Der Beauftragte der
Bundesregierung
für Informationstechnik

Dienstekonsolidierung

Domänenarchitektur Infrastruktur

Version 2019

Management Summary

Die vorliegende Domänenarchitektur beschreibt für die Domäne Infrastruktur (INF) die „dynamischen Aspekte und Abhängigkeiten der Dienste einer Domäne untereinander sowie zu Diensten anderer Domänen“ (vgl. [1.], Glossar). Sie baut auf der Strategie Dienstekonsolidierung 2018-2025 auf (vgl. [1.]). Domänenübergreifende Aspekte, Motivation, Definitionen, Notationen und Methoden werden im Rahmendokument behandelt (vgl. [2.]).

Diese Domänenarchitektur beschreibt in Kapitel 2 exemplarisch Szenarien, die wesentliche Anwendungsfälle verbinden und Abhängigkeiten der Dienste verdeutlichen. Der Domäne INF sind aktuell 25 Dienste mit etwa 100 Funktionalitäten zugeordnet.

Im Kapitel 3 werden die Architekturfelder Entwicklungs- und Betriebsdienste, Sicherheitsdienste sowie Infrastrukturdienste eingeführt, beschrieben und anschließend zur Domänenarchitektur INF verbunden. Die Architekturfelder entsprechen in der Domäne INF weitgehend den Diensteklassen. Dabei werden relevante Abhängigkeiten zwischen domäneneigenen und gegebenenfalls externen Diensten betrachtet.

Die Domänenarchitektur INF bildet eine Grundlage für die Referenz- und Facharchitekturen. Die Szenarien der Domänenarchitektur INF werden in der Konzeption der IT-Maßnahmen als Vorgaben für die Facharchitekturen berücksichtigt. Die Architekturfelder der Domänenarchitektur INF definieren die Ausrichtung der Referenzarchitekturen.

Ziel der Domänenarchitektur INF ist es, den Behörden eine architektonische Grundlage für Infrastrukturleistungen zu standardisierter, harmonisierter und großflächig nutzbarer IT zu geben.

Inhaltsverzeichnis

1 Domäne Infrastruktur (INF)

Die Dienstedomäne Infrastruktur (INF) umfasst standardisierte IT-Infrastrukturdienste für die Nutzung und den Betrieb von Basis- und Querschnittsdiensten sowie Fachdiensten. Die Dienste der Domäne INF umfassen insbesondere Funktionen für die Bereitstellung von IT-Arbeitsplätzen (Diensteklasse Clientdienste sowie Druck- und Scandienste) und den Betrieb der Rechenzentrums-IT auf konventionellen und cloudbasierten Betriebsplattformen (Diensteklasse Entwicklungs- und Betriebsdienste). Der Zugriff auf die Dienste erfolgt über sichere Verwaltungsnetze (Diensteklasse Netzdienste). Darüber hinaus werden Dienste zur Authentifizierung und zum Schutz des Zugriffs auf die IT-Infrastruktur definiert (Diensteklasse Sicherheitsdienste). In der Diensteklasse Kommunikationsdienste werden Dienste zusammengefasst, die die behördenspezifische Kommunikation sicherstellen sollen.

Folgende Ziele sollen dabei insbesondere erreicht werden:

- Service-Plattform: zukunftsorientiertes Service- und Produktportfolio mit einheitlichen Liefermodellen IaaS, PaaS und SaaS
- Standardisierung: Bundesclients inkl. der zugehörigen Services
- Unabhängigkeit: Entkopplung von Anwendungen und Client sowie Gewährleistung von Hersteller- und Geräteunabhängigkeit

Zur Erreichung der Zielsetzung wurden in der Strategie Dienstekonsolidierung fünf Handlungsfelder identifiziert:

- Einführung cloudbasierter Servicemodelle,
- Software-Entwicklung für neue IT-Lösungen auf Basis einer Cloud-Entwicklungsplattform,
- Einführung eines standardisierten Client-Arbeitsplatzes,
- Gewährleistung der IT-Sicherheit sowie
- Aufbau einer Netz- und Kommunikationsinfrastruktur.

Der grundlegende Zusammenhang zwischen den Handlungsfeldern, den Diensteklassen der Domäne Infrastruktur und den Diensten anderer Dienstedomänen ist in der nachfolgenden Abbildung 1 dargestellt.

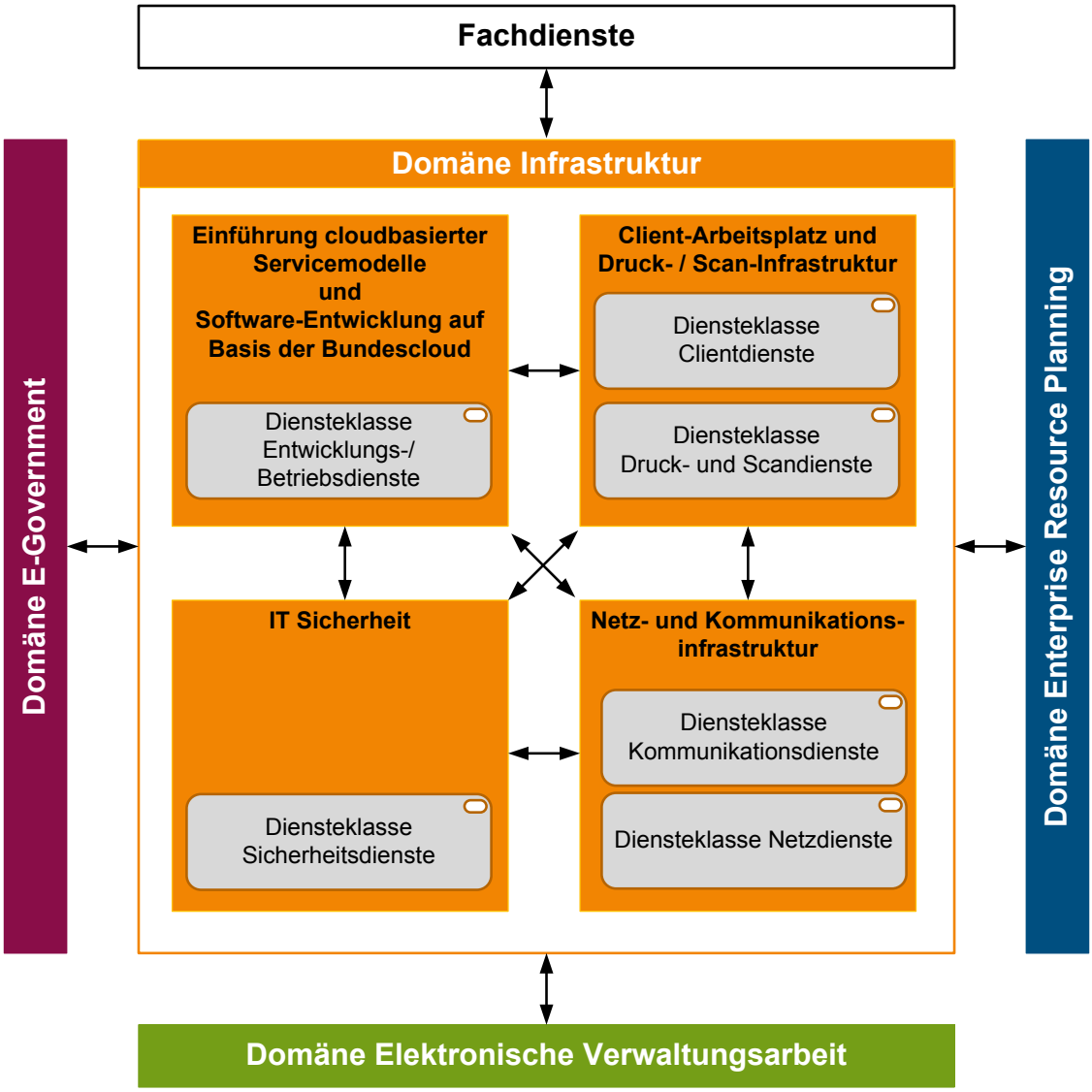

Abbildung 1: Handlungsfelder und Diensteklassen der Domäne INF

Für jede der vier Domänen der Dienstekonsolidierung liegt ein separates Dokument zur Domänenarchitektur vor. Die Struktur, die Notation und Methoden sowie die domänenübergreifenden Vorgaben der Dienstekonsolidierung sind im „Rahmendokument für die Domänenarchitekturen“ dargestellt (vgl. [2.]).

Die Handlungsfelder, Dienstesteckbriefe und Kernfunktionalitäten der Domäne ERP sind der „Strategie Dienstekonsolidierung“ zu entnehmen (vgl. [1.]).

2 Szenarien der Domäne INF

Szenarien sind eine typische Abfolge von Anwendungsfällen (vgl. [2.]). Die Anwendungsfälle nutzen die Funktionalitäten der Dienste gemäß der Strategie Dienstekonsolidierung (vgl. [1.]). Eine detaillierte Beschreibung der Anwendungsfälle findet sich im Anhang.

Ein Szenario besteht jeweils aus der textuellen Beschreibung und einer grafischen Repräsentation des Ablaufs. Bei der Repräsentation der Abläufe wurde bewusst ein hohes Abstraktionsniveau gewählt und auf die Abbildung behördenspezifischer Besonderheiten verzichtet, um eine möglichst hohe Allgemeingültigkeit und Anwendbarkeit der Szenarien auf die Mehrheit der Behörden sicherzustellen. Es handelt sich um exemplarische Szenarien, die verbindliche Ausgestaltung der Szenarien wird im Rahmen der korrespondierenden IT-Maßnahmen erfolgen. Es werden Voraussetzungen für die Nutzung der Dienste der Domäne sowie Schnittstellen zu anderen Domänen und Fachdienste identifiziert. Die Beschreibung der in der grafischen Repräsentation genutzten Elemente (Notation) findet sich im übergreifenden Rahmendokument der Gesamtarchitektur (vgl. [2.]).

Um die Lesbarkeit und Nachvollziehbarkeit des Dokuments durchgängig sicherzustellen, wurde die Nummerierung der Szenarien von der Abschnittsnummerierung abgeleitet. So ist z.B. das Szenario S2.1 in Abschnitt 2.1 beschrieben. Zur Nummerierung der Anwendungsfälle werden die Nummern der Szenarien um die Platzierung der Aktivität im Szenario ergänzt. So ist der Anwendungsfall S2.1.3 die dritte Aktivität im Szenario S2.1 . Eine Referenz auf den zugehörigen ausführlichen Anwendungsfall ist am Ende der textuellen Beschreibung in den Szenarien in Klammern angegeben.

2.1 Szenario „Bereitstellung eines IT-Arbeitsplatzes“

Das Szenario S2.1 stellt die Bereitstellung eines IT-Arbeitsplatzes für einen neuen Mitarbeiter dar. Es wird davon ausgegangen, dass der Entscheidungsprozess für die Einstellung abgeschlossen ist („Neuer Mitarbeiter wird eingestellt“) und dass die Stammdaten des Mitarbeiters im Personalmanagement angelegt worden sind.

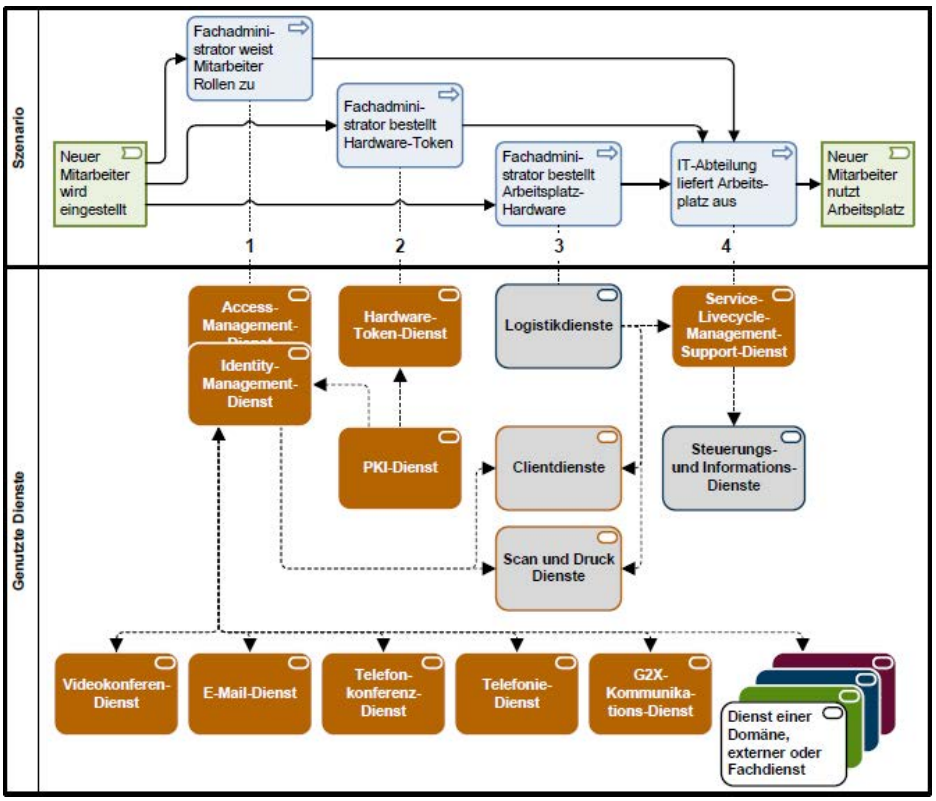

Abbildung 2: Bereitstellung eines IT-Arbeitsplatzes (Szenario S2.1)

Das Szenario besteht aus folgender Sequenz von Anwendungsfällen:

1. **Fachadministrator weist Mitarbeiter Rollen zu.**
   Voraussetzung für dieses Szenario ist, dass in den Personaldiensten der Domäne ERP die Stammdaten des Mitarbeiters erzeugt und die notwendigen Daten für den Aufbau einer elektronischen Identität zum zentralen Identity-Management-Dienst übertragen worden sind. Diese Übertragung kann z.B. durch einen Trigger im Personaladministrationsdienst angestoßen oder über einen täglichen Abgleich zwischen den beiden Systemen realisiert werden. Nach der Initialisierung der elektronischen Identität weist ein Fachadministrator mit Hilfe der Identity- und Access-Management-Dienste dem Mitarbeiter die notwendigen Rechte und Rollen für die ihm zugeordneten IT-Lösungen zu. Eine Grundvoraussetzung für die Nutzung des IT-Arbeitsplatzes ist die Erteilung der Rechte für die Endgeräte aus der Diensteklasse Clientdienste und aus der Diensteklasse Druck- und Scandienste. Die Identitätsdaten werden weiteren Diensten, z.B. Telefonie-Dienst oder E-Mail-Dienst, zur Verfügung gestellt. (Anwendungsfall S2.1.1)
2. **Fachadministrator bestellt Hardware-Token.**
   Ein Fachadministrator bestellt für den Mitarbeiter einen Hardware-Token, z.B. für die Authentifizierung an Endgeräten. Über den Hardware-Token-Dienst wird die Bereitstellung des Hardware-Tokens und dessen Initialisierung/Personalisierung durchgeführt. Über die Public Key Infrastructure (PKI) werden die benötigten Zertifikate für den Hardware-Token bereitgestellt (PKI-Dienst). Personenbezogene Zertifikate werden über den Identity-Management-Dienst mit der Identität des Mitarbeiters verknüpft. (Anwendungsfall S2.1.2)

3. **Fachadministrator bestellt Arbeitsplatz-Hardware.**
   Ein Fachadministrator bestellt die Arbeitsplatz-Hardware für den Mitarbeiter. Über die Diensteklasse Logistikdienste der Domäne ERP erfolgt die Bestellung der notwendigen Hardware für den IT-Arbeitsplatz. Dazu wird ein IT-Arbeitsplatztyp aus den Diensten der Diensteklasse Clientdienste (Arbeitsplatz-PC, Mobiles-Gerät, Ultra-Mobiles Gerät) ausgewählt. Nach der Anlieferung der bestellten Komponenten wird der IT-Arbeitsplatz (Endgerät und Peripheriegeräte) entsprechend der gewählten Ausstattung konfiguriert und zur Auslieferung an den Mitarbeiter vorbereitet. Informationen aus den Lieferdaten wie Seriennummern, Informationen zu Wartungsverträgen etc. werden an den Service-Lifecycle-Management-Support-Dienst zur Dokumentation übergeben. (Anwendungsfall S2.1.3)

4. **Arbeitsplatz wird bereitgestellt.**
   Der IT-Arbeitsplatz wird mit den definierten Leistungen zur Verfügung gestellt. Die Details zur Konfiguration werden im Service-Lifecycle-Management-Support-Dienst dokumentiert. Darüber werden die genutzten Leistungen an die Diensteklasse Steuerung und Information der Domäne ERP zur Verrechnung gegenüber der beziehenden Behörde übermittelt. (Anwendungsfall S2.1.4)

2.2 Szenario „Erweiterung eines IT-Arbeitsplatzes“

Das Szenario S2.2 stellt den vereinfachten Ablauf bei der Erweiterung eines IT-Arbeitsplatzes um zusätzliche Komponenten aus Sicht des Mitarbeiters dar.

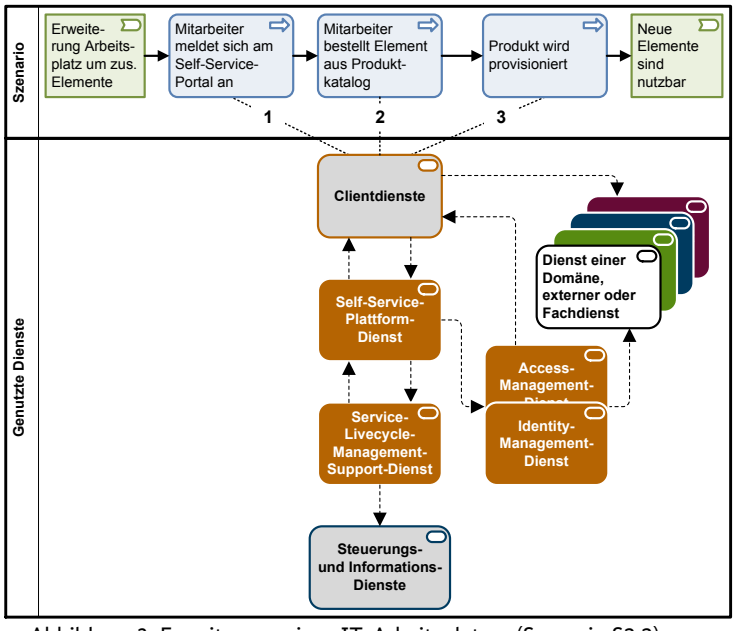

Abbildung 3: Erweiterung eines IT-Arbeitsplatzes (Szenario S2.2)

Das Szenario besteht aus folgender Sequenz von Anwendungsfällen:

1. **Mitarbeiter meldet sich am Self-Service-Portal an.**
   Der Mitarbeiter meldet sich über seinen IT-Arbeitsplatz (Diensteklasse Clientdienste) am Self-Service-Portal an, das durch den zentralen Self-Service-Plattform-Dienst realisiert wird. Der Mitarbeiter navigiert darin in den Bereich, in dem der Produktkatalog für den IT-Arbeitsplatz zur Auswahl steht. Die Identity- und Ac-

cess-Management-Dienste generieren die für den Zugriff auf das Self-Service-Portal notwendigen Anmeldedaten für das Single-Sign-On am Portal. (Anwendungsfall S2.2.1)

2. **Mitarbeiter bestellt Element aus Produktkatalog.**
   Der Mitarbeiter wählt die gewünschte Leistung aus dem Produktkatalog aus und bestellt diese. Die Daten für den Produktkatalog werden über den Service-Lifecycle-Management-Support-Dienst dem Portal zur Verfügung gestellt. Die im Produktkatalog zur Auswahl stehenden Angebote werden über die in den Identity- und Access-Management-Diensten hinterlegten Rollen und Rechte des Mitarbeiters eingeschränkt. (Anwendungsfall S2.2.2)

3. **Produkt wird provisioniert.**
   Nach Genehmigung und Bearbeitung des Bestellvorgangs werden die bestellten Produkte provisioniert. Dies erfolgt über die Diensteklasse Clientdienste. Die notwendigen Berechtigungen, die für die Nutzung der gebuchten Leistung erforderlich sind, werden über die Identity- und Access-Management-Dienste vergeben. Die zusätzliche Leistungsnutzung wird wiederum im Service-Lifecycle-Management-Support-Dienst dokumentiert und die Verbrauchsdaten zur Abrechnung dem entsprechenden Dienst der Diensteklasse Steuerungs- und Informationsdienste der Domäne ERP zugeführt. Nach Abschluss der Provisionierung, kann der Mitarbeiter die zusätzliche Komponente am IT-Arbeitsplatz nutzen. (Anwendungsfall S2.2.3)

2.3 Szenario „Software-Entwicklung auf der Cloud-Entwicklungsplattform“

Das Szenario S2.3 beschreibt den Ablauf für die Entwicklung von IT-Lösungen, die mit dem Cloud-Entwicklungsplattform-Dienst realisiert und über den Cloud-Betriebsplattformdienst bereitgestellt werden sollen.

