



Interoperable Servicekonten

Bericht der PG eID-Strategie zum Abschluss der
Entwicklung und Migration

V 1.0 / 15.01.2020

Inhaltsverzeichnis

1	Management Summary	3
2	Ausgangssituation	4
3	Ergebnisse Entwicklung und Betrieb	5
4	Informationsplattform	7
5	Ergebnis	9
6	Zeitschiene	10

1 Management Summary

Die flächendeckende Bereitstellung von Servicekonten für Bürger und Unternehmen in Deutschland ist ein zentrales Aufgabenfeld der PG eID-Strategie. Im Kontext der Anforderungen der PG eID-Strategie des IT-Planungsrates wurde durch Bayern ein Prototyp für Interoperable Servicekonten konzipiert und realisiert.

Die Pilotierung des Prototypen befindet sich nach Abschluss der Entwicklung und Migration in der Umsetzung. Die organisatorische und inhaltliche Ausgestaltung von KIOSK (**K**ompetenzzentrum **I**nteroperable **S**ervicekonten, Organisationseinheit des IT-DLZ in BY), die Migration des Metadatenservers und des FINK (**F**öderiertes **I**dentitätsmanagement interoperabler **N**utzerkonten in Deutschland). Labors-Bürgerkonten in das Rechenzentrum des IT-Dienstleistungszentrum des Freistaats Bayern (IT-DLZ) sowie die beauftragte Entwicklung sind abgeschlossen.

Dieser Zwischenbericht dokumentiert somit den Stand der Pilotierung nach Abschluss der Migration des Metadatenservers und des FINK.Labs-Bürgerkonten in die Umgebung von KIOSK. Die Services Metadatenserver, FINK.Lab-Bürgerkonten und die Informationsplattform stehen allen Interessenten mit berechtigtem Interesse zur Verfügung.

Im Rahmen der Vorbereitung der Pilotierung der Interoperabilität mit Echtdateien gilt es insbesondere für KIOSK die rechtlichen Rahmenbedingungen und Voraussetzungen für Datenschutz und Datensicherheit für die zukünftige sichere, interoperable Anwendung in Deutschland zu berücksichtigen. Die konkrete rechtliche Betrachtung und Bewertung ist allerdings nicht Bestandteil der durch KIOSK durchgeführten Pilotierung, sondern ist federführend durch das BMI in Zusammenarbeit mit der PG-eID-Strategie und den Ländern durchzuführen.

2 Ausgangssituation

Der IT-Planungsrat hat sich in einem Beschluss vom 17.06.2015 initial für eine flächendeckende Verbreitung von Servicekonten für BürgerInnen und Unternehmen ausgesprochen. In der Folge wurden die Konzeption und Umsetzung der Interoperablen Servicekonten innerhalb der PG eID-Strategie weiter vorangetrieben. Mit der Entscheidung 2018/41 des IT-Planungsrates vom 25.10.2018 wurde die konkrete Umsetzung der Interoperabilität der Servicekonten gemäß der bestehenden Planung der PG eID-Strategie nochmals bestätigt, dass die stufenweise Umsetzung zur weiteren Pilotierung fortgesetzt wird.

Die technische Implementierung des Prototypen hat gezeigt, dass für die Pilotierung keine technischen Risiken vorliegen. Die Teilnehmenden am fachlichen Prototypen haben bestätigt, dass die gemeinsam getroffenen Entscheidungen zur Anbindung von Servicekonten für BürgerInnen, Unternehmen und interoperable Postfächer samt Implementierungen risikofrei durchführbar sind.

Aufgrund derzeit noch unklarer Interpretationen der konkreten Auswirkungen der eIDAS-Verordnung, der Umsetzung des Single-Digital-Gateways, weiterer Anforderungen aus Bund und Ländern, die zur Zeit der Erstellung der dem Projekt zugrunde liegenden Arbeits- und Ressourcenplanung aus 2018 nicht vorlagen, an die und weitere Basisdienste liegen die Schnittstellen zum Stand dieses Berichtes in einer Version 0.8. vor.

