IT-Planungsrat

Digitale Zukunft gestalten

Anforderungen an ein Unternehmenskonto/en

Ergebnisse Workshop PG eID-Strategie vom 20/21.03.2019

Stand: 05.04.2019

Inhaltsverzeichnis

1 Einleitung

Der IT-Planungsrat hat in seinen Sitzungen am 25.10.2018 und am 12.03.2019 folgende Beschlüsse mit dem Kontext Unternehmenskonten getroffen:

- **Entscheidung 2018/41 - eID-Strategie:** In einem ersten Schritt erfolgt die Herstellung der Interoperabilität der Service/Nutzerkonten.
- **Entscheidung 2018/40 – Portalverbund:** Der IT-Planungsrat beschließt die folgenden Kriterien, die stufenweise bis 2022 zu erfüllen sind: Jedes am Verbund teilnehmende Verwaltungsportal muss als Ziel mindestens Funktionen zu folgenden Diensten bereitstellen:
    - ein interoperables Nutzerkonto für natürliche Personen und Organisationen
    - eine marktübliche elektronische Bezahlmöglichkeit
    - ein Postfach
- **Entscheidung 2019/02 – Unternehmenskonto:**
    1. Der IT-Planungsrat richtet ein länderoffenes Koordinierungsprojekt „Unternehmenskonto/-en“ unter der Federführung Bremens und unter Beteiligung des Bundes sowie der Länder Hessen, Bayern, Hamburg, Baden-Württemberg, Rheinland-Pfalz, und Nordrhein-Westfalen ein.
    2. Der IT-Planungsrat bittet das Koordinierungsprojekt „Unternehmenskonto/-en“ unter Einbindung der Ergebnisse des Workshops der PG eID-Strategie am 20./21. März 2019 die Anforderungen der Unternehmen an ein Unternehmenskonto/-en zu definieren und diese Bedarfe mit den bestehenden Lösungen aus der Wirtschaft und der öffentlichen Verwaltung abzugleichen.
    3. Der IT-Planungsrat bittet darum, ihm zur 29. Sitzung einen beschlussreifen Vorschlag zur weiteren Vorgehensweise vorzulegen.

Die PG eID-Strategie hat im Rahmen dieser Beschlussfassung auf Ihrem Workshop am 20./21. März 2019 zur weiteren Ausgestaltung von Nutzerkonten den Bereich Unternehmenskonten als Schwerpunkt festgelegt und im Workshop Anforderungen an Unternehmenskonten definiert, unabhängig von der Fragestellung, ob zukünftig ein zentrales Unternehmenskonto oder interoperable Unternehmenskonten umgesetzt werden sollen.

Gegenstand des Workshops war es dagegen nicht, eine Entscheidung des IT-Planungsrates vorzubereiten, ob es künftig ein oder mehrere Unternehmenskonten geben soll.

Die in diesem Papier beschriebenen Anforderungen basieren u.a. auf den bisherigen Dokumenten der PG eID-Strategie zur Interoperabilität:

- Eckpunktepapier „Interoperables Identitätsmanagement von Servicekonten für Bürgerinnen, Bürger und Unternehmen“ Stand: 29.06.2016
- Rechtliche Rahmenbedingungen für interoperable Servicekonten, Stand: 29.06.2016
- Entschließung Datenschutz Servicekonten, Stand 06.04.2016
- Anforderungen Interoperabilität Servicekonten Unternehmen, Stand: 21.12.2016
- Anforderungen Interoperabilität Servicekonten Postfächer, Stand: 08.02.2017

Weiterhin wurden die Anforderungen auf Basis einführender Vorträge folgender Länder und deren IT-Dienstleister zu bereits bestehenden Unternehmenskonten erarbeitet:

- Baden-Württemberg und Sachsen mit Seitenbau
- Bayern, Hessen und Bund mit AKDB
- Hamburg, Schleswig-Holstein, Sachsen-Anhalt und Berlin mit Dataport
- Nordrhein-Westfalen mit Governikus
- Rheinland-Pfalz mit KommWis

Die in diesem Papier definierten Anforderungen sind als gemeinsam von der PG eID-Strategie abgestimmte Eckpunkte für die weitere Ausgestaltung von einem oder mehreren interoperablen Unternehmenskonten zu verstehen.

