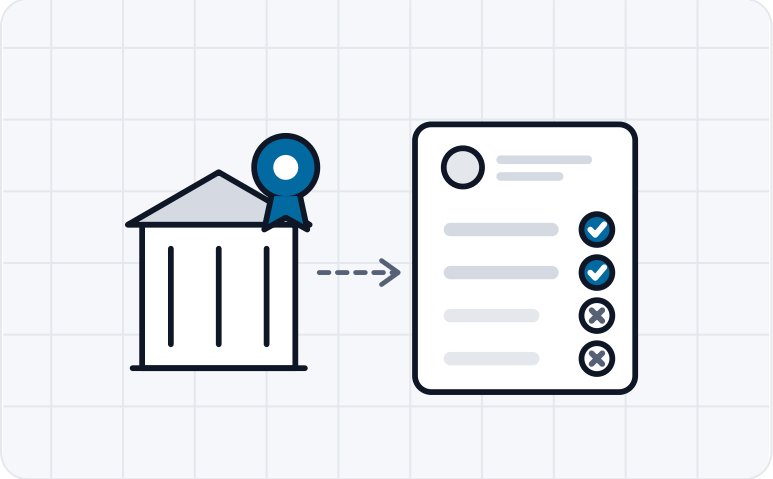
A-SIT Technology
E-Government Innovationszentrum

29. April 2024 Konzept · Digitale Identität · Privatsphäre & Krypto · 28 Min. Lesezeit

# Service Provider Akkreditierung mit Attributbeschränkungen

Stefan More



| | |
|---|---|
| **Autorinnen und Autoren** | Stefan More |
| **Quelle** | https://technology2.a-sit.at/veroeffentlichungen/service-provider-akkreditierung-mit-attributbeschraenkungen/ |
| **Hinweis** | Maschinell übersetzt. |

## Kernaussagen

- Akkreditierungen werden mit Beschränkungen gekoppelt, damit Service Provider nur Daten abfragen können, die sie rechtmäßig verarbeiten dürfen.
- Beschränkungen sind maschinell durchsetzbar und erlauben der Wallet, die Legitimität einer Anfrage automatisiert zu prüfen.
- Beschränkungen können Credentials, Attribute, Zero-Knowledge-Prädikate (z. B. nur Altersprüfung) und die Nutzung von Pseudonymen umfassen.
- Akkreditierung per Zertifikat und Register lässt sich kombinieren, sodass die Prüfung zu freizügiger Akkreditierungen auf zuständige Stellen verlagert wird.

- Grenzen: Gesetzliche Identifizierungspflichten und zu freizügige Akkreditierungsstellen; öffentliche Logs ermöglichen zumindest deren Erkennung.

In Credential-basierten Authentifizierungssystemen übermitteln Benutzer persönlich identifizierbare und potenziell sensible Daten an Dienstanbieter (Service Provider, SP; auch als Relying Party, RP, bezeichnet). Dabei müssen sich Benutzer oft darauf verlassen, dass sie mit einem legitimen Dienstanbieter kommunizieren, und darauf vertrauen, dass der SP einen legitimen Grund für die Anforderung aller Attribute über den Benutzer hat. Im Falle eines Missbrauchs von Daten kann es schwierig sein, den SP zu identifizieren und zur Rechenschaft zu ziehen. Eine Lösung dafür besteht darin, eine gegenseitige Authentifizierung vor der Übertragung sensibler Daten durchzuführen. Um einen SP vollständig zu authentifizieren und Vertrauen in ihn aufzubauen, wird der SP von einer von allen Benutzern vertrauten Stelle akkreditiert. Um sicherzustellen, dass der SP nur auf der Grundlage einer rechtlichen Basis auf Daten zugreifen kann, werden diese Akkreditierungen mit einem Satz von Zugriffsbeschränkungen kombiniert, d.h. einer Richtlinie, die die abfragbaren Daten einschränkt.

