IT-Planungsrat

Digitale Zukunft gestalten

Bayerisches Staatsministerium der Finanzen, für Landesentwicklung und Heimat

&

Beauftragter der Landesregierung Nordrhein-Westfalen für Informationstechnik (CIO)

&

AKDB

KDN

Prototyp Interoperable Servicekonten

Abschlussbericht vom 27. April 2017

Version 1.0

(Federführung Bayern)

Version	Inhalt	Mitwirkende
0.8	Initiale Erstellung	Herr Kronseder (H&D GmbH) Herr Reiner (H&D GmbH)
0.9	Freigabe zur Abstimmung	Herr Kirschenbauer (StMFLH)
0.9.1	Übernahme von Anmerkungen von Bayern, NRW und dem BSI.	Herr Kronseder (H&D GmbH) Herr Reiner (H&D GmbH)
0.9.2	Übernahme der Anmerkungen bzw. Klarstellungen aufgrund der Anmerkungen des BSI.	Herr Kronseder (H&D GmbH) Herr Kirschenbauer (StMFLH)
1.0	Finalisierung	Herr Kirschenbauer (StMFLH)

Inhaltsverzeichnis

1 EINFÜHRUNG 6

2 MANAGEMENT-ZUSAMMENFASSUNG 7

2.1 ERGEBNISSE 7

2.2 WEITERES VORGEHEN 8

3 ZIELE 9

3.1 QUALITÄTSZIELE 9

3.1.1 Interoperabilität 9

3.1.2 Sicherheit 13

3.1.3 Benutzbarkeit 16

3.2 ANWENDUNGSFÄLLE 18

3.2.1 Nutzer verwendet Verwaltungsdienst seines Bundeslandes 18

3.2.2 Nutzer verwendet Verwaltungsdienst eines anderen Bundeslandes 18

3.2.3 Nutzer verwendet Servicekonto eines anderen Bundeslandes 19

4 UMFANG 20

4.1 TECHNISCHE KONZEPTION 22

4.2 PROTOTYPISCHE UMSETZUNG 23

4.3 ABGRENZUNG 24

4.3.1 Infrastrukturkomponenten 24

4.3.2 Anwendungsfälle der Verwaltung 24

4.3.3 Keine Berücksichtigung zukünftiger Entwicklungen 24

4.3.4 Rechtliche Rahmenbedingungen 25

4.3.5 Datenschutzrechtliche Betrachtung 25

4.3.6 Wirtschaftlichkeitsbetrachtung 25

4.3.7 Fachkonzept 26

4.3.8 Pilotierung 28

4.3.9 Grafiken und Texte 28

5 MEILENSTEINE 29

5.1 TECHNISCHE KONZEPTION 29

5.2 TECHNISCHER PROTOTYP 29

5.3 FACHLICHER PROTOTYP 30
5.4 ABSCHLUSSBERICHT 30

6 ERGEBNISSE DES FACHLICHEN PROTOTYPS 31

6.1 TECHNISCHE DOKUMENTATION 31
6.1.1 Dokumentation der implementierten Schnittstellen 31
6.1.2 Technischer Prototyp 34
6.2 SICHERHEITSBETRACHTUNG 35
6.2.1 Dokumentation der implementierten Sicherheitsmechanismen 35
6.2.2 Umgesetzte Vertrauensniveaus für die Nutzeridentifizierung 36
6.3 PRAXISTAUGLICHKEIT 37
6.3.1 Aufwand zur Anbindung an die Servicekonten-Infrastruktur 37
6.3.2 Bewertung des Fachkonzepts 38
6.3.3 Einschätzung der Praxistauglichkeit in Bezug auf die Nutzergruppen 39
6.3.4 Abweichungen vom Eckpunktepapier 41
6.4 AUSBLICK 41
6.4.1 Votum für die Umsetzung und für eine Technische Richtlinie 41
6.4.2 Ergänzende Themen 41

7 GLOSSAR 44

8 ANHANG 51

8.1 DOKUMENTATION ZUM TECHNISCHEN PROTOTYP 51
8.2 ERFAHRUNGSBERICHTE DER TEILNEHMER 52
8.3 LITERATURVERWEISE 52
8.4 INFORMATIONSPORTAL 53

Abbildungsverzeichnis

Abbildung 1: Diensteigene und dienstfremde Servicekonten 10

Abbildung 2: Vertrauenszonen in der Föderation 14

Abbildung 3: Anmeldemaske diensteigenes Servicekonto 16

Abbildung 4: Anmeldemaske dienstfremdes Servicekonto 17

Abbildung 5: Maske für Weiterleitung von personenbezogenen Informationen 17

Abbildung 6: Nutzung des Servicekontos 1 zur Anmeldung 20

Abbildung 7: Nutzung des Servicekontos 2 zur Anmeldung 20

Abbildung 8: Architektur Interoperabler Servicekonten mit Metadatenserver 21

Abbildung 9: Zentraler Metadaten-Server für interoperable Servicekonten 22

Tabellenverzeichnis

Tabelle 1: Untersuchung von Servicekonten 12

Tabelle 2: Bereiche der technischen Teilnehmer 29

1 Einführung

Der IT-Planungsrat hat sich in seiner 17. Sitzung vom 17. Juni 2015 für eine **flächendeckende Verbreitung von Servicekonten für Bürgerinnen, Bürger[1] und Unternehmen** ausgesprochen. Die Projektgruppe „eID-Strategie“ wurde beauftragt, folgende Punkte zu erarbeiten:

1. eine Konzeption interoperabler Servicekonten
2. die Konstruktion eines Prototyps für die interoperable Kommunikation zwischen Servicekonto-Angeboten verschiedener Hersteller
3. die Durchführung einer Wirtschaftlichkeitsbetrachtung für die Umsetzung interoperabler Servicekonten
4. eine Definition der rechtlichen Rahmenbedingungen interoperabler Servicekonten

Im vorliegenden Abschlussbericht stellen wir die erarbeiteten Ergebnisse zu den Punkten 1 und 2 dar. Wir tun dies im Kontext der in der Projektskizze beschriebenen Ziele und Aufgaben. Dabei orientieren wir uns soweit wie möglich an der Struktur der Projektskizze. Zu den Punkten 3 und 4 liegen noch keine finalen Ergebnisse der Projektgruppe „eID-Strategie“ vor.

Wir verwenden in diesem Abschlussbericht den Begriff „Bürger“, um diese Nutzerzielgruppe ins Zentrum der Betrachtung von Interoperabilität zu rücken. Prinzipiell greift der Begriff „Bürger“ hier eher zu kurz, da jede natürliche Person in den meisten Servicekonten aktiv werden kann. In der Regel auch unabhängig von der Staatsbürgerschaft und damit vom Status "Bürger". Wenn eher technische Zusammenhänge erläutert werden sollen, verwenden wir allgemein den Begriff „Nutzer“.

[1] Auf männlich-weibliche Doppelformen wird nachfolgend im Sinne der besseren Lesbarkeit verzichtet.

2 Management-Zusammenfassung

Der Abbau von Bürokratie und die Modernisierung der Verwaltung sind zentrale Themen des E-Governments und Voraussetzungen für den wirtschaftlichen Erfolg Deutschlands. Im Zentrum dieser Betrachtungen zum E-Government steht der Bürger. Er soll in erster Linie von einer modernen öffentlichen Verwaltung profitieren, die einfach, praktikabel und sicher ist. Durch den föderativen Ansatz profitieren gleichfalls die Bundesländer – durch die Entwicklung und den Betrieb eines E-Government-Angebots auf der Basis von gemeinsam entwickelten Konzepten und durch zentral bereitgestellte Komponenten. Für ein föderatives E-Government leisten interoperable Servicekonten einen elementaren Baustein.

Das Projekt „Prototyp für interoperable Servicekonten“ soll die technische Machbarkeit der folgenden Ziele überprüfen.

- Dem Bürger wird ein einfaches und sicheres E-Government angeboten.
- Die Teilnehmer der Föderation binden ihre E-Governmentdienste einfach und sicher an.
- Die Teilnehmer der Föderation schützen ihre Investitionen.
- Die Teilnehmer der Föderation erhalten und stärken ihre Innovationskraft.
- Die Teilnehmer der Föderation können ihre Erfolge teilen.

Auf Grundlage dessen haben wir ein Konzept entwickelt und einen Prototyp erstellt. Parallel wurden eine Wirtschaftlichkeitsbetrachtung und eine Betrachtung der rechtlichen Rahmenbedingungen durchgeführt.

2.1 Ergebnisse

Durch die erfolgreiche Umsetzung des Konzepts im technischen Prototyp in allen überprüften Anwendungsfällen konnten wir die technische Machbarkeit aller genannten Ziele zweifelsfrei unter Beweis stellen.

Die von uns gewählte Architektur von Interoperablen Servicekonten mit einem Metadatenserver, in der jeweils nur die beiden an einer Kommunikation beteiligten Servicekonten die Daten des Nutzers austauschen, wird von allen Projektteilnehmern begrüßt und erweist sich als technisch leicht umsetzbar.

Der Metadatenserver dient den Servicekonten als zentrale Infrastrukturkomponente, um die Kommunikationsparameter zu lesen und stellt mit diesen die SAML-konforme, direkte, signierte und verschlüsselte Kommunikation zwischen zwei Servicekonten her. Zusätzlich werden in der gesamten Kommunikation zwischen zwei interoperablen Servicekonten die Daten der Nutzer transportverschlüsselt ausgetauscht.

Die **erfolgreiche Anbindung von konkreten Servicekonten** der zwei Föderationsteilnehmer **Bayern** und **Nordrhein-Westfalen** (NRW) an den Prototyp belegt zudem die **absolute Praxistauglichkeit unseres Ansatzes im föderativen Kontext**.

2.2 Weiteres Vorgehen

In einer Folgephase werden weitere Aspekte der Interoperabilität von Servicekonten untersucht. Sobald der Abschlussbericht der Folgephase vorliegt, kann das **Bundesamt für Sicherheit in der Informationstechnik** (BSI) die gesammelten Erkenntnisse als Grundlage für die Erstellung eines **Fachkonzepts** verwenden. Einer sofortigen Pilotierungsplanung steht aus unserer Sicht nichts entgegen.

3 Ziele

Interoperable Servicekonten sind für die Nutzung von Verwaltungsdiensten einer Föderation notwendig. Die Teilnehmer der Föderation sind der Bund und die Länder. Sie betreiben für die Föderation jeweils genau ein ausgezeichnetes Servicekonto. Über die föderativ einheitlich spezifizierten Schnittstellen dieser Servicekonten werden Informationen ausgetauscht.

Ziel der technischen Untersuchung ist es, die Umsetzung unabhängig von Anwendungsfällen mit konkreten Verwaltungsdiensten und konkreten Technologien zu spezifizieren.

3.1 Qualitätsziele

Wir haben drei zentrale Qualitätsziele für interoperable Servicekonten identifiziert: Interoperabilität, Sicherheit und Benutzbarkeit.

3.1.1 Interoperabilität

Auf Basis offener Standards und Technologien soll föderationsübergreifend der Austausch von Informationen sichergestellt werden. Wir verwenden den Standard der Security Assertion Markup Language (SAML) in der Version 2.0 für die Implementierung dieser Schnittstelle zwischen den Servicekonten der Föderation.

Die Interoperabilität gewährleistet folgende Anforderungen:

- Einfache Anbindung
- Investitionen schützen
- Innovationskraft stärken

Bei der Interoperabilität von Servicekonten wird pro Teilnehmer genau ein Servicekonto in der Föderation angemeldet. Jeder Dienst kann im Rahmen der Föderation ausschließlich über dieses Servicekonto teilnehmen. Die Dienste können sowohl direkt an dieses Servicekonto angebunden werden, als auch indirekt über ein anderes Servicekonto z. B. ein kommunales Servicekonto dieses Teilnehmers. Im indirekten Fall ist der Dienst über dieses (z. B. kommunale) Servicekonto an das Servicekonto des Teilnehmers angebunden. Der Dienst ist also transitiv an das Servicekonto des Teilnehmers angebunden. Im Weiteren unterscheiden aber wir nicht zwischen einer direkten und einer transitiven Anbindung eines Diensts an das Servicekonto des

Teilnehmers, da dies in der Ausgestaltungsfreiheit des Teilnehmers liegt. Für die Interoperabilität unterscheiden wir Servicekonten aufgrund der Eigenschaftenpaare **diensteigen** / **dienstfremd** und **temporär** / **permanent**.

3.1.1.1 Diensteigene und dienstfremde Servicekonten

Die Eigenschaften diensteigen und dienstfremd sind aus dem **Blickwinkel des Diensts** zu sehen.

