Föderales Single-Sign-On im Portalverbund

Prüfung möglicher IT-Architekturansätze sowie technischer und rechtlicher Fragestellungen

Version 1.0

Stand: 01.02.2019

Inhalt

1. Einleitung

Der IT-Planungsrat hat den Aufbaustab FITKO beauftragt, einen Workshop mit IT-Experten des Bundes, der Länder und Kommunen sowie ihrer jeweiligen Dienstleister durchzuführen. Gegenstand des Workshops soll die Erarbeitung eines Architekturkonzeptes zur Realisierung eines Single-Sign-On (SSO) im Portalverbund sein. Berücksichtigt werden sollen ebenfalls die sicherheits- und datenschutzrechtlichen Anforderungen sowie eine Prüfung der Auswirkungen auf Fachverfahren im Backend. Die erarbeiteten Ergebnisse sollen die Grundlage für eine Wirtschaftlichkeitsbetrachtung bilden, die anschließend erstellt werden soll.

Der Aufbaustab FITKO hat aufgrund dieses Beschlusses Anfang Dezember 2018 zu einem zweitägigen Workshop am 16. und 17.01.2019 nach Frankfurt eingeladen. Der Einladung sind zahlreiche Experten aller föderalen Ebenen sowie deren Dienstleister gefolgt. FITKO konnte aus Kapazitätsgründen nicht alle Anmeldungen (ca. 70 Anmeldungen) berücksichtigen. Insgesamt haben 50 Personen an dem Workshop teilgenommen.

Die finalen Ergebnisse wurden am Ende des Workshops zwischen allen Beteiligten schriftlich festgehalten. Die Ergebnisse zu den technischen Fragestellungen wurden im Nachgang zum Workshop durch einen kleineren Arbeitskreis weiter ausgearbeitet und zusammen mit den weiteren Ergebnissen des Workshops unter Leitung der FITKO im vorliegenden Dokument zusammengefasst und mit den Teilnehmern abgestimmt.

2. Ablauf des Workshops

Zu Beginn des Workshops wurde zunächst der aktuelle Sachstand der interoperablen Nutzerkonten vorgestellt und eine Einführung und Begriffsbestimmung zum Thema SSO durchgeführt. Ziel war es, die Teilnehmer mit den aktuellen Rahmenbedingungen vertraut zu machen und eine gemeinsame SSO Begriffsdefinition als Arbeitsgrundlage für den Workshop zu erarbeiten.

Um den Auftrag des IT-Planungsrats ganzheitlich zu betrachten, wurden die Teilnehmer thematisch in zwei Arbeitsgruppen aufgeteilt:

- Alle anwesenden Dienstleister und technischen Experten wurden gebeten, die technischen Aspekte eines SSO zu prüfen und einen möglichen Architekturvorschlag zu erarbeiten.
- Die anderen Teilnehmer behandelten insbesondere die Sicherheits- und Datenschutzanforderungen aus einer rechtlichen Perspektive. Hierbei wurden auch fachliche und organisatorische Fragestellungen behandelt, die im Zusammenhang mit den Auswirkungen von SSO auf die Anwendungslandschaft stehen.

Aufgrund der Komplexität der Fragstellungen, haben die Arbeitsgruppen in mehreren Iterationen gearbeitet und sich zwischen jeder Iteration zu den Ergebnisständen und offenen Diskussionspunkten ausgetauscht.

3. Begriffsdefinition SSO

Im Rahmen des Workshops wurde zunächst mit allen Beteiligten über eine einheitliche SSO Begriffsdefinition diskutiert, um für die spätere Arbeit in den zwei Arbeitsgruppen eine einheitliche Grundlage für die Bearbeitung der Fragestellungen zu haben.

Es wurde übereinstimmend festgestellt, dass SSO ein mehrdeutiger Begriff ist und in der bisherigen Diskussion zum Thema der SSO-Begriff nicht einheitlich verwendet wurde. Zwei Dimensionen wurden als wesentlich für SSO im Kontext des Portalverbunds erachtet:

- **„Single Log-In“ bzw. „Single Account“:** Die Möglichkeit, sich mit nur einem Satz an Zugangsdaten in verschiedene geschützte Dienste einzuloggen bzw. gegenüber verschiedenen Diensten mit einem definierten Vertrauensniveau zu authentisieren.
- **„Anwendungsübergreifende Sessions“ bzw. „SSO-Sessionmanagement“:** Der Zugriff auf verschiedene geschützte Dienste bzw. die Authentisierung gegenüber verschiedenen Diensten mit einem definierten Vertrauensniveau nach einer einmaligen Anmeldung, indem eine anwendungsübergreifende Sitzung (Session) während der Nutzung systemseitig aufrechterhalten wird.

Es wurde im Rahmen der Diskussion übereinstimmend festgestellt, dass die aktuelle Konzeption der interoperablen Servicekonten den ersten Aspekt von SSO („Single Log-In“ bzw. „Single Account“) erfüllt und **daher gängige SSO-Mehrwerte** (bspw. Vereinfachung des Nutzerzugangs sowie leichtere Administration und Weiterentwicklung der Identitäts-managementkomponente) **durch die interoperablen Servicekonten größtenteils realisiert sind**.

Für den weiteren Workshop wurde daher festgehalten, dass sich alle technischen und rechtlichen Betrachtungen auf die Fragestellungen und Herausforderungen im Kontext eines anwendungsübergreifenden Sessionmanagement fokussieren. Daher sind alle Betrachtungen und Bemerkungen im weiteren Dokument in Bezug auf „SSO“ im Sinne eines anwendungsübergreifenden Sessionmanagement zu verstehen.

