POSITIONSPAPIER

Interoperable Postfächer und Servicekonten

Vitako-Position zur Konzeption von interoperablen Postfächern und Servicekonten

Stand: 14. Januar 2019

VITAKO
Bundes-Arbeitsgemeinschaft der
Kommunalen IT-Dienstleister e.V.

Zur Konzeption von interoperablen Postfächern und Servicekonten

- Vitako-Position zum Servicekonto und zu Postfächern -

1. Servicekonto

Motivation und Begriffsklärung

Das Onlinezugangsgesetz (OZG) sieht für die Digitalisierung der Verwaltung einen ambitionierten Zeitplan vor: Bis 2022 müssen die Verwaltungsleistungen von Bund und Ländern auch elektronisch über Verwaltungsportale angeboten werden. Für die Nutzung der Leistungen sind von Bund und Ländern Nutzerkonten bereitzustellen, „über die sich Nutzer für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich identifizieren können."[1] Die Leistungen der Länder und des Bundes sollen in Portalen verbunden und die einzelnen Portale wiederum über einen Gesamtverbund (Portalverbund) logisch und technisch miteinander verknüpft werden. Sicherzustellen ist dabei, dass mit jedem Nutzerkonto jede Verwaltungsleistung nutzbar ist. Hierzu müssen die dem Verbund angehörigen Nutzerkonten kompatibel (fortan: interoperabel) sein.

Zum Kreis der Nutzer von Leistungen zählt das OZG neben Bürgerinnen und Bürgern ausdrücklich auch Unternehmen. Genau wie Bürgerinnen und Bürger nehmen auch Unternehmen Leistungen der Verwaltung in Anspruch. Bereits heute werden verschiedene Verwaltungsleistungen wie zum Beispiel Registerauskünfte regelmäßig und intensiv von Unternehmen nachgefragt. Die hohen Kontaktzahlen deuten darauf hin, dass eine rein elektronische Abwicklung der Leistungserbringung im Kontakt zwischen Verwaltung und Unternehmen (G2B) Vereinfachungen und Erleichterungen auf beiden Seiten bedeuten können. Insofern stimmt Vitako mit der Feststellung der Projektgruppe eID-Strategie überein, wonach „Servicekonten für Unternehmen (…) ein wichtiger Treiber für das E-Government"[2] sind und begrüßt die Arbeit der Projektgruppe bei der Implementierung von Standards für die Kommunikation zwischen den Beteiligten am Portalverbund.

Im engeren Sinne geht es bei dem als Unternehmenskonto bezeichneten Dienst um ein Nutzerkonto für juristische Personen. Neben Unternehmen sind damit auch Vereine, Stiftungen etc. angesprochen.[3] Angesichts der Vielfalt der Organisationsformen juristischer Personen, die Interesse an einem Servicekonto haben könnten, regt Vitako an, das Unternehmenskonto als **Organisationskonto** zu bezeichnen, um so auch sprachlich den Kreis der Adressaten über die Unternehmen hinaus zu erweitern.

Natürliche und juristische Personen

Aus Vitako-Sicht handelt für eine Organisation immer eine natürliche Person. Organisationen können hingegen nicht aus sich selbst heraus handeln. Vitako begrüßt daher die Feststellungen der Projekt-

[1] Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG), § 3 (2) S. 1.
[2] PG eID-Strategie, Abschlussbericht Phase 3, V1.0, S. 36.
[3] Vgl. ebenda, S. 37.

gruppe eID-Strategie, wonach die Kernaufgabe (interoperabler) Servicekonten in der Speicherung personenbezogener Daten und der Feststellung der Identität von natürlichen und juristischen Personen anhand dieser Daten besteht[4].

Bei Organisationskonten können juristische Personen Nutzerkonten anlegen, über die ein oder mehrere Vertretungsberechtigte im Auftrag dieser juristischen Person digital handeln können. Die Daten der jeweils im Auftrag handelnden Personen können beliebig wechseln, die juristische Person dagegen bleibt bestehen.