3 Ergebnisse Entwicklung und Betrieb

Metadatenserver

Ein Metadatenserver stellt Kommunikationskonfigurationen für Systeme der Föderation sicher und zuverlässig bereit. Die Konfigurationen dienen beispielsweise der Vertrauensstellung von Interoperablen Servicekonten der Föderationsteilnehmenden. Metadatenserver können in unterschiedlichen Umgebungen, zum Beispiel in der Umgebung FINK.Lab-Bürgerkonten, betrieben werden.

Der Zugriff auf die Metadaten auf dem Server wird über zwei REST-Schnittstellen realisiert, die aus Sicherheitsgründen physisch voneinander getrennt sind. Über die lesende Schnittstelle können die öffentlich zugänglichen Metadaten von den Teilnehmern abgerufen werden. Über die schreibende Schnittstelle können Administratoren die Metadaten verwalten.

Der für die Pilotierung entwickelte Metadatenserver wurde für den Rechenzentrumsbetrieb auf Produktionsniveau angehoben und wird nun im IT-DLZ betrieben.

Integrationsumgebung FINK.Lab-Bürgerkonten

Die FINK.Labs stellen Umgebungen z. B. eine Integrationsumgebung zur Verarbeitung von Testdaten zur Verfügung, damit die Vertreter von Bund und Ländern das Zusammenspiel verschiedener Komponenten live ausprobieren und eigene Komponenten unabhängig von Dritten anbinden können. Die Umgebungen werden vom IT-DLZ betrieben.

Das FINK.Lab-Bürgerkonto ist eine Integrationsumgebung mit Testdaten, die die Anbindung der Testsysteme von Interoperablen Servicekonten für BürgerInnen ermöglicht. In der Umgebung sind beispielhaft drei Teilnehmer konfiguriert. Jeder dieser drei technischen Teilnehmer stellt ein Servicekonto und eine Verwaltungsleistung bereit.

Die Teilnehmer Bund und Länder können durch Einspielen Ihrer Verbindungsdaten in den Metadatenserver des FINK.Lab-Bürgerkonten eigene Servicekonten mit Testdaten in diese Umgebung integrieren.

Die Systeme können mit den Kennungen der technischen Nutzer von FINK.Lab-Bürgerkonten und den Testnutzern, die die Teilnehmer auf ihren Systemen einrichten, verwendet werden. Die Zugangsdaten der technischen Nutzer sind in der Informationsplattform bekannt gegeben. Ebenso ist eine Anleitung für die Integrationsarbeit auf der Informationsplattform abrufbar.

Diese Integrationsumgebung für die Pilotierung wurde für einen Rechenzentrumsbetrieb erweitert und wird im IT-DLZ betrieben.

4 Informationsplattform

Die Informationsplattform für Interoperable Servicekonten umfasst verschiedene Informationssysteme, die Informationen und Services zu Interoperablen Servicekonten für die verschiedenen Nutzerkreise bereitstellen. Den Einstieg in die Informationsplattform erhalten die Nutzer durch den URL **<https://informationsplattform.efink.services>**. Über diesen URL sind alle Informationen der Plattform erreichbar.

In der aktuellen Ausbaustufe werden Informationen für Föderationsmitglieder, Servicekontohersteller und Interessenten bereitgestellt. Föderationsmitglieder sind dabei die Teilnehmenden, die offiziell an der Föderation teilnehmen und ihr Servicekonto über die interoperable Schnittstelle anbinden. Konkret sind dies der Bund und die Länder. Servicekontohersteller sind die Technologielieferanten der Föderationsmitglieder, die technische Informationen für die Anbindung benötigen. Interessenten sind ein definierter Personenkreis, der durch einen formlosen Antrag eines Föderationsmitglieds an KIOSK Zugang zu dem Bereich erhält. Die Nutzer der Informationsplattform benötigen eine Kennung, um Zutritt zu den Informationen zu erhalten.