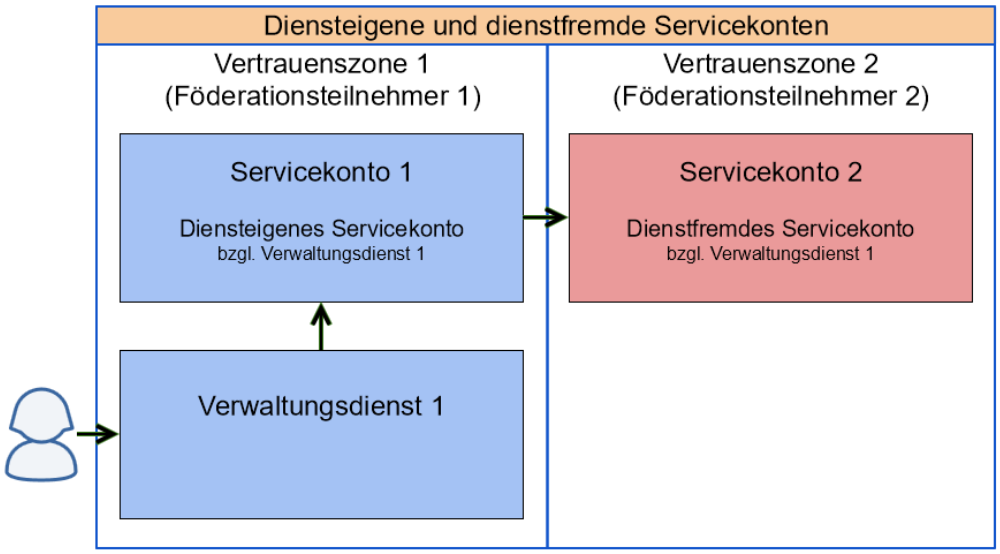

Abbildung 1: Diensteigene und dienstfremde Servicekonten

1. Diensteigenes Servicekonto

   Ein Servicekonto bezeichnen wir als **diensteigen**, wenn gewählter Dienst und Servicekonto aus der Vertrauenszone eines Teilnehmer stammen. Das diensteigene Servicekonto ist das vom Teilnehmer an der Föderation angemeldete Servicekonto.

   Ist der Kontext klar, sprechen wir anstelle von einem diensteigenen Servicekonto auch von einem eigenen Servicekonto. Das 'eigen' bezieht sich dabei immer auf den Dienst und niemals auf den Nutzer. Vollständig klar wäre die Formulierung "diensteigener Servicekontodienst"[2].

[2] Die Teilnehmer und die Projektgruppe unterscheiden aber nicht zwischen dem Servicekonto, das die Daten eines Nutzers enthält, und dem Servicekontodienst, der die Schnittstelle für den Zugriff auf die Servicekonten bereitstellt. Für beides wird der Begriff Servicekonto verwendet.

2. Dienstfremdes Servicekonto

Ein Servicekonto bezeichnen wir als dienstfremd, wenn der gewählte Dienst von einem Teilnehmer, das Servicekonto aber von einem anderen Teilnehmer stammt. Der Dienst kommuniziert nie direkt mit dem fremden Servicekonto, sondern erhält die Daten des Nutzers ausschließlich über sein eigenes Servicekonto.

Ist der Kontext klar, sprechen wir - analog zum diensteigenen Servicekonto - auch verkürzt von einem fremden Servicekonto.

3.1.1.2 Temporäre und permanente Servicekonten

Unverändert zum Eckpunktepapier unterscheiden wir mit temporär und permanent die Art der Speicherung der Nutzerdaten im Servicekonto. Die Eigenschaften temporär und permanent sind aus dem Blickwinkel des Nutzers zu sehen.

Auch im Kontext der Föderation sind permanente Servicekonten für die Umsetzung von Anwendungsfällen mit personenbezogenen Diensten (wie z. B. dem Postfach) notwendig.

3.1.1.3 Nutzung von interoperablen Servicekonten

Für interoperable Servicekonten berücksichtigen wir in dieser Phase ausschließlich eine temporäre Nutzung des diensteigenen Servicekontos.

Der Nutzer verwendet sein permanentes Servicekonto eines Föderationsteilnehmers, um einen Dienst eines anderen Föderationsteilnehmers zu nutzen. Der Dienst greift dabei auf den diensteigenen Servicekontodienst zu und dieser erstellt für den Nutzer ein temporäres Servicekonto.

Szenarien, bei denen für den Nutzer durch den diensteigenen Servicekontodienst ein permanentes Servicekonto erstellt wird, sind nicht Teil dieser Arbeit. Beim Thema „Postfachdienste“ wird diese Erweiterung jedoch benötigt und daher in Folgephasen von uns behandelt. Verwaltungsdienste der Teilnehmer bieten bereits Services an, die diese Erweiterung benötigen.

Für die temporäre Nutzung eines fremden Servicekontos, sowohl für diensteigene Servicekontodienste mit temporärem als auch mit permanentem Servicekonto, könnten ebenfalls Anwendungsfälle spezifiziert werden. Diese Fälle werden aktuell nicht betrachtet, da noch keine konkreten Anforderungen durch die produktiv betriebenen Servicekonten der Teilnehmer existieren.

Die folgende Tabelle zeigt die Kombinationsmöglichkeiten von temporären und permanenten Servicekonto-Ausprägungen und den Status der Untersuchungen.

diensteigen / dienstfremd	temporär	permanent
permanent	UNTERSUCHTER ANWENDUNGSFALL	ZUKÜNFTIGER ANWENDUNGSFALL
temporär	AKTUELL KEIN ANWENDUNGSFALL	AKTUELL KEIN ANWENDUNGSFALL

Tabelle 1: Untersuchung von Servicekonten

Eine Betrachtung der Interoperabilität auf Ebene der EU ist laut Projektskizze für diese prototypische Umsetzung nicht vorgesehen.

In der Projektskizze ist gefordert worden, dass die Interoperabilität die **Innovationskraft** der Föderationsteilnehmer stärken soll. Dies erreichen wir durch eine weitgehende Entkopplung der SAML-Entities. Bei der Implementierung von Verwaltungsdiensten erhalten die Teilnehmer keinerlei Vorgaben zur Identifizierung von Nutzern. Lediglich die **Interaktion zwischen den Servicekonten** wird definiert. Diese Festlegungen beinhalten aber keine Vorschriften für die Organisation von Servicekonten, Identity-Providern oder Service-Providern innerhalb der Vertrauenszone der Teilnehmer.

Die Schnittstellen sind so ausgelegt, dass sie außerhalb der Föderation erweitert werden könnten. Die Teilnehmer der Föderation können dadurch zunächst **individuelle Anforderungen proprietär umsetzen** und sind somit in ihrer **Entwicklungsarbeit nicht gehemmt**. Zum Vorteil der Föderation können bewährte Lösungen allgemeingültig vereinbart werden. Auf diese Weise werden erfolgreiche Lösungen geteilt.

Soweit wie möglich wurden bei der Implementierung **offene Standards verwendet**. Wo keine offenen Standards vorliegen, zeigen wir exemplarisch, wie die Umsetzung aussehen könnte. Diese Umsetzungen könnten dann beispielsweise vom BSI spezifiziert und offen gelegt werden.

Auf individuelle Festlegungen, die spezifisch für das E-Government in den einzelnen Bundesländern sind, haben wir bewusst verzichtet. Dies betrifft beispielsweise die Definition von Syntax und Semantik der ausgetauschten personenbezogenen Informationen nach der erfolgreichen Anmeldung. Wir empfehlen diese Festlegungen im Rahmen der Pilotierung zu treffen.

Alle Festlegungen haben wir so gewählt, dass sie **keinen Teilnehmer zur Nutzung eines Produkts eines Anbieters zwingen**.

Für den technischen Prototyp haben wir **keine personenbezogenen Dienste** (beispielsweise Postfach) betrachtet. Gegenwärtig gibt es keine Anzeichen, dass die bis jetzt getätigten Festlegungen die Anbindung von Postfächern verhindern könnten. Für eine abschließende Bewertung muss jedoch eine Definition von interoperablen Postfächern vorliegen. Diese Untersuchung wird in der Phase 3 oder im Rahmen des Pilotprojekts fortgeführt.

3.1.2 Sicherheit

Im E-Government werden sensible, personenbezogene Daten von Bürgern verarbeitet oder bereitgestellt. Der **Schutz dieser Daten** vor dem Zugriff unberechtigter Dritter ist essentiell und eine **zentrale Aufgabe der interoperablen Servicekonten**.

Darüber hinaus muss auch die **Authentizität der Daten** für die Nutzung von Verwaltungsdiensten gewährleistet werden.

Zum Schutz der personenbezogenen Daten haben wir für den Prototyp festgelegt, die **Assertions zwischen den SAML-Entities zu verschlüsseln und signiert auszutauschen**. SAML-Anfragen müssen lediglich signiert übertragen werden, da sie keine personenbezogenen Daten beinhalten.

Auch die Verschlüsselungstechnik wurde für den Prototyp festgelegt. Unabhängig davon bestimmen die Teilnehmer der Föderation und das BSI die für den Piloten oder die Produktivsetzung zu wählenden algorithmischen Verfahren.

Der Verwaltungsdienst nimmt die Daten des Nutzers entgegen. Der Anbieter des Verwaltungsdiensts verantwortet die Sicherheit dieser Daten. Weiterhin muss er die Authentifizierung dieses Nutzers über sein Servicekonto vornehmen, um entscheiden zu können, ob der Nutzer zur Nutzung des Diensts berechtigt ist. Lässt der Anbieter diese Authentifizierung durch einen Dritten, außerhalb der eigenen Vertrauenszone, vornehmen, darf dies nur mit Zustimmung des Nutzers geschehen. Auch die Authentifizierungsantwort enthält Daten des Nutzers und darf nur mit dessen Zustimmung von der außerhalb der Vertrauenszone liegenden Authentifizierungsstelle an den Verwaltungsdienst (direkt oder indirekt) übertragen werden.

Stimmt der Nutzer auch nur einer der beiden Übertragungen nicht zu, kann er den Verwaltungsdienst nicht nutzen.

Die folgende Grafik zeigt, an welchen Stellen die Daten des Nutzers auftreten. Die Föderation schreibt vor, dass die Daten über die grün markierten Kommunikationswege **verschlüsselt übertragen** werden müssen.

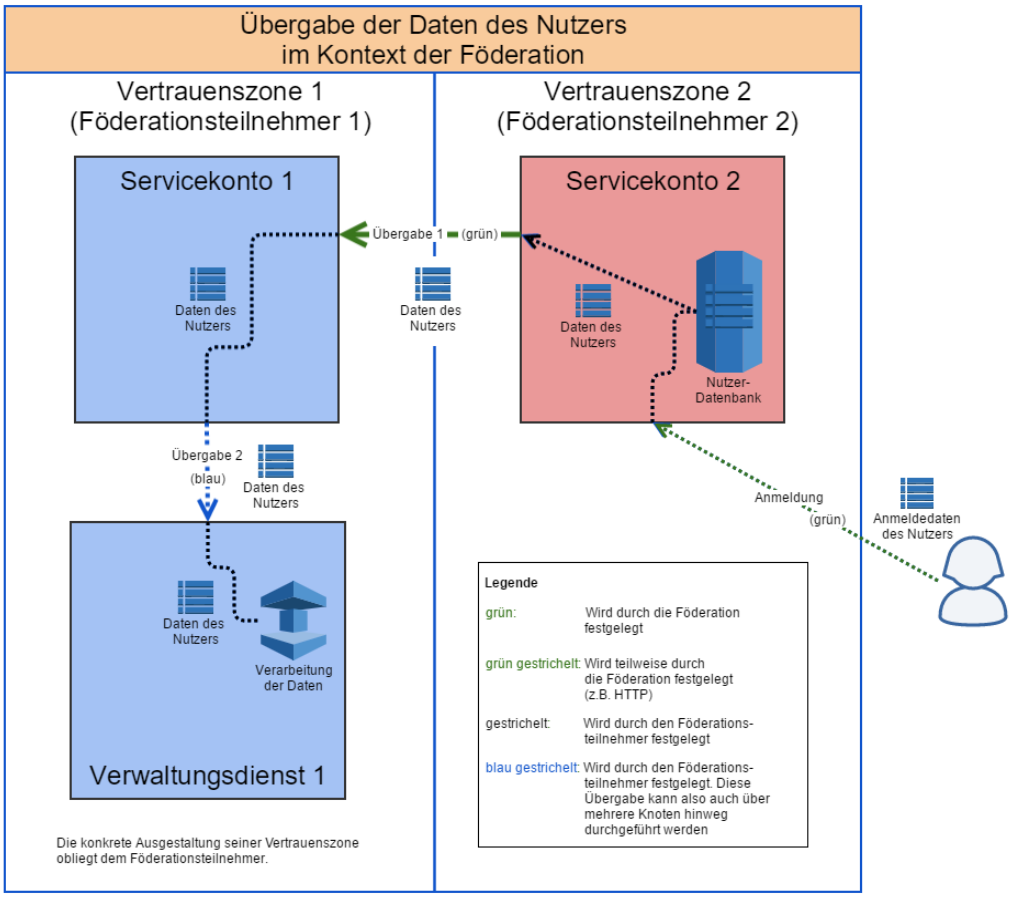

Abbildung 2: Vertrauenszonen in der Föderation

Die Servicekonten und Verwaltungsdienste des Teilnehmers bilden eine **Vertrauenszone**. In diese Vertrauenszone können weitere Servicekonten und Verwaltungsdienste aufgenommen werden. Jede Vertrauenszone definiert aber genau **ein** Servicekonto, das diese Vertrauenszone vertritt und in der Föderation bekannt ist. Ausschließlich zwischen diesem Servicekonto und den Servicekonten der anderen Föderationsmitglieder werden die Informationen verschlüsselt übertragen. **Kein Dritter kann diese mitlesen**.

Eine Vertrauenszone muss nicht homogen sein. Es ist möglich, eine Vertrauenszone in weitere, kleinere Vertrauenszonen zu unterteilen. Innerhalb der Vertrauenszone eines Teilnehmers kann es mehrere Servicekonten geben, die in einer durch den Teilnehmer definierten Weise miteinander kommunizieren. Die **konkrete Ausgestaltung der Vertrauenszone obliegt somit dem Teilnehmer**. Aus Sicht der Föderation ist die Vertrauenszone des Teilnehmers eine Blackbox mit einem ausgezeichneten Servicekonto.