Zur Realisierung des Organisationskontos ist eine Schnittstelle zu schaffen, die neben den Informationen der für die Organisation handelnden Person auch Informationen zur Organisation, für das die (natürliche) Person handelt, gespeichert und übermittelt werden können. Die handelnde natürliche Person muss dabei stets eindeutig zuzuordnen sein.

Hieraus ergibt sich, dass ein Organisationskonto den Zweck hat, dass Organisationen online Verwaltungsleistungen in Anspruch nehmen können. Dazu muss im interoperablen Anwendungsfall ein Austausch von (Identitäts-)Daten der Organisation und der für die Organisation handelnden natürlichen Person zwischen den Teilnehmern am Portalverbund erfolgen.

Die Frage, welche Anforderungen an eine Authentifizierung die einzelnen Verwaltungsdienste stellen, bleibt davon unberührt. Wir teilen die Einschätzung, dass die einzelnen Verwaltungsdienste innerhalb des jeweilig verwendeten Servicekontos abgewickelt werden und damit Fragen der Interoperabilität an dieser Stelle keine Rolle spielen.[5]

Rechte und Rollen

Servicekonten für Organisationen bedürfen einer Definition, wer sie benutzen darf, welchen Umfang die Nutzung beinhaltet und ob es Vertretungsberechtigte geben soll. Beispielsweise stellt sich für Unternehmen und Organisationen die Frage, wer die Rechte innehaben und wie diese verwaltet werden sollen.

Zur Frage, wie eine Nutzerverwaltung umgesetzt wird oder wie ein Rechte- und Rollenkonzept gestaltet werden kann, wie sie im IT-Planungsrat diskutiert worden ist, wurde noch keine konkrete Festlegung getroffen. Einigkeit bestand hingegen darin, dass die bereits in Kommunen bestehenden Servicekonten einfach an den Verbund angeschlossen werden können müssen und damit getätigte Investitionen nicht verloren gehen. Dies ist aus unserer Sicht begrüßenswert. Allerdings ist festzustellen, dass es, obwohl eine praktische Lösung für ein Organisationskonto vorliegt, im IT-Planungsrat dafür noch kein abgestimmtes Konzept gibt. Bereits praktisch auf kommunaler Ebene vorhandenen Servicekonto-Architekturen im Bereich der Organisationskonten sind aufgrund unterschiedlich umgesetzter Rechte- und Rollenkonzepte nur bedingt kompatibel.

Wir schlagen daher in einem ersten Schritt ein Rechte- und Rollenkonzept vor, das auf den beiden Rollen „Administrator“ und „(fachlicher) Benutzer“ beruht, wobei fachliche Nutzer die tatsächlich stellvertretend für eine Organisation handelnden natürlichen Personen sind und die Rolle „Administrator“ zusätzlich dazu berechtigt, das Konto a) anzulegen und b) weitere natürliche Personen mit dem Konto zu verknüpfen und zu so zu stellvertretenden Handlungen zu befähigen. Dieser Vorschlag hat aber keine unmittelbare Wirkung auf die föderalen Anforderungen an Servicekonten im Portalverbund. Denn unabhängig davon, ob ein Rechte- und Rollenkonzept umgesetzt wird, kann und muss Interoperabilität der Servicekonten gewährleistet werden.

[4] Vgl. ebenda, S. 38.
[5] PG eID-Strategie, Abschlussbericht Phase 3, V1.0, S. 43.

In einem weiteren Schritt regen wir an, die Abbildung von Rechte und Rollen beziehungsweise Vertreterregelungen im Portalverbund nochmals explizit zu untersuchen, damit praktikable Lösungen erarbeitet werden können.

2. Postfächer

Die Umsetzung einer Postfach-Funktionalität ist auch für die Konzeption von Servicekonten relevant. Postfächer sind ein wesentlicher Basisdienst, um Transaktionen medienbruchfrei und benutzerfreundlich abwickeln zu können. Für Bürgerinnen und Bürger wie auch für Organisationen ergibt sich bei der Nutzung einer Verwaltungsleistung in vielen Fällen der Bedarf nach (bidirektionaler) Kommunikation, sodass Postfächer innerhalb der Konzeption von Unternehmenskonten konsequent berücksichtigt werden sollten.