4. Technik

4.1. Annahmen zur Betrachtung möglicher Architekturansätze für die SSO-Umsetzung

Zur Bewertung der SSO-Lösungsansätze (Architektur und Rahmenbedingungen) wurde auf Basis der drei vom BMI vorgestellten Anwendungsfälle ein generischer Authentisierungs-Workflow definiert. Dieser wird unter Beachtung der Anforderungen verschiedener Rahmenbedingungen betrachtet, die sich aus den Datenschutzverordnungen, der eIDAS- / Durchführungs-Verordnung 2015/1502und der technischen Richtlinie TR-03107-1 des BSI ergeben.

Der generische Authentisierungsablauf ist unabhängig von der jeweiligen Fachlichkeit, ermöglicht aber die Betrachtung des SSO über verschiedene Anwendungsgrenzen hinweg. Dazu wurde der Ablauf für die folgenden vier unterschiedlichen Architekturansätze betrachtet:

1. dezentrales Nutzerkonto (IdP) mit Föderation
2. dezentrales Nutzerkonto ohne Föderation
3. zentraler Nutzerkonto-Proxy
4. zentrales Nutzerkonto

Auf Grund der Aufgabenstellung wurden die Vertrauensniveaus „normal“ und „hoch“ von der detaillierten Betrachtung ausgeschlossen, da aufgrund der genannte Vorgaben ein Vertrauensniveau aufgrund der genannten technischen Richtlinie bei den Servicekonten nicht möglich ist.

4.2. Betrachtung der Vertrauensniveaus im Kontext SSO

Die technische Richtlinie [TR-03107-1] definiert Vertrauensniveau wie folgt:

Um die Qualität und Vertrauenswürdigkeit von Mechanismen charakterisieren und vergleichen zu können, müssen verschiedene organisatorische und technische Faktoren im Zusammenhang betrachtet werden

- die technische Sicherheit des Verfahrens, zum Beispiel die Sicherheit
    - der genutzten Authentisierungsmittel (Token, Passwörter, ...),
    - der relevanten IT-Infrastruktur und
    - der eingesetzten kryptographischen Verfahren;
- die organisatorische Sicherheit des Verfahrens, zum Beispiel
    - die Qualität des Identifikationsprozesses, das heißt, wie vertrauenswürdig die persönlichen Daten bei der Registrierungsinstanz nachgewiesen werden, sowie den Nachweis der Zugehörigkeit der Daten zur Person,
    - die Qualität des Ausstellungs- und Auslieferungsprozesses der Authentisierungsmittel (zum Beispiel per E-Mail, Briefpost, Download, persönliche Übergabe),
    - die Vertrauenswürdigkeit des Ausstellers (zum Beispiel Staat, Zertifizierungsstelle, private Organisation)
    - die Vertrauenswürdigkeit der Beteiligten in der Nutzungsphase (zum Beispiel Identity Provider, dritte Stellen bei der Datenübermittlung);
- die rechtlichen Rahmenbedingungen, insbesondere Regelungen in den Prozessordnungen (z.B. Beweislastregelungen wie widerlegliche gesetzliche Vermutungen) oder besondere gesetzliche Verpflichtungen beteiligter Stellen.

Darüber hinaus werden gegebenenfalls bekannte konkrete Schwachstellen oder Sicherheitslücken sowie Angriffe gegen Mechanismen berücksichtigt.

Die technische Richtline [TR-03107-1] definiert drei Vertrauensniveaus:

- normal: Die Schadensauswirkungen bei einer Kompromittierung sind begrenzt und überschaubar. Dieses Vertrauensniveau entspricht in etwa dem Sicherheitsniveau normal gemäß IT-Grundschutz [BSI100-2].
- substantiell: Die Schadensauswirkungen bei einer Kompromittierung sind substantiell. Dieses Vertrauensniveau liegt zwischen den Sicherheitsniveaus normal und hoch gemäß IT-Grundschutz [BSI100-2].
- hoch: Die Schadensauswirkungen bei einer Kompromittierung können beträchtlich sein. Dieses Vertrauensniveau entspricht in etwa dem Sicherheitsniveau hoch gemäß IT-Grundschutz [BSI100-2].

Diese Definition von Vertrauensniveaus findet sich - im Wesentlichen entsprechend - auch in der eIDAS-Durchführungsverordnung [eIDAS LoA] wieder (vgl. auch Anhang A in [TR-03107-1]).

Im Rahmen der technischen Betrachtung SSO wird nur das Vertrauensniveau „substantiell“ analysiert. In diesem Kontext sind im Wesentlichen folgende Bedingungen zu betrachten:

Kriterien	Maßnahmen
Bindung der Identifizierung an den Sitzungskontext	kryptographisch sichere Session-Identifier/-Cookies
Authentisierung (Faktoren/ Verfahren)	Zwei Faktoren aus unterschiedlichen Kategorien (Besitz, Wissen, Biometrie) / dynamische Authentisierung

4.3. Vier mögliche Architektur-Ansätze zu Umsetzung SSO

Single Sign-On (SSO) bedeutet, dass ein Nutzer nach einer einmaligen Authentisierung an einem System auf alle Dienste dieses Systems zugreifen kann, zu denen er berechtigt ist, ohne sich erneut anmelden zu müssen. Ziel des SSO ist es, dass sich der Benutzer nur einmal mit Hilfe eines Authentifizierungsverfahrens identifiziert. Danach übernimmt der SSO-Mechanismus die Aufgabe, den Anwender zu authentifizieren (die erkannte physische Identität zu bestätigen). Somit entfällt jede weitere Authentisierungs-Interaktion zwischen Diensten und Anwender.

Für Webdienste wird in der Regel die Security Assertion Markup Language (SAML) als Protokoll verwendet, um SSO umzusetzen.