Der Nutzer muss also darüber informiert werden, welche Stellen im Kontext der Föderation die von ihm übertragenen Daten mitlesen können und was diese Stellen mit seinen Daten tun dürfen. Die Verantwortlichen der Vertrauenszonen müssen sicherstellen, dass die Beteiligten der Vertrauenszone die Daten nur gemäß der durch den Nutzer erteilten Zustimmung verwenden.

Generell ist anzustreben, dass die Nutzerinformationen von möglichst wenig Beteiligten gelesen werden können. Die Vertrauenszone definiert die Beteiligten und macht so für die Nutzer transparent, wie ihre Daten verwendet werden.

Das Konzept für interoperable Servicekonten schreibt nicht vor, wie die Vertrauenszonen technisch oder organisatorisch ausgestaltet werden. Dementsprechend können Föderationsteilnehmer eigene Lösungen entwickeln, die den spezifischen organisatorischen Rahmenbedingungen gerecht werden.

Unter Datenschutzaspekten ist es notwendig, die potentiell zu übertragenden Attribute (vgl. „Beschreibung der Schnittstellen“, Unterkapitel 8.1) einzeln datenschutzrechtlich zu prüfen. Ebenso sollte für das Gesamtkonzept der Nutzung personenbezogener Daten in dieser Föderation von interoperablen Servicekonten eine datenschutzrechtliche Freigabe erfolgen. Dazu müssen voraussichtlich sowohl der Datenschutz des Bundes als auch die Datenschutzbehörden der an der Föderation interoperabler Servicekonten teilnehmenden Länder eine einheitliche Regelung erarbeiten. Ferner sind der Zweck der zwischen Servicekonten zu übertragenden Daten, deren Speicherung und der Zeitpunkt der Löschung festzuhalten. Es ist auch zu berücksichtigen, dass zukünftig unter Umständen die Daten nicht nur für E-Government-Dienste, sondern auch für andere behördliche Dienstleistungen verwendet werden sollen.

Aktuell wird in der Föderation interoperabler Servicekonten eine beliebige Anzahl der spezifizierten Attribute übertragen. Es gibt noch keine Festlegungen für einen Minimalumfang an Attributen. Hierfür sind gemäß Konzept die fachlichen Teilnehmer gefordert. Im Rahmen dieses Prototyps waren aus fachlicher Sicht die vorgeschlagenen Attribute ausreichend, um alle Anwendungsfälle abzudecken.

Ferner sieht das Konzept vor, dass einzelne Föderationsteilnehmer sich in zusätzlichen und nur für sie verbindlichen Absprachen, auf Attribute einigen können, die ausschließlich zwischen ihnen übertragen werden. Eine datenschutzrechtliche Betrachtung dieser zusätzlichen Daten muss gesondert durchgeführt werden.

Die tatsächlich notwendigen Attribute und deren Spezifikation sollen im Rahmen einer Pilotierung erfasst werden.

Darüber hinaus sollte geprüft werden, inwiefern die Bestimmungen einer Auftragsdatenverarbeitung für die Übertragung von personenbezogenen Nutzerdaten im Rahmen der Interoperabilität anzuwenden sind.

Für diese Phase ist es nicht vorgesehen, die Nutzerdaten im eigenen Servicekonto - außerhalb der Session des Nutzers – zu speichern. Eine Speicherung der Daten im eigenen Servicekonto für die Nutzung von personenbezogenen Diensten wird in der folgenden Phase oder ggf. auch erst in der Pilotierung betrachtet.

3.1.3 Benutzbarkeit

Im **Zentrum des E-Governments** steht der **Nutzen des Bürgers**. Er profitiert von der **Modernisierung der Verwaltung** – durch die Beschleunigung der Prozesse und die Vereinfachung der Kommunikation.

Demzufolge muss **jeder Nutzer** die interoperablen Servicekonten **einfach und sicher** verwenden können. Durch die Einführung interoperabler Servicekonten in der Föderation darf die Nutzung eines Diensts für den Nutzer **keinenfalls unangemessen komplizierter** sein als bisher.

In der Anmeldemaske des diensteigenen Servicekontos ergeben sich für den Nutzer nur minimale Änderungen. So werden dem Nutzer **weitere Servicekonten angezeigt**, bei denen er sich anmelden kann, um einen **konkreten Dienst** zu nutzen.

Abbildung 3: Anmeldemaske diensteigenes Servicekonto

Ignoriert der Nutzer diese Liste, ändert sich nichts am Ablauf der Anmeldung.

Informationen zur „*Anmeldung am eigenen Servicekonto*“ und zur „*Auswahl des Servicekontos*“ finden Sie in den Dokumenten „Überblick über die Anwendungsfälle“ bzw. „Beschreibung der Schnittstellen“.

Die Anmeldung an einem **dienstfremden Servicekonto** unterscheidet sich von der Anmeldung an einem diensteigenen Servicekonto nur in einem Punkt: Der Nutzer muss das fremde Servicekonto auswählen und nach erfolgreicher Anmeldung noch der **Übermittlung seiner personenbezogenen Daten** an das Servicekonto des Verwaltungsdiensts **zustimmen**. Wir gehen davon aus, dass der Nutzer ganz bewusst sein Servicekonto bei einem anderen Föderationsteilnehmer nutzen möchte und daher die zusätzlichen Interaktionen gerne in Kauf nimmt.

Wir visualisieren die Darstellung der Servicekontenauswahl exemplarisch.

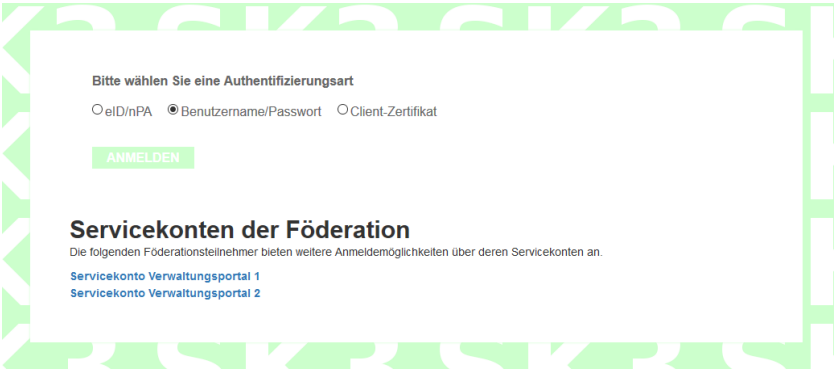

Abbildung 4: Anmeldemaske dienstfremdes Servicekonto

Rein technisch arbeitet der Webbrowser des Nutzers eine Reihe von Umleitungen (redirects) ab, die sich, abhängig vom Produkt, unterschiedlich darstellen können. **Der Nutzer muss nicht eingreifen**.

Nach erfolgreicher Authentifizierung und vor der Übermittlung der personenbezogenen Daten muss der Nutzer seine Zustimmung für die Weiterleitung geben.

Abbildung 5: Maske für Weiterleitung von personenbezogenen Informationen

Erst danach kann der Nutzer den Verwaltungsdienst nutzen.

Informationen zum Anwendungsfall *„Anmelden am femden Servicekonto“* finden Sie im Dokument *„Überblick über die Anwendungsfälle“*.

Der Fokus der bisherigen Betrachtung liegt auf dem Anwendungsfall, dass ein Nutzer nur ein Servicekonto besitzt, das er zur Nutzung beliebiger Dienste in der Föderation nutzen kann. Dem Nutzer steht es jedoch frei, sich bei mehreren Servicekonten zu registrieren und jeweils ein permanentes Servicekonto anzulegen. Vergleichen lässt sich dies mit dem Fall, in dem ein Nutzer mehrere E-Mail-Konten besitzt. Die Komplexität für einen Nutzer mehrerer Servicekonten erhöht sich im interoperablen Fall nicht merklich, da er bereits mit dem Prinzip mehrerer Konten vertraut ist.

3.2 Anwendungsfälle

In der Projektskizze wurden drei Anwendungsfälle zur Spezifizierung skizziert:

1. Nutzer verwendet Verwaltungsdienst seines Bundeslandes
2. Nutzer verwendet Verwaltungsdienst eines anderen Bundeslandes
3. Nutzer verwendet Servicekonto eines anderen Bundeslandes

Auf den ersten Blick beschreibt der technische Prototyp nur zwei der drei in der Projektskizze genannten Anwendungsfälle. Aber eine Zusammenfassung der Anwendungsfälle 2 und 3 ist möglich und sogar notwendig. Denn aktuell unterscheiden wir für den Prototyp nicht zwischen Diensten des Servicekontos und Verwaltungsdiensten. Unter Diensten des Servicekontos verstehen wir weitere personenbezogene Dienste wie z. B. Postfach.

3.2.1 Nutzer verwendet Verwaltungsdienst seines Bundeslandes

Die Anmeldung an den Verwaltungsdienst erfolgt direkt am eigenen Servicekonto. Es wird kein fremdes Servicekonto der Föderation verwendet.

Diesen Anwendungsfall dokumentieren wir für den Prototyp detailliert im Dokument „Überblick über die Anwendungsfälle“ (vgl. Unterkapitel 8.1).

3.2.2 Nutzer verwendet Verwaltungsdienst eines anderen Bundeslandes

Der Nutzer besitzt ein permanentes Servicekonto und wählt einen Verwaltungsdienst bei einem anderen Föderationsteilnehmer.

Diesen Anwendungsfall dokumentieren wir für den Prototyp detailliert im Dokument „Überblick über die Anwendungsfälle“ (vgl. Unterkapitel 8.1).

3.2.3 Nutzer verwendet Servicekonto eines anderen Bundeslandes

Der Nutzer besitzt ein permanentes Servicekonto und wählt einen Dienst des Servicekontos eines anderen Föderationsteilnehmers. Wenn wir nun – wie oben beschrieben - nicht zwischen Verwaltungsdiensten und Diensten von Servicekonten unterscheiden, sind beide Fälle identisch.

Eine detaillierte Betrachtung dieses Sonderfalls entfällt daher.

4 Umfang

Da eine Lösung mit SAML-Proxies durch die Rahmenbedingungen ausgeschlossen wurde und weder ein Discovery-Service noch ein zentraler Metadaten-Server Teil des SAML-Standards sind, haben wir eine Lösung mit dem **Servicekonto als Dipol** definiert. Der **neue Begriff "Dipol"** bezeichnet dabei auch eine Proxy-Architektur. Diese kommt ohne einen zentralen Proxy aus, der alle Daten mitlesen muss. Auf den Begriff "Proxy" verzichten wir allerdings, um eine Verwechslung mit SAML-IdP-Proxies auszuschließen, die in der Regel eine zentrale, mitlesende Proxy-Architektur implementieren und außerdem zusätzlich eine SAML-Kommunikation mit dem Dienst erfordern.

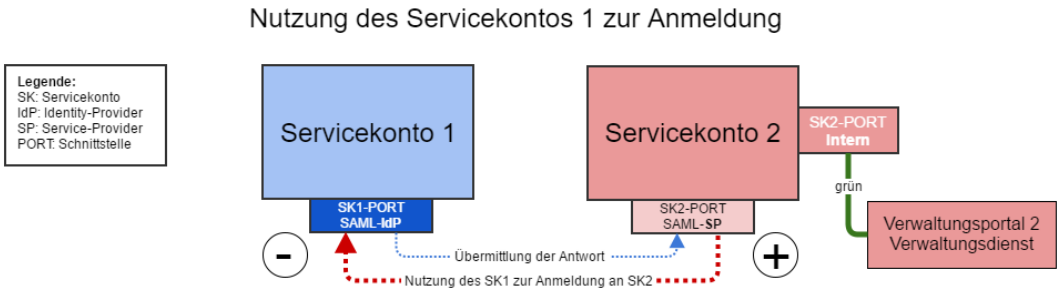

Abbildung 6: Nutzung des Servicekontos 1 zur Anmeldung

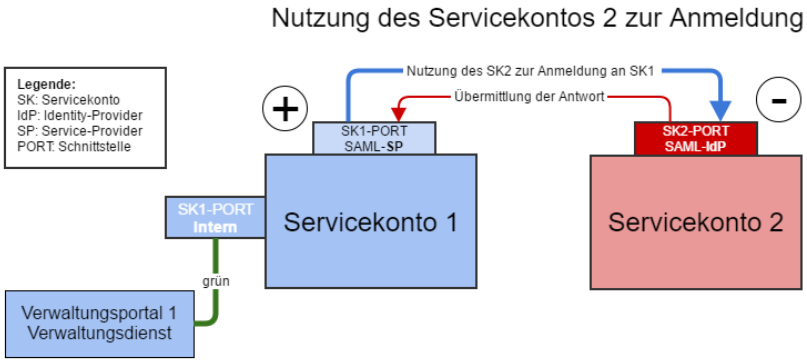

Abbildung 7: Nutzung des Servicekontos 2 zur Anmeldung

In den Abbildungen 6 und 7 zeigen wir, dass jedes Servicekonto einem anderen Servicekonto die Identitätsdaten eines Nutzers übergeben kann. Dazu spezifizieren wir ausschließlich die Kommunikation zwischen den Servicekonten. In einer Kommunikation zwischen zwei Servicekonten tritt ein Servicekonto entweder als SP oder als IdP auf. Bei einem Aufruf wechselt das Servicekonto also seine Rolle nicht. Hier unterscheidet sich der Dipol-Ansatz von einem klassischen SAML-Proxy bei der der Proxy in einer Kommunikation zur einen Seite als SP, zur

anderen als IdP auftritt. Die Kommunikation zwischen einem Verwaltungsdienst oder einem Verwaltungsportal mit seinem Servicekonto, die auf der Grafik grün gekennzeichnet ist, ist nicht Teil der Spezifikation von Interoperablen Servicekonten und kann frei ausgestaltet werden.

