---

[79] Siehe https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/S/Sicherheitsgateway.html.

[80] Siehe https://www.ionos.at/digitalguide/e-mail/e-mail-technik/smtp-relay/.

[81] Siehe https://wiki.de.it-processmaps.com/index.php/Change_Management.

- **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.
- **Kubernetes 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.

7.3 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
NdB-VN	Netze des Bundes - Verbindungsetz
ÖFIT	Kompetenzstelle Öffentliche IT
OS	Open-Source
OSCI	Online Services Computer Interface
OSS	Open-Source-Software
ÖV	Öffentliche Verwaltung
OZG	Onlinezugangsgesetz

Abkürzung	Bedeutung
PaaS	Platform-as-a-Service
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	Verschlusssache – Nur für den Dienstgebrauch