In weiteren Ausbaustufen können auch Informationen für weitere Nutzerkreise bereitgestellt werden.

Die Informationsplattform bietet Informationen zu den folgenden Themen an:

- Prozesse und Services der Föderation
- Anmeldung
- Service Desk
- Informationen zu Interoperablen Servicekonten
- Lösungsstrategie
- Anwendungsfälle
- Technische Schnittstellen
- Technische Richtlinie des BSI
- Verweise zu verwendeten Standards
- Informationen zu Rahmenbedingungen
- Metadatenserver
- FINK.Labs

Die Informationsplattform wird bei jeder Erweiterung der Schnittstelle, beispielsweise um Organisationskonten oder Postfächer, ebenfalls erweitert. Auf diese Weise können alle Nutzerkreise immer die aktuellen Informationen zu Interoperablen Servicekonten über den einen Zugang abrufen. Zudem wird die Informationsplattform weitere Dienste online für Föderationsmitglieder anbieten. Auf diese Weise ist dann nicht nur ein Servicedesk, sondern auch das Changemanagement oder der Innovationsprozess online zugreifbar. Für die Zusammenarbeit der Föderationsmitglieder sollen auch die FINK.Labs weiter ausgebaut werden. Ziel ist es, dass technische Fragen und Unterstützung zur Anbindung von Basiskomponenten weitgehend automatisiert erfolgen. Dies hilft den Föderationsmitgliedern die Anbindung eigener Servicekontofunktionen und Basisdienste weitgehend unabhängig von der Verfügbarkeit anderer Teilnehmenden zu machen.

5 Ergebnis

Die Pilotierung befindet sich nach Abschluss der Entwicklung und Migration in der Umsetzung. Die organisatorische und inhaltliche Ausgestaltung von KIOSK, die Migration des Metadaten-servers und des FINK.Labors-Bürgerkonten in das Bayerische Rechenzentrum des IT-DLZ sowie die beauftragte Entwicklung sind abgeschlossen und werden im Rahmen der Pilotierung bei Bedarf erweitert.

Folgende Aufgaben werden nun prioritär seitens KIOSK fortgesetzt:

- Betreuung der Teilnehmer
- Fortschreibung der Schnittstellen ausgehend von den Erkenntnissen der Pilotierung
- allgemeine Wartung und Pflege der Systeme und Prozesse

6 Zeitschiene

Am 11.11.2019 wurden die Schnittstellen und die Dokumentation für die Teilnehmer der Pilotierung veröffentlicht und am 21.11.2019 auf der 27. Sitzung der PG eID-Strategie vorgestellt. Am 28.11.2019 wurden im Rahmen einer Videokonferenz mit den Servicekonto-Betreibern der Länder die Inhalte und nächsten Schritte der Pilotierung abgestimmt.

Die Ergebnisse der Erhebung der Rolloutplanungen der Länder durch das BMI zur Anbindung an die Interoperabilität werden auf die weitere Umsetzung der Pilotierung Einfluss haben. Daher müssen deren Auswirkungen untersucht und die damit verbundenen notwendigen Änderungen geplant und umgesetzt werden.

Ab November 2019 können die pilotierenden Länder durch KIOSK bei der Implementierung der Bürgerkonten in die interoperable Infrastruktur begleitet werden, weitere Länder können sich bei Bedarf und Kapazität anschließen.

Nach der initialen Bereitstellung der Infrastruktur für Interoperable Servicekonten durch Bayern ist davon auszugehen, dass neben der Weiterentwicklung der Infrastruktur auch die Anbindung der Nutzerkonten an die interoperable Infrastruktur in Bund und Ländern stufenweise bis 2021 andauern wird.