Der **Dipol** ermöglicht die **zentrale Verwaltung von standardisierten SAML-Metadaten** und unterstützt eine **Ende-zu-Ende-Verschlüsselung** zwischen den Servicekonten an den Grenzen der Vertrauenszonen. Durch den Einsatz von SAML wurde die Vorgabe der Verwendung von **offenen Standards** erfüllt.

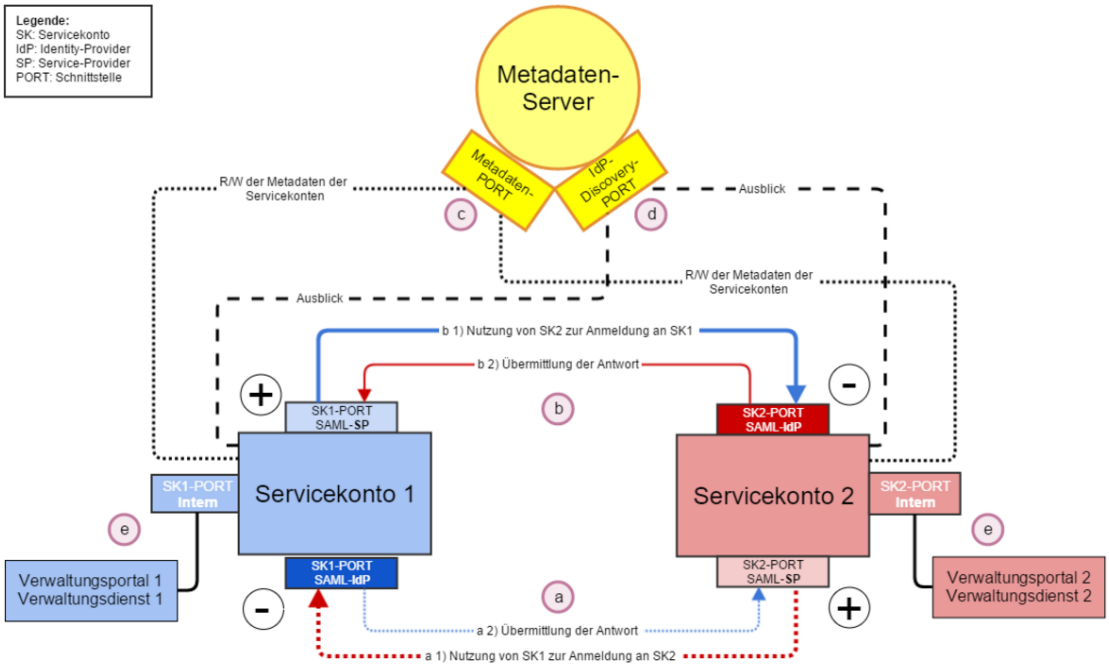

Abbildung 8: Architektur Interoperabler Servicekonten mit Metadatenserver

Die Kommunikation mit dem Metadatenserver findet zeitlich getrennt von der Kommunikation zwischen den Servicekonten statt. Die Servicekonten lesen die SAML-Metadaten vom Metadatenserver, um daraus die Endpunkte und die Verschlüsselungsparameter für eine direkte Kommunikation zwischen den Servicekonten gemäß SAML-Standard zu entnehmen. Die dies bezüglichen Prozesse und Anwendungsfälle werden erst den Folgephasen spezifiziert, da sie für den Prototypen nicht relevant sind.

Der gewählte Dipol-Ansatz ermöglicht es uns, die Verwaltungsdienste aus der Gleichung zu nehmen. So können die Teilnehmer der Föderation die **Anbindung ihrer Verwaltungsdienste frei** gestalten. Dies ist insbesondere deshalb wichtig, da die ohnehin bereits **große Anzahl an Verwaltungsdiensten** voraussichtlich **stetig steigen** wird. Änderungen an den Schnittstellen wären da hinderlich und große Aufwände und Innovationshemmnisse mögliche negative Folgen. Dagegen ist die Anzahl der Servicekonten sehr übersichtlich. **Anpassungen an diesen zentralen Komponenten sind deutlich einfacher zu koordinieren und kostengünstiger zu realisieren**.

4.1 Technische Konzeption

Die Umsetzung interoperabler Servicekonten basiert sowohl für die Kommunikation zwischen den Servicekonten, als auch für das Format der Metadaten auf dem offenen SAML-Standard. Für interoperable Servicekonten definieren wir zusätzliche Schnittstellen für weitere Anwendungsfälle. So können Föderationsteilnehmer beispielsweise Informationen zu Servicekonten anderer Teilnehmer aus einem zentralen Metadatenserver abrufen.

Die Föderationsteilnehmer müssen über einen **individuellen Gestaltungsspielraum** verfügen. Nur so behalten sie ihre **Innovationskraft**, etwa **für die Lösung eigener, spezifischer Problemstellungen**. Teilnehmer können eigene Erweiterungen in ihrem Namensraum vornehmen, andere Teilnehmer diese dann entweder nutzen oder ignorieren. Es liegt an der Föderation, zu einem späteren Zeitpunkt zu beschließen, eine solch **proprietäre Lösung** zu einem **Standard in der Föderation** zu erheben.

Der Informationsaustausch auf Ebene der Föderation findet daher ausschließlich über die Servicekonten der Teilnehmer statt. Die Verwaltungsdienste der Teilnehmer kommunizieren ausschließlich mit ihrem eigenen Servicekonto. Über einen zentralen Metadatenserver werden die Zugriffinformationen zwischen den Teilnehmern an der Föderation ausgetauscht.

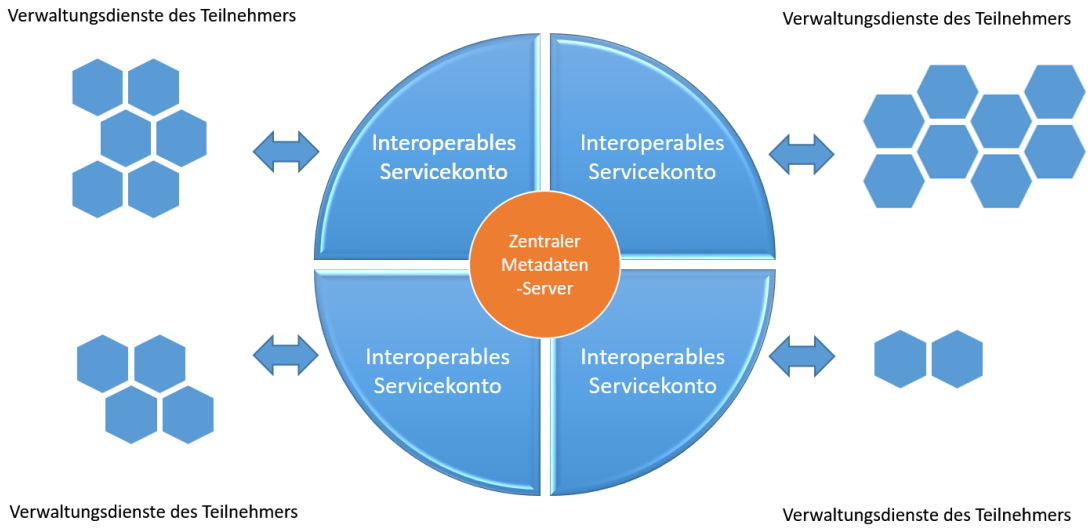

Abbildung 9: Zentraler Metadatenserver für interoperable Servicekonten

Um die Interoperabilität zu erhöhen, soll die Definition der Schnittstellen weitgehend vorwärts- und rückwärtskompatibel sein. Die Kosten zur Aufrechterhaltung der Kompatibilität können deren Nutzen übersteigen. Dies zu bewerten, liegt einzig und allein in den Händen der

Föderationsteilnehmer. Sofern die Versionen einer Schnittstelle nicht kompatibel sind, gehen wir davon aus, dass Servicekonten für eine Übergangszeit **mehrere Versionen zeitgleich unterstützen**. Dadurch kann das Zeitfenster für den Umstieg zwischen zwei Schnittstellenversionen lange offengehalten werden. Auf diese Wiese wird **kein Teilnehmer unter Zugzwang** gesetzt, **Änderungen kurzfristig umsetzen zu müssen**.

4.2 Prototypische Umsetzung

Das Konzept haben wir durch einen technischen Prototyp mit **drei technischen Teilnehmern** und einer Infrastrukturkomponente umgesetzt.

Diese Infrastrukturkomponente (mit REST-Schnittstelle) wurde für den technischen und den fachlichen Prototyp so weit wie nötig bereitgestellt (vgl. „API-Dokumentation“, Unterkapitel 8.1). Die ursprüngliche Planung, die Föderationsmitglieder persönlich zu betreuen, erwies sich bei näherer Betrachtung als nicht praktikabel. Für die **Föderationsteilnehmer** ist es **extrem wichtig, Änderungen an der Kontenkonfiguration selbst vorzunehmen**, um insbesondere in der Phase der konkreten Anbindung zügig Konten anbinden zu können. Längere Wartephasen durch das manuelle Einpflegen von Daten über eine externe Stelle sind für einen reibungslosen Ablauf und damit auch für eine breite Akzeptanz des Ansatzes hinderlich.

Die Infrastrukturkomponente ist **ausschließlich für den technischen Prototyp** konzipiert. Erfahrungen aus der Verwendung können in eine zukünftige Konzeption der Infrastrukturkomponenten einfließen. Für die Wahl der passenden Technologien sind jedoch noch die Anforderungen eines Produktivbetriebs zu berücksichtigen.

Wir konnten dabei beweisen, dass das **Konzept Interoperabler Servicekonten technisch realisierbar** ist.

Die als Ergebnis des technischen Prototyps wesentlichen Informationen sind im Bereich „Spezifikation Interoperable Servicekonten“ des Informationsportals dokumentiert und allen Teilnehmern am Prototyp zugänglich. Die wesentlichen Teile dieses Bereichs liegen diesem Abschlussbericht als separate Dokumente bei.

Mithilfe des fachlichen Prototyps konnten die Teilnehmer beweisen, dass sie ihre **konkreten Servicekonten erfolgreich an den technischen Prototyp anbinden** konnten.

4.3 Abgrenzung

Folgende Themen haben wir im Rahmen des technischen Prototyps nicht behandelt (vgl. auch Projektskizze).

4.3.1 Infrastrukturkomponenten

Aufgrund des engen Zeitrahmens war es nicht Teil unserer Aufgabe, bestehende Infrastrukturkomponenten hinsichtlich ihrer Integrationsfähigkeit in eine föderative Lösung zu untersuchen.

4.3.2 Anwendungsfälle der Verwaltung

Wie in der Projektskizze gefordert, haben wir die beschriebenen Anwendungsfälle von Nutzern untersucht (vgl. hierzu Unterkapitel 3.2 „Anwendungsfälle“).

Weitere Anwendungsfälle bei der Verwaltung von Servicekonten wurden nicht berücksichtigt. Hierunter fallen beispielsweise das Löschen oder das Zusammenführen von Servicekonten eines Nutzers.

Administrative Anwendungsfälle, wie Zertifikatswechsel oder die Hinzunahme von Servicekonten, waren ebenfalls nicht Gegenstand der Implementierung des technischen Prototyps.

Auch Prozesse, die eine Teilnahme an der Föderation betreffen, haben wir nicht betrachtet. Hierunter fallen zum Beispiel der Beitritt zur Föderation oder die Zuordnung von Authentifizierungsmitteln zu Vertrauensstufen.

4.3.3 Keine Berücksichtigung zukünftiger Entwicklungen

Wie in der Projektskizze dargelegt, haben wir die folgenden Punkte nicht untersucht.

1. Interoperabilität mit eIDAS; Berücksichtigung von Anwendungsfällen für Bürger der EU
2. Erweiterung um weitere personenbezogene Dienste, z. B. Postkorb, Safe, Bürgerprofil (IBAN, BIC, ...)
3. Juristische Personen (Unternehmenskonten), Berücksichtigung von Vollmachten

4. Anbindungsmöglichkeiten von Verwaltungsdiensten ohne eigene Servicekonten, wie z. B. Verwaltungsdienste des Bundes
5. Anbindungsmöglichkeiten über landeseigene Vermittlungsdienste

4.3.4 Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen sind laut Projektskizze nicht Teil der prototypischen Umsetzung. Sie werden unabhängig von diesem Prototyp untersucht und gesondert bewertet.

Zur Unterstützung dieser Bewertung haben wir einen Überblick über die Anwendungsfälle erstellt (vgl. „Überblick über die Anwendungsfälle“, Unterkapitel 8.1). Damit können Interessierte sich einen Überblick über die Abläufe verschaffen, ohne selbst die Schritte am Prototyp durchführen zu müssen.

4.3.5 Datenschutzrechtliche Betrachtung

Eine datenschutzrechtliche Bewertung ist ebenfalls nicht Teil der prototypischen Umsetzung. Diese muss für die Pilotierung durchgeführt werden. Die Beschreibung der Anwendungsfälle mit den Übergabepunkten der Nutzerdaten kann als Grundlage für eine Bewertung dienen.

4.3.6 Wirtschaftlichkeitsbetrachtung

Der IT-Planungsrat hat in seiner 17. Sitzung am 17. Juni 2015 die Projektgruppe „eID-Strategie“ u. a. mit der Durchführung einer Wirtschaftlichkeitsbetrachtung für die weitere Umsetzung interoperabler Servicekonten beauftragt. Bereits am Anfang soll dabei berücksichtigt werden, wie das Servicekonto im Endausbau ausgestaltet sein soll.