Entgegen den bei der Formulierung von Anforderungen für Softwaresystemen üblichen Gebrauch von Modalverben wird hier der juristische Gebrauch verwendet. Kann-Formulierungen stellen also eine Ermächtigung dar und haben die Bedeutung von „darf“.

Generell ist festzustellen, dass Kann-Anforderungen in der Regel für ein zentrales Organisationskonto eine Muss-Anforderung darstellen, für interoperable Nutzerkonten allerdings nur eine Kann-Anforderung.

Die Länder haben die Hoheit über die Ausgestaltung der Nutzerkonten in Ihrem Bereich. Die Ausgestaltung der Ländernutzerkonten erfolgt gemäß den Anforderungen der rechtlichen und fachlichen Gegebenheiten der Länder. Bei einer zentralen Lösung ist die Vereinigungsmenge aller Anforderungen verpflichtend umzusetzen.

2 Grundsätzliche Anforderungen zur Ausgestaltung von Unternehmenskonten

Die PG eID-Strategie hat in Ihrem Workshop vom 20./21.03.19 vorab Festlegungen definiert, die grundsätzlich bei der weiteren Ausgestaltung eines oder mehrerer Unternehmenskonten berücksichtigt werden sollen:

- Ein Nutzerkonto ist kein einheitlicher Zugang zu Verwaltungsleistungen, sondern eine Identifizierungskomponente.
- Davon abzugrenzen ist der einheitliche Zugang zu Verwaltungsleistungen, der über den Portalverbund sichergestellt wird (einschließlich EA 2.0, SDG).
- Ein Nutzerkonto muss neben der Identifizierung und Authentifizierung weitere Funktionalitäten berücksichtigen, wie z.B. ein Postfach, über das Bescheide oder Statusmeldungen übermittelt werden können (s. OZG § 8 Abs. 3).
- Im Rahmen der Interoperabilität besteht die Möglichkeit, dass sich ein Unternehmen mit nur einem Organisationskonto bei allen Verwaltungsleistungen identifizieren kann.
- Zur Berücksichtigung der Nutzerfreundlichkeit sind bei der weiteren Gestaltung die Interessen der Wirtschaft entscheidend.

- Darüber hinaus sind die Anforderungen von Fachverfahren an Nutzerkonten zu beachten.

3 Anforderungscluster Begriffsbestimmung

Hinweis: Die PG eID-Strategie hat sich dafür ausgesprochen, Unternehmenskonten zukünftig als Organisationskonten zu bezeichnen.

Erläuterung: Im Sinne der übergreifenden Betrachtung ist nicht nur das Unternehmenskonto mit seiner Registrierung, sondern ganz allgemein auch bei Organisationen (Vereine, Verbände, Kirchen, Parteien und Gewerkschaften, …) von einem allgemeinen Organisationskonto auszugehen. Dahingehend wird bei den Dokumenten nunmehr auf den Begriff Organisationskonto zurückgegriffen.

Anforderung 1: Organisationskonten können nicht nur Unternehmen eröffnen und nutzen, sondern auch weitere Organisationen, wie z.B. Vereine, Stiftungen oder Behörden.

Anforderung 2: Eine Auflistung möglicher nationaler Organisationen enthält die Technische Richtlinie TR 01201 „De-Mail Accountmanagement, Funktionalitätsspezifikation“. Es ist eine Stelle zu benennen, die eine Codeliste möglicher zu nutzender Organisationen initiiert und zukünftig pflegt. Diese Liste muss auch alle möglichen Institutionen im Kontext der eIDAS-Verordnung berücksichtigen, wie z.B. Ltd und SE. Darüber hinaus können auch Organisationen von außerhalb der EU (z.B. Schweiz) sich ein Organisationskonto in Deutschland zulegen. Daher ist mindestens die Angabe „sonstiges“ notwendig.

Eine derartige Liste existiert bereits, siehe: https://www.xrepository.de/details/urn:xoev-de:xgewerbeanzeige:codeliste:rechtsformen. Ltd und SE sind enthalten. Die Liste wird von der KoSIT gepflegt.