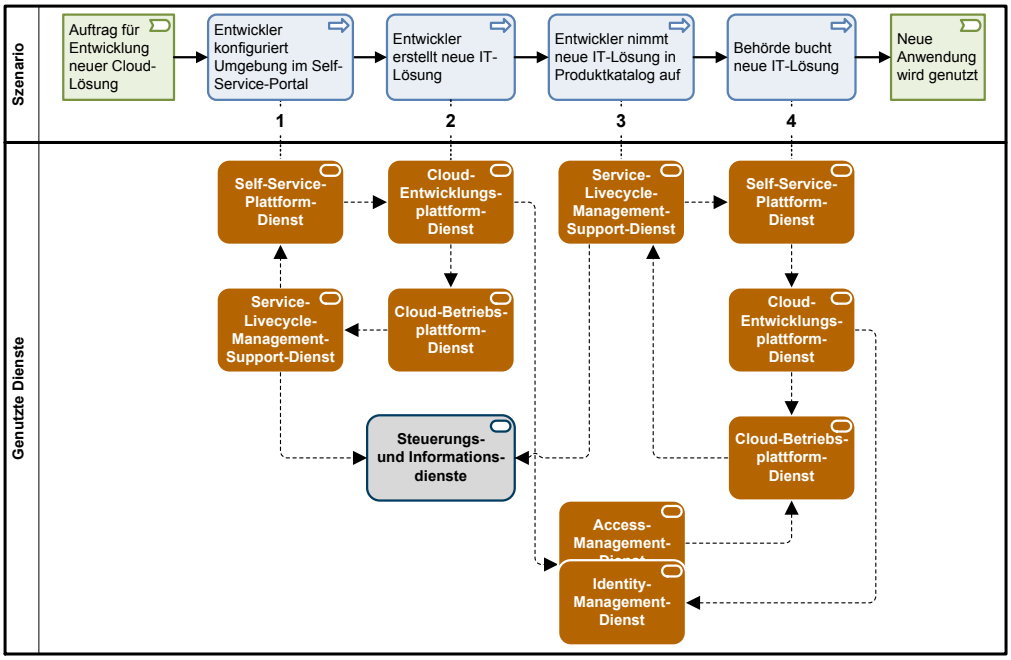

Abbildung 4: Software-Entwicklung auf der Cloud-Plattform (Szenario S2.3)

Das Szenario besteht aus folgender Sequenz von Anwendungsfällen:

1. **Entwickler konfiguriert Umgebung im Self-Service-Portal.**
   Der zur Verfügung stehende Produktkatalog im Self-Service-Portal wird über den Service-Lifecycle-Management-Support-Dienst bereitgestellt. Aus diesem Angebot stellt sich der Entwickler die benötigte Umgebung zusammen. Die Provisionierung der Umgebung erfolgt über die bereitgestellten Funktionalitäten im Cloud-Entwicklungsplattform-Dienst. Der Cloud-Betriebsplattform-Dienst stellt die notwendigen Compute-, Storage- und Netzwerk-Ressourcen für die verwendeten Cloud-Service-Angebote (Produktkatalog) bereit. Die ausgewählten Katalogelemente werden im Service-Lifecycle-Management-Support-Dienst dokumentiert, die Abrechnung der für die Entwicklungsumgebungen verwendeten Ressourcen erfolgt über die Daten, die der Service-Lifecycle-Management-Support-Dienst dem ERP Steuerungs- und Informationsdienst bereitstellt. (Anwendungsfall S2.3.1)
2. **Entwickler erstellt eine neue IT-Lösung.**
   Der Entwickler erstellt eine neue IT-Lösung unter Verwendung der gebuchten Entwicklungs- und Testumgebungen. Der Entwickler nutzt die vorhandenen Funktionen im Cloud-Entwicklungsplattform-Dienst für die Automatisierung der Provisionierung neuer Umgebungen und Software-Releases über Continuous Integration/Continuous Delivery (CI/CD). Bestandteil der Automatisierung ist die Bereitstellung der für die Nutzung der neuen IT-Lösung notwendigen Rollen/Rechte an den Identity- und Access-Management-Dienst, damit darüber später die Zuweisung an den Anwender erfolgen kann. (Anwendungsfall S2.3.2)
3. **Entwickler nimmt neue IT-Lösung in Produktkatalog auf.**
   Durch die Aufnahme der IT-Lösung in den Produktkatalog steht diese für die Behörden zur Buchung bereit. Die buchbaren Elemente der neuen IT-Lösung werden über den Service-Lifecycle-Management-Dienst dem Self-Service-Plattform-Dienst zur Verfügung gestellt und sind damit durch die Behörden bestellbar. (Anwendungsfall S2.3.3)
4. **Behörde bucht neue IT-Lösung.**
   Über den Self-Service-Plattform-Dienst kann eine Behörde aus dem Produktkatalog die gewünschte Lösung auswählen und bestellen. Nach Durchlaufen der notwendigen Genehmigungs- und Freigabeprozesse wird über den Cloud-Entwicklungsplattform-Dienst die Provisionierung der Lösung auf den Cloud-Betriebsplattform-Dienst ausgelöst. Die gebuchten Ressourcen werden wiederum im Service-Lifecycle-Management-Support-Dienst protokolliert und der Ressourcenverbrauch den Steuerungs- und Informationsdiensten zyklisch für die Abrechnung bereitgestellt. Bei der Provisionierung werden die vordefinierten Rechte und Rollen an die IT-Lösung übergeben. Zusätzlich kann der Fachadministrator in der Behörde den Anwendergruppen weitere Rechte und Rollen zuordnen. Beide Zuweisungen erfolgen über die Identity- und Access-Management-Dienste. Damit steht die IT-Lösung den Anwendern zur Verfügung, sobald sie das Angebot zum IT-Arbeitsplatz hinzugebucht haben. Aus der IT-Lösung wird dadurch eine Anwendung für die Mitarbeiter der Behörde. (Anwendungsfall S2.3.4)

2.4 Szenario „Automatisierte Bereitstellung einer IT-Arbeitsplatzausstattung“

Das Szenario S2.4 stellt den Ablauf bei der automatisierten Bereitstellung eines IT-Arbeitsplatzes für einen neuen Mitarbeiter dar.

Es wird davon ausgegangen, dass:

- eine IT-Arbeitsplatzausstattung aus folgenden Bestandteilen besteht:
  - Dienstausweis
  - Arbeitsplatz-PC (Laptop inkl. Dockingstation oder klassischer PC)
  - Externer Monitor
  - Tastatur
  - Maus
  - Arbeitsplatz-Telefon (inkl. Headset)
  - Optionale Bestandteile: Drucker und ggfs. weitere mobile Endgeräte
- der Entscheidungsprozess für die Einstellung abgeschlossen ist.
- der HR Mitarbeiter über einen IT-Arbeitsplatz und die notwendigen Rechte verfügt, um neue Mitarbeiter anzulegen.
- vordefinierte Rollenprofile im Personalverwaltungssystem (PVS) hinterlegt sind, die neuen Mitarbeitern zugewiesen werden können. Ein Rollenprofil besteht aus einer Rolle innerhalb einer Behörde, einer dazugehörigen Rollenbeschreibung, einer Auswahl vordefinierter Rechte (bspw. Zutrittsrechte, Zugriff auf Systeme, etc.), einer definierten IT-Arbeitsplatzausstattung und ggfs. weiteren notwendigen Merkmalen.

Abgrenzung:

- Die vordefinierten Rollenprofile umfassen keine spezifischen Rollen- und Rechtezuordnungen für die Nutzung von Fachverfahren.

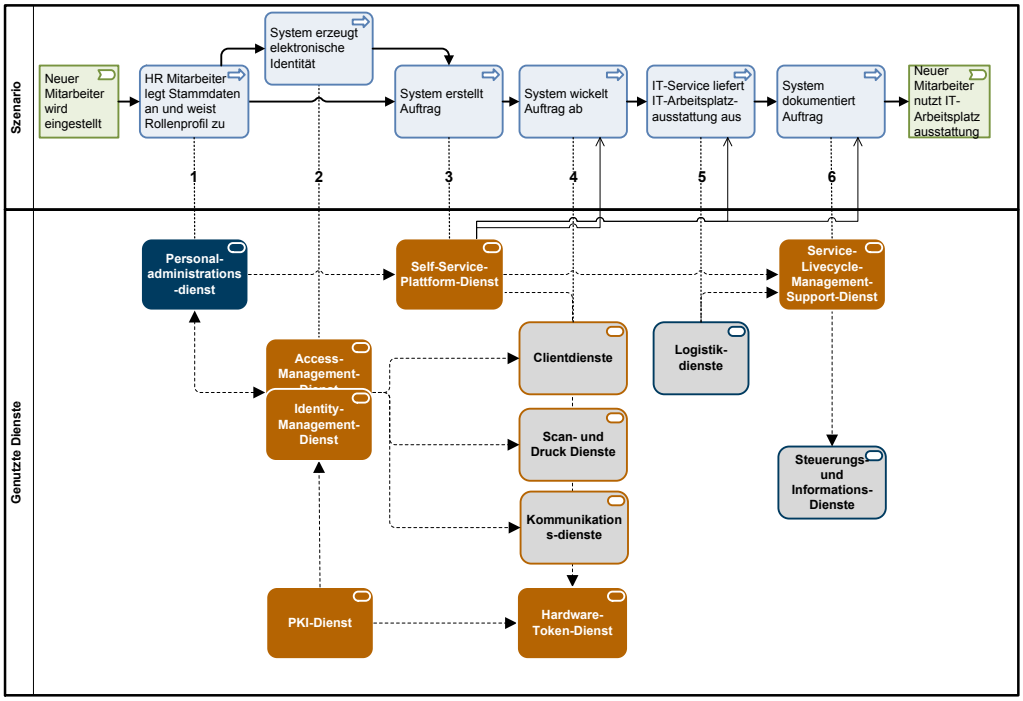

Abbildung 5: Bereitstellung eines IT-Arbeitsplatzes (Szenario S2.4)

Das Szenario besteht aus folgender Sequenz von Anwendungsfällen:

1. **HR Mitarbeiter legt Stammdaten an und weist Rollenprofil zu.**
   Der HR Mitarbeiter greift auf den Personaladministrationsdienst der Domäne ERP zu. Anschließend legt der HR Mitarbeiter die Stammdaten des neuen Mitarbeiters an und weist ein vordefiniertes Rollenprofil zu. Über die Identity- und Access-Management-Dienste der Domäne INF werden die für den Zugriff notwendigen Anmeldedaten für das Single-Sign-On am Portal generiert. (Anwendungsfall S2.4.1)

2. **System erzeugt elektronische Identität.**
   In der Personalverwaltung wird nach erfolgreicher Speicherung der Informationen automatisch das Anlegen einer elektronischen Identität des neuen Mitarbeiters initiiert. Alle notwendigen Informationen zum Anlegen dieser Identität werden vom Personaladministrationsdienst der Domäne ERP zum Identity- / und Access-Management-Dienst der Domäne INF transferiert. Dem neuen Mitarbeiter wird im IAM eine globale Identifikationsnummer (GID) zugewiesen. (Anwendungsfall S2.4.2)

3. **System erstellt Auftrag.**
   In der Personalverwaltung wird nach erfolgreicher Speicherung der Informationen ein Vorgang im Self-Service-Plattform-Dienst ausgelöst, der wiederum einen Auftrag zur Bereitstellung der IT-Arbeitsplatzausstattung auslöst. Der Auftrag enthält die bereit zu stellende IT-Arbeitsplatzausstattung, die aus dem Rollenprofil übernommen wird. (Anwendungsfall S2.4.3)

4. **System wickelt Auftrag ab.**
   Zur Provisionierung nutzt der Self-Service-Plattform-Dienst die DK Clientdienste, DK Druck- und Scandienste, DK Kommunikationsdienste sowie den Hardware-Token-Dienst aus der DK IT-Sicherheitsdienste aus der Domäne INF. Über die Public Key Infrastructure werden die benötigten Zertifikate für den Hardware-

Token bereitgestellt (PKI-Dienst). Personenbezogene Zertifikate werden über den Identity-Management-Dienst der Domäne INF mit der Identität des Mitarbeiters verknüpft. (Anwendungsfall S2.4.4)

5. **IT-Service liefert IT-Arbeitsplatzausstattung aus.**
   Der IT-Service nutzt die DK Logistikdienste der Domäne ERP, um die physischen Bestandteile der IT-Arbeitsplatzausstattung dem Mitarbeiter auszuliefern. (Anwendungsfall S2.4.5)
6. **System dokumentiert Auftrag.**
   Das System dokumentiert den Auftrag. Die Dokumentation des Auftrages (Informationen zur Auftragsabwicklung) erfolgt im Self-Service-Plattform-Dienst der Domäne INF. Die Dokumentation des Auftrages (Technische Konfiguration) im Service-Lifecycle-Management-Support-Dienst der Domäne INF. Die genutzten Leistungen werden an die Diensteklasse Steuerung und Information der Domäne ERP zur Verrechnung gegenüber der beziehenden Behörde übermittelt. (Anwendungsfall S2.4.6)

2.5 Szenario „Sichere Kommunikation im elektronischen Rechtsverkehr“

Die Szenarien S2.5.1 und S2.5.2 beschreiben die Abläufe bei der Nutzung eines Postfachs im elektronischen Rechtsverkehr. Dieser Postfachserver wird als Intermediär bezeichnet.

2.5.1 Nachrichtenversand im elektronischen Rechtsverkehr

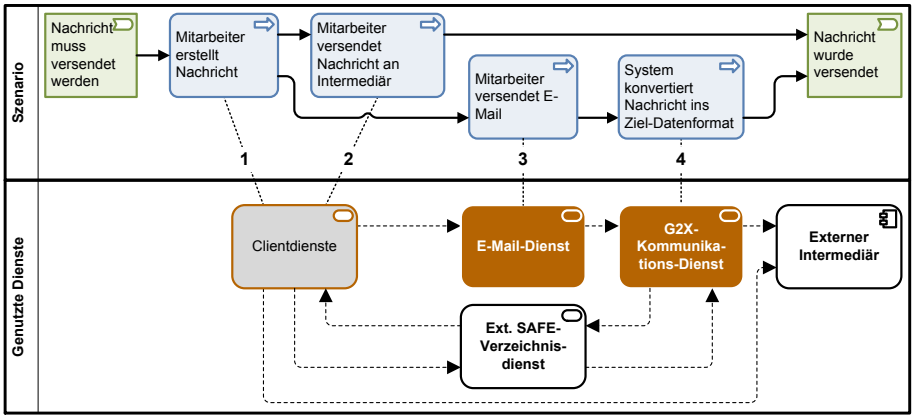

Abbildung 6: Nachrichtenversand im elektronischen Rechtsverkehr (Szenario S2.5.1)

Das Szenario besteht aus folgender Sequenz von Anwendungsfällen:

1. **Mitarbeiter erstellt eine Nachricht.**
   Auf dem IT-Arbeitsplatz des Arbeitsplatz-PC-Dienstes wird die zu versendende Nachricht erstellt oder aus einem Fachdienste für den Versand bereitgestellt. (Anwendungsfall S2.5.1.1)
2. **Mitarbeiter versendet Nachricht an Intermediär.**
   Der Mitarbeiter versendet die Nachricht aus einer Client-Anwendung oder mittels einer Web-Schnittstelle (bspw. beBPo-Web), die für den direkten Zugriff auf einen Intermediär geeignet ist. Für die Ermittlung der Adresse des Intermediärs greift der

Client auf den externen SAFE-Registrierungsdienst der Justiz zu und ermittelt dort die URI-Adresse für den externen Intermediär. Anschließend wird die Nachricht im Postfach des Intermediärs abgelegt. (Anwendungsfall S2.5.1.2)

3. **Oder: Mitarbeiter versendet E-Mail.**
   Der Mitarbeiter nutzt seinen E-Mail Client für die Nachrichtenübertragung an den externen Intermediär. Im ersten Schritt ermittelt er über ein Web-Portal die E-Mail-Adresse des Kommunikationspartners. Wenn er die E-Mail an diese Adresse versendet, wird sie vom E-Mail-Dienst an den G2X-Kommunikations-Dienst weitergereicht und dort in eine für den elektronischen Rechtsverkehr konforme Nachricht umgewandelt. Über den externen SAFE-Registrierungsdienst der Justiz wird die Adresse des externen Intermediärs ermittelt und diesem zugestellt. (Anwendungsfall S2.5.1.3)
4. **System konvertiert Nachricht ins Ziel-Datenformat.**
   Die E-Mail Nachricht inklusive aller Anhänge wird im G2X-Kommunikations-Dienst auf Sicherheitsrisiken (z.B. Viren, Trojaner etc.) überprüft und in das Ziel-Datenformat des Intermediärs konvertiert. Dabei wird die Nachricht elektronisch signiert und verschlüsselt. Die dafür notwendigen Zertifikate sind im G2X-Kommunikations-Dienst vorab hinterlegt worden. (Anwendungsfall S2.5.1.4)

2.5.2 Nachrichtenempfang im elektronischen Rechtsverkehr

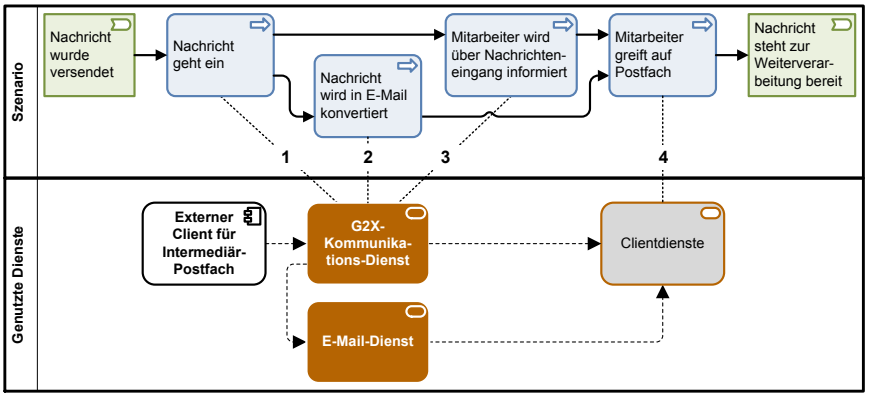

Abbildung 7: Nachrichtenempfang im elektronischen Rechtsverkehr (Szenario S2.5.2)

Das Szenario besteht aus folgender Sequenz von Anwendungsfällen:

1. **Nachricht geht ein.**
   Ein externer Client, der für den Zugriff auf das Postfach des Intermediärs verwendet wird, liefert eine Nachricht am Intermediär an. Der G2X-Kommunikations-Dienst holt diese Nachricht ab und weist über eine Abgleichslogik die Mail der richtigen Person zu. (Anwendungsfall S2.5.2.1)
2. **Nachricht wird in E-Mail konvertiert.**
   Für die Anwendergruppe in der Behörde, die als E-Mail Empfänger im G2X-Kommunikations-Dienst hinterlegt sind, prüft eine Middleware den Intermediär auf Eingang neuer Nachrichten. Ist eine neue Nachricht eingegangen, dann wird diese abgeholt, die notwendigen Routinen für eine Konvertierung ins E-Mail Format, u.a. mit Protokollierung der verwendeten Zertifikate, Erstellung einer Empfangsbestätigung, durchgeführt und über den E-Mail-Dienst an den Empfänger weitergeleitet. (Anwendungsfall S2.5.2.2)

3. **Oder: Mitarbeiter wird über Nachrichteneingang informiert.**
   Die Logik des G2X-Kommunikations-Dienstes informiert den Mitarbeiter mit Hilfe des E-Mail-Dienstes (Info-Mail via Outlook) über den Eingang einer neuen Nachricht auf dem Intermediär. (Anwendungsfall S2.5.2.3)
4. **Mitarbeiter greift auf Postfach zu.**
   Der Mitarbeiter ruft die Nachricht aus einer Client-Anwendung oder mittels einer Web-Schnittstelle (bspw. beBPo-Web) ab. Je nach Client-Anwendung greift der Mitarbeiter von seinem IT-Arbeitsplatz entweder mit seinem lokalen Client, der für die direkte Kommunikation mit einem Intermediär geeignet ist, auf das Postfach auf dem Intermediär zu, oder er verwendet seinen E-Mail-Client, um die konvertierte Nachricht abzurufen. (Anwendungsfall S2.5.2.4)

2.6 Szenario „Beantragung eines elektronischen Dienstausweises“

Das Szenario S2.6 stellt den Ablauf der Beantragung eines elektronischenDienstausweises (eDA) dar.