Eine qualitative Bewertung der Wirtschaftlichkeit wurde vom Bundesministerium des Innern (BMI) durchgeführt. Mit folgenden Ergebnissen:

- Der Umsetzung interoperabler Servicekonten ist eine hohe Bedeutung beizumessen. Gründe hierfür sind die Verankerung in den Strategien des Bundes und der Länder, die Technik-Neutralität und die damit verbundene Nachnutzung vorhandener Servicekonten.
- Im Zuge des Ausbaus interoperabler Servicekonten werden Rahmenbedingungen vereinheitlicht. So sollen Vertrauensniveaus und der Einsatz der hierfür erforderlichen Identifizierungsmittel festgelegt werden. Dies wirkt sich positiv auf die Benutzerfreundlichkeit für den Bürger aus.

- Ein einmal eingerichtetes Servicekonto kann auch für Online-Leistungen außerhalb des Zuständigkeitsbereichs des Servicekontos genutzt werden. Da erneute Registrierungen entfallen, werden Kosten eingespart.
- Interoperable Servicekonten ermöglichen es dem Bürger, weitere Online-Leistungen der öffentlichen Verwaltung zu nutzen. Das Dienstleistungsangebot wird erweitert, das Image verbessert.

Für die Phase des interoperablen Ausbaus der Identifizierungskomponente in Servicekonten wurden die Kostenblöcke für die Entwicklung des Prototyps mit dem Freistaat Bayern und dem Land Nordrhein-Westfalen bestimmt. In der Folge sind die Erkenntnisse weiterer Pilotierungspartner sowie die weiteren Stufen bis zum Endausbau des Servicekontos in die Kostenbewertung für Entwicklung und Betrieb einzubeziehen. Dabei ist auch der Ausbau interoperabler Postfächer in Servicekonten zu berücksichtigen.

4.3.7 Fachkonzept

Das Fachkonzept ist nicht Teil der prototypischen Umsetzung. Das vom BSI erstellte Fachkonzept wurde in Version 0.6 zum 2. November 2015 eingefroren. Die Projektgruppe entscheidet im Rahmen der Pilotierung über die Fortschreibung dieses Fachkonzepts. Die Ergebnisse des technischen und fachlichen Prototyps dienen hierfür als Informationsquelle.

Aus Sicht des technischen Prototyps ergeben sich folgende Abweichungen zu dem Fachkonzept.

4.3.7.1 Discovery-Service

Der im Fachkonzept beschriebene Discovery-Service hat zwei Aufgaben.

1. Die Verbindungsdaten zu den Servicekonten der Föderationsteilnehmer sollen ausgetauscht werden.
2. Nutzer sollen über diesen Service das für sie passende Servicekonto innerhalb der Föderation auswählen können.

Sofern der im Fachkonzept dokumentierte Informationsaustausch bei der Authentifizierung des Nutzers auf Basis von SAML erfolgt, weicht die Implementierung des Prototyps nicht davon ab. Details zur Anbindung von Servicekonten der Föderation über SAML sind den als Anlage beigefügten Dokumenten zu entnehmen.

4.3.7.1.1 Zugriff auf die Metadaten

Die ad hoc-Übermittlung von Verbindungsdaten, als Ermittlung der Verbindungsdaten zum Zeitpunkt der Anfrage durch den Nutzer, ***kann*** ein Sicherheitsrisiko darstellen. Daher werden die Verbindungsdaten in der gegenwärtigen Lösung über einen gesicherten Kanal gesondert zwischen den Föderationspartnern ausgetauscht. Aufgrund der einschränkenden Rahmenbedingungen wurde von uns lediglich ein Produkt für die Anbindung von Servicekonten an den technischen Prototypen gewählt: OpenAM. In diesem Produkt müssen die Verbindungsparameter bei der Konfiguration der Föderation bereits vorliegen.

Aufgrund der Rahmenbedingungen konnten wir keine ad hoc-Übermittlung untersuchen. Entsprechende Untersuchungen sollten in nachfolgenden Projektphasen durchgeführt werden.

Aus Sicht des technischen Prototyps ergeben sich keine Nachteile bei der gewählten Umsetzung. Nachteilige Berichte von den Föderationsteilnehmern liegen uns ebenso nicht vor.

4.3.7.1.2 Wahl des Servicekontos

Bei der Umsetzung des technischen Prototyps hat der Nutzer in jedem Fall die Wahl, mit welchem seiner Servicekonten er sich anmelden möchte.

Der im Fachkonzept dargestellte Ansatz ermöglicht zentral die Auswahl eines bekannten Identity-Providers. Der Nutzer hat somit stets dieselbe Benutzererfahrung (user experience, UX). Das Ergebnis dieses Auswahlprozesses ist dann die ID des selektierten Identity-Providers, über den dann die Verbindungsinformationen zu dem lokal konfigurierten Identity-Provider eines anderen Föderationsteilnehmers ermittelt werden können.

Aufgrund der Rahmenbedingungen haben wir jedoch von diesem Ansatz abweichend die Auswahl des Identity-Providers innerhalb der Website des Teilnehmers gewählt. Da die IDs der Identity-Provider der Föderation dem Teilnehmer bereit bekannt sind, stellen wir sie in einem Auswahlmenü im Look-and-Feel der eigenen Website dar, ohne eine zusätzliche Komponente befragen zu müssen. Vorteil war eine einfachere und schnellere Umsetzung. Zudem wurde die User Experience innerhalb des Teilnehmers aus unserer Sicht verbessert. Der Ansatz im Fachkonzept ist unserem Vorschlag überlegen, wenn wir zusätzliche Informationen (Grafiken, CSS, ...) austauschen (siehe Abschnitt „Grafiken und Text“). Die zentrale Komponente kann dann die Anbindung für die Föderationsteilnehmer erleichtern. Diese Lösung ist aber aufwendiger in der Realisierung und lag daher außerhalb der Möglichkeiten bei der Umsetzung des technischen Prototyps. Für eine Pilotierung sollte die Vorgabe aus dem Fachkonzept berücksichtigt und auf eine feste Verlinkung in den jeweiligen Webseiten verzichtet werden.

4.3.7.2 DVDV

Auf eine Untersuchung der Anbindung des DVDVs mussten wir ebenfalls aufgrund der Rahmenbedingungen verzichten. Der technische Prototyp kann nicht feststellen, inwiefern das DVDV eine Rolle in der Kommunikation innerhalb der Föderation spielen kann oder nicht.

Die Rolle des Föderationsdatenverwaltungsdiensts übernimmt ein für den technischen Prototyp implementierter REST-Dienst (siehe hierzu Unterkapitel „Infrastrukturkomponenten“). Dieser Dienst ist aber nur als Lösung für den technischen Prototyp zu sehen, um die Zusammenarbeit der Teilnehmer in dieser und in den nachfolgenden Phasen zu vereinfachen.

4.3.8 Pilotierung

Auch die Pilotierung ist nicht Teil der prototypischen Umsetzung und wird nach Abschluss des Fachkonzepts geplant.

4.3.9 Grafiken und Texte

Um eine einheitliche Darstellung der Föderation für den Nutzer zu erreichen, sind Logos, Grafiken und Texte zu wählen. Dies ist ebenfalls nicht die Aufgabe des technischen Prototyps.

5 Meilensteine

Für die Durchführung des Projekts wurden die Ergebnisse zu den in der Projektskizze definierten Meilensteinen erbracht. Wir verweisen auf diese Ergebnisse, die wir als PDF-Dokumente (vgl. Unterkapitel 8.1) und in einem online für einen begrenzten Teilnehmerkreis verfügbar gemachten Informationssystem (vgl. Unterkapitel 8.4) bereitgestellt haben.

5.1 Technische Konzeption

Das Ergebnis der technischen Konzeption haben wir im Bereich Spezifikation Interoperable Servicekonten im Informationsportal dokumentiert und es steht dort allen Teilnehmern zur Verfügung. Unter dem Abschnitt Touren stellen wir die zentralen Informationen als PDF-Dokumente bereit.

5.2 Technischer Prototyp

Den technischen Prototyp haben wir unter der Adresse (URL)

https://www.interoperable-servicekonten.de

im Internet bereitgestellt. Informationen zu den am technischen Prototyp beteiligten technischen Teilnehmern (bestehend aus jeweils einem Test-Servicekonto und einem Demo-Verwaltungsportal) sind den folgenden Bereichen des Informationsportals zu entnehmen.

Bereich	Beschreibung
Verwaltungsportal 1	Home- und Admin-Bereich des technischen Föderationsmitglieds Verwaltungsportal 1
Verwaltungsportal 2	Home- und Admin-Bereich des technischen Föderationsmitglieds Verwaltungsportal 2
Verwaltungsportal 3	Home- und Admin-Bereich des technischen Föderationsmitglieds Verwaltungsportal 3

Tabelle 2: Bereiche der technischen Teilnehmer

Im Informationsportal sind die Informationen zum technischen Prototyp in unterschiedlichen Bereichen abgelegt.

1. Details zur Integration von Servicekonten der Teilnehmer befinden sich im Bereich Spezifikation Interoperable Servicekonten.
2. Die Startseite zum Informationsportal befindet sich im Bereich Home.
3. Bereichsübergreifende Informationen, wie z. B. ein Glossar, befinden sich im Bereich Index.
4. Informationen zur Konfiguration des Informationsportals befinden sich im Bereich Administration.
5. Informationen zur Lösung und eine Beschreibung des technischen Prototyps befinden sich im Bereich Architekturdokumentation Interoperable Servicekonten.

5.3 Fachlicher Prototyp

Für den fachlichen Prototyp wurden die folgenden Servicekonten an den technischen Prototyp angeschlossen.

- BayernID von Bayern
- Servicekonto.NRW von Nordrhein-Westfalen

Die Berichte zu den Arbeiten an ihren Teilprojekten wurden uns von Herrn Dr. Dürbeck (AKDB) und Herrn Helmer (NRW) als Ergebnisdokumente zur Integration in diesen Abschlussbericht übergeben. Diese Ergebnisse werden in diesem Abschlussbericht im Kapitel 6 „Ergebnisse des fachlichen Prototyps“ wiedergegeben.

5.4 Abschlussbericht

Der vorliegende Abschlussbericht enthält die Zusammenfassung der Ergebnisse aus der technischen Konzeption und aus dem technischen Prototyp. Im Kapitel 6 haben wir explizit die Ergebnisse und die Bewertung des technischen Prototyps durch die fachlichen Teilnehmer Nordrhein-Westfalen mit dem KDN und Bayern mit der AKDB zusammengefasst.

6 Ergebnisse des fachlichen Prototyps

Die Struktur dieses Abschlussberichts folgt in diesem Kapitel soweit wie möglich den Vorgaben des BSI.

In diesem Kapitel beschreiben wir die Arbeiten der Teilnehmer Bayern und NRW am fachlichen Prototyp und bewerten die Arbeitsergebnisse des technischen Prototyps. Diese Ergebnisse werden der Projektgruppe vorgelegt. Sie bilden die Grundlage für die Pilotierung. Die wörtlich übernommenen Beiträge der Teilnehmer Bayern und NRW zum fachlichen Prototyp werden in diesem Kapitel als Zitat (*kursiviert*) gekennzeichnet.

6.1 Technische Dokumentation

6.1.1 Dokumentation der implementierten Schnittstellen

Ein Servicekonto in der Föderation tritt sowohl als Identity-Provider als auch als Service-Provider auf. Dementsprechend empfehlen wir, die direkte Kommunikation zwischen den Servicekonten als verbindlich vorzugeben.

6.1.1.1 Inhalte des Basisdatensatzes

Für die Anbindung der Servicekonten der Teilnehmer an den Prototyp ist der vorgeschlagene Satz an übermittelten personenbezogenen Daten als Basisdatensatz ausreichend. Eine Erweiterung des Basisdatensatzes in einer der nächsten Ausbaustufen ist jedoch wünschenswert.

> *„Im Gegensatz zur ISK-Spezifikation erwarten die Fachportale im BPV[3] darüber hinaus als zusätzliches personenbezogenes Attribut eine eindeutige, pseudonyme Kennziffer, um widerkehrende Benutzer zu einem bereits im Fachportal persistierten Fall-Datensatz (z.B. einer eAkte) zuordnen zu können. Dabei hat sich im BPV die Einführung (und Anpassung) der in der Republik Österreich geläufigen bPK (bereichsspezifische Personen-Kennziffer), hier als Ableitung der Servicekonten-ID in die Anwendungen des BPV hinein, bewährt. Ein Fachportal kann somit feststellen, welcher IDP das Pseudonym und den Basisdatensatz für welches empfangende Fachportal ausgestellt hat.*
>
> *Derzeit stellt der Bayerische Portalverbund nach erfolgter Authentisierung den folgenden*

[3] Bayerischer Portalverbund

personenbezogenen Basisdatensatz an die angebundenen Fachportale aus:

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
bPK	bPK	urn:oid:1.2.40.0.10.2.1.1.149
Vertrauensniveau	EID-CITIZEN-QAALEVEL	urn:oid:1.2.40.0.10.2.1.1.261.94
Postkorb-Handle	legacyPostkorbHandle	urn:oid:2.5.4.18
Vorname(n)	givenName	urn:oid:2.5.4.42
Nachname	surname	urn:oid:2.5.4.4
Emailadresse	mail	urn:oid:0.9.2342.19200300.100.1.3
Strasse	postalAddress	urn:oid:2.5.4.16
PLZ	postalCode	urn:oid:2.5.4.17
Wohnort	localityName	urn:oid:2.5.4.7
Akad. Titel	personalTitle	urn:oid:0.9.2342.19200300.100.1.40
Anrede	gender	urn:oid:1.3.6.1.4.1.33592.1.3.5
Geburtsdatum	birthdate	urn:oid:1.2.40.0.10.2.1.1.55

Es wäre aus oben genannten Erwägungen zum Basisdatensatz wünschenswert, wenn Servicekonten-Anbieter für den interoperablen Fall zusätzlich eine pseudonyme bereichsspezifische Personen-Kennziffer und Äquivalente zum Postkorbversand für das jeweilige Fachportal zur Verfügung stellen könnten. Dies würde einen deutlichen Mehrwert generieren, um den Bürgern die wiederkehrende Benutzung von Fachportalen auch ohne Vorhandensein eines permanenten Servicekontos zu ermöglichen.

