

Föderales IT-Architekturboard (IT-ARB)

Stellungnahme zum Whitepaper „Zentrales Postfach im Kontext der Nutzerkonten“

Vorbemerkung

Das vorliegende Whitepaper stellt drei Lösungen für ein zentrales Postfach vor.

Es bietet einen guten ersten Überblick über vorhandene Lösungen und deren Funktionalitäten. Diese Stellungnahme nimmt eine andere Perspektive ein und betrachtet die Lösungen aus dem Blickwinkel einer IT-Architektur.

Im Rahmen der zur Verfügung stehenden sehr knappen Zeit konnte das Whitepaper nicht alle Aspekte berücksichtigen und methodisch weitere Aspekte überprüfen. Das gleiche gilt für die Stellungnahme des IT-ARB. Beide Papiere sollten daher nicht als Grundlage für eine endgültige Entscheidung genommen werden – sie können dies nicht leisten.

Sie geben aber erste Anhaltspunkte für weitere Maßnahmen, die dann in einer fundierten Entscheidungsvorlage münden können.

Anlass

In der 11. Sitzung der Abteilungsleiterrunde (AL) des IT-Planungsrats (IT-PLR) am 07.12.2021 wurde beschlossen, dass der Bund im Dialog mit den Ländern, insb. Bayern und Bremen, bis zur nächsten Sitzung im Februar 2022 ein vertiefendes Konzept für mögliche zentrale Postfachlösungen erstellt.

In dem Beschluss wurde ferner festgehalten, dass die Vorlage eines Konzeptes „zentrales Postfach“ in der AL-Runde am 09.02.2022 vorgestellt werden soll unter vorheriger Beteiligung des Architekturboards.

Dieses Dokument beschreibt die Sicht des föderalen IT-Architekturboards (IT-ARB) auf die im Whitepaper „Zentrales Postfach im Kontext der Nutzerkonten“ dargestellten Sachverhalte. Das IT-ARB hat sich einen Tag nach der Veröffentlichung des Whitepapers virtuell am 02.02.2022 getroffen und am 03.02.2022 dieses Dokument verabschiedet.

Juristische Fragestellungen

Auch wenn es nicht zu den originären Fragestellungen des IT-ARB gehört, so soll dennoch der Hinweis erfolgen, dass es neben technischen und organisatorischen Fragestellungen auch noch ungeklärte (oder zumindest unklare) juristische Fragestellungen gibt.

Beispielsweise ist die Frage zu klären, ob Nutzerkonten und Postfächer überhaupt als trennbare Komponenten angesehen werden können. § 2 Abs. 7 OZG sagt aus, dass das Postfach Bestandteil eines (jeden) Nutzerkontos ist. § 8 Abs. 4 OZG erlaubt die Verarbeitung elektronischer Dokumente auch nur innerhalb des Nutzerkontos. Und § 9 OZG spricht bei der Bekanntgabe von Verwaltungsakten ausdrücklich von Postfächern, die Bestandteil eines Nutzerkontos sind. Das OZG müsste bei Aufgabe der Interoperabilität unter Umständen angepasst werden.



Darüber hinaus ergeben sich möglicherweise auch datenschutzrechtliche Aspekte einer zentralen Postfachlösung, die bislang noch nicht betrachtet wurden.

Zentrale Fragestellung „zentrales Postfach auch für Bürgerkonten“

Bislang ist die Kernfrage im Bereich der Postfächer noch nicht grundsätzlich beantwortet. Zwar wurde im Beschluss 2018/41 des IT-Planungsrates die Herstellung der Interoperabilität der Nutzerkonten beschlossen, und in Folge auch mehrfach bestätigt.

Jedoch geht es vorliegend um die Frage, ob diese Interoperabilität auch für die angeschlossenen Postfächer gelten muss.

Berücksichtigt werden muss ebenfalls, dass sich inzwischen neue Erkenntnisse aus der OZG-Umsetzung ergeben haben. Diese können dazu führen, die Kernfrage noch einmal aufzugreifen und eine Entscheidung nach umfassender Prüfung technischer, organisatorischer und juristischer Fragestellungen herbeizuführen.

Bei der Beantwortung dieser (strategischen) Frage sollte die konkrete (technische) Lösung zunächst eine untergeordnete Rolle spielen bleiben. Die Beantwortung dieser Fragestellung sollte auch darauf eingehen, wie mit den bestehenden Anbindungen an die bestehenden Nutzerkonten umgegangen wird.