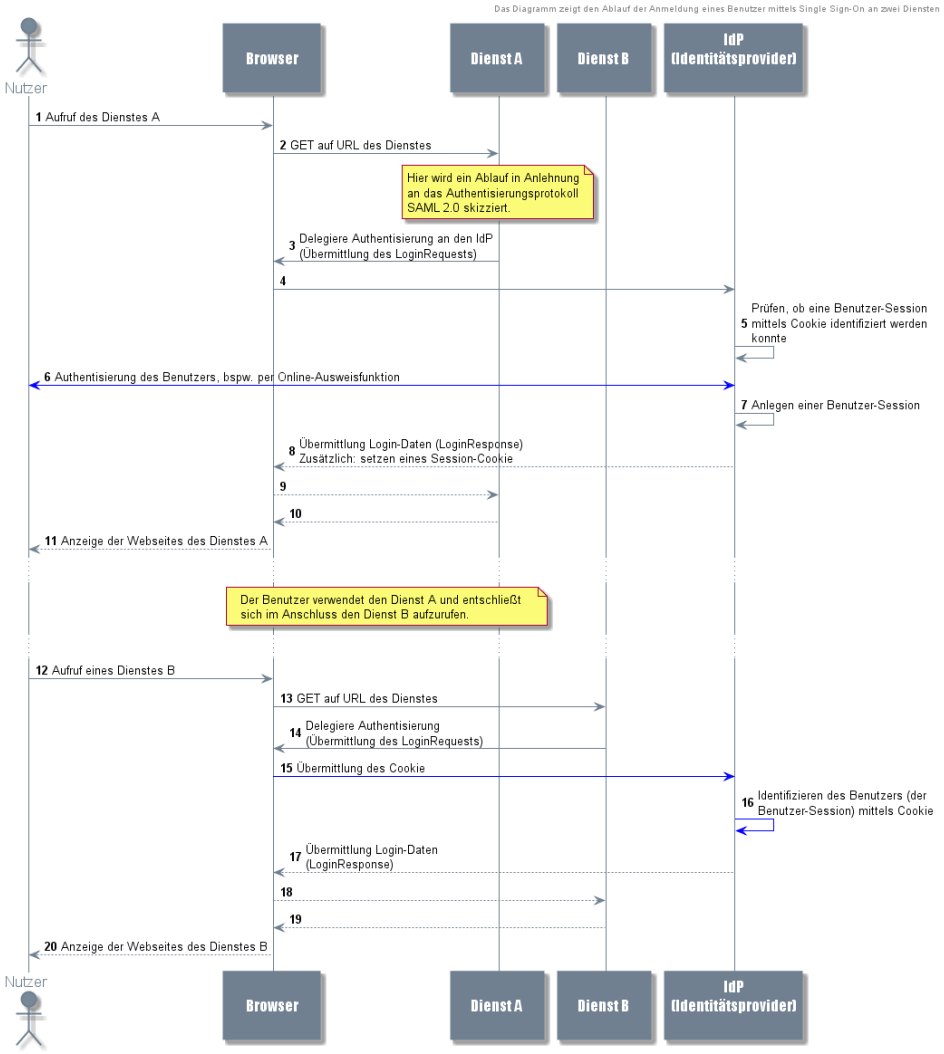
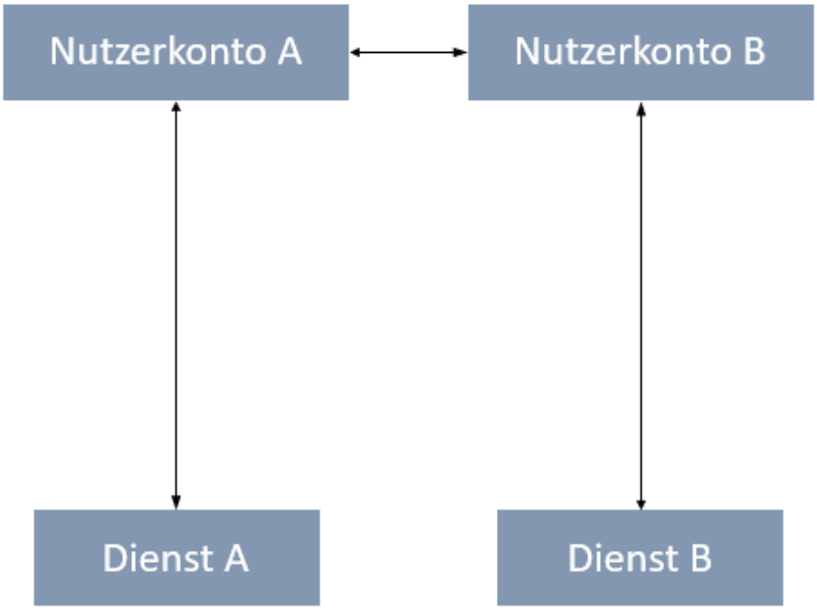