4 Anforderungscluster Freiwilligkeit

Anforderung 3: Eröffnung und Nutzung eines permanenten Nutzerkontos, in dem Daten zur Organisation und zum Nutzer dauerhaft gespeichert werden können, sind freiwillig.

Anforderung 4: Die einmalige Inanspruchnahme von Verwaltungsdienstleistungen muss auch ohne dauerhafte Speicherung der Daten möglich sein.

5 Anforderungscluster Vertrauensniveaus und Identifizierungsmittel

Anforderung 5: Die Nutzung von Organisationskonten für Organisationen steht in Abhängigkeit zum Vertrauensniveau der konkreten Verwaltungsleistung. Die in der Richtlinie TR 03107 „Elektronische Identitäten und Vertrauensdienste im E-Government“ (Version 1.1 vom 31.10.2016) und der eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste festgelegten Vertrauensniveaus sind zu berücksichtigen.

Im Zuge der weiteren Umsetzung des OZG sind die Vertrauensniveaus durch die Fachseite für die Verwaltungsleistungen festzulegen. Grundsätzlich soll das Fachrecht das Vertrauensniveau der Verwaltungsleistung definieren. Grundlage ist die Handreichung des IT-Planungsrates mit Empfehlungen für die Zuordnung von Vertrauensniveaus in der Kommunikation zwischen Verwaltung und Bürgerinnen und Bürger bzw. der Wirtschaft.

Hierbei ist zwingend das von der Fachseite festgelegte Vertrauensniveau in einem der Bausteine von FIM zu verorten.

Anforderung 6: Das jeweilige Vertrauensniveau einer Verwaltungsleistung bestimmt wiederum den Einsatz der Identifizierungsmittel.

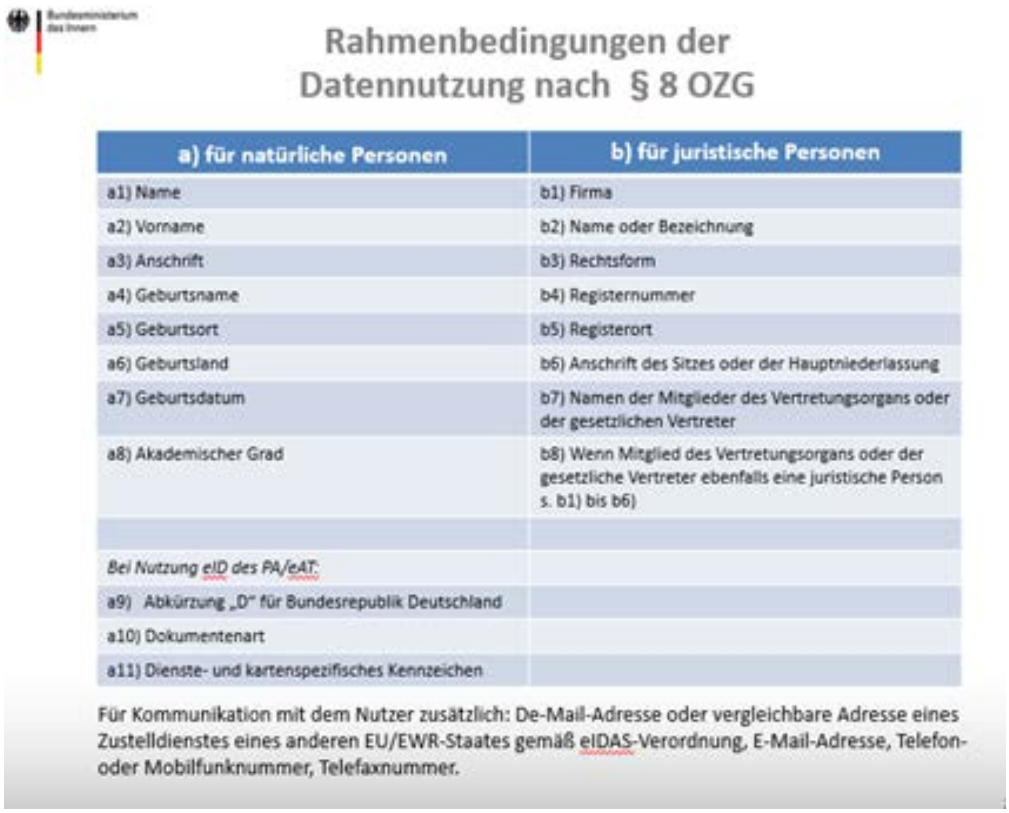
Anforderung 7: Welche Identifizierungsmittel, neben den bereits bestehenden, zum Einsatz kommen, entscheiden die Länder auf Grundlage einer Empfehlung des BSI. Dabei sind die Vorgaben der eIDAS-Verordnung zu berücksichtigen.