Die Frage sollte insbesondere aus Sicht der IT-Architektur beantwortet werden.

Nachnutzung von bestehenden Produkten oder Projekten

Die in dem genannten Whitepaper vorgestellten Möglichkeiten der Realisierung eines zentralen Ansatzes mit bestehenden Projekten bzw. Produkten werden nachstehend aus Sicht des Architekturmanagements beurteilt. Bei dieser Beurteilung spielen die seitens des IT-Planungsrates beschlossenen föderalen IT-Architekturrichtlinien eine zentrale Rolle.

Keine der drei Lösungen hält die Architekturrichtlinien vollständig ein. Die nachstehende Tabelle gibt einen entsprechenden Überblick. Demzufolge besteht bei allen Lösungen perspektivisch entsprechender Entwicklungsbedarf. Die konkreten Lösungsvorschläge müssen insofern als Übergangslösungen betrachtet werden.

Für eine abschließende Bewertung der betrachteten Postfachlösungen zur Herbeiführung einer Entscheidung bezüglich der Umsetzung bedarf es tiefergehender Analysen zur konkreten Realisierung einer Anbindung von Onlinediensten und Fachverfahren.

Zur Bewertung der Benutzer:innenfreundlichkeit und der Integration der Lösungen in die föderale IT-Architektur muss insbesondere die Gestaltung des Zusammenspiels zwischen Nutzerkonten, Postfächern, Onlinediensten und Fachverfahren in Bezug auf die genutzte Postfachreferenz näher beleuchtet werden. Insbesondere sollte hierbei bewertet werden, ob bzw. in welchem Umfang bestehende Nutzerkonten ggf. angepasst werden müssen.

Tabelle 1: Bewertung bestehender Postfachkomponenten gemäß Architekturrichtlinien

	OZG-PLUS- Postfach	Nutzerkonto- ELSTER-Postfach	Nutzerkonto- Bund-Postfach
--	-------------------------------	---	---------------------------------------



SR1: Verwendung von Standards	Ja (Verwendung von XÖV / OSCI)	Ja (Verwendung von XÖV / OSCI)	Ja (Verwendung von XÖV / OSCI)
SR2: Sicherstellung von Wiederverwendung	Ja (Wiederverwendung der ITPLR-Produkte COM Despina und COM Tauri sowie ID Mercury)	Nein ELSTER hatte dies mit "Ja" versehen, aber keine Begründung hinterlassen.	Nein NKB kommt zu einer anderen Einschätzung, jedoch ist die Begründung nicht nachvollziehbar (EfA).
SR3: Bestehende Marktstandards verwenden	Ja (Maschine zu Maschine Kommunikation auf der Grundlage von SOAP, Nutzung von OpenID Connect)	Ja (Maschine zu Maschine Kommunikation auf der Grundlage von RESTful WebServices, Nutzung von SAML)	Ja (Maschine zu Maschine Kommunikation auf der Grundlage von RESTful WebServices, Nutzung von SAML)
SR4: Sichere Systemgrundkonfiguration („Security-by-Default“ und „Privacy-by-Default“)	unbekannt	unbekannt	unbekannt
SR5: API-First Ansatz	Nein	Nein	Nein
SR6: Sicherstellung der Nutzereinbindung („Usability by Design“)	Ja	Ja Die Angabe wurde nicht begründet.	Ja
SR7: Sicherstellung der Herstellerunabhängigkeit	Nein	Nein	Nein
SR8: Einsatz von Open Source	Nein Nach Einschätzung HB wird die Richtlinie erfüllt, da eine Bereitstellung unter einer Open Source-Lizenz geplant ist. Das ist aktuell aber nicht der Fall.	Nein Seitens ELSTER wird die Richtlinie erfüllt, eine Begründung wurde jedoch nicht angegeben.	Nein Nach Ansicht von NKB wird dies erfüllt. Die reine Nutzung von Open Source Komponenten erfüllt jedoch nicht die Richtlinie.
SR9: Gewährleistung der Interoperabilität von IT-Lösungen	Teilweise (Orientierung am „Payload-Profil für	Teilweise	Teilweise



	Postfächer interoperabler Servicekonten")		
SR10: Sicherstellung von loser Kopplung / Modularität	unbekannt	Unbekannt	Unbekannt
SR11: Gewährleistung einer umweltfreundlichen und nachhaltigen Nutzung von Informationstechnik	unbekannt	unbekannt	unbekannt
SR12: Umsetzung des „Once Only“ Prinzips	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
SR13: Open Data by Design	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

Handlungsempfehlungen

Bei der Evaluierung der Nachnutzung von bestehenden Produkten oder Projekten ist eine tiefergehende Analyse notwendig, um eine Bewertung hinsichtlich der zügigen Umsetzbarkeit zu ermöglichen.