Asynchrone Kommunikation

Für die Erbringung von Verwaltungsdiensten werden notwendige Vorgangsdaten vom Antragsteller erhoben. Dies geschieht in der Regel bereits bei Antragstellung auf standardisiertem Weg beispielsweise durch Formulareingabe. Einige Verwaltungsdienste erfordern im laufenden Verwaltungsverfahren zusätzliche Informationen und Angaben vom Antragsteller (Nachweise, Belege etc.). So kann beispielsweise die Abgabe von zusätzlichen Dokumenten nach Durchsicht eines Bauantrages erforderlich sein oder es sind Angaben widersprüchlich und der Sachbearbeiter möchte eine Rückfrage an den Antragsteller richten. Verwaltungsdienste können den Antragsteller außerdem über den Prozessstand mit Statusmeldungen informieren oder Bescheide in elektronischer Form zustellen. Diese Anforderungen setzen eine asynchrone (zeitlich versetzte) Kommunikation zwischen Verwaltungsdienst und Antragsteller voraus. Vitako begrüßt daher die vom IT-Planungsrat beschlossene Einführung einer Postfach-Funktion als weiteren Basisdienst neben der bestehenden Authentisierungs-Funktion für Servicekonten.

Aus unserer Sicht gehört eine Postfach-Funktionalität perspektivisch zu jedem Servicekonto. Die Schaffung einer temporären Übergangslösung mittels Innovationsadapter[6], wie er in der Projektgruppe eID-Strategie diskutiert wurde, halten wir in einer Übergangsphase für angemessen, um den Benutzern zügig interoperable Postfächer zugänglich zu machen. Um die Übergangslösung benutzerfreundlich zu gestalten, halten wir für unabdingbar, dass die Nutzer eine Möglichkeit erhalten, ihre lokal angelegten Postfächer einzusehen. Eine Übersicht an zentraler Stelle vorzuhalten, wie es in der Projektgruppe eID-Strategie diskutiert wurde, widerspricht nach unserer Auffassung dem dezentralen Ansatz von Servicekonten. Aus Sicht der IT-Dienstleister ist es notwendig, eine technische Lösung zu finden, die eine Kommunikation von Postfächern unterschiedlicher Servicekonten erlaubt.

Allerdings sind diese Postfächer nicht für allgemeine Anfragen an die Verwaltung gedacht – dafür existieren bereits vielfältige und etablierte Kontaktmöglichkeiten -, sondern allein für digitale Antragsvorgänge und als Rückkanal.

Bidirektionale Kommunikation

Aus unserer Sicht ist die Kommunikation im benutzerfreundlichen Idealfall von vornherein bidirektional, das heißt mit einer Antwortfunktionalität zu konzipieren. Für den Fall, dass Fachgesetze heute noch eine digitale Abwicklung behindern, sind sicherlich auch andere Prozessabläufe denkbar. Beispielsweise wenn Rückantworten über fachprozessspezifische Antwortformulare oder auch mittels

[6] PG eID-Strategie, Abschlussbericht Phase 3, V1.0, S. 9ff.

Antwortschreiben auf Papier umgesetzt werden müssen. Solange das Ziel einer volldigitalisierten Verwaltung noch nicht verwirklicht ist, müssen Medienbrüche in Kauf genommen werden.

Hier müssen praktikable Kompromisse gefunden werden, die eine schrittweise Digitalisierung und eine schrittweise Optimierung von Prozessen ermöglichen. Aus Vitako-Sicht stellt dies jedoch keinen Widerspruch dar und führt auch nicht zu erhöhter konzeptioneller Komplexität.