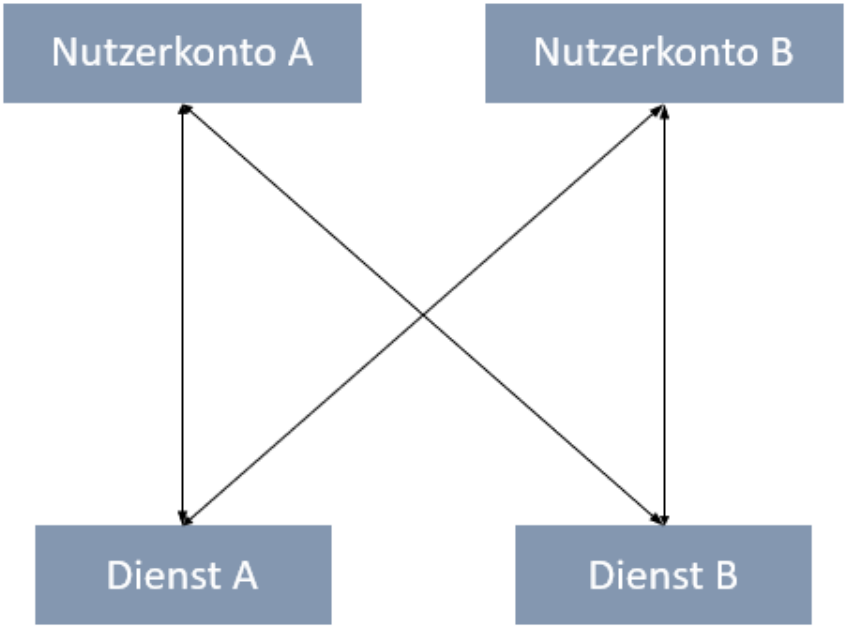
Abbildung 1: Schematischer Ablauf SSO

Dieser prinzipielle Ansatz kann technisch in ganz unterschiedlichen Architektur-Ansätzen realisiert werden. Wesentliche Unterschiede ergeben sich aus einem dezentralen oder zentralen Ansatz der Authentisierung. Der Authentisierungs-Ablauf wurde für die vier nachfolgenden Architektur-Ansätze bewertet:

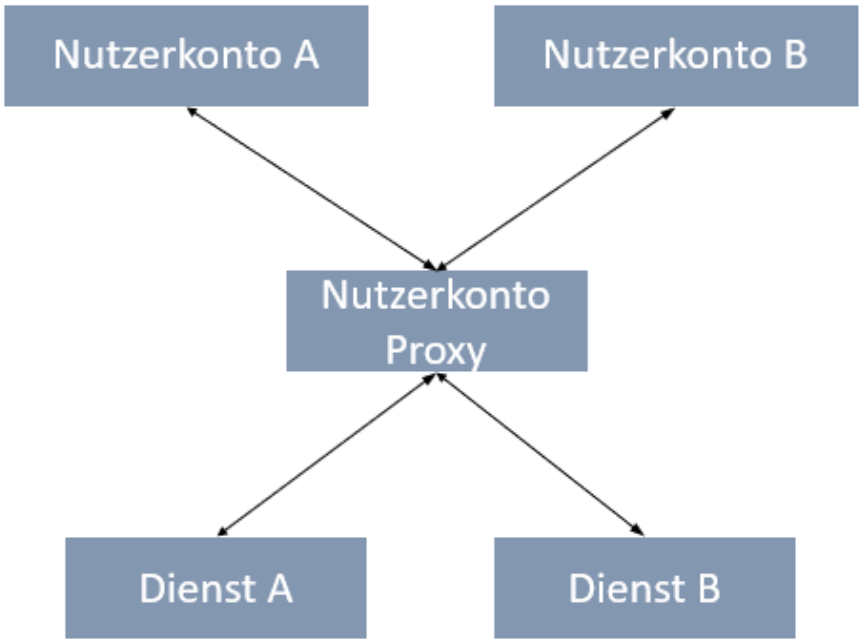
1. **Dezentrales Nutzerkonto mit Föderation**
   Dieser Architektur-Ansatz setzt eine Vertrauensstellung zwischen den Nutzerkonten voraus. Aufgrund der Vertrauensbeziehung der Nutzerkonten untereinander, kann ein Dienst am Nutzerkonto B auch am Nutzerkonto A verwendet werden. Dabei handelt es sich um einen etablierten Standard, welcher in der Praxis heute schon im Rahmen der interoperable Servicekonten Anwendung findet.



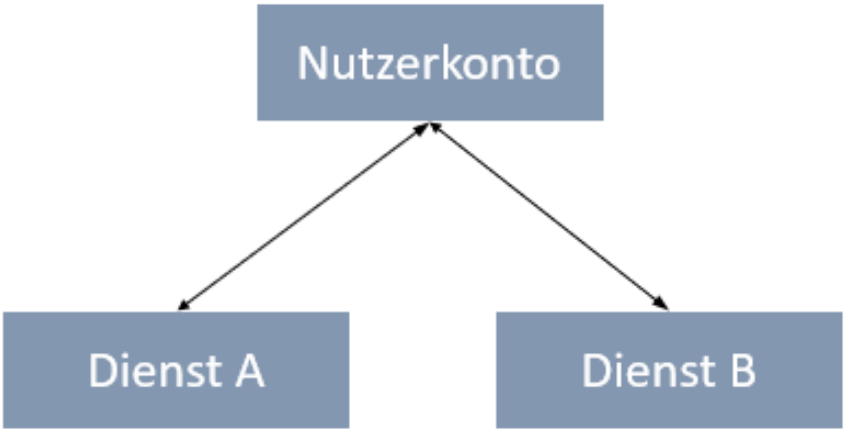
2. **Dezentrales Nutzerkonto ohne Föderation**
   Dieses Model entspricht dem Peer-To-Peer Modell, bei dem ein Onlinedienst allen Nutzerkonten vertraut.



3. **Zentraler Nutzerkontoproxy**
   Bei diesem Architektur-Ansatz greifen alle Onlinedienste über einen zentralen Nutzerkontenproxy auf die dezentralen Nutzerkonten zu.



4. **Zentrales Nutzerkonto**
   Bei einem zentralen Nutzerkonto gibt es nur eine Instanz, welche die Nutzerdaten verwaltet und alle Onlinedienste verwenden genau dieses Nutzerkonto.



Bei der Analyse dieser vier Architektur-Ansätze in Bezug auf das Vertrauensniveau „substantiell“ fällt auf, dass die geforderten Kriterien bereits bei nur einem Nutzerkonto kritisch zu betrachten sind.

So spielt der Wechsel der Anwendung und das für „substantiell“ dann geforderte Kriterium einer Zwei-Faktor-Authentisierung (2FA) eine wesentliche Rolle bei der Betrachtung. Für die 2FA werden zwei Faktoren unterschiedlicher Kategorie (Besitz, Wissen, Inhärenz) benötigt. Es handelt sich dabei um die Schritte 15 und 16 in Abbildung 1.