Darüber hinaus bietet es sich an, im Zuge der Erstellung einer BSI-TR sog. Object Identifier als formale Namen für die einzelnen Attribute zu vergeben, um Kollisionen der Namensräume zu vermeiden.“

Herr Dr. Dürbeck, AKDB (Bayern)

Aus Sicht von NRW sind die folgenden Daten für ihre gegenwärtig angebotenen Verwaltungsdienste ausreichend:

- Benutzername
- E-Mail-Adresse

- Passwort
- Familienname
- Vorname
- Postanschrift

Mit Inkrafttreten der Verordnung „Verordnung zur Regelung der behördenübergreifenden Bereitstellung und zum Betrieb von IT-Infrastrukturkomponenten und Anwendungen zum elektronischen Nachweis der Identität nach § 3 Absatz 3 des E-Government-Gesetzes Nordrhein-Westfalen“ wird der in NRW verwandte Basisdatensatz entsprechend erweitert.

6.1.1.2 Beschreibung der Prozesse und deren technischer Abläufe

> *„Hierzu empfiehlt es sich, allen teilnehmenden Bürgerkonto-Anbietern über gemeinsame Governance-Prozesse und Vereinbarungen zu einem gemeinsamen Verständnis der Rechte und Pflichten der einzelnen Teilnehmer an der Föderation zu verhelfen.*
>
> *Hierzu zählen organisatorische*
>
> - *Verfahren zum Beitritt nach erfolgtem Integrationstest (für die abzählbar vielen Anbieter von Bürgerkonten sowie für die diversen Fachportale),*
> - *Verfahren zur (dauerhaften) Sanktionierung bei Fehlverhalten einzelner Teilnehmer (z.B. aus Gründen der IT-Sicherheit, nachgewiesener/vermuteter Fahrlässigkeit im Umgang mit den personenbezogenen Datensätzen),*
> - *Verfahren zur gemeinsamen Verabschiedung neuer Maßnahmen zur langfristigen Strategie der vorgeschlagenen Spezifikation (z.B. zur Planung der Ablöse/Adoption von Technologien) wie auch daran anschließende technologische*
> - *Prozesse zur technologischen Abnahme von Anwendungen der Beitrittskandidaten im Vorfeld einer Aufnahme in die Föderation interoperabler Servicekonten*
> - *Prozesse zur laufenden Betreuung der Metadatensätze der Teilnehmer (z.B. bei Beitritt/Ausscheiden von Teilnehmern in Wirk- & Testbetrieb, zur Aktualisierung eingesetzter kryptographischer Verfahren nach Vorgabe des BSI).*
>
> *Entsprechende Instrumente dazu wurden teils schon für den Bayerischen Portalverbund vorgeschlagen (gleichlautende Verbundvereinbarung als Grundlage aller weiteren Verfahrenskataloge, Beitrittserklärungen) und sind auf Bundesebene für die Föderation interoperabler Servicekonten auch sinnvollerweise vorzusehen.“*
>
> *Herr Dr. Dürbeck, AKDB (Bayern)*

6.1.2 Technischer Prototyp

Für die Arbeiten am technischen Prototyp haben wir folgende Schnittstellen realisiert:

1. die Abwicklung der Identitätsprüfung eines Nutzers
2. die Administration der Föderation
3. den Zugriff auf die Dokumentation

6.1.2.1 Identitätsprüfung

Die Beschreibung der Schnittstellen liefert u. a. Informationen zu den ausgetauschten Daten des identifizierten Nutzers sowie zum Vertrauensniveau der Identifizierung. Die Inhalte des Basisdatensatzes sind durch den technischen Prototyp lediglich als Vorschlag zu betrachten.

6.1.2.2 Administration der Föderation

Folgende Informationen müssen die Teilnehmer der Föderation bereitstellen:

- Beschreibung der SAML-Metadaten (Informationsmaterial) - Informationen zu den SAML-Entitys (IdP und SP) (vgl. „Beschreibung der SAML-Metadaten“, Unterkapitel 8.1)
- API-Dokumentation - Dokumentation der Administrationsschnittstellen für die Mitglieder der Föderation (vgl. „API-Dokumentation“, Unterkapitel 8.1)
- Kurzanleitung für Föderationsteilnehmer - Liste von Kurzanleitungen, die Aufgaben der Föderationsteilnehmer beschreiben (vgl. „Kurzanleitung für Föderationsteilnehmer“, Unterkapitel 8.1).

6.1.2.3 Dokumentation

Die Dokumentation für die Stakeholder ist online unter https://www.interoperable-servicekonten.de/ abrufbar. Dort wird auch ein API-Browser bereitgestellt, der die Schnittstelle der Administrationsprozesse dokumentiert.

6.1.2.4 Prozesse und Abläufe

Informationen zu den Prozessen und Abläufen sind in folgenden Dokumenten dokumentiert:

- Überblick über den Lösungsvorschlag - zeigt das Lösungskonzept für die Kommunikation zwischen den Servicekonten und dem Verwaltungsportal mit seinem Servicekonto (vgl. „Überblick über den Lösungsvorschlag“, Unterkapitel 8.1)

- Überblick über die Anwendungsfälle - zeigt die beiden Anwendungsfälle "Anmeldung am eigenen Servicekonto" und "Anmeldung am fremden Servicekonto". Darüber hinaus stellen wir auch den technischen Ablauf in der Kommunikation zwischen dem Browser des Nutzers, dem Verwaltungsportal und den Servicekonten dar. Alternative Abläufe skizzieren wir kurz. (vgl. „Überblick über die Anwendungsfälle“, Unterkapitel 8.1)

6.1.2.5 Orientierung am Fachkonzept

Im Unterkapitel Fachkonzept grenzen wir den Lösungsweg des Prototyps gegenüber den Überlegungen laut Vorabversion 0.6 des Fachkonzepts ab. Die relevanten Ergebnisse haben wir diesem Abschlussbericht als Anlage beigelegt.

6.2 Sicherheitsbetrachtung

6.2.1 Dokumentation der implementierten Sicherheitsmechanismen

Die Sicherheitsniveaus müssen von den Teilnehmern der Föderation spezifiziert werden. Dies schließt Richtlinien ein, welche die Teilnehmer einhalten, um das Melden eines Sicherheitsniveaus an das anfragende Servicekonto zu rechtfertigen. Eine fachliche Betrachtung muss aus juristischer und organisatorischer Sicht ebenfalls die Konsequenzen aus dem Handeln der Teilnehmer abklären und dokumentieren.

Die Projektgruppe eID-Strategie hat vorgeschlagen, dass das BSI die in den Servicekonten eingesetzten oder vorgesehenen Identifizierungsmittel prüft und eine Empfehlung zu deren Einsatz und Einstufung in die Vertrauensniveaus der Servicekonten ausspricht.

Um die Übertragung der hochsensiblen, personenbezogenen Daten zu gewährleisten, haben wir SAML 2.0 gewählt. Die Teilnehmer tauschen die Nutzerdaten über SAML 2.0-kompatible Servicekonten verschlüsselt und signiert aus. Zudem haben wir auf Basis des technischen Prototyps beispielhaft aufgezeigt, wie beim Nutzer die Zustimmung zur Übertragung seiner Daten eingeholt werden kann. Eine detaillierte Ausgestaltung muss durch die Teilnehmer am fachlichen Prototyp erfolgen, da diese ihre Praxiserfahrung (insbesondere in Hinblick auf den Datenschutz) gezielt einbringen können.

Für die Datenübertragung wurde eine Verschlüsselung und Übertragung über TLS zwischen definierten Vertrauenszonen festgelegt. Die genaue Ausgestaltung kann aus unserer Sicht das

BSI am besten leisten, wenn es um Arten der Verschlüsselungsverfahren und die Schlüssellänge geht.

Die Session im dienstfremden Servicekonto ist auf ein Minimum beschränkt. Nach Übermittlung der Daten an das anfragende (diensteigene) Servicekonto eines Teilnehmers wird die Session im Identity-Provider beendet.

Die Verwaltungsprozesse wurden im Kontext des technischen Prototyps von uns nicht im Detail untersucht. Dies gilt auch für die Sicherheitsbetrachtung. Die Implementierung im Rahmen des fachlichen Prototyps stellt lediglich einen Vorschlag für die Umsetzung der Abläufe dar. Die Implementierung in weiteren Phasen muss durch noch zu bestimmende Technologien erfolgen.

Durch die Vorgaben der Anbindung an den Prototyp war es für die Teilnehmer nicht notwendig, zusätzliche Sicherheitsmechanismen zu realisieren.

6.2.2 Umgesetzte Vertrauensniveaus für die Nutzeridentifizierung

Die durch den Prototyp definierten Vertrauensniveaus sind im Abschnitt Authentifizierungsgrade im PDF „Beschreibung der Schnittstellen“ (vgl. „Beschreibung der Schnittstellen“, Unterkapitel 8.1) dokumentiert.

> *„Im Servicekonto NRW gibt es derzeit die Möglichkeit der Identifizierung auf den Vertrauensniveaus ‚Normal’ und ‚Hoch’. NRW prüft, inwieweit Funktionen einer Hochstufung eines vorhandenen Servicekontos, ggf. durch dafür geschulte Ämter oder Einrichtungen, eingebunden werden sollen.*
>
> *Im Prototyp wird gegen die zentral bereitgestellte Infrastruktur ausschließlich auf dem Vertrauensniveau ‚normal’ getestet. Daher sind, wie [... im vorherigen Abschnitt. d.V.] ausgewiesen, keine weiteren Sicherheitsmechanismen eingebunden.*
>
> *Es wird ausdrücklich darauf hingewiesen, dass keine Aspekte berücksichtigt wurden, die den Schriftformersatz und damit das Vertrauensniveau ‚Hoch plus’ betreffen.“*
>
> *Herr Helmer, NRW*

> *„In der laufenden Pilotierungsphase werden die beiden Vertrauensniveaus ‚normal’ und ‚substantiell’ unterstützt. Nach Abschluss der Pilotierungsphase ist vorgesehen, das Vertrauensniveau ‚hoch’ zur Servicekonten-Interoperabilität spätestens zur Produktivsetzung zu unterstützen.“*
>
> *Herr Dr. Dürbeck. AKDB (Bayern)*

6.3 Praxistauglichkeit

6.3.1 Aufwand zur Anbindung an die Servicekonten-Infrastruktur

> *„Im Falle einer Produktivsetzung des Ansatzes zur Interoperabilität zwischen Servicekonten entstünden dem Betreiber des Bayerischen Servicekontos / der Zentralen Komponenten im Bayerischen Portalverbund Aufwände für*
>
> - *die gleichzeitige Unterstützung zweier Datenschemata am Identity Provider*
> - *die dauerhafte Hinzunahme und initiale (bzw. fallweise) software-seitige Anpassung weiterer Softwarebestandteile (sog. ‚tailored, off the Shelf' Produkte) um die interoperablen Anwendungsszenarien am BPV-Identity Provider bedienen zu können*
>
> *Für die dauerhafte Bereitstellung in der Produktivumgebung entstünden dem Betreiber des Bayerischen Servicekonto einmalig initiale Investitionskosten sowie fortlaufende jährliche Kosten (exkl. fallweiser Anpassungen im Zuge von Änderungen der ISK-Spezifikation). Eine Abschätzung der Kosten kann erst nach Ablauf des Projektes erstellt werden.*
>
> *Da bereits mehrere Fachportale das nunmehr seit 2015 stabile Datenschema für permanente Servicekonten des Bayerischen Portalverbunds verarbeiten, und eine bundesweit-einheitliche BSI-TR zum Zeitpunkt der initialen Produktivsetzung (erstmals 2013) noch nicht vorlag, bestünde für die Betreiber der bayerischen Fachportale zukünftig die Notwendigkeit eines Investments zur interoperablen Anpassung ihrer Anwendung hinsichtlich:*
>
> - *Verarbeitung von SAML-Responses mit teils vom bisher bekannten Datenschema abweichenden Attributen für den interoperablen Fall*
>
> *Da es dies zu vermeiden gilt, wären, wie weiter oben angemerkt, anschließende Betrachtungen zur Einführung des Postkorbversands sowie zur dauerhaften pseudonymen Identifizierung wiederkehrender Benutzer von temporären interoperablen Servicekonten vonnöten."*
>
> *Herr Dr. Dürbeck, AKDB (Bayern)*

> *„Aus Sicht NRW ist der Aufwand zur Anbindung an die Servicekonten-Infrastruktur in der prototypischen Ausgestaltung zwischen Bayern und NRW angemessen."*
>
> *Herr Helmer, NRW*