Es wird davon ausgegangen, dass:

- der HR Mitarbeiter über einen IT-Arbeitsplatz und die notwendigen Rechte verfügt, um neue Mitarbeiter anzulegen.
- der Mitarbeiter der Dienstausweisstelle über einen IT-Arbeitsplatz und die notwendigen Rechte verfügt, um eine Dienstausweis-Bestellung zu initiieren.
- die Bestellabwicklung über den HTD insbesondere dem Card-Management-System (CMS) erfolgt.

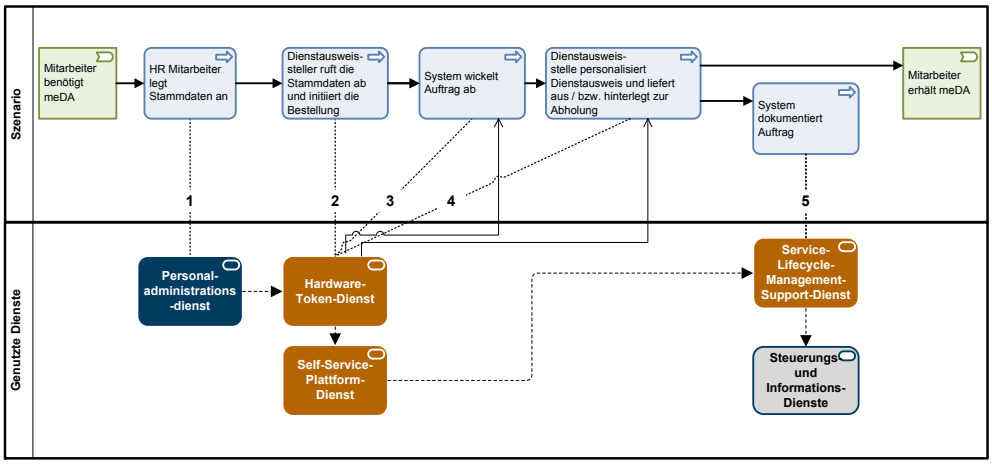

Abbildung 8: Beantragung eines Dienstausweises (Szenario S2.6)

Das Szenario besteht aus folgender Sequenz von Anwendungsfällen:

1. **HR Mitarbeiter legt Stammdaten an.**
   Der HR Mitarbeiter greift auf den Personaladministrationsdienst der Domäne ERP zu, legt die Stammdaten des neuen Mitarbeiters an und hinterlegt die Zutrittsberechtigungen für Liegenschaften und Räume. (Anwendungsfall S2.6.1)
2. **Dienstausweissteller ruft die Stammdaten ab und initiiert die Bestellung.**
   Der Mitarbeiter der Dienstausweisstelle ruft die Stammdaten aus dem Personalad-

ministrationsdienst ab, erfasst das Lichtbild und die Unterschriftsprobe des Mitarbeiters mit Hilfe des Hardware-Token-Dienstes. Nach erfolgreicher Speicherung wird die Bestellung im Self-Service-Plattform-Dienst hinterlegt, der für die Abwicklung der Bestellung auf den Hardware-Token-Dienst zurückgreift. Die notwendigen Dienstausweisdaten werden in einem eDA-Register gespeichert, das durch den Hardware-Token-Dienst ausgeprägt wird. (Anwendungsfall S2.6.2)

3. **System wickelt Auftrag ab.**
   Die zu definierende Stelle / Das zu definierende System nimmt die Bestellung des Dienstausweises entgegen, produziert den elektronischen Dienstausweis und liefert diesen an die entsprechende Dienstausweisstelle aus. (Anwendungsfall S2.6.3)
4. **Dienstausweisstelle personalisiert Dienstausweis und liefert aus oder hinterlegt diesen zur Abholung.**
   Die Dienstausweisstelle nutzt den Hardware-Token-Dienst der Domäne INF, um eine elektronische Personalisierung des ausgelieferten Dienstausweises durchzuführen. Anschließend wird der Dienstausweis an den Mitarbeiter ausgegeben bzw. für ihn zur Abholung hinterlegt. (Anwendungsfall S2.6.4)
5. **System dokumentiert Auftrag.**
   Das System dokumentiert den Auftrag. Die Dokumentation des Auftrages (Informationen zur Auftragsabwicklung) erfolgt im Self-Service-Plattform-Dienst der Domäne INF. Die Dokumentation des Auftrages (Technische Konfiguration) im Service-Lifecycle-Management-Support-Dienst der Domäne INF. Die genutzten Leistungen werden an die Diensteklasse Steuerung und Information der Domäne ERP zur Verrechnung gegenüber der beziehenden Behörde übermittelt. (Anwendungsfall S2.6.5)

2.7 Szenario „Zutrittskontrolle mit Hilfe des elektronischen Dienstausweises“

Das Szenario stellt den Ablauf der Zutrittskontrolle mit Hilfe des elektronischen Dienstausweises dar.

Es wird davon ausgegangen, dass:

- der Mitarbeiter über einen elektronischen Dienstausweis verfügt.
- die entsprechenden Anwendungen: Zutritt zu der Liegenschaft und Zutritt zum Büro (Schließanlage) auf dem elektronischen Dienstausweis des Mitarbeiters installiert und aktiviert sind.

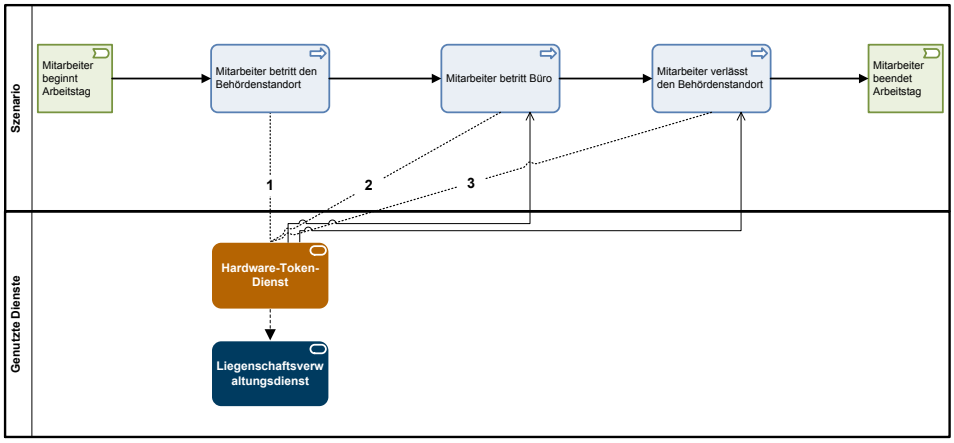

Abbildung 9: Zutrittskontrolle mit Hilfe des Dienstausweises (Szenario S2.7)

Das Szenario besteht aus folgender Sequenz von Anwendungsfällen:

1. **Mitarbeiter betritt den Behördenstandort**
   Der Mitarbeiter nutzt den elektronischen Dienstausweis, um den Zutritt zu der Liegenschaft / dem Behördenstandort zu erlangen. Das Zutrittskontrollsystemprüft die Zutrittsberechtigung auf dem elektronischen Dienstausweis. Nach erfolgreicher Überprüfung wird automatisch über den Statusdienst des Hardware-Token-Dienstes der Sperrstatus des verwendeten elektronischen Dienstausweises geprüft (im Falle der Prüfung des Zutritts zu einer Liegenschaft). Nach wiederholt erfolgreicher Prüfung wird anschließend der Zutritt gewährt. Der Eintritt des Mitarbeiters kann zusätzlich über den Liegenschaftsverwaltungsdienst im entsprechenden Zeiterfassungssystem der ERP Domäne dokumentiert werden. Hinweis: Der elektronische Dienstausweis könnte außerdem als Hardware-Token für die elektronischen Schließanlagen innerhalb einer Liegenschaft bzw. dem Behördenstandort genutzt werden. (Anwendungsfall S2.7.1)
2. **Mitarbeiter betritt Büro**
   Der Mitarbeiter nutzt ebenfalls den elektronischen Dienstausweis, um Zutritt zum Büro zu erhalten. (Anwendungsfall S2.7.2)
3. **Mitarbeiter verlässt den Behördenstandort**
   Für das Verlassen des Geländes wird der elektronische Dienstausweis ebenfalls an dem Zeiterfassungssystem verwendet. Der Mitarbeiter nutzt den Zeitwirtschaftsdienst um das Verlassen des Behördenstandorts zu dokumentieren.. Notwendige Daten vom elektronischen Dienstausweis werden zur Dokumentation an die ERP Personaldienste übertragen. (Anwendungsfall S2.7.3)

2.8 Szenario „Anmelden und Signieren mit elektronischem Dienstausweis“

Das Szenario stellt den Ablauf der Anmeldung am Arbeitsplatz und der Erstellung einer elektronischen Signatur mit Hilfe des elektronischen Dienstausweises dar.

Es wird davon ausgegangen, dass:

- der Mitarbeiter über einen IT-Arbeitsplatz mit Kartelesegerät und einen elektronischen Dienstausweis verfügt.
- die Anmeldung am IT-Arbeitsplatz und die Erstellung einer elektronischen Signatur mit Hilfe des elektronischen Dienstausweises erfolgt.

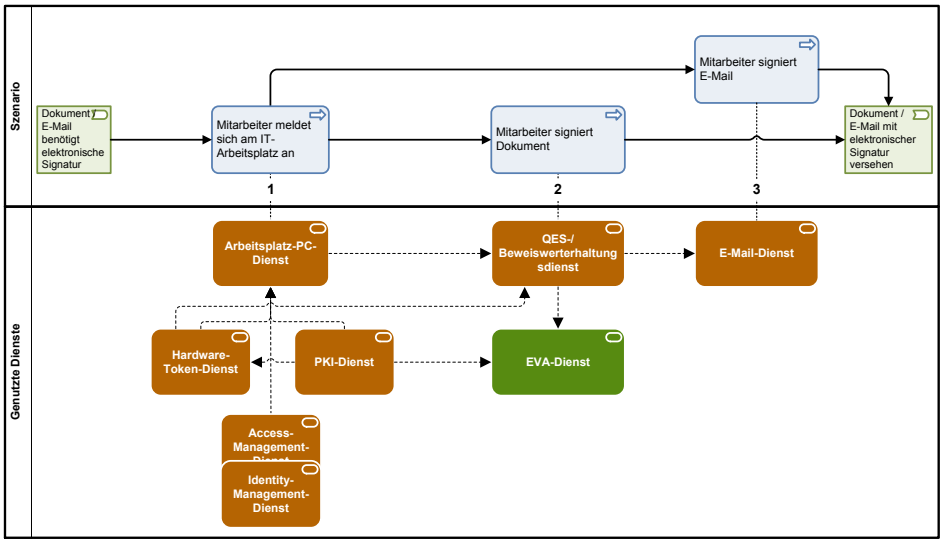

Abbildung 10: Erstellung einer elektronischen Signatur mit Hilfe des Dienstausweises (Szenario S2.8)

Das Szenario besteht aus folgender Sequenz von Anwendungsfällen:

1. **Mitarbeiter meldet sich am IT-Arbeitsplatz an.**
   Der Mitarbeiter verwendet den Dienstausweis als Hardware-Token zur Anmeldung am Arbeitsplatz-PC-Dienst der Domäne INF. Über den PKI-Dienst wird die Gültigkeit des verwendeten Zertifikats auf dem Hardware-Token geprüft. Identity- und Access-Management-Dienste liefern die elektronische Identität des Mitarbeiters und die ihr zugeordneten Rechte und Rollen. (Anwendungsfall S2.8.1)

2. **Mitarbeiter signiert ein Dokument.**
   Der Mitarbeiter versieht ein elektronisches Dokument mit einer elektronischen Signatur, um dieses z.B. einem Dienst aus der Elektronischen Verwaltungsarbeit (EVA) für die Weiterverarbeitung zuzuführen. Dafür wird eine Signaturerstellungskomponente (QES-/Beweiswerterhaltungs-Dienst) verwendet, die der elektronische Dienstausweis ansteuert, um die qualifizierte elektronische Signatur (QES) zu erstellen. Das für das Signieren notwendige Zertifikat ist auf dem Dienstausweis gespeichert. Über den PKI-Dienst prüft der verwendete EVA-Dienst die Gültigkeit des Zertifikats. (Anwendungsfall S2.8.2)

3. **Mitarbeiter signiert eine E-Mail.**
   Der Mitarbeiter versieht eine E-Mail mit einer qualifizierten elektronischen Signatur (QES). Dafür wird analog dem Anwendungsfall S2.2.5.2, eine Signaturerstellungskomponente (QES-/Beweiswerterhaltungs-Dienst) verwendet. Der Arbeitsplatz-PC-Dienst greift auf den PKI-Dienst zu, um das Schlüsselpaar zu prüfen. Nach erfolgreicher Prüfung, wird der E-Mail-Dienst genutzt, um die Nachricht zu versenden. (Anwendungsfall S2.8.3)

3 Domänenarchitektur der Domäne INF

Eine hochverfügbare, vertrauenswürdige und sichere Infrastruktur setzt zueinander kompatible Funktionalitäten für Betrieb und Zugriffssteuerung voraus. Um Sicherheit und Wirtschaftlichkeit der Infrastruktur durchgängig sicherzustellen, sind Verknüpfungen zwischen Diensten auf die notwendigen Schnittstellen zu reduzieren und Redundanzen zu vermeiden. Dazu müssen Abhängigkeiten zwischen den Diensten betrachtet werden.

Eine Abhängigkeit zwischen zwei Diensten besteht, wenn ein Dienst mindestens eine Funktionalität eines anderen Dienstes nutzt. Um die Lesbarkeit des Kapitels zu erhöhen, wurde auf die umfassende Darstellung aller Abhängigkeiten verzichtet. Die Auswahl basiert sowohl auf Erkenntnissen, die durch Diskussionen in der Domäne Infrastruktur, insbesondere zwischen Architekturmanagement und IT-Maßnahmen, gewonnen wurden, als auch auf der Expertise von Architekten bei der Konzeption von IT-Infrastrukturen. Eine umfassende Übersicht über die Abhängigkeiten der Domäne Infrastruktur ist im Anhang 4.4 enthalten. Die Abhängigkeiten sind auf Basis der Diensteklassen dargestellt. Die Zugehörigkeit eines Dienstes zu einer Diensteklasse ist anhand der Dienstelandkarte nachvollziehbar (siehe Abbildung 11).

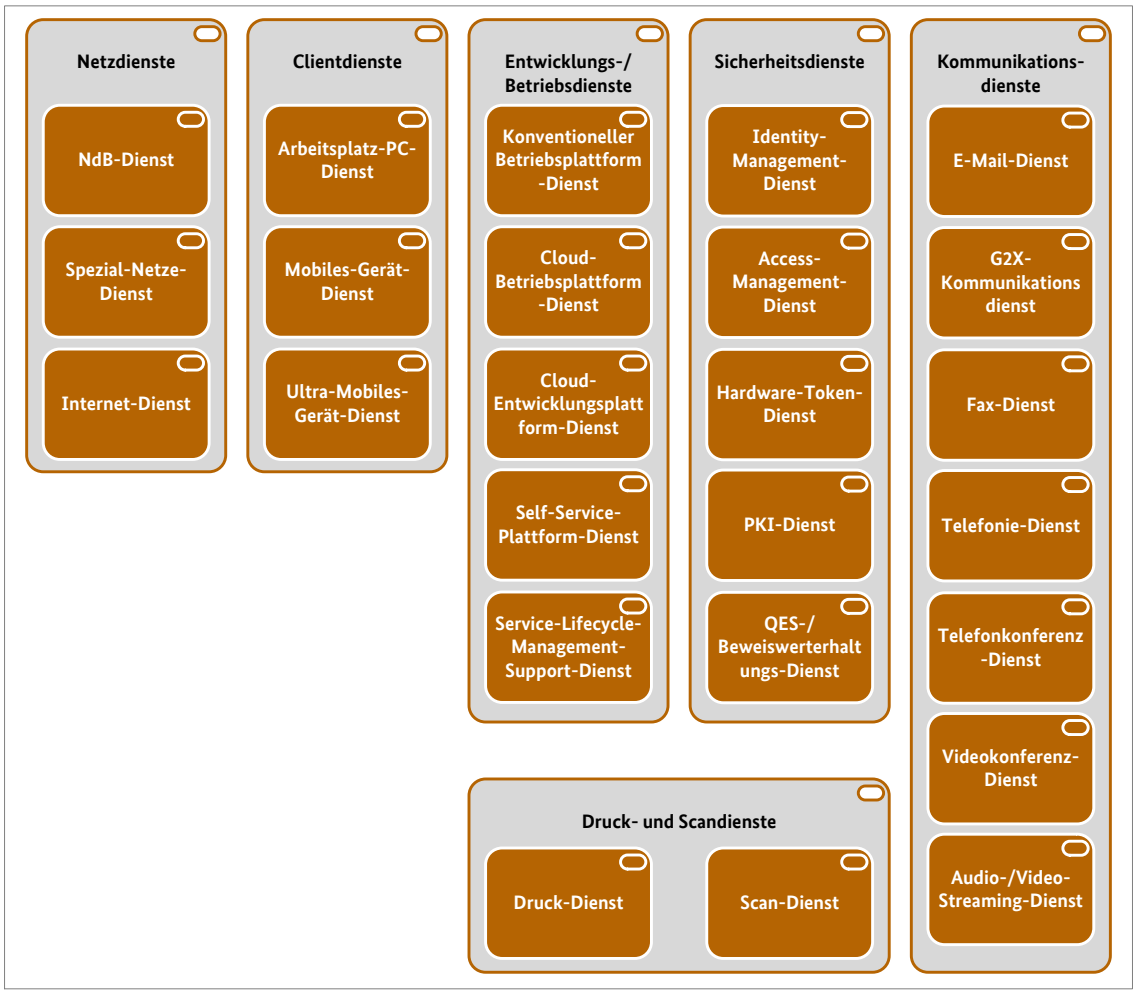

Abbildung 11: Ausschnitt Dienstelandkarte Infrastruktur in Anlehnung an [1.]

3.1 Architekturfeld Entwicklungs- und Betriebsdienste

Die Diensteklasse Entwicklungs- und Betriebsdienste stellt die zentralen Betriebsplattformen bereit, auf der nach erfolgter Konsolidierung sämtliche IT-Lösungen im Wirkbetrieb angeboten werden. Die Zusammenhänge innerhalb dieser Diensteklasse werden in diesem Abschnitt aufgezeigt.

1. Der Konventionelle-Betriebsplattform-Dienst und der Cloud-Betriebsplattform-Dienst liefern Informationen aus dem Betrieb von IT-Lösungen an den Service-Lifecycle-Management-Support-Dienst. Der Cloud-Entwicklungsplattform-Dienst liefert Informationen über neu entwickelte IT-Lösungen an den Service-Lifecycle-Management-Support-Dienst.
2. Aufbauend auf der Infrastruktur des Cloud-Betriebsplattform-Dienstes wird der Cloud-Entwicklungsplattform-Dienst mit seinen Unterstützungsfunktionen für die Entwicklung neuer IT-Lösungen implementiert.
3. Der Service-Lifecycle-Management-Support-Dienst stellt sowohl dem Konventionellen- als auch dem Cloud-Betriebsplattform-Dienst die Funktionalität für die Dokumentation der dort implementierten IT-Lösungen, der genutzten Lizenzen und der angebotenen Katalogelemente zur Verfügung.
4. Der Service-Lifecycle-Management-Support-Dienst stellt die Daten aus dem Produktkatalog dem Self-Service-Plattform-Dienst zur Anzeige von bestellbaren Katalogelementen zur Verfügung.
5. Der Self-Serviceplattform-Dienst initiiert die Provisionierung und dokumentiert deren Status im Konventionellen-Betriebsplattform-Dienst, Cloud-Betriebsplattform-Dienst und/oder Cloud-Entwicklungsplattform-Dienst.

Abbildung 12: Architekturfeld Entwicklungs- und Betriebsdienste

3.2 Architekturfeld Sicherheitsdienste

Die Erreichung einer hohen Informations- und IT-Sicherheit ist ein zentrales Ziel der Dienstekonsolidierung. Die Diensteklasse Sicherheitsdienste bietet dafür verschiedene Dienste an. Der Zusammenhang dieser Dienste wird nachfolgend beschrieben und in Abbildung 13 dargestellt.