Die Motivationen für diese Arbeit sind Datenschutzanforderungen sowie rechtliche Anforderungen (z.B. DSGVO: Artikel 5 „Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden“, Artikel 6 „Die Verarbeitung ist nur rechtmäßig, wenn [...] die Verarbeitung erforderlich ist“).

Dieses Projekt zielt darauf ab, die Akkreditierung von Dienstanbietern zu analysieren, wobei der Schwerpunkt auf der Begrenzung der Attribute liegt, die ein SP aufgrund bereitgestellter Nachweise für die Anfrage vom Benutzer anfordern kann. Dieser Bericht diskutiert auch die Durchsetzung einer Pseudonym-Unterstützung durch SPs. Darüber hinaus integriert der Bericht datenschutzfördernde Maßnahmen in die Beschränkungen, wie z.B. die Begrenzung ausführbarer Zero-Knowledge-Prädikate.

## 1. Einleitung

In Credential-basierten Authentifizierungssystemen ist der Austausch personenbezogener Daten zwischen Benutzern und Dienstanbietern (Service Providern, SPs) die Grundlage für die Authentifizierungsentscheidung des SP. Diese Praxis wirft jedoch erhebliche Bedenken hinsichtlich Datenschutz, Datensicherheit und Vertrauen der Benutzer auf. Benutzer befinden sich häufig in der Lage, SPs sensible Informationen anvertrauen zu müssen und sich dabei allein auf die Annahme zu stützen, dass der SP legitim ist und die angeforderten Daten tatsächlich benötigt.

Der mögliche Missbrauch dieser Daten stellt eine erhebliche Herausforderung dar, da es komplex sein kann, SPs bei solchen Verstößen zu identifizieren und zur Rechenschaft zu ziehen. Als Antwort auf diese Herausforderungen hat sich das Konzept der gegenseitigen Authentifizierung als vielversprechende Lösung herausgebildet. Durch die Umsetzung von Protokollen zur gegenseitigen Authentifizierung können Benutzer und SPs vor dem Datenaustausch gegenseitig ihre Identität überprüfen und so eine Vertrauensgrundlage schaffen.

Gegenseitige Authentifizierung allein reicht jedoch nicht aus, um die umfassenderen Fragen des Datenschutzes und der Datensicherheit zu lösen. Um Vertrauen in die Identität des SP aufzubauen, ist es unerlässlich, über die Authentifizierung hinauszugehen und die Akkreditierung von SPs einzubeziehen. Die Akkreditierung umfasst die Validierung von SPs durch eine vertrauenswürdige Stelle, die ihre Legitimität und die Einhaltung bestimmter Standards und Vorschriften (z.B. DSGVO) sicherstellt. Dieser Akkreditierungsprozess dient in Verbindung mit Zugriffsbeschränkungen als Mechanismus, um die Daten einzuschränken, die SPs von Benutzern anfordern können, und schützt so sensible Informationen. Im Gegensatz dazu, die Akkreditierungsinformationen lediglich dem Benutzer anzuzeigen und sich auf dessen Urteil zu verlassen, sind Beschränkungen maschinell durchsetzbar und ermöglichen damit die automatisierte Prüfung der Legitimität einer Anfrage.

Die Motivation für diesen Bericht ist vielschichtig und ergibt sich sowohl aus Datenschutzanforderungen als auch aus rechtlichen Überlegungen. Da Vorschriften wie die Datenschutz-Grundverordnung (DSGVO) verlangen, dass personenbezogene Daten nur für eindeutige und legitime Zwecke erhoben und verarbeitet werden, besteht ein dringender Bedarf an robusten Mechanismen, die diese Grundsätze wahren. Darüber hinaus ermöglichen Fortschritte bei datenschutzfördernden Technologien noch bessere Datenschutzmaßnahmen in Authentifizierungssystemen, um Datenschutzrisiken wirksam zu verringern.

