Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

der Bundeswehr Universität München

Projekt DISKURS: Digitale Identitäten für ServiceKonten: Umsetzungsstrategien, Richtlinien und Sicherheitsaspekte

gefördert durch:

Bayerisches Staatsministerium für Digitales

Abschlussbericht

Bedarfsträger	Bayerisches Staatsministerium für Digitales (StMD)
Zuwendungsempfänger	Universität der Bundeswehr München (UniBw M)
Laufzeit des Vorhabens	01.12.2019 – 31.03.2021

Autoren: Michael Grabatin, Wolfgang Hommel

Stand: 30. März 2021

1 Zusammenfassung

Die Aktivitäten des Projekts DISKURS sind zu drei größeren Blöcken, die als *Schritte* bezeichnet werden, zusammengefasst: *technischer Föderationsbetrieb*, *organisatorischer Föderationsbetrieb* und *Demonstration technischer Weiterentwicklungen.*

Dieses Dokument fasst vereinbarungsgemäß die Ergebnisse des Projekts in knapper Berichtsform zusammen. Die geplanten Aktivitäten wurden im vorgesehenen Zeitrahmen und budgetierten Aufwand durchgeführt, alle vereinbarten Meilensteindokumente vorgelegt, besprochen und abgenommen.

Die einzelnen Arbeitsschritte des Projektes, auf die im Folgenden näher eingegangen wird, waren im Wesentlichen:

- **Schritt 1**: Im ersten Schritt wurde der auf Skalierbarkeit ausgelegte Aufbau der zentralen Komponenten zur Erreichung der Interoperabilität von Servicekonten wissenschaftlich begleitet. Hier wurden insbesondere grundlegende Fragen zum Föderationsbetrieb und zu Best-Practice-Ansätzen besprochen. Grundlage hierfür waren Erfahrungen aus dem Umfeld der Wissenschaftsföderationen DFN-AAI und eduGAIN.
- **Schritt 2**: Im zweiten Schritt wurde der Aufbau der notwendigen Organisationsstruktur zum Betrieb einer Identitätsföderation und ihrer Prozesse unterstützt. Im Austausch mit dem IT-Dienstleistungszentrum des Freistaats Bayern (IT-DLZ) wurden in diesem Schritt Föderationsprozesse nach ITIL erstellt und verbessert. Basis hierfür waren wiederum langjährige Erfahrung im IT-Service-Management, insbesondere im Umfeld von Identitätsföderationen.
- **Schritt 3**: Im dritten Schritt wurde die nahtlose Integration von eGovernment-Diensten in das Online-Nutzungsverhalten der Bürger untersucht und exemplarisch demonstriert, wie zukünftige Identitätsnachweisverfahren und Authentifizierungssysteme aussehen können. In Anbetracht aktueller Entwicklungen wurde hier Self-Sovereign Identity Management vorgestellt und im Rahmen eines Prototyps demonstriert.

2 Ergebnisse

Dieser Abschnitt beschreibt die Aufgaben und Ergebnisse, die im Projekt DISKURS erarbeitet wurden, näher. Zunächst werden die Ziele der einzelnen Schritte in Abschnitt 2.1 beschrieben. Wie diese Ziele erreicht wurden, ist im darauffolgenden Abschnitt 2.2 zusammengefasst.

2.1 Zielsetzung und Anpassungen

Der folgende Abschnitt beschreibt die Kernthemen des ursprünglichen Projektplans für DISKURS und daran – in Absprache mit dem StMD – durchgeführte Anpassungen.

Schritt 1: Technischer Föderationsbetrieb Die Unterstützung im Schritt 1 erfolgte wie geplant nach dem Projektplan.

Es wurde eine Analyse der Vertrauensniveaus (normal/niedrig, substantiell, hoch) entsprechend des OZG, der Technischen Richtlinie TR-03107-1 des BSI und eIDAS hinsichtlich des Bedarfs verschiedener Verwaltungsleistungen vorgenommen. Dabei wurde ermittelt, welche Vertrauensniveaus technisch erreichbar und notwendig sind. Zusätzlich wurde in diesem Projektteil auch die Verwendung von Elster-Zertifikaten zur Authentifizierung über normal (Elster-Kompromiss) betrachtet.