Anforderung 8: Für die Nutzung von Verwaltungsleistungen melden sich Nutzer am Nutzerkonto mit einem Identifizierungsmittel an (sofern sich die Nutzer nicht für die einmalige Inanspruchnahme von Verwaltungsleistungen ohne Datenspeicherung entscheiden, vgl. Anforderung 4 und 9), das mindestens dem von der Verwaltungsleistung geforderten Vertrauensniveau entspricht.

Anforderung 9: Außerhalb des Nutzerkontos ist eine anonyme Nutzung von Verwaltungsleistungen möglich.

6 Anforderungscluster Datennutzung

Anforderung 10: Nach OZG dürfen folgende Daten für natürliche bzw. juristische Personen im Nutzerkonto gespeichert werden:



Rahmenbedingungen der Datennutzung nach § 8 OZG

a) für natürliche Personen	b) für juristische Personen
a1) Name	b1) Firma
a2) Vorname	b2) Name oder Bezeichnung
a3) Anschrift	b3) Rechtsform
a4) Geburtsname	b4) Registernummer
a5) Geburtsort	b5) Registerort
a6) Geburtsland	b6) Anschrift des Sitzes oder der Hauptniederlassung
a7) Geburtsdatum	b7) Namen der Mitglieder des Vertretungsorgans oder der gesetzlichen Vertreter
a8) Akademischer Grad	b8) Wenn Mitglied des Vertretungsorgans oder der gesetzliche Vertreter ebenfalls eine juristische Person s. b1) bis b6)
Bei Nutzung eID des PA/eAT:	
a9) Abkürzung „D" für Bundesrepublik Deutschland	
a10) Dokumentenart	
a11) Dienste- und kartenspezifisches Kennzeichen	

Für Kommunikation mit dem Nutzer zusätzlich: De-Mail-Adresse oder vergleichbare Adresse eines Zustelldienstes eines anderen EU/EWR-Staates gemäß eIDAS-Verordnung, E-Mail-Adresse, Telefon- oder Mobilfunknummer, Telefaxnummer.

Den Ländern steht es jedoch frei, in Ihrem Bereich über Landesgesetze die Rechtsgrundlage zur Verarbeitung weiterer Daten in ihren Nutzerkonten zu schaffen.

Anforderung 11: Folgende weitere Daten sollen zukünftig Berücksichtigung finden:

Für natürliche Personen:

- Staatsangehörigkeit
- Postkorb-Referenz (handelnde Personen)

Für juristische Personen:

- Registergericht
- Registerart
- Postkorb-Referenz

Es müssen zwingend die Daten der notifizierten eID-Systeme im eIDAS-Kontext erfasst werden können. Die Anerkennungspflicht für die ersten Staaten greift ab dem 29.08.19. Diese Daten müssen auch an die Fachprozesse übergeben werden und in der Interoperabilität Berücksichtigung finden. Es kann z.B. vorkommen, dass keine Adresse geliefert wird, dafür aber das Geschlecht. Auch alle angeschlossenen Fachverfahren müssen darauf vorbereitet sein.

7 Anforderungscluster Rollen und Berechtigungen

Anforderung 12: Im Organisationskonto handeln natürliche Personen für eine Organisation.

Anforderung 13: Im Organisationskonto gibt es grundsätzlich Rollen (z.B. Admin und Nutzer), um zu gewährleisten, dass nur berechtigte Nutzer neue Nutzer zu einem Organisationskonto anlegen und bearbeiten können.

Anforderung 14: Das Organisationskonto kann vom Admin und weiteren berechtigten Personen nach vorherigem Log-In an deren persönlichen Nutzerkonten für Bürger genutzt werden.