Um die Bedeutung dieses Projekts zu veranschaulichen, seien einige Beispiele betrachtet. Man stelle sich ein Szenario vor, in dem ein Benutzer ein Online-Gesundheitsportal aufruft, um einen Termin zu vereinbaren. In diesem Kontext benötigt der SP Zugriff auf bestimmte gesundheitsbezogene Attribute, um seinen Dienst zu erbringen. Ohne angemessene Akkreditierung und Zugriffsbeschränkungen besteht jedoch das Risiko eines unbefugten Zugriffs auf sensible medizinische Informationen, was möglicherweise die Datenschutzrechte des Benutzers verletzt.

Ähnlich stellen Benutzer im Kontext von Finanzdienstleistungen SPs häufig personenbezogene und finanzielle Daten für Transaktionen und die Kontoverwaltung zur Verfügung. Ohne wirksame Akkreditierungsmaßnahmen und Zugriffsbeschränkungen können SPs bei ihren Datenanfragen über das Ziel hinausschießen und Benutzer finanziellen Risiken und Datenschutzverletzungen aussetzen.

Diese Beispiele unterstreichen die große Bedeutung, die Akkreditierung von SPs zu analysieren und wirksame Zugriffsbeschränkungen umzusetzen, um die Privatsphäre und Datensicherheit der Benutzer zu schützen. Durch die Einbeziehung datenschutzfördernder Maßnahmen wie Pseudonym-Unterstützung und Zero-Knowledge-Prädikaten betrachtet dieser Bericht darüber hinaus neue Wege des Datenschutzes in Credential-basierten Authentifizierungssystemen.

## 1.1. Überblick: Konzept

In diesem Abschnitt wird aus Sicht des Benutzers ein Überblick darüber gegeben, wie eine Akkreditierungsprüfung abläuft. Das Konzept wird im weiteren Verlauf dieses Berichts ausführlicher behandelt.

1. Service Access (Dienstzugriff): Der Benutzer möchte auf einen Dienst oder eine Ressource zugreifen. Da der Dienst durch ein Zugriffskontrollsystem geschützt ist, fordert der Service Provider (SP) den Benutzer auf, Credentials vorzulegen (zu präsentieren), damit er den Benutzer authentifizieren und den Zugriff gewähren (oder verweigern) kann.

2. Presentation Request (Präsentationsanfrage): Der Benutzer erhält vom SP eine Anfrage, seine Credentials zur Authentifizierung zu präsentieren. In dieser Anfrage teilt der SP dem Benutzer mit, welche Credentials (oder Attribute) er benötigt. Da der SP beispielsweise eine Altersverifikation durchführen muss, fordert er vom Benutzer ein behördlich ausgestelltes Credential an, das das Geburtsdatum des Benutzers enthält.

3. Authenticate SP (SP authentifizieren): Der Benutzer überprüft die Identität des SP, indem er kontrolliert, dass die bereitgestellte SP-Akkreditierung die Stelle repräsentiert, die die Präsentationsanfrage gesendet hat.

4. Check SP Trustworthiness (Vertrauenswürdigkeit des SP prüfen): Der Benutzer validiert das Zertifikat des SP auf Vertrauenswürdigkeit. Dazu gehört die Überprüfung, ob das Akkreditierungsdokument von einer vertrauenswürdigen Akkreditierungsstelle ausgestellt wurde. Ferner prüft der Benutzer den Widerrufsstatus und konsultiert ein Akkreditierungsregister mit Certificate-Transparency-Logs (CT-Logs), um den Akkreditierungsstatus des SP sicherzustellen. Der letzte Schritt ist erforderlich, damit zuständige Stellen (wie Datenschutzbehörden und NGOs) die Liste der akkreditierten Stellen prüfen können.

5. Check Constraints (Beschränkungen prüfen): Der Benutzer bewertet die Zugriffsbeschränkungen, die der SP von der Akkreditierungsstelle auferlegt bekommen hat, und stellt sicher, dass die angeforderten Attribute den Vorschriften entsprechen und der SP einen rechtlich vertretbaren Zweck für die Verarbeitung dieser Daten hat. Fragt der SP beispielsweise nach einem Geburtsdatum, prüft der Benutzer, ob dieser konkrete SP zur Abfrage dieses Datums berechtigt ist.