Der Identity-Management-Dienst stellt (1) dem Access-Management-Dienst die Infrastruktur der Verzeichnisdienste für die Implementierung von Rechten und Rollen sowie von Schnittstellen in die Verzeichnisdienste zur Integration von Identitäten, Rechten und Rollen in IT-Lösungen zur Verfügung. Der PKI-Dienst nutzt ebenfalls die (2) vom Identity-Management-Dienst bereitgestellte Infrastruktur der Verzeichnisdienste für die Verknüpfung von personenbezogenen Zertifikaten mit ihren elektronischen Identitäten. Der PKI-Dienst stellt die Infrastruktur für die sichere Verwaltung von elektronischen Zertifikaten dem Hardware-Token-Dienst und (3) dem QES-Beweiswerterhaltungsdienst zur Verfügung. Der PKI-Dienst stellt (4) dem QES-Beweiserhaltungsdienst die Zertifikate zum Erstellen einer fortgeschrittenen elektronischen Signatur, nach dem deutschen Signaturgesetz, zur Verfügung. Zusätzlich wird der PKI-Dienst zur Erzeugung von elektronischen Zertifikaten verwendet, die auf (5) Hardware-Token gespeichert und z.B. für die sichere Anmeldung am IT-Arbeitsplatz oder zur Signierung von elektronischen Dokumenten verwendet werden.

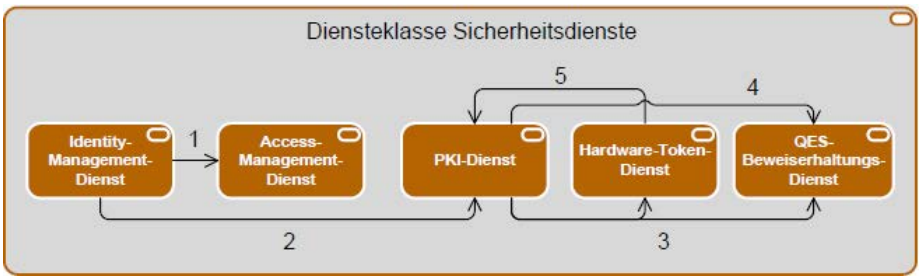

Abbildung 13: Architekturfeld Sicherheitsdienste

3.3 Architekturfeld Kern-Infrastrukturdienste

Die Diensteklassen bauen hierarchisch aufeinander auf: Die unterste Schicht bildet die Diensteklasse der Netzdienste. Darauf baut die Diensteklasse der Entwicklungs- und Betriebsdienste auf. Innerhalb des Konventionellen-Betriebsplattform-Dienstes werden sämtliche Systeme betrieben, die nicht dem Cloud-Betriebsplattform-Dienst zugeordnet sind. Diese umfassen auch die für den Betrieb der Netzdienste notwendigen Systeme. Darüber liegt die Diensteklasse der Sicherheitsdienste. Diese drei Diensteklassen bilden den Kern der Infrastrukturdienste, die allen anderen Diensten ihre Funktionalität zur Verfügung stellen. Die Details der Zusammenhänge und Abhängigkeiten zwischen diesen Infrastrukturdiensten werden nachfolgend entsprechend der Hierarchie schichtenweise beschrieben und sind in Abbildung 14 grafisch dargestellt. Die jeweiligen Abhängigkeiten werden in der Abbildung über Pfeile angezeigt. Der zugehörige Pfeil ist durch eine Nummer gekennzeichnet, die wiederrum auf die Beschreibung in den folgenden Abschnitten referenziert.

Diensteklasse Netzdienste (Schicht 1):
Die Diensteklasse Netzdienste realisiert die Vernetzung von verteilten Rechenzentren und deren Anbindung an die Behördenstandorte sowie deren Anbindung untereinander. Des Weiteren wird über die Netzdienste die Anbindung von mobilen und Heim-Arbeitsplätzen sowie die Anbindung zwischen dem NdB-, Spezialnetze- und Internet-Dienst implementiert. Darüber wird (1) der direkte Zugriff auf die Betriebsplattformen (Diensteklasse Entwicklungs- und Betriebsdienste) ermöglicht. Die Diensteklasse Netzdienste stellt darüber hinaus (2) die Netzinfrastruktur für das behördenübergreifende Identitäts- und Zugriffs-

management zur Verfügung, die über die Diensteklasse Sicherheitsdienste abgebildet werden.

Diensteklasse Entwicklungs- und Betriebsdienste (Schicht 2):
Über diese Diensteklasse wird sämtliche Betriebsinfrastruktur für alle anderen BQI-Dienste bereitgestellt. Die netznahen Dienste aus der Diensteklasse Netzdienste greifen auf (3) die durch den Konventionellen Betriebsplattform-Dienstes bereitgestellte Infrastruktur zur Abbildung von grundlegender Netz-Funktionalitäten zurück, wie z.B. zur Namensauflösung via DNS oder zur Absicherung und Prüfung der Kommunikation in andere Netzsegmente über Firewalls oder IDS/IPS. Die Diensteklasse Netzdienste bedient sich zusätzlich der Funktionalität des Service-Lifecycle-Management-Support-Dienstes zur Dokumentation der Netz-Infrastruktur und der Integration des Netz-Betriebs. Die Diensteklasse Entwicklungs- und Betriebsdienste stellt die Betriebsplattform für (4) die Diensteklasse Sicherheitsdienste bereit. Des Weiteren wird der Service-Lifecycle-Management-Support-Dienst auch für die Sicherheitsdienste verwendet.

Diensteklasse Sicherheitsdienste (Schicht 3):
Dienste der Diensteklasse Sicherheitsdienste werden bei (5) der Diensteklasse Entwicklungs- und Betriebsdienste für die Anmeldung und die Zuweisung von Rechten und Rollen im Self-Service-Plattform-Dienst sowie für den Zugang der Nutzer aus den Behörden auf die Betriebsplattformen verwendet (Identity- und Access-Management-Dienste). Der PKI-Dienst umfasst Beantragung, Ausstellung, Verwaltung und Prüfung digitaler Zertifikate. Die notwendige Schlüsselverwaltung kann mithilfe des PKI-Dienstes realisiert werden. Die Dienste Identity- und Access-Management-Dienste sowie den PKI- und Hardware-Token-Dienst der Diensteklasse Sicherheitsdienste dienen der Absicherung von Einwahlverfahren für die bereits beschriebenen mobilen und Heim-Arbeitsplätze und unterstützen damit (6) die Diensteklasse Netzdienste.

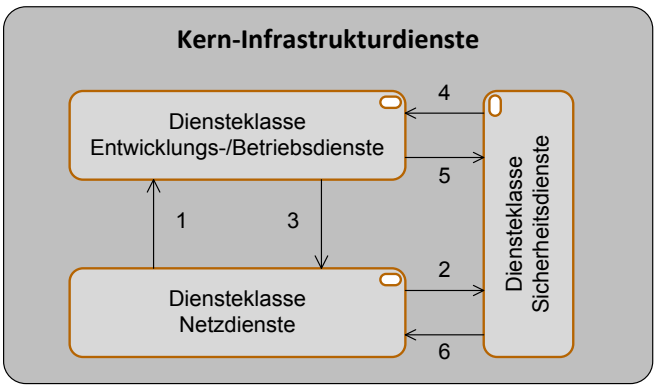

Abbildung 14: Infrastrukturdienste und ihre Abhängigkeiten

3.4 Gesamtarchitektur der Domäne INF

In den vorausgehenden Abschnitten wurde die aggregierte Darstellung der Infrastrukturdienste entwickelt. Diese werden für die folgenden Schichten als Block bei der Interaktion mit den restlichen Basis-, Querschnitts- und Fachdiensten betrachtet. Der Gesamtzusammenhang ist in Abbildung 15 dargestellt.

Die Infrastrukturdienste stellen den Diensteklassen (1) Clientdienste, (2) Kommunikationsdienste und (3) Scan- und Druckdiensten sowie (4) den anderen Domänen und Fachdiensten grundlegende Netz-, Betriebs- und Sicherheitsfunktionen zur Verfügung. Durch die Anbindungen der Diensteklasse Clientdienste und der dazugehörigen Client-Betriebsinfrastruktur in die Rechenzentren der IT-Dienstleister an die Behördenstandorte wird die Absicherung der Daten, des Datenverkehrs und der Zugriffe ermöglicht.

Diensteklasse Kommunikationsdienste:
Die Diensteklasse Kommunikationsdienste stellt (5) den Domänen und Fachdiensten die notwendige Infrastruktur zur direkten Einbindung von Kommunikationslösungen in IT-Lösungen der Domänen und in Fachdienste der Behörden bereit. So kann z.B. eine IT-Lösung dort direkt die Funktionen des G2X-Kommunikations-Dienstes für die sichere Kommunikation einbinden. (6) Die Diensteklasse Scan- und Druckdienste nutzt die durch die Kommunikationsdienste bereitgestellte Infrastruktur für die Implementierung integrierter Lösungen, z.B. für eine Scan-To-Fax- oder Scan-To-E-Mail Lösung. (7) Die Diensteklasse Clientdienste nutzt die gesamte Breite der bereitgestellten Funktionen der Kommunikationsdienste für die Bereitstellung von Kommunikationslösungen für die Mitarbeiter der Behörden. Angefangen von Telefonfunktionen über Videokonferenzlösungen bis hin zu Nachrichtenübermittlung über elektronische Postfach-Lösungen. (8) Wie bereits oben beschrieben, nutzen die Kommunikationsdienste die Scan- und Druckdienste für die Ein- und Ausgabe von Dokumenten direkt aus in die Kommunikationsdienste integrierten Lösungen.

Diensteklasse Scan- und Druckdienste:
Die Diensteklasse Scan- und Druckdienste stellt (9) den Diensten anderer Domänen und Fachdiensten sowie (10) den Clientdiensten die zentrale und dezentrale Infrastruktur sowohl für die Digitalisierung von Papierdokumenten, als auch zur Ausgabe von elektronischen Dokumenten auf Papier zur Verfügung.

Dienste anderer Domänen und Fachdienste:
Die Dienste anderer Domänen und Fachdienste stellen (11) ihre Funktionalität für die Verwendung durch den Mitarbeiter an dem IT-Arbeitsplatz der Diensteklasse Clientdienste zur Verfügung. Analog kann auch (12) die Diensteklasse Kommunikationsdienste die IT-Lösungen der Domänen und Fachbereiche für die Integration in Kommunikationslösungen verwenden. So kann z.B. ein Fachdienst als Benutzeroberfläche für den Elektronischen Rechtsverkehr, der über den G2X-Kommunikations-Dienst realisiert wird, dienen. Die Funktionen einzelner Dienste anderer Domänen und Fachdienste können bei (13) der Diensteklasse Scan- und Druckdienste als Endpunkte für Scan- und Druck-Lösungen integriert werden.

Diensteklasse Clientdienste:
Die Diensteklasse Clientdienste stellt (14) den Diensten anderer Domänen und Fachdienste die Infrastruktur zu Verfügung, die zur Speicherung von Daten oder Bearbeitung von Dokumenten benötigt wird. Darüber ist auch Zugriff auf (15) Scan- und Druckdienste möglich, was die Ablage von digitalisierten Dokumenten über Scan-Lösungen oder Produktion von Ausgabedokumenten aus anderen IT-Lösungen ermöglicht.

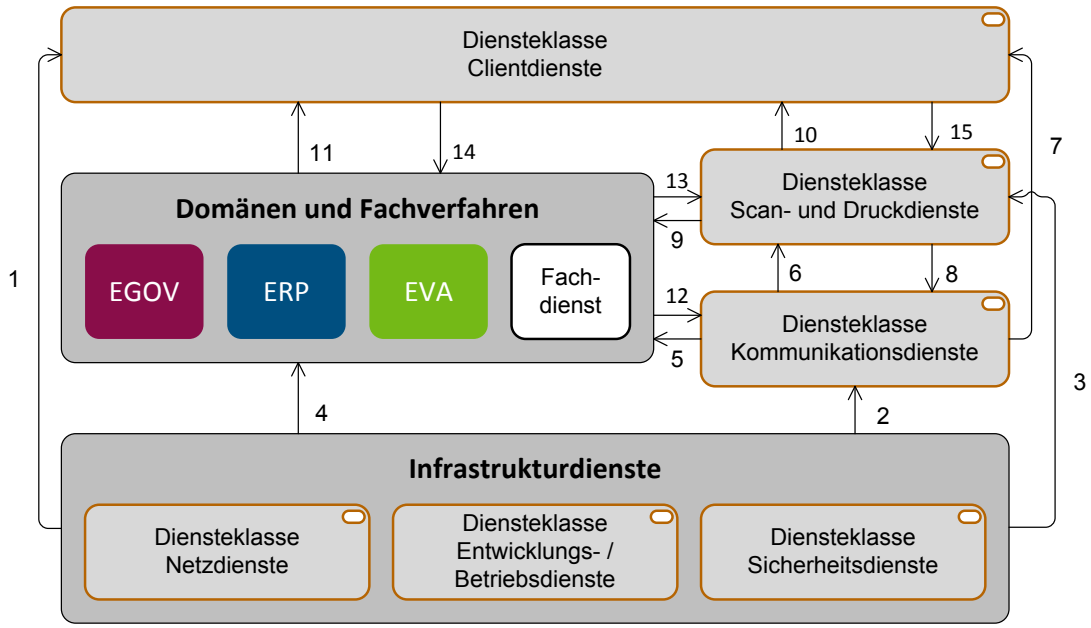

Abbildung 15: Domänenarchitektur INF

4 Anhang Architekturelemente

Der Anhang detailliert die im Hauptteil beschriebenen Architekturelemente

- Anwendungsfälle
- Rollen
- Informationsobjekte
- Diensteabhängigkeiten

4.1 Anwendungsfälle

In diesem Abschnitt werden die Anwendungsfälle der Domäne Infrastruktur detailliert aufgelistet. Die Darstellung gibt einen spezifischen Einblick in die Beziehung zum Dienst und die Funktionalitäten für die Wiederverwendung in Geschäftsprozessen.

S2.1.1: Fachadministrator weist Mitarbeiter Rollen zu	
Beschreibung	Mit dem Durchlaufen des ERP Szenarios werden Stammdaten für den neuen Mitarbeiter erzeugt und die davon notwendigen Daten für den Aufbau einer elektronischen Identität zum zentralen Identity-Management-Dienst übertragen. Die Übertragung kann durch einen Trigger im Personalmanagement-Dienst angestoßen werden, oder es findet ein täglicher Abgleich zwischen den beiden Systemen statt. Nach der Initialisierung der elektronischen Identität weist ein Fachadministrator dem Mitarbeiter die notwendigen Rechte und Rollen für die ihm zugeordneten IT-Lösungen zu. Dazu ergänzt er die vom Personalverwaltungssystem an das Identity-Management gelieferten Daten um weitere Details und um die Rechte und Rollen, die der neue Mitarbeiter für seine Arbeit in der Behörde benötigt. Diese Informationen werden wiederum an weitere IT-Lösungen durchgereicht und ggf. dort um Details wie z.B. zugewiesenen Telefonnummern, E-Mail-Adressen etc. ergänzt. Diese Daten werden wieder an den zentralen Identity- und Access-Management-Dienst zurückgeliefert und stehen damit anderen IT-Lösungen zur Nutzung zur Verfügung. Zum Beispiel werden sie für die zentrale Nutzung im Verzeichnisdienst zur Suche von Mitarbeitern und zur Anzeige der Kontaktdaten verwendet. Aus dem Identity-Management System werden die dem Mitarbeiter zugeordneten Rollen und Rechte zur Vorbereitung des Zugriffs auf die IT-Lösungen an selbige weitergereicht, damit der Benutzer bei seinem ersten Zugriff dort authentifiziert und autorisiert werden kann. Dies kann z.B. durch das Hinzufügen der Identität zu einer für die Anwendung spezifischen Gruppe erfolgen. Für Anwendungen, die über die zentral administrierten Rollen spezifische, anwendungsbezogene Rollen verwenden, muss der zuständige Fachadministrator diese in den IT-Anwendungen einrichten.

Nutzbare Funktionalität(en)	Administration von Anwendungen, Administration von Zugriffsrechten
Nutzbarer Dienst(e)	Identity-Management, Access Management, Arbeitsplatz-PC, Mobiles-Gerät, Ultramobiles-Gerät, Telefonie, Telefonkonferenz, Videokonferenz, E-Mail, Scan und Druck, G2X-Kommunikation, Dienste der Domänen und Fachdienste
Nutzende Rolle(n)	Fachadministrator
Genutzte Information	Anmeldedaten, Rollen und Rechte

Tabelle 1: Anwendungsfall Fachadministrator weist Mitarbeiter Rollen zu

S2.1.2: Fachadministrator bestellt Hardware-Token	
Beschreibung	Ein Fachadministrator bestellt für den Mitarbeiter einen Hardware-Token, z.B. für die Authentifizierung an Endgeräten. Über den Hardware-Token-Dienst wird die Bereitstellung des Hardware-Tokens und dessen Initialisierung/Personalisierung durchgeführt. Über die Public Key Infrastructure (PKI) werden die benötigten Zertifikate für den Hardware-Token bereitgestellt (PKI-Dienst). Personenbezogene Zertifikate werden über den Identity-Management-Dienst mit der Identität des Mitarbeiters verknüpft..
Nutzbare Funktionalität(en)	Generierung von Zertifikaten, Zuweisung von Zertifikaten und Identitätsdaten
Nutzbarer Dienst(e)	Hardware-Token, PKI, Identity-Management
Nutzende Rolle(n)	Fachadministrator
Genutzte Information	Zertifikatsdaten, Identitätsdaten

Tabelle 2: Anwendungsfall Fachadministrator bestellt Hardware-Token Hardware

S2.1.3: Fachadministrator bestellt Arbeitsplatz-Hardware	
Beschreibung	Ein Fachadministrator bestellt für den neuen Mitarbeiter die benötigte Hardware für seinen IT-Arbeitsplatz oder weist ihm ggf. die notwendige Hardware aus einem vorhandenen Hardware-Pool zu oder löst die Bestellung der Hardware aus. Dazu gehören u.a. die Computer-Hardware, ggf. Tablett, Mobil- und Festnetz-telefon sowie Drucker und Scanner. Die Abwicklung der Bestel-lung und Lieferung von neu zu beschaffender Hardware erfolgt über die Diensteklasse Logistik aus der ERP Domäne. Die geliefer-te Hardware wird je nach Typ in dem entsprechenden Dienst der Diensteklasse Client, Scan und Druck-Dienst provisioniert. Die Details wie Seriennummern, zugehörige Wartungsverträge und Softwarelizenzen werden an den Service-Lifecycle-Management-Support-Dienst zur weiteren Dokumentation und Verwaltung zugeliefert.
Nutzbare Funktionalität(en)	Bestellwesen, Provisionierung von IT-Equipment
Nutzbarer Dienst(e)	Dienste aus der ERP Logistik-Diensteklasse, Service-Lifecycle-Management-Support, Arbeitsplatz-PC, Mobiles-Gerät, Ultramo-biles-Gerät
Nutzende Rolle(n)	Fachadministrator
Genutzte Information	Konfigurationsdaten, Abrechnungsdaten, Bestelldaten

Tabelle 3: Anwendungsfall Fachadministrator bestellt Arbeitsplatz-Hardware

S2.1.4: Arbeitsplatz wird bereitgestellt	
Beschreibung	Dem Mitarbeiter wird sein neuer IT-Arbeitsplatz mit den definier-ten Leistungen zur Verfügung gestellt. Die genutzten Leistungen entsprechend den bestellten Produktkatalog-Elementen (Hard-ware, Software) werden über den Service-Lifecycle-Management-Support-Dienst an die Diensteklasse der ERP Steuerungs- und Informationsdienste zur Verrechnung gegenüber der beziehenden Behörde übermittelt.
Nutzbare Funktionalität(en)	Nutzung IT-Arbeitsplatz, Nutzung von Buchungs- und Abrech-nungsdaten
Nutzbarer Dienst(e)	Diensteklasse der ERP Logistik-Dienste, Service-Lifecycle-Management-Support, Diensteklasse der ERP Steuerungs- und Informationsdienste
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Produktkatalog-Daten, Abrechnungsdaten

Tabelle 4: Anwendungsfall Arbeitsplatz wird bereitgestellt

S2.2.1: Mitarbeiter meldet sich am Self-Service-Portal an	
Beschreibung	Der Mitarbeiter möchte seinen IT-Arbeitsplatz um weitere optionale Komponenten aus dem Produktkatalog auf dem Self-Service-Portal erweitern. Der Mitarbeiter meldet sich über seinen IT-Arbeitsplatz (Diensteklasse Clientdienste) am Self-Service-Portal an, das zum zentralen Self-Service-Plattform-Dienst gehört, und navigiert in den Bereich, wo der Produktkatalog für den IT-Arbeitsplatz zur Auswahl steht. Die Identity- und Access-Management-Dienste generieren die für den Zugriff auf das Self-Service-Portal notwendigen Anmeldedaten für das Single-Sign-On am Portal.
Nutzbare Funktionalität(en)	Nutzung des Self-Service-Portals
Nutzbarer Dienst(e)	Arbeitsplatz-PC, Mobiles-Gerät, Ultra-Mobiles-Gerät, PKI, NdB, Spezialnetze, Identity-Management, Access-Management, Hardware-Token, Self-Service-Plattform
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Anmeldedaten, Konfigurationsdaten, Zertifikatsdaten