Anforderung 15: Bei Nutzung eines Organisationskontos muss eindeutig nachvollziehbar sein, welche natürliche Person für die Organisation im Rahmen der Inanspruchnahme einer Verwaltungsdienstleistung handelt, falls die Verwaltungsleistung eine Identifizierung fordert (s. § 12 VwVfG).

Anforderung 16: Organisationskonten können grundsätzlich von mehreren Mitarbeitern der Organisation genutzt werden.

Anforderung 17: Organisationskonten sind von den dazu berechtigten Personen zu eröffnen und zu verwalten. Vertretungsberechtigt für Organisationen sind Personen, die in den organisationsspezifischen Nachweisen zur Existenz der Organisation als vertretungsberechtigt benannt sind (z.B. Geschäftsführer eines Unternehmens im Handelsregister) bzw. Personen die von diesen über ihre internen Organisationsprozesse zur Vertretung der Organisation bevollmächtigt wurden. Die für die Organisation zur Eröffnung eines Organisationskontos vertretungsberechtigte Person (Admin) hat die Möglichkeit, Berechtigungen für Mitarbeiterinnen und Mitarbeiter der Organisation oder auch für Personen außerhalb der Organisation anzulegen, damit diese über das Organisationskonto für die Organisation handeln können.

Die Verantwortung für das Handeln von Personen für Organisationen (und ggfls. der Nachweis der Nichtberechtigung) liegt damit auf Seiten der Organisation.

Anforderung 18: Im Organisationskonto können Berechtigungen für Mitarbeiterinnen und Mitarbeiter einer Organisation angelegt werden.

Anforderung 19: Eine berechtigte Person (z.B. Rolle Admin) administriert das Organisationskonto. Die Administration umfasst:

- Eintragen, Ändern, Löschen von Daten zur Organisation
- Anlegen und Löschen von Stellvertretern mit den gleichen administrativen Rechten wie der Admin selbst
- Anlegen und Löschen von Nutzern, die online Verwaltungsleistungen für die Organisation nutzen

Anforderung 20: Nutzer eines Organisationskontos sind natürliche Personen, die von einer berechtigten Person (z.B. Admin) die Berechtigung erhalten haben, die Organisation über das eingerichtete Organisationskonto gegenüber einer Behörde zu vertreten. Auch die ein Organisationskonto einrichtende Person (z.B. Admin) ist berechtigt, das Organisationskonto für Verwaltungsdienstleistungen zu nutzen.

Anforderung 21: Nutzer eines Organisationskontos A können auch Mitarbeiterinnen und Mitarbeiter einer anderen Organisation mit dem Organisationskonto B sein. Dazu können Organisationskonten mit anderen Organisationskonten verknüpft werden.

Anforderung 22: Die vom Organisationskonto bereitgestellten Rollen und Berechtigungen sind von den Organisationen in unternehmerischer Selbstverantwortung eigenverantwortlich zu steuern.

Anforderung 23: Vertretungsberechtigung innerhalb eines Nutzerkontos: Jeder berechtigte Nutzer kann das vom Admin angelegte Organisationskonto für die Abwicklung von Verwaltungsleistungen nutzen. Inwieweit ein Mitarbeiter berechtigt ist, eine konkrete Verwaltungsleistung für die Organisation tatsächlich abzuwickeln, hat die Organisation intern organisatorisch zu regeln. Dafür kann das Organisationskonto technische Lösungen anbieten. Im Außenverhältnis kann jeder für ein Organisationskonto berechtigte Nutzer die Organisation gegenüber einer Behörde vertreten.

8 Anforderungscluster Registrierung

Anforderung 24: Für das Organisationskonto werden keine unterschiedlichen Vertrauensniveaus gemäß eIDAS benötigt. Die Erstanlage eines Organisationskontos (Registrierung) erfolgt ohne Berücksichtigung der Vertrauensniveaus gemäß der eIDAS-VO durch Selbstauskunft. Die eingegebenen Daten können gegen eine vertrauenswürdige Datenquelle verifiziert werden. Für die Inanspruchnahme des jeweiligen Online-Verfahrens ist die Authentifizierung der für die Organisation handelnden Person maßgeblich. Die Organisationskonten können auf verschiedenen Wegen registriert werden.