Ebenso wurde das für FINK überarbeitete und eingeschränkte SAML 2.0 Web Browser Single-Sign-On-Profil, welches die Kommunikation zwischen den verschiedenen Identity-Providern (IdP) und Service-Providern (SP) in der Dipol-Architektur regelt, analysiert und auf potenzielle Konflikte, Inkompatibilitäten und eingebrachte Schwachstellen hin untersucht. Es wurde getestet, ob die Änderungen zu Problemen mit üblicherweise verwendeter und frei verfügbarer SAML-Software (Shibboleth, simpleSAMLphp) führen können.

Ein weiterer Punkt dieses Abschnitts war die Betrachtung der Syntax und Semantik von Nutzerattributen, die zwischen den verschiedenen Teilnehmern ausgetauscht werden sollen, im Allgemeinen aber in nicht einheitlichen Quellformaten vorliegen. Hierbei wurden potenzielle Herangehensweisen vorgestellt und diskutiert.

Abschließend in Schritt 1 wurden die technischen Sicherheitsmaßnahmen für den Betrieb der Föderation näher betrachtet. Der Fokus wurde hierbei, entsprechend aktueller Diskussionen und in Absprache mit den Projektbeteiligten, auf den Metadatenserver sowie die Konfiguration von Zertifikaten bei IdPs und SPs gelegt.

Schritt 2: Organisatorischer Föderationsbetrieb Die Unterstützung im Schritt 2 erfolgte nach Projektplan mit Anpassungen an Umfang und Zeitplan, die im Einvernehmen mit dem Auftraggeber und den Projektbeteiligten abgesprochen wurden.

Zum Betrieb einer großen Identitätsföderation regelt die Föderationssatzung zentrale Aspekte, Ziele und Regelungen. Die sich in Entwicklung befindliche Verwaltungsvereinbarung wurde von Projektpartnern zur Verfügung gestellt und gemeinsam über Änderungsvorschläge diskutiert.

In Absprache mit dem StMD und den weiteren Projektbeteiligten wurden Aktivitäten aus dem zweiten Schritt zur Betrachtung der IT-Service-Management-Prozesse verzögert, um eine ausgereiftere Basis der notwendigen Dokumente zur Diskussion abzuwarten. Dadurch wurde dieser Projektabschnitt etwas verkürzt, wird aber im Nachfolgeprojekt weitergeführt. Zu den Themen Change Management, Incident Management und Security Incident Management wurden allerdings noch während der Projektlaufzeit Besprechungen durchgeführt und Hinweise zur Verbesserung der jeweiligen Dokumente gegeben.

Ein weiterer Punkt aus Schritt 3 war die Definition eines geeigneten Onboarding-Prozesses, der es den Diensten ermöglicht, nach einem vorgegebenen und überprüfbaren Ablauf an der Föderation teilzunehmen. Dieser Teilschritt, vor allem auch die ursprünglich geplante exemplarische Demonstration in einer Testumgebung, wurde in Absprache mit den Projekt-

beteiligten nicht durchgeführt und die gewonnene Zeit in andere Projektteile (insbesondere Schritt 3) investiert.

Schritt 3: Self-Sovereign Identity Management (SSI) Die Optionen für Schritt 3 waren bewusst offen formuliert, um in Abstimmung mit dem StMD interessante Aspekte im Identitätsmanagement zu identifizieren und gezielt zu untersuchen.