Tabelle 5: Anwendungsfall Mitarbeiter meldet sich am Self-Service-Portal an

S2.2.2: Mitarbeiter bestellt Element aus Produktkatalog	
Beschreibung	Im Self-Service-Portal navigiert der Mitarbeiter in den Bereich für den IT-Arbeitsplatz und wählt die gewünschten Elemente aus dem Produktkatalog zur Ergänzung der Funktionalität aus. Der zur Verfügung stehende Produktkatalog wird über den Service-Lifecycle-Management-Support-Dienst am Self-Service-Portal bereitgestellt. Die im Produktkatalog zur Auswahl stehenden Angebote werden über die in den Identity- und Access-Management-Diensten hinterlegten Rollen und Rechte des Mitarbeiters eingeschränkt. Mit der Bestätigung der Auswahl wird der Bestell-Workflow ausgelöst.
Nutzbare Funktionalität(en)	Self-Service-Portal Es wird das für jeden Mitarbeiter zugängliche, zur Diensteklasse Client zugehörige, Self-Service-Portal genutzt
Nutzbarer Dienst(e)	Self-Service-Plattform, Service-Lifecycle-Management-Support
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Konfigurationsdaten

Tabelle 6: Anwendungsfall Mitarbeiter bestellt Element aus Produktkatalog

S2.2.3: Produkt wird provisioniert	
Beschreibung	Nach Abschluss des gegebenenfalls notwendigen Genehmigungsprozesses wird der Bestellprozess mit der Provisionierung der Komponenten abgeschlossen. Bei den Komponenten kann es sich um Hardware oder Software, die auf dem IT-Arbeitsplatz installiert und konfiguriert werden muss, handeln, andernfalls ist die Zuteilung der Zugriffsrechte in der zugehörigen IT-Lösung ausreichend. Die gebuchten Katalogelemente werden im Service-Lifecycle-Management-Support-Dienst dokumentiert, z.B. die Nutzung von zugehörigen Lizenzen. Innerhalb des Provisionierungsprozesses erfolgt die für die Nutzung notwendige Zuweisung von Rollen und Rechten in den beteiligten IT-Lösungen für die gebuchten Komponenten. Dies erfolgt über die Identity- und Access-Management-Dienste. Die gebuchten Katalogelemente werden über den Service-Lifecycle-Management-Dienst an die ERP Steuerungs- und Informationsdienste zur Abrechnung gegenüber der Behörde geliefert. Provisionierung nutzt automatisierte Mechanismen der Diensteklasse Clientdienste und die Mechanismen der Identity- und Access-Management-Dienste. Anschließend stehen sie dem Mitarbeiter zur Nutzung zur Verfügung.
Nutzbare Funktionalität(en)	Automatisierte Provisionierung
Nutzbarer Dienst(e)	Arbeitsplatz-PC, Mobiles-Gerät, Ultra-Mobiles-Gerät, Identity- und Access-Management, Service-Lifecycle-Management-Support, Dienste aus den Domänen und Fachdienste
Nutzende Rolle(n)	System
Genutzte Information	Konfigurationsdaten, Rollen und Rechte

Tabelle 7: Anwendungsfall Produkt wird provisioniert

S2.3.1: Entwickler konfiguriert Umgebung im Self-Service-Portal	
Beschreibung	Der Anwendungsentwickler konfiguriert über die Self-Service-Plattform seine benötigte Umgebung, in der er die Anwendungsentwicklung betreiben möchte. Die Umgebung wird dabei aus Produktkatalog-Elementen zusammengestellt, die im Service-Lifecycle-Management-Support-Dienst hinterlegt sind. Darauf greif die Self-Service-Plattform zur Anzeige des Produktkatalogs zu. Zur Auswahl stehen hier Laufzeitumgebungen als PaaS oder SaaS-Angebote und diverse Cloud-Services wie DaaS, DBaaS, CaaS bis hin zu IaaS. Die Self-Service-Plattform triggert nach dem Durchlaufen des Bestell- und Genehmigungsprozesses anschließend die in der Cloud-Entwicklungsplattform existierenden Provisionierungsmechanismen, um die Grundkonfiguration der notwendigen Umgebung auf der Cloud-Betriebsplattform zu provisionieren. Die verwendeten Produktkatalogelemente werden im Service-Lifecycle-Management-Support-Dienst dokumentiert. Dieser liefert auch die Verbrauchswerte aus der Cloud-Betriebsplattform für die Verrechnung an die Diensteklasse der ERP Steuerungs- und Informationsdienste, über die die bezogenen Leistungen an die beauftragende Behörde verrechnet werden.
Nutzbare Funktionalität(en)	Bestell- und Abrechnungsportal, Provisionierungsmechanismen
Nutzbarer Dienst(e)	Self-Service-Plattform, Service-Lifecycle-Management-Support, Diensteklasse der ERP Steuerungs- und Informationsdienste, Cloud-Betriebsplattform, Cloud-Entwicklungsplattform
Nutzende Rolle(n)	Entwickler / Fachadministrator
Genutzte Information	Produktkatalog-Daten, Konfigurationsdaten, Abrechnungsdaten

Tabelle 8: Anwendungsfall Entwickler konfiguriert Umgebung im Self-Service-Portal

S2.3.2: Entwickler erstellt eine neue IT-Lösung	
Beschreibung	Der Entwickler entwickelt die eigentliche neue Anwendung auf der Basis der bereitgestellten Umgebung auf der Cloud-Plattform. Während der Entwicklung greift er auf die in der Cloud-Entwicklungsplattform vorhandenen Funktionen für die Quellcodeverwaltung, für das Build- und Testmanagement, sowie auf Issue-Tracker und andere Tools zur Unterstützung der Entwicklungszyklen zu. Falls nötig stehen ihm virtualisierte Entwicklungsumgebungen mit der benötigten Ausstattung zur Verfügung. Die für die Anwendungsnutzung erforderlichen initiale Rechte und Rollen werden an das Identity- und Access-Management für die spätere Verwendung im Provisionierungsprozess weitergegeben. Der Entwickler oder mitarbeitende Fachadministrator nutzt die im Cloud-Entwicklungsplattform-Dienst bereitgestellten Tools und Mechanismen, um die Provisionierung der neuen Anwendung zu automatisieren und z.B. zur Umsetzung von agilen CI/CD Konzepten.
Nutzbare Funktionalität(en)	Verwendung von Tools zur Unterstützung des Entwicklungsprozesses, Provisionierungsmechanismen
Nutzbarer Dienst(e)	Cloud-Entwicklungs-Plattform, Cloud-Betriebsplattform, Identity-Management, Access-Management
Nutzende Rolle(n)	Entwickler, Fachadministrator
Genutzte Information	Produktkatalog-Daten, Konfigurationsdaten, Rollen und Rechte

Tabelle 9: Anwendungsfall Entwickler erstellt eine neue IT-Lösung

S2.3.3: Entwickler nimmt neue IT-Lösung in Produktkatalog auf	
Beschreibung	Der Entwickler, oder ein Administrator im Auftrag des Entwicklers, nimmt die neue, fertige Lösung in den Produktkatalog auf, damit sie dort über das Self-Service-Portal durch die Behörden gebucht werden kann. Für das oder die neuen Produktkatalog-Elemente sind dabei neben der Referenz auf die zugehörigen Provisionierungsmechanismen auch die Kostenblöcke (wie z.B. Lizenzkosten) für die Elemente zu hinterlegen, damit eine automatisierte Abrechnung erfolgen kann.
Nutzbare Funktionalität(en)	Produktkatalog Der Produktkatalog enthält alle Produkte, die über das Self-Service-Portal als eigenständige Entitäten gebucht werden können. Für diese sind auch entsprechende Kosten hinterlegt, sodass sie als Leistung abgerechnet werden können.
Nutzbarer Dienst(e)	Self-Service-Plattform, Service-Lifecycle-Management-Support, Cloud-Entwicklungsplattform Die Self-Service-Plattform stellt das Bestellportal für IT-Produkte zur Verfügung, der Produktkatalog wird über den Service-Lifecycle-Management-Support-Dienst beigesteuert. Die Katalogelemente enthalten die notwendigen Referenzen auf die Provisionierungsabläufe im Cloud-Entwicklungsplattform-Dienst
Nutzende Rolle(n)	Entwickler, Fachadministrator
Genutzte Information	Produktkatalog-Daten Konfigurationsdaten, Abrechnungsdaten

Tabelle 10: Anwendungsfall Entwickler nimmt neue IT-Lösung in Produktkatalog auf

S2.3.4: Behörde bucht IT-Lösung	
Beschreibung	Ein Fachadministrator der Behörde bucht über das Self-Service-Portal die neue Anwendung, d.h. z.B. eine Instanz der IT-Lösung für die Behörde. Über die Tools der Cloud-Entwicklungsplattform wird der Provisionierungsprozess gestartet und die neue Anwendungsumgebung auf der Cloud-Betriebsplattform bereitgestellt. Die verwendeten Cloud-Leistungen werden im Service-Lifecycle-Management-Support dokumentiert und die benutzten Cloud-Ressourcen zur Verrechnung an die ERP Steuerungs- und Informationsdienste weitergegeben. Die im Entwicklungsprozess definierten Rollen und Rechte werden im Zuge des Provisionsierungsverfahrens auf die IT-Lösung angewandt. Der Fachadministrator in der Behörde ordnet den Anwendergruppen die benötigten Rechte und Rollen zu, die Zuweisung erfolgt über den Identity- und Access-Management-Dienst. Damit steht die IT-Lösung steht Anwendern zur Verfügung, sobald sie das Angebot zum IT-Arbeitsplatz hinzugebucht haben.
Nutzbare Funktionalität(en)	Nutzung Self-Service-Portal, Produktkatalog, Rechte- und Rollen-Vergabe, Provisionierungsmechanismen und automatisiertes Abrechnungsverfahren

Nutzbarer Dienst(e)	Self-Service-Plattform, Cloud-Entwicklungsplattform, Cloud-Betriebsplattform, Service-Lifecycle-Management-Support, Identity- und Access-Management, Diensteklasse der ERP Steuerungs- und Informationsdienste
Nutzende Rolle(n)	Fachadministrator
Genutzte Information	Produktkatalog-Daten, Konfigurationsdaten, Rollen und Rechte, Abrechnungsdaten

Tabelle 11: Anwendungsfall Behörde bucht IT-Lösung

S2.4.1: HR Mitarbeiter legt Stammdaten an und weist Rollenprofil zu	
Beschreibung	Der HR Mitarbeiter greift auf den Personaladministrationsdienst der Domäne ERP zu. Anschließend legt der HR Mitarbeiter die Stammdaten des neuen Mitarbeiters an und weist ein vordefiniertes Rollenprofil zu. Über die Identity- und Access-Management-Dienste der Domäne INF werden die für den Zugriff notwendigen Anmeldedaten für das Single-Sign-On am Portal generiert.
Nutzbare Funktionalität(en)	Management von Personalstammdaten und Rollenprofilen
Nutzbarer Dienst(e)	Personaladministrationsdienst, Identity- und Access-Management-Dienst
Nutzende Rolle(n)	HR Mitarbeiter
Genutzte Information	Mitarbeiterstammdaten, Rollenprofilinformationen

Tabelle 12: Anwendungsfall HR Mitarbeiter legt Stammdaten an und weist Rollenprofil zu

S2.4.2: System erzeugt elektronische Identität	
Beschreibung	In der Personalverwaltung wird nach erfolgreicher Speicherung der Informationen automatisch das Anlegen einer elektronischen Identität des neuen Mitarbeiters ini-tiiert. Alle notwendigen Informationen zum Anlegen dieser Identität werden vom Personaladministrationsdienst der Domäne ERP zum Identity- / und Access- Management-Dienst der Domäne INF transferiert. Dem neuen Mitarbeiter wird im IAM eine globale Identifikationsnummer (GID) zugewiesen.
Nutzbare Funktionalität(en)	Anlegen einer elektronischen Identität im IAM
Nutzbarer Dienst(e)	Personaladministrationsdienst, Identity- und Access-Management-Dienst
Nutzende Rolle(n)	System
Genutzte Information	Mitarbeiterstammdaten, Rollenprofilinformationen, Identifikationsnummer

Tabelle 13: Anwendungsfall System erzeugt elektronische Identität

S2.4.3: System erstellt Auftrag	
Beschreibung	In der Personalverwaltung wird nach erfolgreicher Speicherung der Informationen ein Vorgang im Self-Service-Plattform-Dienst ausgelöst, der wiederum einen Auf-trag zur Bereitstellung der IT-Arbeitsplatzausstattung auslöst. Der Auftrag enthält die bereit zu stellende IT-Arbeitsplatzausstattung, die aus dem Rollenprofil über-nommen wird.
Nutzbare Funktionalität(en)	Automatische Erstellung eines Provisionierungsauftrag
Nutzbarer Dienst(e)	Personaladministrationsdienst, Self-Service-Plattform-Dienst, Identity- und Access-Management-Dienst
Nutzende Rolle(n)	System
Genutzte Information	Provisionierungsinformationen

Tabelle 14: Anwendungsfall System erstellt Auftrag

S2.4.4: System wickelt Auftrag ab	
Beschreibung	Zur Provisionierung nutzt der Self-Service-Plattform-Dienst der Domäne INF die DK Clientdienste, DK Druck- und Scandienste, DK Kommunikationsdienste sowie den Hardware-Token-Dienst aus der DK IT-Sicherheitsdienste aus der Domäne INF. Über die Public Key Infrastructure werden die benötigten Zertifikate für den Hardware-Token bereitgestellt (PKI-Dienst). Personenbezo-gene Zertifikate werden über den Identity-Management-Dienst der Domäne INF mit der Identität des Mitarbeiters verknüpft.
Nutzbare Funktionalität(en)	Automatische Provisionierung über das SSP
Nutzbarer Dienst(e)	Self-Service-Plattform-Dienst, DK Druck- und Scandienste, DK Kommunikationsdienste, Hardware-Token-Dienst, PKI-Dienst, Identity-Management-Dienst
Nutzende Rolle(n)	System
Genutzte Information	Provisionierungsauftrag

Tabelle 15: Anwendungsfall System wickelt Auftrag ab

S2.4.5: IT-Service liefert IT-Arbeitsplatzausstattung aus	
Beschreibung	Der IT-Service nutzt die DK Logistikdienste der Domäne ERP, um die physischen Bestandteile der IT-Arbeitsplatzausstattung dem Mitarbeiter auszuliefern.
Nutzbare Funktionalität(en)	Physikalische Bereitstellung von IT-Services
Nutzbarer Dienst(e)	DK Logistikdienste
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Logistikinformationen

Tabelle 16: Anwendungsfall IT-Service liefert IT-Arbeitsplatzausstattung aus

S2.4.6: System dokumentiert Auftrag	
Beschreibung	Das System dokumentiert den Auftrag. Die Dokumentation des Auftrages (Informationen zur Auftragsabwicklung) erfolgt im Self-Service-Plattform-Dienst der Domäne INF. Die Dokumentation des Auftrages (Technische Konfiguration) im Service-Lifecycle-Management-Support-Dienst der Domäne INF. Die genutzten Leistungen werden an die Diensteklasse Steuerung und Information der Domäne ERP zur Verrechnung gegenüber der beziehenden Behörde übermittelt.
Nutzbare Funktionalität(en)	Dokumentation des Auftrages
Nutzbarer Dienst(e)	Self-Service-Plattform-Dienst, Service-Lifecycle-Management-Support-Dienst, DK Steuerung und Information
Nutzende Rolle(n)	System
Genutzte Information	Informationen zur Auftragsabwicklung

Tabelle 17: Anwendungsfall System dokumentiert Auftrag

S2.5.1.1: Mitarbeiter erstellt eine Nachricht	
Beschreibung	Der Mitarbeiter erstellt oder bearbeitet auf seinem IT-Arbeitsplatz eine Nachricht im Umfeld des elektronischen Rechtsverkehrs. Die Nachricht kann neu erstellt werden oder z.B. aus einem Fachdienst oder einer elektronischen Akte stammen.
Nutzbare Funktionalität(en)	Nutzung des IT-Arbeitsplatzes, Nutzung von IT-Lösungen aus dem Umfeld des elektronischen Rechtsverkehrs
Nutzbarer Dienst(e)	Arbeitsplatz-PC, Mobiles-Gerät, Ultra-Mobiles-Gerät, Nutzung von Diensten aus den Domänen oder von Fachdienste
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Nachricht

Tabelle 18: Anwendungsfall Mitarbeiter erstellt eine Nachricht

S2.5.1.2: Mitarbeiter versendet Nachricht an Intermediär	
Beschreibung	Der Mitarbeiter versendet die Nachricht aus einer Client-Anwendung, die für den direkten Zugriff auf einen Intermediär geeignet ist. Für die Ermittlung der Adresse des Intermediärs greift der Client auf den externen SAFE-Registrierungsdienst der Justiz zu und ermittelt dort die URI-Adresse für den externen Intermediär. Anschließend wird die Nachricht im Postfach des Intermediärs abgelegt.
Nutzbare Funktionalität(en)	Nachrichtenversand
Nutzbarer Dienst(e)	Arbeitsplatz-PC, Mobiles-Gerät, Ultra-Mobiles-Gerät, G2X-Kommunikation
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Nachricht

Tabelle 19: Anwendungsfall Mitarbeiter versendet Nachricht an Intermediär

S2.5.1.3: Mitarbeiter versendet E-Mail	
Beschreibung	Der Mitarbeiter nutzt seinen normalen E-Mail Client für die Nachrichtenübertragung an den externen Intermediär. Im ersten Schritt ermittelt er über ein Web-Portal die E-Mail-Adresse des Kommunikationspartners. Wenn er die E-Mail an diese Adresse versendet, wird sie vom E-Mail-Dienst an den G2X-Kommunikations-Dienst weitergeleitet.
Nutzbare Funktionalität(en)	Nachrichtenversand
Nutzbarer Dienst(e)	Arbeitsplatz-PC, Mobiles-Gerät, Ultra-Mobiles-Gerät, G2X-Kommunikation, E-Mail
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Nachricht

Tabelle 20: Anwendungsfall Anwender versendet E-Mail

S2.5.1.4: System konvertiert Nachricht ins Ziel-Datenformat	
Beschreibung	Die E-Mail Nachricht wird in der Middleware des G2X-Kommunikations-Dienstes in das Ziel-Datenformat des Intermediärs konvertiert. Dabei wird die Nachricht elektronisch signiert und verschlüsselt. Die dafür notwendigen Zertifikate sind im G2X-Kommunikations-Dienst bei der Einrichtung der Anwender hinterlegt worden.
Nutzbare Funktionalität(en)	Automatische Datenkonvertierung
Nutzbarer Dienst(e)	G2X-Kommunikations-Dienst
Nutzende Rolle(n)	System

Genutzte Information	Nachricht

Tabelle 21: Anwendungsfall System konvertiert Nachricht ins Ziel-Datenformat

S2.5.2.1: Nachricht geht ein	
Beschreibung	Ein externer Client liefert eine Nachricht am Intermediär, dem Postfachserver für elektronische Nachrichten im Rechtsverkehr, an. Dieser wird über den G2X-Kommunikations-Dienst bereitgestellt.
Nutzbare Funktionalität(en)	Nachrichtenempfang
Nutzbarer Dienst(e)	G2X-Kommunikation
Nutzende Rolle(n)	System
Genutzte Information	Nachricht

Tabelle 22: Anwendungsfall Nachricht geht ein

S2.5.2.2: Nachricht wird in E-Mail konvertiert	
Beschreibung	Für die Anwendergruppe in der Behörde, die als E-Mail Empfänger im G2X-Kommunikations-Dienst hinterlegt sind, prüft eine Middleware den Intermediär auf Eingang neuer Nachrichten. Ist eine neue Nachricht eingegangen, dann wird diese abgeholt, die notwendigen Routinen für eine Konvertierung ins E-Mail Format, u.a. mit Protokollierung der verwendeten Zertifikate, Erstellung einer Empfangsbestätigung, durchgeführt und über den E-Mail-Dienst an den Empfänger weitergeleitet.
Nutzbare Funktionalität(en)	Nachrichtenkonvertierung Eine Nachricht wird in eine E-Mail konvertiert und diese um die während der Konvertierung erzeugte Protokolldatei ergänzt.
Nutzbarer Dienst(e)	G2X-Kommunikation, E-Mail Der Intermediär sowie die Middleware, die die Konvertierung der Nachricht in eine E-Mail übernimmt, gehört zum G2X-Kommunikations-Dienst. Der Versand der E-Mail an das E-Mail-Postfach des Adressaten wird über den E-Mail-Dienst abgewickelt.
Nutzende Rolle(n)	System
Genutzte Information	Nachricht