Grundsätzlich gehört die asynchrone Kommunikation, ob klassisch per Brief oder digital, untrennbar zu vielen Verwaltungshandlungen. Im Bereich der digitalen asynchronen Kommunikation betreten wir mit dem Basisdienst Postfach für viele Bürger und Unternehmen indessen Neuland. Hier sollten die Benutzer behutsam an das in diesem Kontext neue Medium herangeführt werden. Andererseits eröffnet erst die Nutzung von Postfächern mit sicherer Übermittlung von Anträgen, Nachweisen, Bescheiden und Informationen für beide Seiten die Potenziale einer weitgehend medienbruchfreien Verfahrensabwicklung.

Wir raten daher ausdrücklich dazu, nur dann mit Bürgern und Unternehmen digital zu kommunizieren, wenn sie einen Verwaltungsprozess digital initiiert oder einer antragsunabhängigen Kommunikation via Postfach ausdrücklich zugestimmt haben. Ein dem Nutzer unerwartet digital zugestelltes Knöllchen wirkt erfahrungsgemäß gegenwärtig noch stark akzeptanzmindernd.

Pseudonymisierung

Vitako unterstützt den empfohlenen sensiblen Umgang mit Personen-IDs aus Gründen des Datenschutzes und hält Pseudonymisierung für eine sinnvolle Verfahrensweise. Allerdings ist der Einsatz transienter (flüchtiger) IDs, wie er gegenwärtig diskutiert wird, an dieser Stelle nicht zielführend. Die Zustellung von Nachrichten zwischen Postfächern verschiedener Servicekonten (beispielsweise Bundesland übergreifend), kann technisch nur dann realisiert werden, wenn der Benutzer (Postfachinhaber) eindeutig identifiziert werden kann. Aus unserer Sicht wäre Domänen-spezifische pseudonymisierte IDs, die eine Verkettbarkeit über Domänengrenzen hinweg verhindern, die bessere, günstigere und leichter umsetzbare Lösung.

3. Vorschläge für einen interoperablen Postfach-Basisdienst

Die Europäische Kommission hat sich im Programm „Connecting Europe Facility“[7] (CEF) mit der Übermittlung von elektronischen Nachrichten und Dokumenten über die Grenzen der Mitgliedsstaaten hinweg beschäftigt. Aus Sicht von Vitako ist es geboten, sich mit solchen vorhandenen Konzepten auseinanderzusetzen und geeignete Lösungen zu adaptieren. Internationale Standards können die Nutzung von digitalen Verfahren und Interoperabilität erleichtern. Für die Postfachfunktionalität von Servicekonten würden sich Anleihen beim CEF eDelivery-Konzept anbieten.

Wichtige Funktionsbausteine in einem derart verteilten Netzwerk sind sogenannte Access Points, die als Kommunikationsknoten[8] verstanden werden können.
Auch interoperable Servicekonten im Portalverbund sind ein verteiltes Netzwerk, sodass die entsprechenden Kommunikations-Basisdienste der jeweiligen Servicekonten (für die geforderte Postfach-Funktionalität) ein verteiltes Netzwerk von Kommunikationsknoten darstellen.

[7] Siehe auch https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home, abgerufen am 24.05.2018
[8] Siehe auch https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery, abgerufen am 24.05.2018

CEF-eDelivery führt für die Kommunikation das 4-Corner-Model ein[9]:

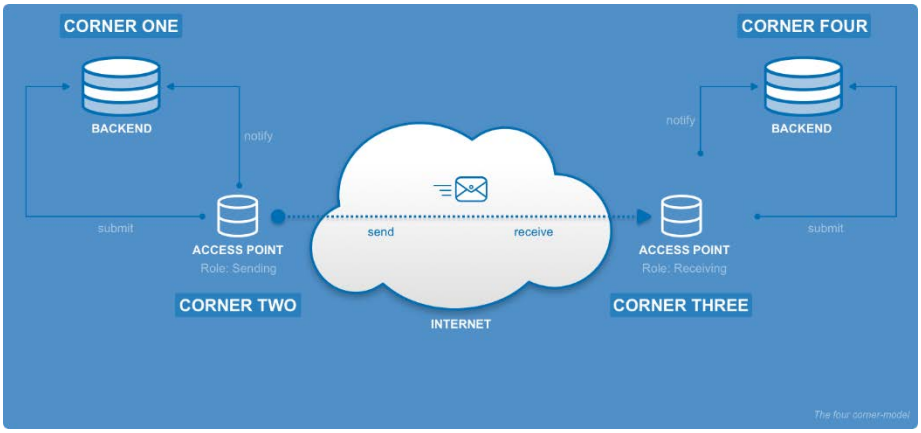

Abbildung 1: 4-Corner-Model nach CEF-eDelivery

Dieses Modell lässt sich leicht auf die Postfachfunktionalität von Servicekonten übertragen:

Möchte ein Verwaltungsdienst, der an ein bestimmtes Serviceportal angebunden ist und mit zu diesem eine „Vertrauensbeziehung“ hat, einem Bürger (der wiederum an einem beliebigen Servicekonto im Portalverbund registriert ist) eine Nachricht schicken, so wird diese Nachricht nach dem 4-Corner-Model nicht direkt mit dem Zielsystem des Bürgers ausgetauscht. Dies hätte ansonsten die Herausforderung, dass der jeweilige Verwaltungsdienst mit diversen „Kommunikationssystemen“ direkt interagieren können müsste. Dies ist auch aus praktischen Erwägungen (Vertrauensstellung und sichere Anbindung von Verwaltungsdiensten an/mit Portalen und der hieraus resultierenden Betriebsinfrastrukturen) selten umsetzbar und nicht zu empfehlen.

Vielmehr ist es so, dass der Verwaltungsdienst (Corner One) sich eines vom Servicekonto seines Verwaltungsportals bereitgestellten Messagingdienstes (Corner Two) bedient. Zu diesem „Messagingdienst“ besteht über die konkrete Anbindung am Verwaltungs-/Serviceportal eine Vertrauensbeziehung und etablierte technische Anbindung, die in der Praxis eine Varianz aufweisen kann. Dieser Messagingdienst nimmt die Übermittlung der Nachricht an den Messagingdienst des Servicekontos des Bürgers (Corner Three) vor. Von dort wird die Nachricht dem Bürger zugestellt (Corner Four).

[9] Für die Grafik, siehe https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/How+does+eDelivery+work+-+Message+exchange, abgerufen am 24.05.2018

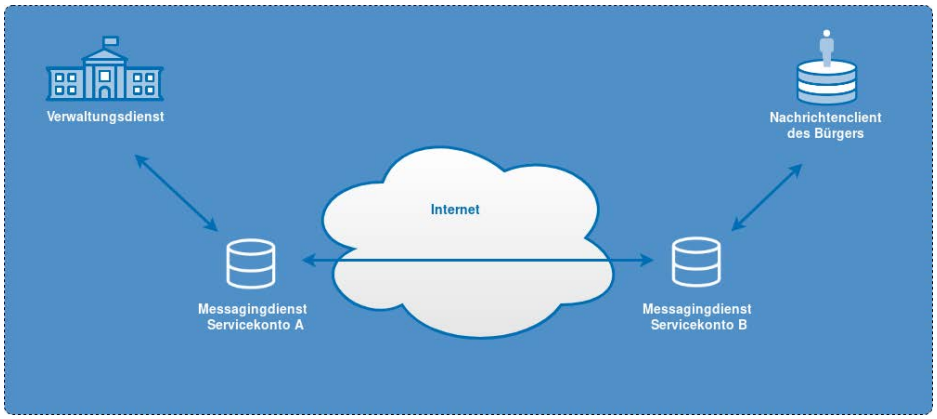

Abbildung 2: 4-Corner-Model für Postfachfunktionalität von Servicekonten

Eine Übernahme dieses Modells für die Postfach-Funktionalität von Servicekonten hierzulande vereinfacht eine strukturierte Betrachtung und Entwicklung des Vorhabens:

- für Verwaltungsdienste ist die Kommunikation zwischen Corner One und Corner Two relevant,
- für die Interoperabilität der Postfach-Funktionalität ist die Kommunikation zwischen Corner Two und Corner Three relevant,
- für Entwicklung und Anbindung eines Postfach-Frontends (Nachrichtenclients) als funktionales Element eines Servicekontos ist die Kommunikation zwischen Corner Three und Corner Four relevant.