Der erste identifizierte Punkt für Erweiterungen im Identitätsmanagement wurde in der Untersuchung zum Potenzial von Self-Sovereign Identity Management gefunden. SSI ermöglicht es, nutzerzentriert Identitätsdaten von einem Provider zu einem anderen zu übermitteln. Da die Provider nur über den Nutzer kommunizieren, kann der Nutzer alle Transaktionen kontrollieren und beobachten. Dadurch wird der Datenschutz gestärkt und die Portabilität von Identitätsdaten erhöht. Letztes ermöglicht die Nutzung von Diensten ohne aufwändige Registrierung und erhöht dadurch die Usability und Sicherheit des Gesamtsystems.

Die Relevanz des Themas SSI hat im Laufe des Projektes deutlich zugenommen, weshalb in Absprache mit dem StMD die Bemühungen in diesem Bereich verstärkt wurden. Dadurch war es möglich einen Prototyp für die Integration von SSI im Kontext BayernID und Föderation FINK zu entwickeln. Untersuchungen zu mit SAML konkurrierenden Standards wie OpenID Connect wurden dadurch aus dem Projekt genommen. Diese werden im Anschlussprojekt jedoch wieder eine Rolle spielen.

Im Anschluss an den Prototyp wurde eine Roadmap erstellt und im Projekt diskutiert, die langfristige Optionen zur Verwendung von bestehenden eGovernent-Systemen, wie der Föderation FINK, und SSI-basierten Systemen aufzeigt. Dabei wurden auch Kontakte zu weiteren SSI-Projekten hergestellt.

2.2 Zielerreichung

Die in den jeweiligen Arbeitsschritten erreichten Ziele werden hier kurz vorgestellt. Im Detail wird auf die entsprechenden Berichte und Dokumente im Anhang verwiesen.

Schritt 1: Technischer Föderationsbetrieb Zur Analyse der Vertrauensniveaus wurde festgestellt, dass es weiterhin Hürden bei der Erreichung der Vertrauensniveaus *substantiell* und *hoch* gibt. Dazu eignet sich aktuell hauptsächlich die Authentifizierung über den neuen Personalausweis (nPA/eAT). Gleichzeitig sind die Anforderungen an Verwaltungsleistungen so strikt, dass der Großteil mindestens auf Vertrauensniveau *substantiell* angeboten werden muss. Dadurch wird die Verwendung von Onlineangeboten der Verwaltung erschwert. Ziel sollte es daher sein, Verwaltungsleistungen auf einem möglichst niedrigen Vertrauensniveau anbieten zu können und die Authentifizierung über den Personalausweis nur für besonders kritische Vorgänge zu benötigen. Die ausführliche Betrachtung der Vertrauenslevel erfolgt in dem *Bericht zu den Schritten 1a und 1b* vom 05.03.2020.

Die Analyse des modifizierten SAML 2.0 Web Single-Sign-On Profils für die Föderation FINK kam zu dem Schluss, dass durch die zusätzlichen Einschränkungen in dem Profil kei-

ne sicherheitsrelevanten Schwachstellen geschaffen werden. Die üblicherweise verwendeten Implementierungen von SAML können mit den geplanten Einschränkungen umgehen. Eine detaillierte Aufstellung der Änderungen an dem Profil und der Auswirkungen auf die Kommunikation über SAML erfolgt in dem *Bericht zu den Schritten 1a und 1b* vom 05.03.2020.

Bei der Betrachtung der für die Föderation benötigten Attribute wurden verschiedenen Quellen von Attributsdefinitionen im eGovernment analysiert. Dabei waren die von eIDAS (*required* und *optional*) spezifizierten, die durch die BSI TR-03160 als Mindestsatz angegebenen, die durch das OZG erlaubten, sowie die von nPA/eAT und in FINK erfassten Attribute aufgelistet und auf Überschneidungen und Differenzen hin untersucht. Es wurde empfohlen, die Definition der Attributsdatensätze in der Föderation nach bewährter Vorgehensweise und zur Vereinheitlichung soweit möglich mithilfe von existierenden Attributsdefinitionen und wo notwendig über die Spezifikation von eigenen Attributen innerhalb eines eigenen OID-Namensraums durchzuführen. Die Ergebnisse sind in dem *Bericht zu Attributen in SAML-Föderationen* vom 30.04.2020 näher beschrieben.