Tabelle 23: Anwendungsfall Nachricht wird in E-Mail konvertiert

S2.5.2.3: Mitarbeiter wird über Nachrichteneingang informiert	
Beschreibung	Der Intermediär im G2X-Kommunikations-Dienst informiert den Mitarbeiter mit Hilfe des E-Mail-Dienstes über den Eingang einer neuen Nachricht auf dem Intermediär. Dort ist die Empfängeradresse des Mitarbeiters bei der Konfiguration hinterlegt worden.
Nutzbare Funktionalität(en)	E-Mail-Nachrichtenempfang
Nutzbarer Dienst(e)	Arbeitsplatz-PC, Mobiles-Gerät, Ultra-Mobiles-Gerät, E-Mail
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Nachricht

Tabelle 24: Anwendungsfall Mitarbeiter wird über Nachrichteneingang informiert

S2.5.2.4: Mitarbeiter greift auf Postfach zu	
Beschreibung	Je nach Client-Anwendung greift der Mitarbeiter von seinem IT-Arbeitsplatz entweder mit seinem lokalen Client, der für die direkte Kommunikation mit einem Intermediär geeignet ist, das Postfach auf dem Intermediär zu, oder er verwendet seinen E-Mail-Client, um die konvertierte Nachricht abzurufen.
Nutzbare Funktionalität(en)	Nutzung der Postfächer
Nutzbarer Dienst(e)	Arbeitsplatz-PC, Mobiles-Gerät, Ultra-Mobiles-Gerät, G2X-Kommunikation, E-Mail-Dienst
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Nachricht

Tabelle 25: Anwendungsfall Anwender greift auf Postfach zu

S2.6.1: HR Mitarbeiter legt Stammdaten an	
Beschreibung	Der HR Mitarbeiter greift auf den Personaladministrationsdienst der Domäne ERP zu, legt die Stammdaten des neuen Mitarbeiters an und hinterlegt die Zutrittsberechtigungen für Liegenschaften und Räume.
Nutzbare Funktionalität(en)	Erstellung von Mitarbeiterstammdaten
Nutzbarer Dienst(e)	Personaladministrationsdienst
Nutzende Rolle(n)	HR Mitarbeiter
Genutzte Information	Mitarbeiterstammdaten

Tabelle 26: HR Mitarbeiter legt Stammdaten an

S2.6.2: Dienstausweisstelle ruft die Stammdaten ab und initiiert die Bestellung	
Beschreibung	Der Mitarbeiter der Dienstausweisstelle ruft die Stammdaten aus dem Personaladministrationsdienst ab, erfasst das Lichtbild und die Unterschriftsprobe des Mitarbeiters mit Hilfe des Hardware-Token-Dienstes. Die notwendigen Dienstausweisdaten werden in einem eDA-Register gespeichert, das durch den Hardware-Token-Dienst ausgeprägt wird.
Nutzbare Funktionalität(en)	Speicherung Dienstausweisdaten, Initiierung der Bestellung
Nutzbarer Dienst(e)	Personaladministrationsdienst, Hardware-Token-Dienst, Self-Service-Plattform-Dienst
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Mitarbeiterstammdaten, Dienstausweisdaten, (eDA) Bestelldaten

Tabelle 27: Dienstausweissteller ruft die Stammdaten ab und initiiert die Bestellung

S2.6.3: System wickelt Auftrag ab	
Beschreibung	Die zu definierende Stelle / Das zu definierende System nimmt die Bestellung des elektronischen Dienstausweises entgegen, produziert den Dienstausweis und liefert diesen an die entsprechende Dienstausweisstelle aus.
Nutzbare Funktionalität(en)	Produktion des elektronischen Dienstausweises
Nutzbarer Dienst(e)	-
Nutzende Rolle(n)	System
Genutzte Information	Dienstausweisdaten

Tabelle 28: Anwendungsfall System wickelt Auftrag ab

S2.6.4: Dienstausweisstelle personalisiert Dienstausweis und liefert aus oder hinterlegt diesen zur Abholung	
Beschreibung	Die Dienstausweisstelle nutzt den Hardware-Token-Dienst der Domäne INF, um eine elektronische Personalisierung des bestellten elektronischen Dienstausweises durchzuführen. Anschließend wird der elektronische Dienstausweis an den Mitarbeiter ausgegeben bzw. für ihn zur Abholung hinterlegt.
Nutzbare Funktionalität(en)	Elektronische Personalisierung des elektronischen Dienstausweises
Nutzbarer Dienst(e)	Hardware-Token-Dienst
Nutzende Rolle(n)	System, Mitarbeiter der Dienstausweisstelle
Genutzte Information	Dienstausweisdaten

Tabelle 29: Anwendungsfall Dienstausweisstelle personalisiert Dienstausweis und liefert aus / bzw. hinterlegt zur Abholung

S2.6.5: System dokumentiert Auftrag	
Beschreibung	Die Dokumentation des Auftrages (Informationen zur Auftragsabwicklung) erfolgt im Self-Service-Plattform-Dienst der Domäne INF. Die Dokumentation des Auftrages (Technische Konfiguration) im Service-Lifecycle-Management-Support-Dienst der Domäne INF. Die genutzten Leistungen werden an die Diensteklasse Steuerung und Information der Domäne ERP zur Verrechnung gegenüber der beziehenden Behörde übermittelt.
Nutzbare Funktionalität(en)	Dokumentation des Auftrages
Nutzbarer Dienst(e)	Self-Service-Plattform-Dienst, Service-Lifecycle-Management-Support-Dienst, Diensteklasse Steuerung und Information
Nutzende Rolle(n)	System
Genutzte Information	Informationen zur Auftragsabwicklung

Tabelle 30: Anwendungsfall System dokumentiert Auftrag

S2.7.1: Mitarbeiter betritt den Behördenstandort	
Beschreibung	Der Mitarbeiter nutzt den elektronischen Dienstausweis um den Zutritt zu der Liegenschaft / dem Behördenstandort zu erlangen. Das Zutrittskontrollsystem prüft die Zutrittsberechtigung auf dem elektronischen Dienstausweis. Nach erfolgreicher Überprüfung wird automatisch über den Statusdienst des Hardware-Token-Dienstes der Sperrstatus des verwendeten Dienstausweises geprüft (im Falle der Prüfung des Zutritts zu einer Liegenschaft). Nach wiederholt erfolgreicher Prüfung wird anschließend der Zutritt gewährt. Der Eintritt des Mitarbeiters kann zusätzlich über den Liegenschaftsverwaltungsdienst im entsprechenden Zeiterfassungssystem der ERP Domäne dokumentiert werden.
Nutzbare Funktionalität(en)	Zugang zu Liegenschaft
Nutzbarer Dienst(e)	Hardware-Token-Dienst, Liegenschaftsverwaltungsdienst
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Sperrinformationen

Tabelle 31: Anwendungsfall Mitarbeiter betritt den Behördenstandort

S2.7.2: Mitarbeiter betritt Büro	
Beschreibung	Der Mitarbeiter nutzt den elektronischen Dienstausweis um den Zutritt zum Büro zu erlangen. Das Zutrittskontrollsystem prüft die Zutrittsberechtigung auf dem elektronischen Dienstausweis. Nach erfolgreicher Überprüfung wird automatisch über den Statusdienst des Hardware-Token-Dienstes der Sperrstatus des verwendeten Dienstausweises geprüft (im Falle der Prüfung des Zutritts zu einer Liegenschaft). Nach wiederholt erfolgreicher Prüfung wird anschließend der Zutritt gewährt.
Nutzbare Funktionalität(en)	Zugang zu Büro
Nutzbarer Dienst(e)	Hardware-Token-Dienst, Liegenschaftsverwaltungsdienst
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Sperrinformationen

Tabelle 32: Anwendungsfall Mitarbeiter betritt Büro

S2.7.3: Mitarbeiter verlässt den Behördenstandort	
Beschreibung	Für das Verlassen des Geländes wird der Dienstausweis ebenfalls an dem Zeiterfassungssystem verwendet. Der Mitarbeiter nutzt den Zeitwirtschaftsdienst um das Verlassen des Behördenstandorts zu dokumentieren. Notwendige Daten vom elektronischen Dienstausweis werden zur Dokumentation an die ERP Personaldienste übertragen.
Nutzbare Funktionalität(en)	Dokumentation im Zeitwirtschaftssystem
Nutzbarer Dienst(e)	Personaladministrationsdienst, Zeitwirtschaftsdienst
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Zeiterfassungsinformationen

Tabelle 33: Anwendungsfall Mitarbeiter verlässt den Behördenstandort

S2.8.1: Mitarbeiter meldet sich am IT-Arbeitsplatz an	
Beschreibung	Der Mitarbeiter verwendet den Dienstausweis als Hardware-Token zur Anmeldung am Arbeitsplatz-PC-Dienst der Domäne INF. Über den PKI-Dienst wird die Gültigkeit des verwendeten Zertifikats auf dem Hardware-Token geprüft. Identity- und Access-Management-Dienste liefern die elektronische Identität des Mitarbeiters und die ihr zugeordneten Rechte und Rollen.
Nutzbare Funktionalität(en)	Nutzung des IT-Arbeitsplatzes, Nutzung Dienstausweis, Nutzung von Authentifizierungs- und Autorisierungsmechanismen
Nutzbarer Dienst(e)	Arbeitsplatz-PC, Mobiles-Gerät, Ultra-Mobiles-Gerät, Hardware-Token, Identity-Management, Access-Management
Nutzende Rolle(n)	Mitarbeiter

Genutzte Information	Anmeldedaten, Zertifikatsdaten

Tabelle 34: Anwendungsfall Mitarbeiter meldet sich am IT-Arbeitsplatz an

S2.8.2: Mitarbeiter signiert ein Dokument	
Beschreibung	Der Mitarbeiter versieht ein elektronisches Dokument mit einer elektronischen Signatur, um dieses z.B. einem Dienst aus der Elektronischen Verwaltungsarbeit (EVA) für die Weiterverarbeitung zuzuführen. Dafür wird eine Signaturerstellungskomponente (QES-/Beweiswerterhaltungs-Dienst) verwendet, die der Hardware-Token-Dienst ansteuert, um die qualifizierte elektronische Signatur (QES) zu erstellen. Das für das Signieren notwendige Zertifikat ist auf dem Ausweis gespeichert. Über den PKI-Dienst prüft der verwendete EVA-Dienst die Gültigkeit des Zertifikats.
Nutzbare Funktionalität(en)	Nutzung des IT-Arbeitsplatzes, Nutzung Dienstausweis
Nutzbarer Dienst(e)	Arbeitsplatz-PC, Mobiles-Gerät, Ultra-Mobiles-Gerät, Hardware-Token, PKI, Identity-Management, Access-Management
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Zertifikatsdaten

Tabelle 35: Anwendungsfall Mitarbeiter signiert ein Dokument

S2.8.3: Mitarbeiter signiert eine E-Mail	
Beschreibung	Der Mitarbeiter versieht eine E-Mail mit einer qualifizierten elektronischen Signatur (QES). Dafür wird analog dem Anwendungsfall in S2.2.3.2 eine Signaturerstellungskomponente (QES-/Beweiswerterhaltungs-Dienst) verwendet. Der Arbeitsplatz-PC-Dienst greift auf den PKI-Dienst zu, um das Schlüsselpaar zu prüfen. Nach erfolgreicher Prüfung, wird der E-Mail-Dienst genutzt, um die Nachricht zu versenden.
Nutzbare Funktionalität(en)	Nutzung des IT-Arbeitsplatzes, Nutzung Dienstausweis Auf dem IT-Arbeitsplatz werden die notwendigen Anwendungen bereitgestellt, der elektronische Mitarbeiterausweis dient als Speicher für die benötigten Zertifikate.
Nutzbarer Dienst(e)	Arbeitsplatz-PC, Mobiles-Gerät, Ultra-Mobiles-Gerät, Hardware-Token, PKI, E-Mail
Nutzende Rolle(n)	Mitarbeiter
Genutzte Information	Zertifikatsdaten

Tabelle 36: Anwendungsfall Mitarbeiter signiert eine E-Mail

4.2 Rollen

In diesem Abschnitt werden die Rollen in der Domäne Infrastruktur detailliert in alphabetischer Form aufgelistet. Die Darstellung gibt einen spezifischen Einblick in die Akteure der Anwendungsfälle, Dienste und deren Funktionalitäten.

Rolle Anwender	
Beschreibung	Ein interner Mitarbeiter einer Behörde
Aktivität(en), Interesse(n)	Nutzt den IT-Arbeitsplatz und die ihm zugewiesenen Anwendungen ohne besondere Rechte, insbesondere ohne administrative Rechte.
Anforderung(en)	Hat das Recht Bedarfe auszulösen, bspw. Optionalleistungen zum Arbeitsplatz-PC-Dienst.

Tabelle 37: Rolle Anwender

Rolle Entwickler	
Beschreibung	Ein interner Mitarbeiter einer Behörde
Aktivität(en), Interesse(n)	Nutzt den IT-Arbeitsplatz für die Entwicklung von neuen IT-Lösungen.
Anforderung(en)	Hat das Recht sich Entwicklungsumgebungen im Self-Service-Portal der Cloud-Betriebsplattform zusammenzustellen und zu bestellen.

Tabelle 38: Rolle Entwickler

Rolle Fachadministrator	
Beschreibung	Ein Mitarbeiter (Fachadministrator) einer Behörde, der administrative Aufgaben für IT-Lösungen übernimmt.
Aktivität(en), Interesse(n)	Administriert Systeme in der Betriebsplattform oder Anwendungen.
Anforderung(en)	Hat das Recht zur Administration von Systemen / Anwendungen.

Tabelle 39: Rolle Fachadministrator

Rolle System	
Beschreibung	Ein IT-System, das durch vordefinierte Trigger Vorgänge wie Datenübertragungen etc. auslöst.
Aktivität(en), Interesse(n)	Bedient Batch- und andere System-zu-System Prozesse.
Anforderung(en)	Werden im Rahmen der System- / Anwendungskonfiguration festgelegt.

Tabelle 40: Rolle System

4.3 Informationsobjekte

In diesem Abschnitt werden die Informationsobjekte der Infrastruktur detailliert in alphabetischer Form aufgelistet. Die Darstellung gibt einen spezifischen Einblick in die Beziehung zum Dienst und die Funktionalitäten für die Wiederverwendung in Geschäftsprozessen.

Informationsobjekt Anmeldedaten	
Beschreibung	Daten, die zur Anmeldung an einem System oder einer Anwendung verwendet werden.
Primärer Dienst	Identity- und Access-Management-Dienst
Beteiligte(r) Dienst(e)	Hardware-Token-Dienst, PKI-Dienst, Dienste aus den Domänen oder Fachdienste
Schnittstellen, Standards	SSO, LDAP, Kerberos, SAML etc.

Tabelle 41: Informationsobjekt Anmeldedaten

Informationsobjekt Abrechnungsdaten	
Beschreibung	Daten, die zur Leistungsverrechnung gegenüber der beziehenden Behörde benötigt werden.
Primärer Dienst	Service-Lifecycle-Management-Support-Dienst
Beteiligte(r) Dienst(e)	Self-Service-Plattform-Dienst , Diensteklasse der ERP Steuerungs- und Informationsdienste
Schnittstellen, Standards	Zu definieren.

Tabelle 42: Informationsobjekt Abrechnungsdaten

Informationsobjekt Bestelldaten	
Beschreibung	Daten, die zur Bestellabwicklung und Lieferung benötigt werden.
Primärer Dienst	Service-Lifecycle-Management-Support-Dienst
Beteiligte(r) Dienst(e)	Self-Service-Plattform-Dienst , Diensteklasse Logistik aus der ERP Domäne
Schnittstellen, Standards	Zu definieren.

Tabelle 43: Informationsobjekt Bestelldaten

Informationsobjekt Identitätsdaten	
Beschreibung	Daten, die mit einer Identität verknüpft sind.
Primärer Dienst	Zu definieren.
Beteiligte(r) Dienst(e)	Zu definieren.

Schnittstellen, Standards	Zu definieren.

Tabelle 44: Informationsobjekt Identitätsdaten

Informationsobjekt Mitarbeiterstammdaten	
Beschreibung	Persönliche Daten, die den Mitarbeiter beschreiben oder vom Mitarbeiter selbst hinterlegt werden.
Primärer Dienst	Zu definieren.
Beteiligte(r) Dienst(e)	Dienste der ERP-Diensteklasse Personaldienste
Schnittstellen, Standards	Zu definieren.

Tabelle 45: Informationsobjekt Mitarbeiterstammdaten

Informationsobjekt Produktkatalog-Daten	
Beschreibung	Daten, die die Produkte im Produktkatalog beschreiben.
Primärer Dienst	Service-Lifecycle-Management-Support-Dienst
Beteiligte(r) Dienst(e)	Self-Service-Plattform-Dienst
Schnittstellen, Standards	REST, JSON, XML oder IT-lösungsspezifische Objekte uns Schnittstellen

Tabelle 46: Informationsobjekt Produktkatalog-Daten

Informationsobjekt Konfigurationsdaten	
Beschreibung	Daten, die zur automatisierten Provisionierung von IT-Lösungen speziell im Cloud-Umfeld verwendet werden.
Primärer Dienst	Cloud-Entwicklungsplattform-Dienst
Beteiligte(r) Dienst(e)	Dienste aus den Domänen oder Fachdienste
Schnittstellen, Standards	JSON oder XML Objekte

Tabelle 47: Informationsobjekt Konfigurationsdaten

Informationsobjekt Nachricht	
Beschreibung	Daten, die für den elektronischen Versand oder Empfang vorgesehen sind.
Primärer Dienst	E-Mail, G2X-Kommunikation
Beteiligte(r) Dienst(e)	Dienste aus den Domänen oder Fachdienste
Schnittstellen, Standards	OSCI, SMTP, MAPI, XML, RFC 2822, RFC 822, OSCI 1.2, OSCI 2.0

Tabelle 48: Informationsobjekt Nachricht

Informationsobjekt Rollen und Rechte	
Beschreibung	Daten, die zur Autorisierung von Zugriffen verwendet werden.
Primärer Dienst	Identity- und Access-Management-Dienst
Beteiligte(r) Dienst(e)	Dienste aus den Domänen oder Fachdienste
Schnittstellen, Standards	JSON oder XML Objekte, IT-Lösungsspezifische Daten

Tabelle 49: Informationsobjekt Rollen und Rechte

Informationsobjekt Zertifikatsdaten	
Beschreibung	Zertifikatsdaten
Primärer Dienst	PKI-Dienst, Hardware-Token-Dienst
Beteiligte(r) Dienst(e)	Dienste aus den Domänen oder Fachdienste
Schnittstellen, Standards	X.509, PGP, S/MIME, OSCP, SCVP, HTTPS, IPsec, SSH etc.

Tabelle 50: Informationsobjekt Zertifikatsdaten

Informationsobjekt Metadaten	
Beschreibung	Daten, die System-zu-System übertragen werden und anwendungsabhängige Payloads transportieren.
Primärer Dienst	Alle
Beteiligte(r) Dienst(e)	Alle
Schnittstellen, Standards	Fallbezogen

Tabelle 51: Informationsobjekt Metadaten

4.4 Diensteabhängigkeiten

In diesem Abschnitt werden die Abhängigkeiten der Dienste detailliert aufgelistet. Im vorhergehenden Kapitel wurde bereits auf die Abhängigkeiten zwischen den Diensteklassen (DK) eingegangen. Dem dort geschilderten Sachverhalt wird hier insofern Rechnung getragen, indem zum einen die Dienste mit ihren Abhängigkeiten entsprechend der gezeigten Hierarchie aufgeführt werden und zum anderen sich wiederholende Abhängigkeiten falls möglich auf eine gesamte Diensteklasse oder mehrere Dienste zusammengefasst beschrieben werden.

4.4.1 Diensteabhängigkeiten bei den Infrastrukturdiensten

In diesem Abschnitt wird auf die Dienste der Diensteklassen Netzdienste, Entwicklungs- und Betriebsdienste sowie der Sicherheitsdienste eingegangen.