Konzeptionell bedacht und konkret spezifiziert wurden bei eDelivery Fragestellungen wie:

Interoperabilität: Festlegung eines standardisierten Nachrichtenformats mit Attachments.

Sicherheit: Mechanismen zur Sicherung der Nachrichten-Integrität, der Nachrichten-Vertraulichkeit und Identifizierung von Sender und Empfänger.

Skalierbarkeit und Performance: Durch das verteile Netzwerk lassen sich je nach Anforderung beliebig Kommunikationsknoten hinzufügen. Das Verteilen von Metadaten ist konzeptionell bedacht.

Rechtliche Sicherheit und Haftung: Mechanismen zu Quittungen und Bestätigungen.

Gerade was die Betrachtung von Sicherheitsaspekten angeht, bietet die konzeptionelle Aufteilung in das 4-Corner-Model Vorteile, da Anforderungen auf einzelne Bereiche abgebildet werden können:[10]

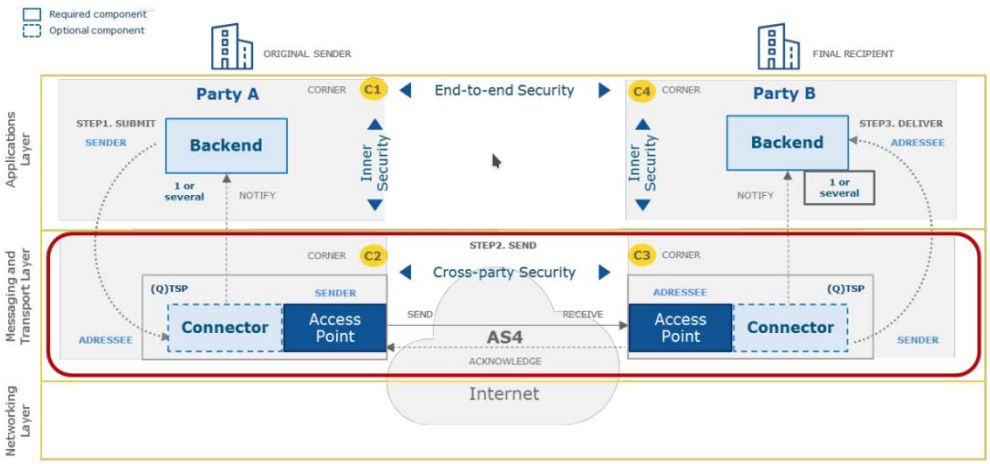

Abbildung 3: Security Domains des 4-Corner-Model

4. Fazit

Vitako begrüßt die Umsetzung des Online-Zugangsgesetzes und die Schaffung des Portalverbunds. Wir weisen darauf hin, dass vorhandene Lösungen aus dem kommunalen Raum in den Portalverbund integriert werden müssen. Man darf die Vorreiter der Digitalisierung nicht dadurch bestrafen, dass neue Konzepte zur Interoperabilität von Servicekonten alte vernichten. Dies würde im Übrigen auch hohe Investitionen zunichtemachen.

Durch Interoperabilität entsteht ein Wettbewerb der Ideen um gute Lösungen zwischen den Anbietern von Servicekonten. Ziel muss es sein, gemeinsame Standards zu entwickeln. Dabei sollten wir auf vorhandene Industriestandards wie beispielswiese SAML und eDelivery setzen, statt proprietäre Lösungen zu entwickeln.

Vitako hat alle Hersteller von Servicekonten (unabhängig von einer Mitgliedschaft bei Vitako) an einem Tisch versammelt und ein gemeinsames Verständnis von Interoperabilität bei der technischen Umsetzung von Servicekonten im Portalverbund geschaffen. Wir empfehlen, dieses Know-how der Hersteller bei allen weiteren Konzepten im IT-Planungsrat zu nutzen.

[10] Siehe „Security Controls and Recommendations“, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Security+Controls+guidance, abgerufen am 24.05.2018