Anforderung 25: Berechtigte Personen haben die für die Inanspruchnahme der Verwaltungsleistung erforderlichen Identitätsdaten zur Organisation zu übermitteln, die für spätere Verwaltungsdienstleistungen genutzt werden sollen.

Anforderung 26: Es gibt verifizierte und nicht-verifizierte Organisationskonten. Das Eröffnen eines verifizierten Organisationskontos setzt die Verifizierung der Organisationsdaten voraus. Nicht-verifizierte Organisationkonten können in verifizierte Organisationkonten umgewandelt werden.

Anforderung 27: Die Verifizierung von Organisationen kann unter Nutzung von technischen Hilfsmitteln (z.B. Elster oder Registerzugriffe) durch Selbsterfassung oder in Registrierungsstellen (§ 7 Abs. 2 OZG) oder durch andere geeignete Verfahren erfolgen.

9 Anforderungscluster Nutzung und Löschung

Anforderung 28: Die Nutzung des Organisationskontos ist abhängig vom

- Authentifizierungsniveaus (normal, substantiell, hoch) des für die Organisation handelnden Nutzers
- Verifikationsstand des Organisationskontos

Beides gibt das Fachverfahren vor.

Anforderung 29: Im Fall von eingerichteten, aber nicht genutzten Organisationskonten kann die Löschung eines Organisationskontos nach einer vom Verordnungsgeber zu definierenden Frist durch den Anbieter des Organisationkontos erfolgen.

10 Anforderungscluster Postfach

Funktionalitäten

Anforderung 30: Das Postfach dient der Kommunikation zwischen der Verwaltung und Bürgerinnen, Bürgern und Organisationen und deren Mitarbeitern. Nutzer können auf erhaltene Nachrichten der Behörde antworten, z. B. Nachweise auf Anforderung übermitteln.

Anforderung 31: Eine Behörde kann Nachrichten an das Postfach des Organisationskontos und/oder an die zu dessen Nutzung Berechtigten versenden, z. B. Bescheide, Mitteilungen zum Verfahrensstand oder Anforderungen von Nachweisen. Die Postfachsysteme können die Annahme von Nachrichten, z.B. bei Erreichen von Speicherlimits, ablehnen. Die absendende Behörde ist darüber automatisch zu informieren (s. auch Anforderung 42). Eine Zugangseröffnung durch den Nutzer muss allerdings vorliegen.

Anforderung 32: Die Nachrichten einer Behörde werden an das ihr bekannt gegebene Postfach des Organisationskontos übermittelt.

Anforderung 33: Die Organisation kann über das Postfach ihres Organisationskontos auf eine Nachricht antworten (einschl. Freitextfeld). Der Antwort können auch Anlagen beigefügt werden, z. B. angeforderte Nachweise. Das Hochladen kann über einen lokalen Speicherort oder einer vergleichbaren Funktionalität (z.B. Dokumentensafe) erfolgen.

Anforderung 34: Um auf Nachrichten des Postfachs zugreifen zu können, hat sich der Nutzer des Organisationskontos mit dem von der Nachricht abhängigen Vertrauensniveau an

seinem Organisationskonto anzumelden, wenn die Nachricht ein entsprechendes Attribut hat.

Anforderung 35: Sofern eine Nachricht im Postfach des Organisationskontos eingegangen ist, wird der Nutzer des Organisationskontos über den Weg, den er im Organisationskonto ausgewählt hat, informiert, dass eine Nachricht zum Abruf im Postfach des Organisationskontos bereitsteht. Nach erfolgreicher Anmeldung kann der Nutzer die erhaltene Nachricht öffnen.

Anforderung 36: Es darf möglich sein, dass ein Nutzer eine Behörde über sein Postfach ohne vorherige Nachricht der Behörde aktiv anschreiben kann.

Eineindeutigkeit von Postfächern

Anforderung 37: Jedes Postfach verfügt über eine bundesweit eineindeutige Postfach-ID, über die das Postfach adressierbar ist.

Anforderung 38: Das Postfach muss eine Abrufbestätigung an die Versendebehörde versenden können, falls die Versendebehörde für diese Nachricht eine Abrufbestätigung angefordert hat.