Diensteabhängigkeit DK Netzdienste / Konventioneller-Betriebsplattform-Dienst	
Beschreibung	**Internet-, NdB- und Spezial-Netze-Dienst** nutzt **Konventioneller-Betriebsplattform-Dienst** Die Infrastruktur der Betriebsplattformen wird für die Bereitstellung der netznahen Services und der Geräte für die Netz-Infrastruktur genutzt.
Art der Abhängigkeit	Nutzung einer Betriebsplattform
Standard(s), Protokoll(e)	

Tabelle 52: Diensteabhängigkeit DK Netzdienste / Konventioneller-Betriebsplattform-Dienst

Diensteabhängigkeit DK Netzdienste / Hardware-Token-Dienst	
Beschreibung	**Internet-, NdB- und Spezial-Netze-Dienst** nutzt **Hardware-Token-Dienst** Die DK Netzdienste nutzt den Hardware-Token-Dienst zur Bereitstellung von Hardware-Sicherheitsmodulen (HSM) für die effiziente und sichere Ausführung kryptographischer Operationen oder Applikationen, Transaktionssicherung, Zeitstempeldienste, Signaturserver, Archivierungssysteme, und DNS-Absicherung.
Art der Abhängigkeit	Nutzung von kryptographischen Funktionen
Standard(s), Protokoll(e)	

Tabelle 53: Diensteabhängigkeit DK Netzdienste / Hardware-Token-Dienst

Diensteabhängigkeit DK Netzdienste / PKI-Dienst	
Beschreibung	**Internet-, NdB- und Spezial-Netze-Dienst** nutzt **PKI-Dienst** Die DK Netzdienste nutzt den PKI-Dienst zur Bereitstellung und für das Management von Zertifikaten innerhalb der netznahen Dienste
Art der Abhängigkeit	Nutzung von elektronischen Zertifikaten
Standard(s), Protokoll(e)	

Tabelle 54: Diensteabhängigkeit DK Netzdienste / PKI-Dienst

Diensteabhängigkeit DK Netzdienste / Service-Lifecycle-Management-Support-Dienst	
Beschreibung	**Internet-, NdB- und Spezial-Netze-Dienst** nutzt **Service-Lifecycle-Management-Support-Dienst** Zur Dokumentation der vorhandenen Infrastruktur.
Art der Abhängigkeit	Nutzung von Dokumentationsfunktionen.
Standard(s), Protokoll(e)	

Tabelle 55: Diensteabhängigkeit DK Netzdienste / Service-Lifecycle-Management-Support-Dienst

Diensteabhängigkeit Cloud- & Konventioneller-Betriebsplattform-Dienst / DK Netzdienste	
Beschreibung	**Cloud- & Konventioneller-Betriebsplattform-Dienst** nutzt **DK Netzdienste** Die Betriebsplattformen nutzen die Netzdienste zum einen als Infrastruktur für die Vernetzung der Betriebsplattformen mit den Behördenstandorten und den Rechenzentren und zum anderen werden die Funktionen der netznahen Services für die Namensauflösung, zur Absicherung von Netzverbindungen, Basis-Services und der Management-Plattform für den Betrieb der Betriebsplattformen sowie zur Implementierung von Hochverfügbarkeit genutzt.
Art der Abhängigkeit	Nutzung der Netz-Infrastruktur, Nutzung von netznahen Diensten
Standard(s), Protokoll(e)	

Tabelle 56: Diensteabhängigkeit Cloud- & Konventioneller-Betriebsplattform-Dienst / DK Netzdienste

Diensteabhängigkeit Cloud- & Konventioneller-Betriebsplattform-Dienst / Hardware-Token-Dienst	
Beschreibung	**Cloud- & Konventioneller-Betriebsplattform-Dienst** nutzt **Hardware-Token-Dienst** Nutzt den Hardware-Token-Dienst zur Bereitstellung von Hardware-Sicherheitsmodulen (HSM) für die effiziente und sichere Ausführung kryptographischer Operationen oder Applikationen, Transaktionssicherung, Zeitstempeldienste, Signaturserver und Archivierungssysteme.
Art der Abhängigkeit	Nutzung von kryptographischen Funktionen
Standard(s), Protokoll(e)	

Tabelle 57: Diensteabhängigkeit Cloud- & Konventioneller-Betriebsplattform-Dienst / Hardware-Token-Dienst

Diensteabhängigkeit Cloud- & Konventioneller-Betriebsplattform-Dienst / PKI-Dienst	
Beschreibung	**Cloud- & Konventioneller-Betriebsplattform-Dienst** nutzt **PKI-Dienst** Nutzt den PKI-Dienst zur Bereitstellung und für das Management von Zertifikaten innerhalb der netznahen Dienste
Art der Abhängigkeit	Nutzung von elektronischen Zertifikaten
Standard(s), Protokoll(e)	

Tabelle 58: Diensteabhängigkeit Cloud- & Konventioneller-Betriebsplattform-Dienst / PKI-Dienst

Diensteabhängigkeit Cloud- & Konventioneller-Betriebsplattform-Dienst / Service-Lifecycle-Management-Support-Dienst	
Beschreibung	**Cloud- & Konventioneller-Betriebsplattform-Dienst** nutzt **Service-Lifecycle-Management-Support-Dienst** Zur Dokumentation der vorhandenen Infrastruktur.
Art der Abhängigkeit	Nutzung von Dokumentationsfunktionen
Standard(s), Protokoll(e)	

Tabelle 59: Diensteabhängigkeit Cloud- & Konventioneller-Betriebsplattform-Dienst / Service-Lifecycle-Management-Support-Dienst

Diensteabhängigkeit Cloud-Betriebsplattform-Dienst / Konventioneller-Betriebsplattform-Dienst	
Beschreibung	**Cloud-Betriebsplattform-Dienst** nutzt **Konventionellen-Betriebsplattform-Dienst** Der Cloud-Betriebsplattform-Dienst nutzt die durch den Konventionellen-Betriebsplattform-Dienst bereitgestellte Infrastruktur zur Implementierung der Cloud-Infrastruktur.
Art der Abhängigkeit	Nutzung der Infrastruktur
Standard(s), Protokoll(e)	

Tabelle 60: Diensteabhängigkeit Cloud-Betriebsplattform-Dienst / Konventioneller-Betriebsplattform-Dienst

Diensteabhängigkeit Cloud-Betriebsplattform-Dienst / Cloud-Entwicklungsplattform-Dienst	
Beschreibung	**Cloud-Betriebsplattform-Dienst** nutzt **Cloud-Entwicklungsplattform-Dienst** Der Cloud-Betriebsplattform-Dienst nutzt den Cloud-Entwicklungsplattform-Dienst zur automatisierten Bereitstellung von Basis-Cloud-Produkten.
Art der Abhängigkeit	Nutzung der Infrastruktur für die Entwicklung neuer Cloud-Basis-Services und deren automatisierte Provisionierung.
Standard(s), Protokoll(e)	

Tabelle 61: Diensteabhängigkeit Cloud-Betriebsplattform-Dienst / Cloud-Entwicklungsplattform-Dienst

Diensteabhängigkeit Cloud-Betriebsplattform-Dienst / Self-Service-Plattform-Dienst	
Beschreibung	**Cloud-Betriebsplattform-Dienst** nutzt **Self-Service-Plattform-Dienst** Der Cloud-Betriebsplattform-Dienst bietet über den Self-Service-Plattform-Dienst die Cloud-Basis-Services zur Buchung durch Entwickler und Administratoren an.
Art der Abhängigkeit	Nutzung der Bestellfunktionen
Standard(s), Protokoll(e)	

Tabelle 62: Diensteabhängigkeit Cloud-Betriebsplattform-Dienst / Self-Service-Plattform-Dienst

Diensteabhängigkeit Cloud-Entwicklungsplattform-Dienst / Self-Service-Plattform-Dienst	
Beschreibung	**Cloud-Entwicklungsplattform-Dienst** nutzt **Self-Service-Plattform-Dienst** Der Cloud-Entwicklungsplattform-Dienst bietet über den Self-Service-Plattform-Dienst die Cloud-Entwickler-Services zur Buchung durch Entwickler und Fachdministratoren an.
Art der Abhängigkeit	Bereitstellung neuer IT-Services
Standard(s), Protokoll(e)	

Tabelle 63: Diensteabhängigkeit Cloud-Entwicklungsplattform-Dienst / Self-Service-Plattform-Dienst

Diensteabhängigkeit Cloud-Entwicklungsplattform-Dienst / Service-Lifecycle-Management-Support-Dienst	
Beschreibung	**Cloud-Entwicklungsplattform-Dienst** nutzt **Service-Lifecycle-Management-Support-Dienst** Zur Dokumentation der vorhandenen Infrastruktur
Art der Abhängigkeit	Nutzung von Dokumentationsfunktionen
Standard(s), Protokoll(e)	

Tabelle 64: Diensteabhängigkeit Cloud-Entwicklungsplattform-Dienst / Service-Lifecycle-Management-Support-Dienst

Diensteabhängigkeit DK Sicherheitsdienste / DK Netzdienste	
Beschreibung	**Access- & Identity-Management-Dienst, PKI- und Hardware-Token- sowie QES-Beweiswerterhaltungs-Dienst** nutzen **Diensteklasse Netzdienste** Sämtliche Dienste der Diensteklasse Sicherheitsdienste nutzen die Netz-Infrastruktur sowie netznaher Services für die Namensauflösung, zur Absicherung der Kommunikation oder zur Implementierung von Hochverfügbarkeit.
Art der Abhängigkeit	Nutzung der Netz-Infrastruktur, Nutzung netznaher Services
Standard(s), Protokoll(e)	

Tabelle 65: Diensteabhängigkeit DK Sicherheitsdienste / DK Netzdienste

Diensteabhängigkeit DK Sicherheitsdienste / Cloud- & Konventioneller-Betriebsplattform-Dienst	
Beschreibung	**Access- & Identity-Management-Dienst, PKI- und Hardware-Token- sowie QES-Beweiswerterhaltungs-Dienst** nutzen **Cloud- & Konventionellen-Betriebsplattform-Dienst** Sämtliche Dienste der Diensteklasse Sicherheitsdienste nutzen die Infrastruktur der Betriebsplattformen zur Abbildung der IT-Lösungen in der Diensteklasse der Sicherheitsdienste
Art der Abhängigkeit	Nutzung der Infrastruktur
Standard(s), Protokoll(e)	

Tabelle 66: Diensteabhängigkeit DK Sicherheitsdienste / Cloud- & Konventioneller-Betriebsplattform-Dienst

Diensteabhängigkeit DK Sicherheitsdienste / Service-Lifecycle-Management-Support-Dienst	
Beschreibung	**Access- & Identity-Management-Dienst, PKI- und Hardware-Token- sowie QES-Beweiswerterhaltungs-Dienst** nutzt **Service-Lifecycle-Management-Support-Dienst** Zur Dokumentation der vorhandenen Infrastruktur
Art der Abhängigkeit	Nutzung von Dokumentationsfunktionen
Standard(s), Protokoll(e)	

Tabelle 67: Diensteabhängigkeit DK Sicherheitsdienste / Service-Lifecycle-Management-Support-Dienst

Diensteabhängigkeit Access-Management-Dienst / Identity-Management-Dienst	
Beschreibung	**Access-Management-Dienst** nutzt **Identity-Management-Dienst** Zur Speicherung von Rechten und Rollen in den Identitäts-Repositorien, die über den Identity-Management-Dienst bereitgestellt werden
Art der Abhängigkeit	Nutzung gemeinsamer Infrastruktur
Standard(s), Protokoll(e)	

Tabelle 68: Diensteabhängigkeit Access-Management-Dienst / Identity-Management-Dienst

Diensteabhängigkeit Identity-Management-Dienst / DK Kommunikationsdienste	
Beschreibung	**Identity-Management-Dienst** nutzt **E-Mail-, Fax-, G2X-Kommunikations-, Telefonie-, Telefonkonferenz- und Videokonferenz-Dienst** Für die Ergänzung von Identitäts-Attributen, um sie über den zentralen Identity-Management-Dienst wiederum anderen Diensten zur Weiternutzung bereitstellen zu können.
Art der Abhängigkeit	Nutzung von Identitäten
Standard(s), Protokoll(e)	

Tabelle 69: Diensteabhängigkeit Identity-Management-Dienst / DK Kommunikationsdienste

Diensteabhängigkeit Identity-Management-Dienst / Dienste der Domänen und Fachdienste	
Beschreibung	**Identity-Management-Dienst** nutzt **ERP, EVA, EGOV sowie Fachdienste der Behörden** Für die Ergänzung von Identitäts-Attributen, um sie über den zentralen Identity-Management-Dienst wiederum anderen Diensten zur Weiternutzung bereitstellen zu können.
Art der Abhängigkeit	Nutzung von Identitäten
Standard(s), Protokoll(e)	

Tabelle 70: Diensteabhängigkeit Identity-Management-Dienst / Dienste der Domänen und Fachdienste

Diensteabhängigkeit PKI-Dienst / Hardware-Token-Dienst	
Beschreibung	**PKI-Dienst** nutzt **Hardware-Token-Dienst** Der PKI-Dienst nutzt den Hardware-Token-Dienst für die sichere Ablage und Bereitstellung von elektronischen Benutzerzertifikaten.
Art der Abhängigkeit	Verknüpfung von Zertifikaten mit Identitäten
Standard(s), Protokoll(e)	

Tabelle 71: Diensteabhängigkeit PKI-Dienst / Hardware-Token-Dienst

Diensteabhängigkeit PKI-Dienst / Identity-Management-Dienst	
Beschreibung	**PKI-Dienst** nutzt **Identity-Management-Dienst** Um personifizierte Zertifikate mit der zugehörigen Identität der Person zu verknüpfen

Art der Abhängigkeit	Verknüpfung von Zertifikaten mit Identitäten
Standard(s), Protokoll(e)	

Tabelle 72: Diensteabhängigkeit PKI-Dienst / Identity-Management-Dienst

Diensteabhängigkeit QES-Beweiswerterhaltungs-Dienst / Hardware-Token-Dienst	
Beschreibung	**QES-Beweiswerterhaltungs-Dienst** nutzt **Hardware-Token-Dienst** Nutzt den Hardware-Token-Dienst zur Bereitstellung von Hardware-Sicherheitsmodulen (HSM) für die effiziente und sichere Ausführung kryptographischer Operationen oder Applikationen, Transaktionssicherung, Zeitstempeldienste, Signaturserver und Archivierungssysteme.
Art der Abhängigkeit	Nutzung von kryptographischen Funktionen
Standard(s), Protokoll(e)	

Tabelle 73: Diensteabhängigkeit QES-Beweiswerterhaltungs-Dienst / Hardware-Token-Dienst

Diensteabhängigkeit QES-Beweiswerterhaltungs-Dienst / PKI-Dienst	
Beschreibung	**QES-Beweiswerterhaltungs-Dienst** nutzt **PKI-Dienst** Zur Generierung von neuen Zertifikaten und zur Prüfung der Gültigkeit vorhandener Zertifikate
Art der Abhängigkeit	Nutzung von elektronischen Zertifikaten
Standard(s), Protokoll(e)	

Tabelle 74: Diensteabhängigkeit QES-Beweiswerterhaltungs-Dienst / PKI-Dienst

4.4.2 Diensteabhängigkeiten bei den Basisdiensten der Infrastruktur

In diesem Abschnitt wird auf die Dienste der Diensteklassen Kommunikation, Client, Druck und Scan eingegangen.

Diensteabhängigkeit DK Kommunikationsdienste / DK Netzdienste	
Beschreibung	**Audio-/Video-Streaming-, E-Mail-, Fax-, G2X-Kommunikations-, Telefonie-, Telefonkonferenz- und Video-konferenz-Dienst** nutzen **DK Netzdienste** Die Kommunikationsdienste nutzen die Netzdienste zum einen als Infrastruktur für die Vernetzung der IT-Lösungen in den Rechenzentren, als auch zur Anbindung der Clients in den Behörden und zur Anbindung der Kommunikationslösungen an externe Gegenstellen. Des Weiteren werden die Funktionen der netznahen Services für die Namensauflösung, zur Absicherung von Netzverbindungen sowie zur Implementierung von Hochverfügbarkeit genutzt.
Art der Abhängigkeit	Nutzung der Netz-Infrastruktur, Nutzung von netznahen Diensten
Standard(s), Protokoll(e)	

Tabelle 75: Diensteabhängigkeit DK Kommunikationsdienste / DK Netzdienste

Diensteabhängigkeit DK Kommunikationsdienste / Cloud- & Konventioneller-Betriebsplattform-Dienst	
Beschreibung	**Audio-/Video-Streaming-, E-Mail-, Fax-, G2X-Kommunikations-, Telefonie-, Telefonkonferenz- und Video-konferenz-Dienst** nutzen **Cloud- & Konventionellen-Betriebsplattform-Dienst** Sämtliche Dienste der Diensteklasse Kommunikation nutzen die Infrastruktur der Betriebsplattformen zur Abbildung der IT-Lösungen in der Diensteklasse der Kommunikation.
Art der Abhängigkeit	Nutzung der Infrastruktur
Standard(s), Protokoll(e)	

Tabelle 76: Diensteabhängigkeit DK Kommunikationsdienste / Cloud- & Konventioneller-Betriebsplattform-Dienst

Diensteabhängigkeit DK Kommunikationsdienste / Cloud-Entwicklungsplattform-Dienst	
Beschreibung	**Audio-/Video-Streaming-, E-Mail-, Fax-, G2X-Kommunikations-, Telefonie-, Telefonkonferenz- und Videokonferenz-Dienst** nutzen **Cloud-Entwicklungsplattform-Dienst** Die IT-Lösungen aus der Diensteklasse der Kommunikationsdienste, die auf der Cloud-Betriebsplattform implementiert werden, nutzen zum einen für die Entwicklung der IT-Lösung, als auch für die Provisionierung der fertigen IT-Lösung, die Funktionen, die über den Cloud-Entwicklungsplattform-Dienst bereitgestellt werden.
Art der Abhängigkeit	Nutzung der Funktionen zur Entwicklung neuer Lösungen und zur Provisionierung von Cloud-Lösungen
Standard(s), Protokoll(e)	

Tabelle 77: Diensteabhängigkeit DK Kommunikationsdienste / Cloud-Entwicklungsplattform-Dienst

Diensteabhängigkeit DK Kommunikationsdienste / Self-Service-Plattform-Dienst	
Beschreibung	**Audio-/Video-Streaming-, E-Mail-, Fax-, G2X-Kommunikations-, Telefonie-, Telefonkonferenz- und Videokonferenz-Dienst** nutzen **Self-Service-Plattform-Dienst** Die IT-Lösungen der DK Kommunikationsdienste die über die Cloud-Betriebsplattform bereitgestellt werden, nutzen für die Bestellung der Lösung durch den Anwender oder die Behörden den Self-Service-Plattform-Dienst.
Art der Abhängigkeit	Nutzung einer Bestellplattform
Standard(s), Protokoll(e)	

Tabelle 78: Diensteabhängigkeit DK Kommunikationsdienste / Self-Service-Plattform-Dienst

Diensteabhängigkeit DK Kommunikation / Service-Lifecycle-Management-Support-Dienst	
Beschreibung	**Audio-/Video-Streaming-, E-Mail-, Fax-, G2X-Kommunikations-, Telefonie-, Telefonkonferenz- und Videokonferenz-Dienst** nutzen **Service-Lifecycle-Management-Support-Dienst** Zur Dokumentation der vorhandenen Infrastruktur und zur Unterstützung von Abrechnungsprozessen für die Leistungen, die die Behörden beziehen.
Art der Abhängigkeit	Nutzung von Dokumentationsfunktionen, Abrechnungsverfahren
Standard(s), Protokoll(e)	

Tabelle 79: Diensteabhängigkeit DK Kommunikationsdienste / Service-Lifecycle-Management-Support-Dienst

Diensteabhängigkeit DK Kommunikationsdienste / Access-Management-Dienst	
Beschreibung	**Audio-/Video-Streaming-, E-Mail-, Fax-, G2X-Kommunikations-, Telefonie-, Telefonkonferenz- und Video-konferenz-Dienst** nutzen **Access-Management-Support-Dienst** Für die Anwendung von Rechten und Rollen in den Kommunikationsdiensten und für die Zuweisung dieser über automatisierte Provisionierungsverfahren in Verbindung mit dem Self-Service-Plattform-Dienst.
Art der Abhängigkeit	Zentrales Rechte- und Rollen-Management
Standard(s), Protokoll(e)	

Tabelle 80: Diensteabhängigkeit DK Kommunikationsdienste / Access-Management-Dienst

Diensteabhängigkeit DK Kommunikationsdienste / Identity-Management-Dienst	
Beschreibung	**Audio-/Video-Streaming-, E-Mail-, Fax-, G2X-Kommunikations-, Telefonie-, Telefonkonferenz- und Video-konferenz-Dienst** nutzen **Identity-Management-Dienst** Für die Bereitstellung der in den Diensten genutzten Identitäten.
Art der Abhängigkeit	Nutzung von Identitäten
Standard(s), Protokoll(e)	

Tabelle 81: Diensteabhängigkeit DK Kommunikationsdienste / Identity-Management-Dienst

Diensteabhängigkeit G2X-Kommunikations-Dienst / E-Mail-Dienst	
Beschreibung	**G2X-Kommunikations-Dienst** nutzt **E-Mail-Dienst** Der G2X-Kommunikations-Dienst nutzt den E-Mail-Dienst zum einen als Eingangs- und Ausgangskanal für die Übertragung von internen Nachrichten von und zu den Anwendern des G2X-Kommunikations-Dienstes in den Behörden. Zum anderen wird der E-Mail-Dienst für die interne Benachrichtigung der Anwender in den Behörden über den Eingang von Nachrichten auf den Intermediären des Bundes verwendet.
Art der Abhängigkeit	Nachrichtenübermittelung
Standard(s), Protokoll(e)	