Für das Vertrauensniveau „normal“ ist dieser Ansatz durchaus mit den geltenden Vorgaben umsetzbar, da hier keine 2FA erforderlich ist. Für das Vertrauensniveau „substantiell“ ist ein Anwendungswechsel mit SSO aber genauer zu betrachten.

4.4. Analyse eines Wechsels der Anwendungen mit Niveau substantiell im Kontext SSO

Aus der Abbildung 1 geht hervor, dass ein Nutzer der einen Dienst verwenden möchte, von diesem zur Authentisierung zu einem Nutzerkonto (IdP) weitergeleitet wird. Dieses führt die Authentisierung entsprechend dem Vertrauensniveau durch. Dazu ist zum Beispiel die Anmeldung mit einer Smartcard durchzuführen, welche Besitz (Besitz der Karte) und Wissen (Kenntnis der PIN) trennt.

Der IdP kann über ein Token Binding (z.B. [IETF-Drafts]) die Session des Nutzers kryptografisch mit der Identifikation des Nutzers verknüpfen. Zur Umsetzung des Szenarios ist es wichtig, dass alle beteiligten Komponenten die verwendeten Technologien unterstützen. Der Einsatz von Token Binding erfüllt allerdings nicht die Anforderungen an das Vertrauensniveau „substantiell“, da in diesem Fall zwar zwei Faktoren zum Einsatz kommen, diese aber nicht aus zwei unterschiedlichen Kategorien stammen. Zusätzlich unterstützen nicht alle aktuell verfügbaren Browser Token Binding.

Erfolgt nach erfolgreicher Authentisierung ein Wechsel zu einer zweiten Anwendung, welche ebenfalls eine Authentisierung erfordert, so erfolgt ebenfalls eine Weiterleitung zum IdP. Anhand des Session-Cookies erkennt dieser, dass der Nutzer bereits erfolgreich authentisiert ist und reicht die Informationen ohne erneute Abfrage der Authentisierungsinformationen an den Dienst weiter. Hier ist anhand der Durchführungsverordnung (EU) 2015/1502 und der Technischen Richtlinie [TR-03107-1] zu bewerten, ob diese erneute Authentisierung nur anhand des Tokens und der Session-Informationen für das Niveau „substantiell“ ausreichend sind.

Geht man davon aus, dass beide Dienste im Rahmen einer einzelnen Anwendung (d.h. eines Vertrauensraums) verwendet werden, so sollte dies durchaus zulässig sein (z.B. bei einem Enterprise-SSO). Anders sieht es bei anwendungsübergreifenden Diensten aus. Von der Authentisierung am ersten Dienst steht nur das Session-Cookie als Authentisierungsfaktor zur Verfügung. Dieser reicht nicht aus, um die Bedingung einer Zwei-Faktor Authentisierung am zweiten Dienst zu erfüllen. Deshalb ist hier eine erneute Zwei-Faktor-Authentisierung notwendig. Dies wäre dann genauso wie bei interoperablen Servicekonten jedoch kein SSO im engeren Sinne mehr.

Aus diesem Grund ist es notwendig, die Grenzen einer „Anwendung“ zu definieren. Diese liegen in der Regel bei der Datenhoheit und der damit verbunden Datenschutz-Verantwortlichkeit.

Ein übergreifendes Thema ist die Logout-Funktion in verschiedenen Anwendungen. Da ein Logout nicht pauschal aus allen aktiven Anwendungen möglich/gewünscht ist, wären in den Anwendungen unterschiedliche Logout-Funktionen gleichzeitig anzubieten. So muss der Anwender entscheiden, aus welcher Anwendung die Abmeldung (lokal/global, Reihenfolge) erfolgen soll. Eine zeitliche Befristung der Authentisierung würde nach Ablauf der Zeit zu einer automatischen Abmeldung führen. Dazu müssen alle Fachanwendungen die zeitlich begrenzte Gültigkeit der Authentisierung automatisch erneuern (Renew). Diese Funktionalität müssten alle Fachanwendungen zur Verfügung stellen.

Grundsätzlich sind auch Fragen zur Usability zu klären. Die Nutzung unterschiedlicher Anwendungen/Dienste wird durch den SSO- Einsatz vereinfacht. Wenn durch die erhöhten Anforderungen der Vertrauensniveaus eine automatisierte Authentisierung technisch nicht möglich ist (2FA), sind andere Mechanismen (z.B. mTAN) ein möglicher Ansatz, wobei hierbei der SSO-Mehrwert hinsichtlich einer einmaligen Authentifizierung nicht gegeben ist.

Abschließend lässt sich hierbei feststellen mit den aktuellen technischen und organisatorischen Regelungen ein SSO auf substantiellem Niveau mit allen 4 Architekturansätzen nicht möglich scheint.

5. Rechtliche Bewertung der Sicherheits- und Datenschutz-anforderungen

5.1. Bewertung der Rechtsgrundlagen für eine SSO Einführung

5.1.1. Gesetzliche Rahmenbedingungen für die föderale SSO Umsetzung

Rechtsgrundlagen / Bewertung:

Nach Einschätzung der anwesenden Fachleute sind keine rechtlichen Verpflichtungen und Ermächtigungen für die SSO Umsetzung vorhanden. Weder im Onlinezugangsgesetz noch in europäischen Regelungen wie der eIDAS und Single Digital Gateway Verordnung lassen sich Vorgaben für die Umsetzung eines SSO erkennen. Diese werden jedoch als notwendig erachtet, um eine rechtlich konforme und verbindliche Einführung von SSO im Portalverbund zu ermöglichen.