6.3.2 Bewertung des Fachkonzepts

> *„Die Umsetzbarkeit der vorgeschlagenen Spezifikation für den Zentralen Servicekonten-Anbieter im Bayerischen Portalverbund konnte im Rahmen des Proof-of-Concept anhand der Produkte zweier Technologie-Hersteller (u.a. mittels der Software-Module des derzeit in Verwendung befindlichen Hersteller-Konsortiums) veranschaulicht werden. Eine spätere Umsetzung und Produktivsetzung der vorgeschlagenen Maßnahmen (nach oben angeratener Ergänzung der Spezifikation) ist daher zu begrüßen.“*
>
> *Herr Dr. Dürbeck, AKDB (Bayern)*
>
> *„Die Projektskizze und insbesondere die darin definierten technischen Protokolle und Schnittstellen geben nach Einschätzung NRW den richtigen Weg wieder. Die Nutzung von Standards hat sich bewährt.*
>
> *Diese Aspekte sollten verbindlich in dem vom BSI zu erstellenden Fachkonzept und der daraus zu entwickelnden Technischen Richtlinie niedergelegt und nicht zuletzt im Rahmen der weiteren Sicherheitsbetrachtung zugrunde gelegt werden.*
>
> *Insbesondere sei erwähnt, dass ein zentraler Adressierungsdienst, ausgeführt beispielsweise in einer zentral vorgehaltenen flachen Liste oder im DVDV, definiert und festgelegt werden muss.“*
>
> *Herr Helmer, NRW*

Im Auftrag des Teilnehmers Bundesland Berlin implementiert der Dienstleister Dataport aktuell (Stand Dezember 2016) eine Anbindung an den technischen Prototyp. Da die Implementierungsarbeiten noch nicht abgeschlossen sind, können zum Zeitpunkt der Abgabe dieses Abschlussberichts keine konkreten Ergebnisse mitgeteilt werden. Dataport hat aber bereits eine erste Einschätzung zum Konzept des Prototyps vorab schriftlich mitgeteilt:

> *„...*
>
> *Aber ich kann bereits sagen, dass Dataport den von Bayern veröffentlichten Ansatz zum Prototyp mitträgt und grundsätzlich begrüßt. Es mag die eine oder andere Detailfrage geben, die in den folgenden Phasen des Projektes noch mal diskutiert werden mag (z.B. die Form der Metadaten-Veröffentlichung), aber das generelle Konzept hinter dem bayerischen Prototyp findet unsere Zustimmung.*
>
> *...*
>
> *Sie können gern unsere Zustimmung zum Prototypkonzept erwähnen.“*
>
> *Herr Krause, Dataport (Berlin)*

6.3.3 Einschätzung der Praxistauglichkeit in Bezug auf die Nutzergruppen

„Die Bereitstellung der Servicekonten-Interoperabilität betrifft Anbieter von Fachportalen in weitaus geringerem Umfang (falls überhaupt) als die Anbieter von Servicekonten.

Betreiber eines Diensts	Rein transaktionale Fachportale, die keinerlei personenbezogene Datensätze für wiederkehrende Benutzer speichern und auf die Möglichkeit zum Versand von sog. Postkorbnachrichten verzichten, werden keinerlei Auswirkungen vernehmen. Für Betreiber von Fachportalen, die bereits gegenwärtig im BPV Postkorbnachrichten versenden und benutzerbezogene Datensätze persistieren, entstünde aufgrund der o. g. Änderungen mindestens ein einmaliger, anfänglicher Investitionsbedarf und bei fallweiser Änderung der ISK-Spezifikation (bzw. dann der BSI-TR) zusätzliche Kosten. Andernfalls steht zu vermuten, dass einzelne Fachportale teilweise im interoperablen Anwendungsfall nicht alle Funktionalitäten in gleicher Weise wie Fall einer landesspezifischen Servicekonto- Nutzung bereitstellen können. Hier ist es daher zu vermeiden, dass einige Fachportale in diesem Fall auf die Benutzung zusätzlicher Funktionalität wie der Erstellung einer Postkorb-Nachricht oder das Anlegen eines personenbezogenen Datensatzes für wiederkehrende Dienstenutzung verzichten würden. Weitergehende Überlegungen sind daher wie im ersten Abschnitt erwähnt wünschenswert.
Nutzer eines Diensts	Die Benutzung von rein transaktionalen Fachportalen gestaltet sich im Falle von interoperablen Servicekonten gleichwertig zum Fall einer Authentisierung am bundeslandeigenen Servicekonten-Anbieter. Benutzer, die ihre Sitzung über die Authentisierung in interoperablen Szenarien aufbauen, erfahren andernfalls bei Fachportalen die auf permanente Servicekonten angewiesen sind, ggf. einen leicht eingeschränkten Nutzungsumfang. Dies könnte durchaus auch wahrnehmbar sein, z. B. in Form von ausgegrauten/ausgeblendeten Funktionen wie „Meine Fallakten für die wiederkehrende Benutzung speichern“ oder „Benachrichtigen Sie mich per Postkorbnachricht zu meiner BayernID über den aktuellen Bearbeitungsstatus“.

Betreiber eines Servicekontos	Falls Servicekonto-Betreiber lange vor Spezifikation und Veröffentlichung der BSI-TRs für die Interoperabilität von Servicekonten bereits eigene Datenschemata für die Attribute ihrer landesweiten Portalverbunde vorgeschrieben haben, so stehen diese nun vor der Aufgabe, den interoperablen Basisdatensatz auf das Format zurückzuführen, das die bereits angeschlossenen Fachportale verarbeiten können. Hierdurch entstünden einmalig initiale Aufwände und dauerhafte gleichbleibende Zusatzkosten für die Pflege beider Formate (je nachdem, inwieweit diese voneinander abweichen und sich im Laufe der Zeit ändern/auseinanderentwickeln/aufeinander zubewegen). Dies beträfe aber wohl nur den Bayerischen Portalverbund als einen der ersten bundeslandweiten Portalverbunde mit Servicekonto. Neu im Aufbau und Planung befindliche bundeslandweite Portalverbunde mit Servicekonten in anderen Bundesländern könnten ggf. aus Gründen der Kostenersparnis gleich das ISK-eigene Datenschemata für den Basisdatensatz adoptieren, um etwaige Parallelaufwände im Vorfeld auszuschließen.“

Herr Dr. Dürbeck, AKDB (Bayern)

„Grundsätzlich sind nach dem Verständnis von NRW verschiedene Nutzergruppen an der Interoperabilität von Servicekonten beteiligt:

- *Betreiber eines Diensts: dezentrale kommunale IT-Dienstleister und Kommunen, die Portale bzw. Webangebote mit dem zentralen Servicekonto.NRW verknüpft haben*
- *Nutzer eines Diensts: Bürgerinnen und Bürger, die auf die dezentralen Portale bzw. Webangebote zugreifen*
- *Betreiber eines Servicekontos: zentraler Betreiber des Servicekonto.NRW*
- *Hochstufungsbehörden: dezentrale Ämter und Einrichtungen, die nach entsprechender Schulung befugt sind, das Sicherheitsniveau eingerichteter Servicekonten im Auftrag der Servicekontenbesitzer hoch zu stufen*
- *Betreiber zentraler Interoperabilitätskomponenten: im jetzigen Stadium ist das ausschließlich der Betreiber einer flachen Liste der beteiligten Servicekonten oder – perspektivisch – das DVDV*

Für den Prototyp ist aus Sicht NRW ausschließlich die Nutzergruppe ‚Betreiber eines Servicekontos’ eingebunden worden. Für diese Gruppe war die Nutzung des Prototyps praktikabel.

> *Es ist aber keine neue Erkenntnis, sondern bewusst und ausdrücklich in der Projektskizze so angelegt, dass die prototypische Umsetzung keinen Maßstab für die konkrete Umsetzung in der Praxis darstellt. Insofern kann aus dem Prototyp kein Rückschluss auf die ganzheitliche Praxistauglichkeit über alle Nutzergruppen gezogen werden."*
>
> *Herr Helmer, NRW*

6.3.4 Abweichungen vom Eckpunktepapier

Die für die Umsetzung des technischen Prototyps zu berücksichtigenden Punkte aus dem Eckpunktepapier konnten wir ohne weitere Anpassungen übernehmen.

Weitere Themen wie Unternehmenskonten, Vertrauensstellung innerhalb der EU oder Postfächer haben wir in dieser Phase nicht betrachtet.

6.4 Ausblick

6.4.1 Votum für die Umsetzung und für eine Technische Richtlinie

Alle Teilnehmer begrüßen die Initiative zu interoperablen Servicekonten innerhalb einer Föderation.

Die notwendigen Festlegungen für die Schnittstellen der Interoperabilität von Servicekonten in Form einer Technischen Richtlinie durch das BSI werden von allen Teilnehmern ausdrücklich begrüßt. Die Erfahrungen und Anforderungen der Teilnehmer dabei zu berücksichtigen, ist ebenfalls ein positiv bewerteter Ansatz.

6.4.2 Ergänzende Themen

- *„NRW sieht eine zwingende Notwendigkeit zur Einordnung der über die interoperablen Servicekonten erreichbaren Verfahren hinsichtlich der Frage, wann welches Vertrauensniveau gefordert ist. Unklar ist derzeit, wer diese Einordnung definiert. Sollen nicht alle Länder, Kommunen und kommunalen IT-Dienstleister individuelle Einordnungen vornehmen müssen, wäre eine zentrale Vorgabe hilfreich. Richtschnur sollte sein, dass derjenige, der ein LOGIN benötigt, hierfür auch die Güte / das Vertrauensniveau definiert.*
- *Es ist notwendig zu definieren, wie ein Vertrauensniveau servicekontoübergreifend übergeben*

wird. Dies betrifft insbesondere den Anwendungsfall, wenn eine Anwendung die Schriftformerfordernis vorgibt und die Daten eines interoperablen Servicekontos herangezogen werden sollen.

- *Zusätzlich wird insbesondere für das Vertrauensniveau „Substantiell" ein zweiter Faktor benötigt. Aus NRW wurde hierzu in einer ersten Runde bereits im Sommer 2016 Kontakt mit dem BSI aufgenommen. Diese Überlegungen sind fortzuführen und zu berücksichtigen.*
- *Mit der Neufassung der TR 3107-1 im Oktober 2016 sind für die Vertrauensniveaus ‚Substantiell' und ‚Hoch' Zeiten für die Sperrfristen eingeführt worden, die in der Praxis nicht nutzbar sind. Auch hierauf wurde aus NRW im Sommer 2016 hingewiesen. Die in der TR 3107-1 ausgewiesenen Sperrfristen sollten geprüft und überarbeitet werden.*
- *Die rechtliche Betrachtung der Interoperabilität von Servicekonten ist Thema eines eigenen Teilprojektes. Daher soll an dieser Stelle nur darauf verwiesen werden, dass die rechtliche Frage der länderübergreifenden Übermittlung von Servicekonto-Daten noch zu klären ist.*
- *In der Projektphase des Prototyps wurde erneut deutlich, dass über die rein technische Befassung hinaus in jedem Fall eine Usabilitybetrachtung erforderlich ist. Wie bereits in der Umsetzung der eID-Funktionen ist auch hier deutlich erkennbar, dass die Nutzung für die Bürgerinnen und Bürger nicht selbsterklärend ist. Diese Usabilitybetrachtung sollte aus Sicht NRW Bestandteil der Pilotierung werden.*
- *Nicht zuletzt aus den genannten Gründen sieht NRW die zwingende Notwendigkeit, nach Abschluss des Prototyps eine Pilotierung wie in der Projektskizze vorgesehen durchzuführen. In der Pilotierungsphase müssen neben der technischen praxisnahen Umsetzung die Themen der Usability, des Datenschutzes und der Sicherheitsanforderungen berücksichtigt werden."*

Herr Helmer, NRW

Zusätzlich sollten die folgenden Punkte bei der Erstellung der Technischen Richtlinie genauer untersucht werden.

1. Single-Sign-On-Lösungen werden an verschiedenen Stellen gefordert. Es ist aus unserer Sicht ratsam, die konkreten Anforderungen an die Usability zu betrachten und passgenaue Lösungen zu suchen.
2. Da die Session in der Föderation nach der Anmeldung sofort beendet wird, gibt es auf föderativer Ebene keine Notwendigkeit für Up- und Downgrades bzgl. der Vertrauensstufe.
3. Die Vertrauensstufen von personenbezogenen Daten sind derzeit an die Vertrauensstufe der Anmeldung gebunden. Es ist fraglich, ob eine separate Einstufung der Vertrauensstufe der übermittelten Daten notwendig ist. Wenn die Identität des Nutzers eindeutig

festgestellt ist, kann der Nutzer auch für eventuell fehlerhafte Angaben verantwortlich gemacht werden.

4. Die Prüfung, ob eine verlangte Vertrauensstufe sichergestellt werden konnte, obliegt stets dem die Zusicherung empfangenden Föderationsteilnehmer. Dies gilt auch für Problemstellungen wie interner Single-Sign-On, Up- und Downgrades von Vertrauensstufen, Vertrauensstufen von übermittelten Daten des Nutzers. Hierzu könnten Hilfestellungen für die Anbindung von Servicekonten durch die Föderationsteilnehmer angeboten werden.
5. Für die Erweiterung der übertragenen Informationen müssen den Teilnehmern von der Föderation Namensräume zugewiesen werden.