Tabelle 82: Diensteabhängigkeit G2X-Kommunikations-Dienst / E-Mail-Dienst

Diensteabhängigkeit E-Mail-Dienst / Fax-Dienst	
Beschreibung	**E-Mail-Dienst** nutzt **Fax-Dienst** Der E-Mail-Dienst nutzt den Fax-Dienst für die Realisierung von E-Mail-zu-Fax-Funktionen.
Art der Abhängigkeit	Nachrichtenübermittelung
Standard(s), Protokoll(e)	

Tabelle 83: Diensteabhängigkeit E-Mail-Dienst / Fax-Dienst

Diensteabhängigkeit Fax-Dienst / E-Mail-Dienst	
Beschreibung	**Fax-Dienst** nutzt **E-Mail-Dienst** Der Fax-Dienst nutzt den E-Mail-Dienst für die Zustellung von eingehenden Fax-Nachrichten an den Adressaten per E-Mail.
Art der Abhängigkeit	Nachrichtenübermittelung
Standard(s), Protokoll(e)	

Tabelle 84: Diensteabhängigkeit Fax-Dienst / E-Mail-Dienst

Diensteabhängigkeit Telefonkonferenz-Dienst / Telefonie-Dienst	
Beschreibung	**Telefonkonferenz-Dienst** nutzt **Telefonie-Dienst** Der Telefonkonferenz-Dienst nutzt die Infrastruktur des Telefonie-Dienstes für den Aufbau von Telefonkonferenzen.
Art der Abhängigkeit	Nutzung von Infrastrukturdiensten
Standard(s), Protokoll(e)	

Tabelle 85: Diensteabhängigkeit Telefonkonferenz-Dienst / Telefonie-Dienst

Diensteabhängigkeit Videokonferenz-Dienst / Telefonie-Dienst	
Beschreibung	**Videokonferenz-Dienst** nutzt **Telefonie-Dienst** Der Videokonferenz-Dienst nutzt die Infrastruktur des Telefonie-Dienstes für den Aufbau von Videokonferenzen.
Art der Abhängigkeit	Nutzung von Infrastrukturdiensten
Standard(s), Protokoll(e)	

Tabelle 86: Diensteabhängigkeit Videokonferenz-Dienst / Telefonie-Dienst

Diensteabhängigkeit DK Druck- und Scandienste / Cloud- & Konventioneller-Betriebsplattform-Dienst	
Beschreibung	**Druck- und Scan-Dienst** nutzen **Cloud- & Konventionellen-Betriebsplattform-Dienst** Sämtliche Dienste der Diensteklasse Kommunikationsdienste nutzen die Infrastruktur der Betriebsplattformen zur Bereitstellung der IT-Lösungen.
Art der Abhängigkeit	Nutzung der Infrastruktur
Standard(s), Protokoll(e)	

Tabelle 87: Diensteabhängigkeit DK Druck- und Scandienste / Cloud- & Konventioneller-Betriebsplattform-Dienst

Diensteabhängigkeit DK Druck- und Scandienste / Cloud-Entwicklungsplattform-Dienst	
Beschreibung	**Druck- und Scan-Dienste** nutzen **Cloud-Entwicklungssplattform-Dienst** Die IT-Lösungen aus der Diensteklasse der Druck- und Scandienste, die auf der Cloud-Betriebsplattform implementiert werden, nutzen zum einen für die Entwicklung der IT-Lösung, als auch für die Provisionierung der fertigen IT-Lösung, die Funktionen, die über den Cloud-Entwicklungsplattform-Dienst bereitgestellt werden.
Art der Abhängigkeit	Nutzung der Funktionen zur Entwicklung neuer Lösungen und zur Provisionierung von Cloud-Lösungen
Standard(s), Protokoll(e)	

Tabelle 88: Diensteabhängigkeit DK Druck- und Scandienste / Cloud-Entwicklungsplattform-Dienst

Diensteabhängigkeit DK Druck- und Scandienste / Self-Service-Plattform-Dienst	
Beschreibung	**Druck- und Scandienste** nutzen **Self-Service-Plattform-Dienst** Die IT-Lösungen, die über die Cloud-Betriebsplattform bereitgestellt werden, nutzen für die Bestellung der Lösung durch den Anwender oder die Behörden den Self-Service-Plattform-Dienst.
Art der Abhängigkeit	Nutzung einer Bestellplattform
Standard(s), Protokoll(e)	

Tabelle 89: Diensteabhängigkeit DK Druck- und Scandienste / Self-Service-Plattform-Dienst

Diensteabhängigkeit Druckdienst / Hardware-Token-Dienst	
Beschreibung	**Druck-Dienst** nutzt **Hardware-Token-Dienst** Freigabe der Druckaufträge am Drucker durch die Authentifizierung am Gerät mit dem Dienstausweis.
Art der Abhängigkeit	Authentifizierung am Drucker
Standard(s), Protokoll(e)	

Tabelle 90: Diensteabhängigkeit Druck-Dienst und Hardware-Token-Dienst

Diensteabhängigkeit Hardware-Token-Dienst / Self-Service-Plattform-Dienst	
Beschreibung	**Hardware-Token-Dienst** nutzt **Self-Service-Plattform-Dienst** Implementierung des Zugriffs auf die CMS-Funktionalitäten, Beantragung von zusätzlichen Funktionen – Sperren des Dienstausweises, etc.
Art der Abhängigkeit	Zugriff
Standard(s), Protokoll(e)	

Tabelle 91: Diensteabhängigkeit Hardware-Token-Dienst und Self-Service-Plattform-Dienst

Diensteabhängigkeit DK Druck- und Scandienste / Service-Lifecycle-Management-Support-Dienst	
Beschreibung	**Druck- und Scandienste** nutzen **Service-Lifecycle-Management-Support-Dienst** Zur Dokumentation der vorhandenen Infrastruktur und zur Unterstützung von Abrechnungsprozessen für die Leistungen, die die Behörden beziehen.
Art der Abhängigkeit	Nutzung von Dokumentationsfunktionen, Abrechnungsverfahren
Standard(s), Protokoll(e)	

Tabelle 92: Diensteabhängigkeit DK Druck- und Scandienste / Service-Lifecycle-Management-Support-Dienst

Diensteabhängigkeit DK Druck- und Scandienste / Access-Management-Dienst	
Beschreibung	**Druck- und Scandienste** nutzen **Access-Management -Dienst** Für die Anwendung der DK Druck- und Scandienste, die Rechte und Rollen nutzen, wird der Access-Management-Dienst für die Zuweisung dieser über automatisierte Provisionierungsverfahren in Verbindung mit dem Self-Service-Plattform-Dienst verwendet.
Art der Abhängigkeit	Zentrales Rechte- und Rollen-Management

Standard(s), Protokoll(e)	

Tabelle 93: Diensteabhängigkeit DK Druck- und Scandienste / Access-Management-Dienst

Diensteabhängigkeit DK Druck- und Scandienste / Identity-Management-Dienst	
Beschreibung	**Druck- und Scandienste** nutzen **Identity-Management-Dienst** Für die Anwendung im Druck- und Scan-Dienst, die Identitäten nutzen, werden diese über den Identity-Management-Dienst zur Verfügung gestellt.
Art der Abhängigkeit	Nutzung von Identitäten
Standard(s), Protokoll(e)	

Tabelle 94: Diensteabhängigkeit DK Druck- und Scandienste / Identity-Management-Dienst

Diensteabhängigkeit DK Druck- und Scandienste / Arbeitsplatz-PC-Dienst	
Beschreibung	**Druck- und Scandienste** nutzen **Arbeitsplatz-PC-Dienst** Der Arbeitsplatz-PC-Dienst stellt den Nutzern Gruppenablagen für Dateien zur Verfügung. Diese können durch die Druck- und Scandienste für die Ablage von Scan-Produkten oder von über den Druck-Dienst erzeugten PDF-Ausgabedokumenten verwendet werden.
Art der Abhängigkeit	Nutzung von Gruppenablagen
Standard(s), Protokoll(e)	

Tabelle 95: Diensteabhängigkeit DK Druck- und Scandienste / Arbeitsplatz-PC-Dienst

Diensteabhängigkeit Scan-Dienst / E-Mail-Dienst	
Beschreibung	**Scan-Dienst** nutzt **E-Mail-Dienst** Der Scan-Dienst nutzt den E-Mail-Dienst für die Zustellung von Scan-Produkten an einen E-Mail-Adressaten.
Art der Abhängigkeit	Nutzung von E-Mail
Standard(s), Protokoll(e)	

Tabelle 96: Diensteabhängigkeit DK Druck- und Scan-Dienst / E-Mail-Dienst

Diensteabhängigkeit Scan-Dienst / Fax-Dienst	
Beschreibung	**Scan-Dienst** nutzen **Fax-Dienst** Der Scan-Dienst nutzt den Fax-Dienst für die Zustellung von Scan-Produkten an einen Fax-Adressaten.

Art der Abhängigkeit	Nutzung von E-Mail
Standard(s), Protokoll(e)	

Tabelle 97: Diensteabhängigkeit Scan-Dienst / Fax-Dienst

Diensteabhängigkeit DK Clientdienste / DK Netzdienste	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **DK Netzdienste** Die Clientdienste nutzen die Netzdienste zum einen als Infrastruktur für die Vernetzung mit den IT-Lösungen in den Rechenzentren, als auch zur Anbindung von mobilen Clients. Des Weiteren werden die Funktionen der netznahen Services z.B. für die Namensauflösung, zur Absicherung von Netzverbindungen genutzt.
Art der Abhängigkeit	Nutzung der Netz-Infrastruktur, Nutzung von netznahen Diensten
Standard(s), Protokoll(e)	

Tabelle 98: Diensteabhängigkeit DK Clientdienste / DK Netzdienste

Diensteabhängigkeit DK Clientdienste / Cloud- & Konventioneller-Betriebsplattform-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Cloud- & Konventionellen-Betriebsplattform-Dienst** Sämtliche Dienste der Diensteklasse Kommunikationsdienste nutzen die Infrastruktur der Betriebsplattformen zur Abbildung der IT-Lösungen in der Diensteklasse der Clientdienste.
Art der Abhängigkeit	Nutzung der Infrastruktur
Standard(s), Protokoll(e)	

Tabelle 99: Diensteabhängigkeit DK Clientdienste / Cloud- & Konventioneller-Betriebsplattform-Dienst

Diensteabhängigkeit DK Clientdienste / Cloud-Entwicklungsplattform-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Cloud-Entwicklungsplattform-Dienst** Die IT-Lösungen aus der Diensteklasse der Clientdienste, die auf der Cloud-Betriebsplattform implementiert werden, nutzen zum einen für die Entwicklung der IT-Lösung, als auch für die Provisionierung der fertigen IT-Lösung, die Funktionen, die über den Cloud-Entwicklungsplattform-Dienst bereitgestellt werden.
Art der Abhängigkeit	Nutzung der Funktionen zur Entwicklung neuer Lösungen und zur Provisionierung von Cloud-Lösungen

Standard(s), Protokoll(e)	

Tabelle 100: Diensteabhängigkeit DK Clientdienste / Cloud-Entwicklungsplattform-Dienst

Diensteabhängigkeit DK Clientdienste / Self-Service-Plattform-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Self-Service-Plattform-Dienst** Die Bestellung von Anwendungen auf den Clients erfolgt über den Self-Service-Plattform-Dienst. Dort können die Nutzer zur Ergänzung ihrer IT-Arbeitsplätze die angebotenen Leistungen buchen.
Art der Abhängigkeit	Nutzung einer Bestellplattform
Standard(s), Protokoll(e)	

Tabelle 101: Diensteabhängigkeit DK Clientdienste / Self-Service-Plattform-Dienst

Diensteabhängigkeit DK Clientdienste / Service-Lifecycle-Management-Support-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Service-Lifecycle-Management-Support-Dienst** Zur Dokumentation der vorhandenen Infrastruktur und zur Unterstützung von Abrechnungsprozessen für die Leistungen, die die Behörden beziehen.
Art der Abhängigkeit	Nutzung von Dokumentationsfunktionen, , Abrechnungsverfahren
Standard(s), Protokoll(e)	

Tabelle 102: Diensteabhängigkeit DK Clientdienste / Service-Lifecycle-Management-Support-Dienst

Diensteabhängigkeit DK Clientdienste / Access-Management-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Access-Management-Support-Dienst** Für die Anwendung von Rechten und Rollen in den Clientdiensten und für die Zuweisung dieser über automatisierte Provisionierungsverfahren in Verbindung mit dem Self-Service-Plattform-Dienst.
Art der Abhängigkeit	Zentrales Rechte- und Rollen-Management
Standard(s), Protokoll(e)	

Tabelle 103: Diensteabhängigkeit DK Clientdienste / Access-Management-Dienst

Diensteabhängigkeit DK Clientdienste / Identity-Management-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Identity-Management-Dienst** Für die Bereitstellung der in den Diensten genutzten Identitäten.
Art der Abhängigkeit	Nutzung von Identitäten
Standard(s), Protokoll(e)	

Tabelle 104: Diensteabhängigkeit DK Clientdienste / Identity-Management-Dienst

Diensteabhängigkeit DK Clientdienste / PKI-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **PKI-Dienst** Die Clientdienste verwenden den PKI-Dienst für den Abruf von zentral gespeicherten Zertifikaten sowie zur Prüfung der Gültigkeit von Zertifikaten. Diese werden für gesicherte Anmeldungen an Client-Geräten, für die Signierung und Verschlüsselung von Daten sowie für die Absicherung von Kommunikationskanälen verwendet.
Art der Abhängigkeit	Nutzung von elektronischen Zertifikaten
Standard(s), Protokoll(e)	

Tabelle 105: Diensteabhängigkeit DK Clientdienste / PKI-Dienst

Diensteabhängigkeit DK Clientdienste / Hardware-Token-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Hardware-Token-Dienst** Die Clientdienste nutzen den Hardware-Token-Dienst in Verbindung mit einer 2-Faktor-Anmeldung am IT-Arbeitsplatz sowie für den Abruf dort gespeicherter personenbezogener Zertifikate für die Signierung und Verschlüsselung von Daten.
Art der Abhängigkeit	Nutzung von elektronischen Zertifikaten
Standard(s), Protokoll(e)	

Tabelle 106: Diensteabhängigkeit DK Clientdienste / Hardware-Token-Dienst

Diensteabhängigkeit Mobiles-Gerät-Dienst / Arbeitsplatz-PC-Dienst	
Beschreibung	**Mobiles-Gerät-Dienst** nutzt **Arbeitsplatz-PC-Dienst** Der Mobiles-Gerät-Dienst nutzt Infrastruktur, die für die Nutzer des Arbeitsplatz-PC-Dienstes bereitgestellt werden. Dazu gehören z.B. Gruppenablagen und andere Services, die allgemein von den IT-Arbeitsplätzen unabhängig von der jeweils genutzten Geräteklasse verwendet werden können.
Art der Abhängigkeit	Datenspeicherung, etc.
Standard(s), Protokoll(e)	

Tabelle 107: Diensteabhängigkeit Mobiles-Gerät-Dienst / Arbeitsplatz-PC-Dienst

Diensteabhängigkeit Ultra-Mobiles-Gerät-Dienst / Arbeitsplatz-PC-Dienst	
Beschreibung	**Ultra-Mobiles-Gerät-Dienst** nutzt **Arbeitsplatz-PC-Dienst** Der Ultra-Mobiles-Gerät-Dienst nutzt Infrastruktur, die für die Nutzer des Arbeitsplatz-PC-Dienstes bereitgestellt werden. Dazu gehören z.B. Gruppenablagen und andere Services, die allgemein von den IT-Arbeitsplätzen unabhängig von der jeweils genutzten Geräteklasse verwendet werden können.
Art der Abhängigkeit	Datenspeicherung, etc.
Standard(s), Protokoll(e)	

Tabelle 108: Diensteabhängigkeit Ultra-Mobiles-Gerät-Dienst / Arbeitsplatz-PC-Dienst

Diensteabhängigkeit DK Clientdienste / Audio-,Video-Streaming-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Audio-/Video-Streaming-Dienst** Die Clientdienste nutzen den Audio-/Video-Streaming-Dienst als Quelle für Audio- und Videodaten, die am IT-Arbeitsplatz angezeigt werden können.
Art der Abhängigkeit	Nachrichtenübermittlung
Standard(s), Protokoll(e)	

Tabelle 109: Diensteabhängigkeit DK Clientdienste / Audio-,Video-Streaming-Dienst

Diensteabhängigkeit DK Clientdienste / E-Mail-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **E-Mail-Dienst** Die Clientdienste nutzen den E-Mail-Dienst für die Übermittlung von Nachrichten innerhalb und außerhalb der Bundesbehörden.

Art der Abhängigkeit	Nachrichtenübermittlung
Standard(s), Protokoll(e)	

Tabelle 110: Diensteabhängigkeit DK Clientdienste / E-Mail-Dienst

Diensteabhängigkeit DK Clientdienste / Fax-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Fax-Dienst** Die Clientdienste nutzen den Fax-Dienst für den Versand und Empfang von Fax-Nachrichten am IT-Arbeitsplatz.
Art der Abhängigkeit	Nachrichtenübermittlung
Standard(s), Protokoll(e)	

Tabelle 111: Diensteabhängigkeit DK Clientdienste / Fax-Dienst

Diensteabhängigkeit DK Clientdienste / G2X-Kommunikations-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **G2X-Kommunikations-Dienst** Die Clientdienste nutzen den G2X-Kommuikations-Dienst für die rechtskonforme Nachrichtenübermittlung z.B. im elektronischen Rechtsverkehr.
Art der Abhängigkeit	Nachrichtenübermittlung
Standard(s), Protokoll(e)	

Tabelle 112: Diensteabhängigkeit DK Clientdienste / G2X-Kommunikations-Dienst

Diensteabhängigkeit DK Clientdienste / Telefonie-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Telefonie-Dienst** Die Clientdienste nutzen den Telefonie-Dienst für die Nutzung softwarebasierten Telefonieanwendungen am IT-Arbeitsplatz.
Art der Abhängigkeit	Nachrichtenübermittlung
Standard(s), Protokoll(e)	

Tabelle 113: Diensteabhängigkeit DK Clientdienste / Telefonie-Dienst

Diensteabhängigkeit DK Clientdienste / Telefonkonferenz-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Telefonkonferenz-Dienst** Die Clientdienste nutzen den Telefonkonferenz-Dienst für die Nutzung softwarebasierter Telefonkonferenzlösungen am IT-Arbeitsplatz.
Art der Abhängigkeit	Nachrichtenübermittlung
Standard(s), Protokoll(e)	

Tabelle 114: Diensteabhängigkeit DK Clientdienste / Telefonkonferenz-Dienst

Diensteabhängigkeit DK Clientdienste / Videokonferenz-Dienst	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Videokonferenz -Dienst** Die Clientdienste nutzen den Videokonferenz-Dienst für die Nutzung softwarebasierter Videokonferenzlösungen am IT-Arbeitsplatz.
Art der Abhängigkeit	Nachrichtenübermittlung
Standard(s), Protokoll(e)	

Tabelle 115: Diensteabhängigkeit DK Clientdienste / Videokonferenz-Dienst

Diensteabhängigkeit DK Clientdienste / Domänen und Fachdienste	
Beschreibung	**Arbeitsplatz-PC-, Mobiles-Gerät-, Ultra-Mobiles-Gerät-Dienst** nutzen **Domänen und Fachdienste** Die Clientdienste nutzen die Domänen und Fachdienste für die Anbindung der Anwendungen auf dem IT-Arbeitsplatz an die Backend-Infrastruktur, die von den Diensten der Domänen und Fachdienste bereitgestellt werden.
Art der Abhängigkeit	Datenaustausch
Standard(s), Protokoll(e)	

Tabelle 116: Diensteabhängigkeit DK Clientdienste / Domänen und Fachdienste

5 Anhang Verzeichnisse

5.1 Abbildungsverzeichnis

5.2 Tabellenverzeichnis

5.3 Quellenverzeichnis

[1.] Bundesministerium des Inneren, „Strategie Dienstekonsolidierung 2018-2025“, Beschluss Nr.: 2018/3 des IT-Rats vom 24. Januar 2018, Berlin 2018

[2.] Bundesministerium des Inneren, für Bau und Heimat, „Rahmendokument für die Domänenarchitekturen“, Berlin 2019

Impressum

Herausgeber
Der Beauftragte der Bundesregierung für Informationstechnik, 10557 Berlin

Ansprechpartner
Arbeitsgruppe DG I 5 - Dienstekonsolidierung
Postanschrift: Alt-Moabit 140, 10557 Berlin
Hausanschrift: Bundesallee 216-218, 10719 Berlin
E-Mail: DGI5AG@bmi.bund.de
Internet: www.cio.bund.de

Stand
Mai 2019

Bildnachweis
JamesBrey / GettyImages

www.cio.bund.de