Handlungsbedarfe:

Die hierfür relevanten Gesetze wären durch Bund und Länder anzupassen. Diese gesetzlichen Anpassungen wären ggf. durch eine Rahmenregelung zu ergänzen, um eine einheitliche Umsetzung von SSO zu gewährleisten. Hierbei sind jedoch rechtliche Bedenken hinsichtlich der föderalen Zuständigkeiten von Ländern und Kommunen zu beachten. (Siehe Abschnitt 5.1.2)

5.1.2. Eingriff in die Länderhoheit/Kommunen

Rechtsgrundlagen / Bewertung:

Gemäß § 4 Abs. 1 i.V.m. § 2 Abs. 6 OZG dürfen nur IT-Komponenten vorgegeben werden, die für die Abwicklung des Portalverbunds erforderlich sind. SSO ist eine IT-Komponente im Sinne § 4 Abs. 1 i.V.m. § 2 Abs. 6.

Es ist zunächst zu prüfen, ob SSO für die Abwicklung des Portalverbunds erforderlich ist und damit eine verpflichtende Vorgabe rechtlich zulässig ist, da im Rahmen des Workshops seitens der Länder angemerkt wurde, dass hierzu Zweifel bestehen und daher eine rechtliche Klärung notwendig ist.

Darüber hinaus wäre zu prüfen, ob die Verpflichtung zu SSO ein Eingriff in die kommunale Selbstverwaltungsgarantie und Gewährleistung der verfassungsmäßigen Ordnung der Länder darstellt. Die Verwaltungsverfahrensgesetzgebung liegt grundsätzlich in den Ländern. Die Abwicklung eines elektronischen Verwaltungsverfahrens wird im Wesentlichen in den Landesverfahrensgesetzen geregelt. Grundsätzlich gilt der Grundsatz der Nichtförmlichkeit des Verfahrens, soweit keine besonderen Rechtsvorschriften für die Form des Verfahrens bestehen.

Fällt ein Verfahren in die Länderkompetenz oder gar in die Selbstverwaltungshoheit einer Kommune, muss es die Vorgaben des Bundes zum elektronischen Verfahren nicht beachten. Die grundlegende Entscheidung, welche Anforderungen an die Authentifizierung gestellt werden oder wie ein Verfahren ausgestaltet wird, würde den Kommunen und Ländern

entzogen. Daher könnte in der Verpflichtung zu SSO ein Verstoß gegen Art. 20, Art. 28 Abs. 2, Art. 70 GG vorliegen.

Handlungsbedarfe:

Es ist zu prüfen, ob eine verpflichtende Umsetzung von SSO für Länder und Kommunen rechtlich zulässig ist.

5.1.3. Europarechtliche Fragestellungen im Kontext eIDAS

Rechtsgrundlagen / Bewertung:

Nach dem aktuellen Stand der deutschen Regelungen zu Vertrauensniveaus, ist ein SSO nur bis zum Niveau „substantiell“ umsetzbar. (Siehe technische Betrachtung Abschnitt 4 ff.) Deutschland fordert bei der Schriftform das Vertrauensniveau „hoch“. Es könnte bei notifizierten Tokens eines EU-Bürgers auf dem Vertrauensniveau „hoch“ zu Verstößen auf Basis der Anerkennungsverpflichtung der eIDAS-Verordnung kommen, wenn ein SSO für diese EU-Bürger ausgeschlossen wird.

Handlungsbedarfe:

Prüfung, ob ein Regelverstoß gegen EU-Recht vorliegt und ob technische und organisatorische Ausnahmeregelungen vom SSO für EU-Bürger für den vorliegenden Fall notwendig und möglich wären.

5.1.4. Beweiswerterhaltung der Willenserklärung bei SSO

Rechtsgrundlagen / Bewertung:

Auch im Bereich der digitalen Verwaltung werden Anträge einer Person als empfangsbedürftige verwaltungsrechtliche Willenserklärungen / Handlungen eingeordnet.

Um im Streitfall beweisen zu können, dass eine Willenserklärung / Handlung von einer bestimmten Person und damit unter Nutzung eines bestimmten Zertifikats zu einem bestimmten Zeitpunkt abgegeben wurde, bedarf es einer komplexen technischen Ausgestaltung des Anmeldevorgangs und der Abgabe der Willenserklärung. Wie SSO im konkreten Fall ausgestaltet werden soll, lässt sich mangels eines vollständigen technischen und organisatorischen Konzepts nicht beurteilen.

Da Sessions serverseitig nur dann zwangsweise beendet werden können, wenn der Nutzer für eine bestimmte Zeit inaktiv war, besteht jedoch bei SSO stets die Gefahr, dass Sessions von Dritten übernommen werden können. Folglich könnte es in einer SSO-Umgebung zweifelhaft sein, ob die Willenserklärung vom eingeloggten Bürger oder jemand anderen (z.B. Ehefrau, Nachnutzer im Internetcafe) abgegeben wird.

Um hier ganz sicher zu gehen, müssten Transaktionsbestätigungen pro Willenserklärung (sich erneut anmelden oder TAN-Verfahren wie bei Banken) in die Antragsverfahren eingebaut werden, was dazu führen würde, dass SSO seinen originären Vorteil verlieren würde.

Handlungsbedarfe:

Um das genannte Problem rechtlich zu umgehen, wäre eine Anpassung der rechtlichen Regelungen hin zur Einführung einer Anscheinsvollmacht im Rahmen von SSO-Sessions eine mögliche Lösung. Alternativ zu einer solchen umfangreichen rechtlichen Anpassung wäre eine verpflichtende technische Lösung zur Transaktionsbestätigung vorzusehen, dass die genannten Risiken minimiert, jedoch den eigentlichen SSO-Mehrwert eines einmaligen Log-Ins bzw. einer einmaligen Authentifizierung nicht mehr ermöglicht.