Entscheidend für den erfolgreichen Rollout einer Postfachkomponente in die Breite ist deren Skalierfähigkeit. Dies gilt sowohl in organisatorischer, als auch in technischer Hinsicht. Damit Onlinedienste und Fachverfahren zügig an eine Postfachkomponente angebunden werden können, müssen Zugangshürden für Hersteller dieser Systeme minimiert werden. Dazu bedarf es einer umfangreichen Dokumentation der anzubindenden Schnittstellen samt Schnittstellenspezifikationen und Entwicklungskits (SDKs). Die Notwendigkeit noch zu schaffender technischer Zugangsvoraussetzungen für Behörden, die bereits jetzt Fachverfahren betreiben, stellt eine weitere Hürde bei der Anbindung von Fachverfahren an eine Postfachkomponente dar und sollte daher vermieden werden.

Darüber hinaus müssen für einen Rollout in der Fläche entsprechende Onboarding-Prozesse für Betreiber:innen von Onlinediensten und insb. von Fachverfahren aufgebaut bzw. optimiert werden und weitgehend im Self-Service-Verfahren durchgeführt werden können.

Unabhängig von der Verfolgung der Ansätze „dezentral bzw. interoperabel“ und „zentral“ ergeben sich für eine Nutzung in der Breite eine Reihe von Standardisierungsbedarfen. Insbesondere die Interaktion zw. Onlinediensten bzw. Fachverfahren und Postfachkomponenten ist derzeit in den existierenden Lösungen jeweils unterschiedlich ausgeprägt. Eine einheitliche Schnittstelle zur Übermittlung von Nachrichten an Postfächer von Bürger- und Organisationskonten existiert derzeit nicht. Auch sind Funktionalitäten in bestehenden Postfächern derzeit unterschiedlich realisiert (z.B. Mechanismen zur Bestätigung des Nachrichtenabrufs/ Lesebestätigung, Festlegung des notwendigen Vertrauensniveaus, etc.). Dies stellt Hersteller von Onlinediensten und Fachverfahren vor einige technische Herausforderungen und erhöht die Komplexität der Anbindung dieser Systeme an Postfachkomponenten enorm. Daher empfiehlt sich kurzfristig eine Festlegung und



gemeinsame Weiterentwicklung einheitlicher Vorgaben für die Umsetzung von Postfachkomponenten, ggf. in Form einer Arbeitsgruppe des Architekturboards. Die zeitnahe Verabschiedung entsprechender Standards unterstützt auch die Umsetzung des OZG und schafft Planungssicherheit.

Ein möglicher Ansatz für die letztliche Entscheidung könnte auch ein Mittelweg zwischen der dezentralen / interoperablen Lösung auf der einen und der zentralen Lösung auf der anderen Seite sein.

Denkbar wäre etwa, dass nach detaillierter Betrachtung ein zentrales Postfachangebot geschaffen / benannt wird, das durch die Nutzerkonten von Bund und Ländern genutzt werden kann. Gleichzeitig wäre das zentrale Postfachangebot an den Verbund der interoperablen Postfächer anzuschließen und schrittweise funktional weiterzuentwickeln, sodass perspektivisch die Anforderung möglichst vieler Stakeholder erfüllt werden.

Damit könnten einerseits die Ressourcen für Betrieb und Pflege schrittweise erprobt und skaliert werden. Andererseits wird so aber auch eine Entscheidungsalternative bei anstehenden Weiterentwicklungsvorhaben an den bestehenden Lösungen aufgebaut. Erfüllt die zentrale Lösung die Anforderungen des eigenen Systems an ein Postfach und ist die Anbindung bei finanzieller Betrachtung vorteilhaft, ist von einer schrittweisen Migration auszugehen. Damit würde sich aus Architektursicht ebenfalls die Komplexität im Bereich der Postfächer schrittweise verringern, da die Anzahl der individuellen Postfachlösungen reduziert wird. Dieser Lösungsansatz sollte daher bei der weiteren Diskussion ebenfalls berücksichtigt werden.