Postfächer für Mitarbeiter von Organisationen

Anforderung 39: Im Organisationskonto können für jeden Nutzer bzw. sofern vorhanden für Organisationseinheiten eigene Postfächer bzw. Funktionspostfächer angelegt werden.

Anforderung 40: Im Hinblick auf mögliche Abwesenheiten kann ein Nutzer festlegen, dass die Nachrichten einer Behörde automatisiert an berechtigte Nutzer mit anderen Postfächern im Organisationskonto weitergeleitet werden.

Anforderung 41: Der Admin kann einen anderen Nutzer berechtigen auf ein Postfach zuzugreifen. Diese berechtigte Person (Notfallvertretung) hat das Recht, lesend auf das Postfach des Nutzers im Organisationskonto zuzugreifen.

Anforderung 42: Das empfangende Nutzerkonto (bzw. das empfangende System) muss die Möglichkeit haben, vorab definierte Fehlermeldungen zurückzuliefern, die durch das sendende Nutzerkonto entsprechend verarbeitet werden können müssen. Beispiele für Fehlermeldungen sind (analog „normalen E-Mail-Systemen“):

- Postfach des empfangenen Nutzerkontos voll / Quota erreicht
- Nutzerkonto gelöscht / nicht mehr verfügbar

11 Anforderungscluster Querschnittsthemen

Protokollierung

Anforderung 43:

Zugriffe und Zugriffsberechtigungen auf das Organisationskonto und dessen Postfach sind so zu protokollieren, dass die notwendige Transparenz über die Berechtigungen entsteht und missbräuchliche Zugriffe erkannt werden können (Aufbewahrungsfrist – gesetzliche Regelung). Die rechtlichen Grundlagen einer Protokollierung sind noch festzulegen.

Mehrsprachigkeit

Anforderung 44:

Das Organisationskonto sollte mehrsprachig angeboten werden, mindestens in englischer Sprache.

12 Empfehlungen der PG eID-Strategie

- Bei der weiteren Konzeption und Umsetzung ist die Herstellung einer Anwendungs- und Betriebsbereitschaft inkl. Finanzierungsmodell zu berücksichtigen (Option: Anwendung des IT-Planungsrats), sowohl für die Herstellung der Schnittstellen und Komponenten zur Interoperabilität von Organisationskonten als auch für ein zentrales Organisationskonto.

- Die Investitionen in bestehende Lösungen von Nutzerkonten in den Ländern und auch bei einzelnen Fachverfahren (z.B. Elster) sind zu schützen.

- Rechte und Rollen sind in der Interoperabilität nicht verpflichtend. Eine Nutzung von Rechten und Rollen ist auf freiwilliger Basis allerdings möglich. In einer weiteren Ausbauphase der Interoperabilität können Rechte und Rollen berücksichtigt werden, so dass Nutzerkonten Rechte und Rollen gemäß eines Standards austauschen können. Es muss allerdings die Möglichkeit, auch ohne Rechte und Rollen an der Interoperabilität teilzunehmen, bestehen bleiben.

- Neben den funktionalen Anforderungen sind weiterhin technische Aspekte zu berücksichtigen, u.a.:
    - Servergröße (im Hinblick auf Postfach, Dokumentenablage)
    - Netzleitungen
    - Ausfallsicherheit
    - Back-Up
    - Datensicherung
    - Weitere Fragen zum Betrieb

- Beim Ansatz eines zentralen Organisationskontos werden insbesondere folgende Punkte als kritisch betrachtet:

    - Pflege mehrerer Schnittstellen pro Verwaltungsleistung für dezentrale Bürgerkonten und zentrale Organisationskonten
    - Agilität der Softwareentwicklung: bei dezentralen Organisationskonten ist es einfacher, auf länderspezifische oder kommunalspezifische Anforderungen einzugehen (s. auch in Bezug auf Landesrecht)
    - Regionale Besonderheiten und Anforderungen der bestehenden Unternehmenskonten der Länder sind zwingend zu berücksichtigen
    - Verfügbarkeit im Kontext OZG-Umsetzung 2022 bei zentralen Organisationskonten fraglich
    - Aus datenschutzrechtlicher Sicht sieht der BfDI ein zentrales Unternehmenskonto kritisch.