5.1.5. Wechsel der Vertrauensniveaus innerhalb einer Session

Rechtsgrundlagen / Bewertung:

Es ist anzunehmen, dass in der Praxis folgende Fälle auftreten können:

- Ein Antragsprozess mit wechselnden Vertrauensniveaus
- Der Nutzer nutzt innerhalb einer Session mehrere Verfahren mit unterschiedlichen hohen Vertrauensniveaus

Dies erfordert nach der Bewertung der aktuellen rechtlichen Vorgaben einen Wechsel der Vertrauensniveaus. Ein Wechsel des Vertrauensniveaus (sowohl nach unten als nach oben) erfordert nach aktueller Einschätzung eine erneute Authentifizierung (nach oben ist dies zwingend). Da das BSI empfiehlt, hohe Vertrauensniveaus so schnell wie möglich zu beenden, wäre bei einem Wechsel auf ein Verfahren mit einem niedrigeren Vertrauensniveau ein „Downgrade“ mit erneuter Anmeldung notwendig. Analoges gilt bekanntermaßen für den „Upgrade“-Fall. Ein echtes SSO für Nutzer des Verwaltungsportals wäre in diesen betrachteten Fällen nicht gegeben.

5.1.6. Abmeldung aus dem SSO

Rechtsgrundlagen / Bewertung:

Um ein SSO einzuführen, ist ein praktikables und rechtssicheres Log-Out Verfahren vorzusehen, das sowohl den Log-Out aus einer einzelnen Anwendung als auch aus der gesamten SSO-Session regelt. Bei der Implementierung einer solchen Log-Out Funktion ist aus Sicht des Nutzers sicherzustellen, dass die Bearbeitung von nicht abgeschlossenen Onlineanträgen nicht unbeabsichtigt beendet wird. Hierbei ist die Benutzerführung des SSO so zu gestalten, dass SSO für den Nutzer weiterhin einen Mehrwert bietet und für alle potentiellen Nutzergruppen verständlich und transparent ist.

Handlungsbedarfe:

Es ist zu prüfen, welche rechtlichen Anforderungen an ein sicheres Log-Out Verfahren in einer SSO-Session bestehen. Auf dieser Basis wäre ein rechtskonformes Log-Out Konzept für SSO zu erstellen, dass die Anforderungen an eine hohe Usability erfüllt und technisch in der bestehenden Anwendungslandschaft umsetzbar ist. Dieses Konzept wäre zwingend vor der Durchführung einer Wirtschaftlichkeitsbetrachtung für die SSO-Umsetzung zu erarbeiten.

5.2. Datenschutzanforderungen von SSO

Aus Sicht der Beteiligten handelt es sich bei SSO um ein datenschutzrelevantes Thema. Hierbei wurden einige datenschutzrelevante Anforderungen und Herausforderungen identifiziert.

Einwilligung zur Teilnahme

Eine verpflichtende Teilnahme am SSO erscheint rechtlich nicht zulässig. Es wäre daher eine Einwilligung zur Teilnahme am SSO notwendig. Es ist jedoch unklar, ob eine Einwilligung gemäß der Datenschutzgrundverordnung möglich ist.

Vorgeschaltete Erklärung

Dem Bürger müsste zu Anfang der Authentifizierung in Onlineverfahren (Nutzerkonten, Portalverbund) umfassend in einer vorgeschalteten Erklärung vermittelt werden, dass er sich bundesweit in einem SSO-Umfeld anmeldet und folglich nach einer Authentifizierung alle Willenserklärungen aus dieser Session gegen sich gelten lassen muss.

Tracking während der SSO Session

Datenschutzrechtlich ist die einfache Verknüpfung verschiedener Datenbestände bedenklich. Theoretisch könnten umfassende Auswertungen über die Nutzeraktivitäten während einer SSO-Session erstellt werden.

Einhaltung der datenschutzrechtlichen Anforderungen während einer Session

Das SSO darf nicht die datenschutzrechtlichen Anforderungen aushebeln, dass Fachverfahren nur solche Daten auslesen, die für die Umsetzung des Verfahrens datenschutzrechtlich erforderlich sind. Hinsichtlich der Übernahme von Daten muss auch während der Session eine Einwilligung des Nutzers für die einzelne Weitergabe erfolgen.

Handlungsbedarfe:

Es ist zu prüfen, ob eine Einwilligung rechtlich zulässig ist. Es müssen zudem technische Maßnahmen geplant und implementiert werden, um die identifizierten datenschutzrechtlichen Anforderungen zu erfüllen.

5.3. Sicherheits- und Risikoaspekte

SSO würde eine zentrale Session erfordern, die einen Angriffsvektor darstellt. Bei Banken sind in aller Regel die Sessions auf ca. 10 Minuten begrenzt, danach erfolgt aus Sicherheitsgründen ein automatisches Log-Out („Session-Timeout“). Zum Ausfüllen eines elektronischen Antrags wird man aber regelmäßig mehr Zeit benötigen, weshalb technische Maßnahmen zu implementieren sind, die eine Verlängerung der Session gemäß den Aktivitäten des Nutzers vorsieht.

Darüber hinaus wäre eine zentrale Komponente für ein SSO, falls dies technisch erforderlich und vorgesehen wäre, eine zentrale Angriffsschwachstelle. Der Ausfall einer solchen zentralen Technologie würde das gesamte E-Government in der Bundesrepublik lahmlegen.