Zur Betrachtung der IT-Sicherheit der Föderationsinfrastruktur wurde untersucht, welche Art von X.509-Zertifikaten benötigt und empfohlen ist für die Signatur der Metadaten auf dem zentralen Metadatenserver sowie bei den jeweiligen IdP- und SP-Endpunkten. Die ausführliche Übersicht zu diesem Thema ist in dem Dokument *Erläuterung zu in Föderationen üblichen X.509-Zertifikatsstrukturen* vom 25.03.2020 dargestellt.

Schritt 2: Organisatorischer Föderationsbetrieb Durch Verzögerungen in der Bereitstellung der notwendigen Prozessbeschreibungen konnten in dem dafür vorgesehenen Zeitfenster nicht alle Prozesse in der geplanten Detailtiefe analysiert werden. Die Aktivitäten aus diesem Teilschritt dauern zu Projektende noch an und werden im Folgeprojekt weiter fortgeführt.

Das IT-Service-Management für den Betrieb der Föderation FINK ist an ITIL angelehnt und wird primär vom IT-DLZ umgesetzt. In zwei Iterationen wurden die Prozessbeschreibungen des IT-DLZ zum Change Management, Incident Management und Security Incident Management durchgesehen und identifizierter Änderungsbedarf mit dem IT-DLZ besprochen.

Zu diesem Teilschritt existiert kein gesondertes Dokument. Der Austausch mit dem IT-DLZ erfolgte hauptsächlich per Annotation der Prozessbeschreibungen des IT-DLZ und durch Videokonferenzen.

Schritt 3: Self-Sovereign Identity Management Begonnen wurde Schritt 3 mit einer Vorstellung des Themas SSI und einem Vorschlag, dieses im Kontext von OZG, der Föderation FINK und allgemeiner Anforderungen von Verwaltungsleistungen näher zu betrachten. Der Vorschlag wurde in dem Dokument *Self-Sovereign Identity Management – Überblick und Vorschlag für einen Demonstrator* vom 01.04.2020 formuliert und nach Besprechungen und Anpassungen mit dem StMD akzeptiert.

Der Demonstrator wurde auf Basis von Hyperledger Indy/Aries und Sovrin in einer eigenen Umgebung aufgesetzt und anhand des im Rahmen von FINK etablierten Beispiels für interoperable Verwaltungsleistungen *Paula sucht Anerkennung* umgesetzt. Dabei wurde ein

eigener Distributed Ledger sowie eine eigens entwickelte Bayern-SSI-ID-Wallet-App verwendet. Die Kompatibilität zu anderen Hyperledger Indy-basierten SSI-Lösungen ist dadurch nicht beeinträchtigt.

Die Ergebnisse dieser Entwicklung wurden vom StMD über die gemeinsam erstellte *Präsentation zum Thema Bayern-SSI-ID-Wallet* vom 30.10.2020 kommuniziert. Da eine Live-Demonstration durch Kontaktbeschränkungen nicht möglich war, wurde zusätzlich eine Videodemonstration vorbereitet, die unter `http://go.unibw.de/DiskursPrototyp` (Passwort: *tie7DooM*) betrachtet werden kann.

Zum Abschluss von Schritt 3 wurden alle Aktivitäten im *Bericht zu Schritt 3: SSI-Demonstrator* vom 29.01.2021 zusammengefasst.

3 Projektablauf

Das Projekt DISKURS wurde im Forschungsinstitut Cyber-Defence (FI CODE) an der Universität der Bundeswehr München am Campus in Neubiberg erfolgreich durchgeführt. Die ursprünglich vorgeschlagen Projektlaufzeit von September 2019 bis Dezember 2020 wurde zum Vertragsschluss angepasst, sodass die tatsächliche Laufzeit von Dezember 2019 bis März 2021 dauerte. In der Zeit davor wurden schon erste Sondierungsgespräche geführt und der direkte Einstieg in das Projekt mit allen Projektbeteiligten vorbereitet.