In der nächsten Entwicklungsphase sind voraussichtlich die folgenden Themen relevant:

1. Postfach und permanente Servicekonten
2. Unternehmenskonten
3. Verwaltung von Metadaten
4. Consent
5. Property-Store

Für eine Pilotierung sind noch weitere Aufgaben relevant. Diese müssen so bald wie möglich durchgeführt werden:

1. Definition der Föderation und der damit verbundenen Funktionen und Prozesse
2. Untersuchungen zum Datenschutz
3. Untersuchungen zur Usability
4. Untersuchungen zum einheitlichen Auftreten der Föderationsteilnehmer (grafisch und textlich)
5. Untersuchungen zur Sicherheit, Angriffsszenarien usw.

7 Glossar

Name	Kurzbeschreibung
Anmeldung	Unter einer Anmeldung versteht man die Authentifizierung und Autorisierung eines Nutzers an einem System. Die Anmeldung etabliert eine Sitzung, die durch den Nutzer oder durch das System beendet werden kann.
Anwendungsfall	Ein Anwendungsfall dokumentiert die möglichen Szenarien aus Sicht eines Akteurs, um ein definiertes, fachlichen Ziel zu erreichen.
API	siehe Application Programming Interface
Application Programming Interface	Programmierschnittstelle eines Systems oder Komponente.
Authentizität	Bezeichnet die Echtheit einer Sache.
Blackbox	Die Außensicht auf ein System oder eine Komponente. Der innere Aufbau ist aus diesem Blickwinkel nicht relevant.
Browser	Programm zur Navigation im Internet, insbesondere des World Wide Webs, um Daten daraus abzurufen oder Nachrichten abzusetzen.
BSI	siehe Bundesamt für Sicherheit in der Informationstechnik
Bundesamt für Sicherheit in der Informationstechnik	Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde am 1. Januar 1991 gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern. Das BSI ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Name	Kurzbeschreibung
Bürger	Bezeichnet den Angehörigen eines Staates oder einer Kommune.
Cascading Style Sheets	Standard des W3C über den Stilinformationen mit Web-Dokumenten verknüpft werden.
CSS	siehe Cascading Style Sheets
Datenschutz	Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).
Deutsches Verwaltungsdiensteverzeichnis	Das Deutsche Verwaltungsdiensteverzeichnis (DVDV) hat die Funktion einer zentralen Registrierungsstelle für Online-Dienste der öffentlichen Verwaltung und ermöglicht eine rechtsverbindliche elektronische Kommunikation von und mit Behörden über die vorhandenen Fachverfahren.
Discovery-Service	Im Kontext von Interoperablen Servicekonten ermöglicht ein Discovery-Service das Auffinden einer Authentifizierungsmöglichkeit. Allgemein bezeichnet es eine Dienstleistung, über die Dienste nach definierten Kriterien ermittelt werden können.
DVDV	siehe Deutsches Verwaltungsdiensteverzeichnis
E-Government	Unter E-Government (dt. E-Regierung) im weiteren Sinn versteht man die Vereinfachung und Durchführung von Prozessen zur Information, Kommunikation und Transaktion innerhalb und zwischen staatlichen, kommunalen und

Name	Kurzbeschreibung
	sonstigen behördlichen Institutionen sowie zwischen diesen Institutionen und Bürgern bzw. Unternehmen durch den Einsatz von digitalen Informations- und Kommunikationstechnologien.
Entität	Eine Entität ist eine Person, eine Organisation, ein Gegenstand, ein Teilsystem oder eine abgrenzbare Gruppe mehrerer davon. Siehe auch SAML-Entity
Föderation	Eine Föderation ist ein Zusammenschluss von Organisationen, die sich auf einen einheitlichen Identifizierungsstandard geeinigt haben. Ein Anbieter einer Dienstleistung kann einen Nutzer zur Identifizierung an einen Föderationspartner weiterleiten. Nach erfolgreicher Identifizierung kann der Anbieter dann entscheiden, ob der Nutzer zur Nutzung des Diensts berechtigt ist.
I14Y	siehe Interoperabilität
Identifizierung	Der Nachweis oder die Verifizierung einer behaupteten Eigenschaft einer Entität. Wird im Kontext des E-Governments häufig mit der Identitätsfeststellung einer Person gleichgesetzt.
Identity-Provider	Eine Form eines Service-Providers, der Identitätsinformationen für Nutzer erzeugt und verwaltet. Die Dienstleistung des Identity-Providers besteht in der Identitätsfeststellung eines Nutzers für einen Service-Provider innerhalb der Föderation.
IdP	siehe Identity-Provider

Name	Kurzbeschreibung
Infrastrukturkomponente	Eine Komponente einer Umgebung mit einer spezifischen Aufgabe.
Interoperabilität	Ein Qualitätsmerkmal, das die Fähigkeit zur Zusammenarbeit von verschiedenen Systemen, Techniken oder Organisationen beschreibt.
Kompatibilität	Bezeichnet die Fähigkeit eines Systems, die Anforderungen an ein anderes System zu erfüllen. Das System ist dann mit dem anderen kompatibel. Man spricht von Abwärtskompatibilität eines Systems, wenn dieses System zugleich die Anforderungen an die vorangegangene Version desselben Systems erfüllt und von Aufwärtskompatibilität, wenn die gegebene Version auch die Anforderungen an die nächste Version des Systems erfüllt.
Login	Englische Bezeichnung für Anmeldung.
Metadaten	Metadaten oder Metainformationen sind Daten, die Informationen über Merkmale anderer Daten enthalten, aber nicht diese Daten selbst.
Namensraum	Definiert einen baumartig organisierten Bereich, der von anderen Namensräumen abgetrennt ist. In einem Namensraum kann der Verantwortliche Namen frei vergeben. Durch den Identifikator des Namensraums ist eine Kollision mit Begriffen aus einem anderen Namensraum ausgeschlossen.
Nutzer	Bezeichnet eine Person, die ein Hilfsmittel zur Erzielung eines Nutzens, z. B. einer Zeit- oder Kostenverringerung, verwendet.

Name	Kurzbeschreibung
OpenAM	Eine Zugriffsverwaltungs- und Föderationsserverplattform auf OpenSource-Basis.
Personenbezogene Daten	Bezeichnet die einer Person zuordenbaren Daten.
Postfach	Personenbezogener Dienst, der Nachrichten an einen Nutzer eines Servicekontos verwaltet.
Prototyp	Ergebnis der ersten Implementierung eines Konzepts, um möglichst früh Feedback bzgl. der Eignung des Lösungsansatzes einzuholen.
Qualitätsziel	Ein für das zu erstellende Produkt wichtiges Qualitätsmerkmal. Das Qualitätsziel verfügt über eine Begründung, warum die Qualität für das Produkt notwendig ist.
Rahmenbedingung	Beschreibt eine unumstößliche Grundvoraussetzung, die von einer technischen Lösung unbedingt beachtet werden muss. Rahmenbedingungen werden zu Beginn eines Projekts festgelegt. Im Gegensatz dazu werden Anforderungen durch Projektprozesse ermittelt und umgesetzt.
Registrierung	Bezeichnet den Vorgang, über den ein Nutzer ein Servicekonto einrichtet. Zur Registrierung übergibt der Nutzer Informationen, die für die Anmeldung verwendet werden. Richtet ein Nutzer ein Servicekonto für sich selbst ein, wird dies auch als Selbstregistrierung bezeichnet.
Representational State Transfer	Bezeichnet ein Programmierparadigma für verteilte Systeme, insbesondere für Webservices.

Name	Kurzbeschreibung
REST	siehe Representational State Transfer
SAML	siehe Security Assertion Markup Language
SAML-Entity	SAML-Entities sind System-Entitäten, die eine SAML-Rolle übernehmen. Identity-Provider und Service-Provider sind Beispiele für SAML-Entities.
Schnittstelle	Bezeichnet den Teil eines Systems oder einer Komponente, welches der Kommunikation dient. Eine Schnittstelle legt dabei durch ein Protokoll fest, wie Informationen ausgetauscht werden.
Secure Sockets Layer	Ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.
Security Assertion Markup Language	Ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen. In allen Dokumenten wird mit SAML stets Bezug auf die Version 2 dieses Standards genommen.
Service-Provider	Eine Rolle einer Systementität, die Nutzern und anderen Systementitäten Dienste anbietet.
Servicedesk	Zentrale Organisationseinheit für die Aufnahme und Abwicklung von Serviceanfragen der Nutzer von Systemen.
Servicekonto	Ein Servicekonto bietet einem Nutzer personenbezogene Dienste zur Verwendung von Online-Verwaltungsdiensten an. Eine zentrale Aufgabe eines Servicekontos ist die Authentifizierung.
SP	siehe Service-Provider

Name	Kurzbeschreibung
SSL	siehe Secure Sockets Layer
TLS	siehe Transport Layer Security
Transport Layer Security	Ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Nachfolger von SSL.
Vertrauenszone	Vertrauenszonen stellen Verwaltungsdienste und Servicekonten eines Föderationsteilnehmers in eine Vertrauensstellung.
Zertifikat	Bestätigt bestimmte Eigenschaften von Personen oder Objekten, sodass deren Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann.

8 Anhang

8.1 Dokumentation zum technischen Prototyp

Die folgenden Dokumente zum technischen Prototyp stellen den aktuellen Stand dar, der mit den Teilnehmern abgestimmt ist. Die Dokumente liegen diesem Abschlussbericht als PDFs bei.

Name	Kurzbeschreibung	Veröffentlicht	Version
Tour für neue Föderationsmitglieder	Geführte Tour durch die Dokumentation für neue Föderationsmitglieder	05.10.2016	0.1
Überblick über den Lösungsvorschlag	Kurzer Überblick über die umgesetzte Lösung	05.10.2016	0.2
Überblick über die Anwendungsfälle	Liste der Anwendungsfälle, die für die Spezifikation des Lösungsvorschlags betrachtet werden	03.03.2017	0.3
Beschreibung der SAML-Metadaten	Dokumentation der SAML-Metadaten für die an der Föderation teilnehmenden IdPs und SPs	03.03.2017	0.3
Beschreibung der Schnittstellen	Dokumentation der Kommunikationsschnittstellen außerhalb der SAML-Metadaten	03.03.2017	0.3
API-Dokumentation	Informationen zur Nutzung des APIs	03.03.2017	0.3
Kurzanleitung für Föderationsteilnehmer	Liste von Kurzanleitungen, die Aufgaben der Föderationsteilnehmer beschreiben	05.10.2016	0.1
Glossar	Beschreibung der zentralen Begriffe im Kontext von interoperablen Servicekonten der Föderation	05.10.2016	0.1

8.2 Erfahrungsberichte der Teilnehmer

Die Teilnehmer haben ihre Erfahrungen mit dem fachlichen Prototyp sowie eine Beurteilung des Konzepts und dessen Umsetzung in einem jeweils eigenen Bericht dokumentiert.

Name	Autor	Version
Ergebnisdokumentation für den Prototyp Interoperable Servicekonten	AKDB	1.0, Januar 2017
Abschlussbericht Teilprojekt „Konzeption und Prototyp“ im Auftrag Interoperable Servicekonten des IT-Planungsrates	NRW	1.0, Januar 2017

Nach der Erweiterung des Teilnehmerkreises durch die Projektgruppe „eID-Strategie“ haben wir auch die Einschätzungen weiterer Teilnehmer in diesen Bericht aufgenommen.

Name	Autor	Version
Einschätzung zum Konzept des Prototyps, als E-Mail	Herr Krause. Dataport (Berlin)	Dezember 2016

Die Abschlussberichte der Teilnehmer bzw. die Einschätzung wurden in den vorliegenden Abschlussbericht eingearbeitet und sind diesem nicht als separate Dokumente beigelegt. Bei Fragen zu Berichten und Einschätzung sind deren Autoren direkt zu kontaktieren.

8.3 Literaturverweise

Übersicht über weitere Dokumente, die wir im Abschlussbericht benennen.

Name	Stand
Projekt Prototyp für Interoperable Servicekonten, Projektskizze	15. Februar 2016
Interoperables Identitätsmanagement von Servicekonten für Bürgerinnen, Bürger und Unternehmen, Eckpunktepapier	29. Juni 2016
Anforderungen an die Ergebnisdokumentation für den Prototyp	28. November 2016
Rechtliche Rahmenbedingungen für interoperable Servicekonten	13. Mai 2016

8.4 Informationsportal

Die nicht in Form von PDF-Dokumenten vorliegenden Informationen sind online abrufbar. Diese sind passwortgeschützt und daher nur für einen begrenzten Personenkreis zugänglich.

Titel	Hinweis	URL bzw. PDF
Administration	Informationen zur Administration des Informationsportals	https://www.interoperable-servicekonten.de/p/x/DgAh
Architekturdokumentation Interoperable Servicekonten	Architekturdokumentation des technischen Prototypen	https://www.interoperable-servicekonten.de/p/x/YQAy
Home	Homepage des Informationsportals	https://www.interoperable-servicekonten.de/
Spezifikation Interoperable Servicekonten	Bereich im Informationsportal zu den interoperablen Servicekonten	https://www.interoperable-servicekonten.de/p/x/qAAy
Touren	Online-Übersicht der als PDF vorliegenden Dokumentation zum technischen Prototypen	https://www.interoperable-servicekonten.de/p/x/rgAy
Verwaltungsportal 1	Online-Informationen zum technischen Teilnehmer 1	https://www.interoperable-servicekonten.de/p/x/oYBH
Verwaltungsportal 2	Online-Informationen zum technischen Teilnehmer 2	https://www.interoperable-servicekonten.de/p/x/H4FH
Verwaltungsportal 3	Online-Informationen zum technischen Teilnehmer 3	https://www.interoperable-servicekonten.de/p/x/-YBH