Aufgrund dieser Angriffs- und Ausfallsrisiken wären auch entsprechende Verantwortlichkeiten und Haftungsregeln zu definieren und vorzusehen. (Siehe Abschnitt 6)

5.4. Abschließende Bewertung des rechtlichen Sachstands einer SSO-Einführung

Aufgrund der identifizierten Handlungsbedarfe, die sich aus der Bewertung der aktuellen Rechtsgrundlagen ergeben sowie der datenschutzrechtlichen und sicherheits- bzw. risikobezogenen Anforderungen, wurden folgende übergreifende Handlungsbedarfe benannt, die vor der Fortführung der SSO-Planung zwingend zu adressieren sind:

- **Validierung und Prüfung der identifizierten Handlungsbedarfe:** Da aufgrund der zeitlichen und personellen Rahmenbedingungen keine tiefgreifende juristische Prüfung aller Handlungsbedarfe und Anforderungen möglich war, wird vorgeschlagen, alle identifizierten Punkte in einem oder mehreren juristischen Gutachten tiefergehend zu überprüfen.
- **Realisierbarkeit der Nutzermehrwerte des SSO prüfen:** Viele der beschriebenen Handlungsbedarfe haben nach derzeitiger Einschätzung einen erheblichen Einfluss auf die technische und konzeptionelle Ausgestaltung des SSO (bspw. durch zwingende Einführung eines zweiten Faktors für Transaktionen) und würden damit jeglichen Vorteilen eines SSO entgegenstehen. Es ist daher zu prüfen, ob und wie eine nutzerorientierte Ausgestaltung eines SSO unter diesen Rahmenbedingungen möglich ist.

6. Organisatorische Anforderungen

Im Rahmen der rechtlichen Prüfung wurden auch einige organisatorischen Aspekte identifiziert, die vor einer SSO Einführung zu klären wären:

- Organisationstrukturen und Zuständigkeiten für die Planung, Einführung und Betrieb des SSO.
- Zertifizierungsprozess für die Anbindung von Anwendungen und Servicekonten an das SSO.
- Klärung von Fristen und Verbindlichkeiten zur Umsetzung der SSO-Anbindung.
- Klärung der Kostenübernahmen für die Entwicklung der Infrastruktur, Anpassung der Anwendungen und mögliche Steigerungen in den Betriebskosten.
- Klärung von Haftungsfragen in Bezug auf Sicherheitsrisiken und Serviceausfälle.
- Klärung, wie die Planung und Umsetzung des SSO von den aktuellen Aktivitäten im Bereich der interoperablen Servicekonten entkoppelt werden kann, um dort die Planungssicherheit zu erhalten und mit Hinblick auf die Vorgaben des OZG und Single Digital Gateway schnell in die weitere operative Umsetzung von Onlinediensten zu kommen.

7. Abschließende Diskussion und Fazit

Bei den identifizierten Hindernissen und Anforderungen gab es eine hohe Übereinstimmung zwischen den Arbeitsgruppen. Die anschließenden Diskussionen im Workshop haben als Ergebnis herausgearbeitet, dass aufgrund dieser identifizierten technischen, rechtlichen und organisatorischen Hindernisse ein SSO im Portalverbund aktuell nicht möglich ist.

Einige der identifizierten Hindernisse wie die fehlenden Voraussetzungen für das Token Binding, lassen sich nach heutigem Stand nicht lösen, da sich die notwendigen Voraussetzungen erst am Markt und bei den Endnutzern im Portalverbund durchsetzen müssen.

Zur Beseitigung vieler anderer Hindernisse wären zunächst umfangreiche juristische Prüfungen und Machbarkeitsuntersuchungen sowie gesetzliche Änderungen seitens Bund und Ländern notwendig, wobei auch hier nach dem heutigen Wissensstand unklar ist, ob letztendlich ein nutzerfreundliches SSO technisch und rechtlich realisierbar wäre. Zudem wären die Auswirkungen auf die Antragsverfahren aktuell gravierend, da sich die hierfür notwendigen Standards (bspw. SAML 2.0, OpenID Connect) erst langsam im Zuge der Weiterentwicklungs- und Erneuerungszyklen durchsetzen.

Aufgrund der noch ungeklärten technischen, rechtlichen und organisatorischen Fragestellungen bestehen daher erhebliche Bedenken, ob eine Wirtschaftlichkeitsbetrachtung im Sinne des IT-Planungsratsbeschlusses zum gegenwärtigen Zeitpunkt erstellt werden kann. Hierzu bedarf es zunächst einer Klärung der weiteren Vorgehensweise, bevor eine seriöse Kosten- / Nutzen-Betrachtung erfolgen kann. Daher wird empfohlen, auf eine Wirtschaftlichkeitsbetrachtung aktuell zu verzichten.

Im Übrigen erfüllt die aktuelle Konzeption der interoperablen Servicekonten den Aspekt „Single Log-In“ bzw. „Single Account“. Daher sind die **gängigen Mehrwerte von SSO** (bspw. Vereinfachung des Nutzerzugangs sowie leichtere Administration und Weiterentwicklung der Identitätsmanagementkomponente) bereits **durch die interoperablen Servicekonten größtenteils realisiert**.

Sofern die Realisierung eines SSO im Portalverbund weiterhin verfolgt werden sollte, wären zunächst die dargestellten Fragestellungen zu klären und zu lösen. Erst danach können valide Aussagen zu Architekturkonzepten, und damit auch die zu erwartenden Aufwände dem realisierbaren Nutzen gegenübergestellt werden.

8. Anhang

8.1. Technische Dokumente und Richtlinien

[BSI100-2]	Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Vorgehensweise, Version 2.0, 2008
[eIDAS LoA]	Europäische Union (EU): DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, September 2015
[TR-03107-1]	Bundesamt für Sicherheit in der Informationstechnik (BSI): Elektronische Identitäten und Vertrauensdienste im E-Government – Teil 1: Vertrauensniveaus und Mechanismen, Version 1.1, November 2016
[IETF-Drafts]	Satz von Requests for Comments (RFC) bei der IETF für eine kryptografische Bindung von Token an Sessions auf Basis einer TLS-Erweiterung (insb. draft-ietf-tokbind-protocol, draft-ietf-tokbind-negotiation und draft-ietf-tokbind-https).