Offiziell wurde das Projekt am 16.12.2019 mit einem Workshop im Bayerischen Staatsministerium für Digitales begonnen. Nachfolgend wurden aktuelle Projektinhalte auf in etwa alle drei Wochen stattfindenden Treffen mit allen Projektbeteiligten, dem StMD, der Unternehmensberatung H&D GmbH sowie dem IT-DLZ besprochen. Diese Treffen fanden, auch aufgrund der Kontaktbeschränkungen durch Corona, in der Regel per Videokonferenz statt.

Einzelne Projektteile wurden während der Projektlaufzeit an aktuell wichtigen Themen ausgerichtet und entsprechend flexibel besprochen.

Schon vor und vor allem während der Laufzeit des Projekts wurden Treffen mit weiteren Behörden, Ämtern und Forschungseinrichtungen durchgeführt. Ziel war es, die Arbeiten im Projekt mit Interessenvertretern zu teilen, neue Informationen und Kontakte zu gewinnen und Synergien zu identifizieren. In diesem Abschnitt werden die wichtigsten Besprechungen kurz hervorgehoben.

- 31.07.2019: In einem ersten Treffen der Projektpartner beim BSI in Bonn wurden die Grundlagen zur OZG-Umsetzung inklusive technischer, organisatorischer und rechtlicher Rahmenbedingungen besprochen. Dieses Treffen ermöglichte einen besseren Einstieg in die Materie.
- Innerhalb des StMD wurde nach der erfolgreichen Präsentation des SSI-Prototyps der Kontakt zum Blockchain-Referat des StMD hergestellt. Dadurch konnten zukünftige Erweiterungen und Projekte besser abgestimmt werden und gemeinsame Interessen identifiziert werden.

- Ebenfalls im Rahmen des SSI-Prototyps wurde der Kontakt zum Projekt SSI@LfSt hergestellt. Dieses Projekt des Landesamts für Steuern entwickelt ebenfalls einen SSI-Use-Case zur Erfassung der Umsatzsteuer über SSI.
- Über das SSI@LfSt wurde auch der Kontakt zu deren Projektpartnern vom Fraunhofer FIT hergestellt. Hier wurde ebenfalls ein reger Austausch bezüglich SSI gestartet.
- Am 17.02.2021 fand eine Besprechung mit einem Vertreter des Bundeskanzleramts zum SSI-Projekt des Bundes statt. Hier wurden Anknüpfungspunkte zwischen den beiden Projekten identifiziert, die im Nachfolgeprojekt integriert wurden.

4 Anschlussprojekt: DISPUT

Die in DISKURS begonnene Arbeit in der Untersuchung von Möglichkeiten zum Einsatz von SSI in eID-Infrastrukturen wird in dem Nachfolgeprojekt DISPUT (**D**igitale **I**dentitäten mit **S**elf-Sovereign Identity Management: **P**rozesse **u**nd **T**echnologien) intensiviert. Gleichzeitig wird die wissenschaftliche Begleitung der Inbetriebnahme der Identitätsföderation FINK fortgesetzt.

5 Administrativa

Im Rahmen von DISKURS sind die folgenden Berichte und Dokumente erstellt worden:

- 25.09.2019: Beiträge zur TR Interoperable Servicekonten
- 05.03.2020: Bericht zu den Schritten 1a und 1b (Vertrauensniveaus und IT-Sicherheitsaspekte)
- 25.03.2020: Erläuterung zu in Föderationen üblichen X.509-Zertifikatsstrukturen
- 01.04.2020: Self-Sovereign Identity Management – Überblick und Vorschlag für einen Demonstrator
- 30.04.2020: Bericht zu Attributen in SAML-Föderationen
- **28.05.2020: Bericht zu Schritt 1: Technischer Föderationsbetrieb**
- 30.10.2020: Präsentation zum Thema Bayern-SSI-ID-Wallet
- **29.01.2021: Bericht zu Schritt 3: SSI-Demonstrator**