6. Ask User for Consent (Benutzer um Einwilligung bitten): Der Benutzer wird aufgefordert, der Weitergabe seiner Credentials und Attribute auf Grundlage der Anfrage des SP zuzustimmen. Dies stellt sicher, dass die angeforderten Attribute den Erwartungen und Datenschutzpräferenzen des Benutzers entsprechen.

7. Build Presentation (Präsentation erstellen): Nach der Einwilligung des Benutzers erstellt dieser eine Präsentation, die die angeforderten Credentials und Attribute enthält.

8. Log Request & Response in Wallet (Anfrage und Antwort in der Wallet protokollieren): Die Details der Anfrage und der Antwort des Benutzers werden zusammen mit relevanten Metadaten zur späteren Verwendung in der digitalen Wallet des Benutzers protokolliert. Dies kann als Beweis dienen, falls später ein Fehlverhalten des SP festgestellt wird, z.B. wenn der SP die Daten anders verarbeitet hat als in der Akkreditierung festgelegt oder dem Benutzer mitgeteilt.

9. Sign & Send (Signieren und Senden): Der Benutzer signiert die Präsentation digital und sendet sie sicher an den SP.

# 2. Hintergrund und Definitionen

## 2.1. Architektur und Entitäten

- Issuer CA/Trust Root: Die Issuer Certificate Authority (CA) oder Trust Root ist die Stelle, die für die Ausstellung digitaler Zertifikate an Issuer zuständig ist und diese zur Ausstellung bestimmter Credentials berechtigt.

- Issuer/IDP: Der Issuer oder Identity Provider (IDP) ist für die Ausstellung von Credentials an Benutzer zuständig. Diese Credentials enthalten digitale Darstellungen der Identitätsattribute des Benutzers, wie Name, E-Mail-Adresse oder andere relevante Informationen. Die Credentials werden mit dem Zertifikat des Issuers signiert.
- Holder/User/Wallet: Der Benutzer oder Holder ist die Stelle, die Credentials besitzt und Service Providern (SPs) zur Authentifizierung präsentiert. Die Wallet ist die Software des Benutzers (typischerweise auf dessen Telefon) und dient als sicherer Speicher zum Aufbewahren und Verwalten digitaler Credentials.
- SP/RP/Verifier: Der Service Provider (SP) oder die Relying Party (RP) ist die Stelle, die einen Dienst betreibt und von Benutzern eine Authentifizierung verlangt. Der Verifier bezeichnet die Werkzeuge oder die Software, die der SP betreibt, um die Echtheit und Gültigkeit der vom Benutzer präsentierten Credentials zu überprüfen (manchmal auch SP-Instanz genannt).
- Accreditation Body: Die Akkreditierungsstelle (Accreditation Body, AB) ist eine maßgebliche Stelle, die für die Akkreditierung von Service Providern auf Grundlage vordefinierter Standards und Vorschriften zuständig ist. Sie stellt SPs Akkreditierungen aus und bestätigt damit deren Legitimität und die Einhaltung etablierter Protokolle. Zusätzlich bewertet sie den vom SP angegebenen Zweck der Datenverarbeitung und stellt im Rahmen der Akkreditierung Beschränkungen aus. Die AB wird ihrerseits üblicherweise von einer rechtlichen Autorität akkreditiert, die im Rahmen eines Governance-Frameworks eine gewisse Haftung ermöglicht.
- Credential: Ein Credential ist eine digitale Darstellung der Identitätsattribute eines Benutzers und wird typischerweise von einem Issuer ausgestellt. Es enthält Informationen wie Name, E-Mail-Adresse, Rolle, Zugehörigkeiten oder andere relevante Angaben. Credentials sind in maschinenlesbarer Form codiert und dienen bei der Präsentation gegenüber Service Providern als Identitätsnachweis zu Authentifizierungszwecken. Kryptographische Signaturen dienen sowohl dazu, die Echtheit der Credentials sicherzustellen (Signatur durch den SP), als auch dazu, ein Credential an einen bestimmten Benutzer zu binden (öffentlicher Schlüssel des Benutzers im Credential).

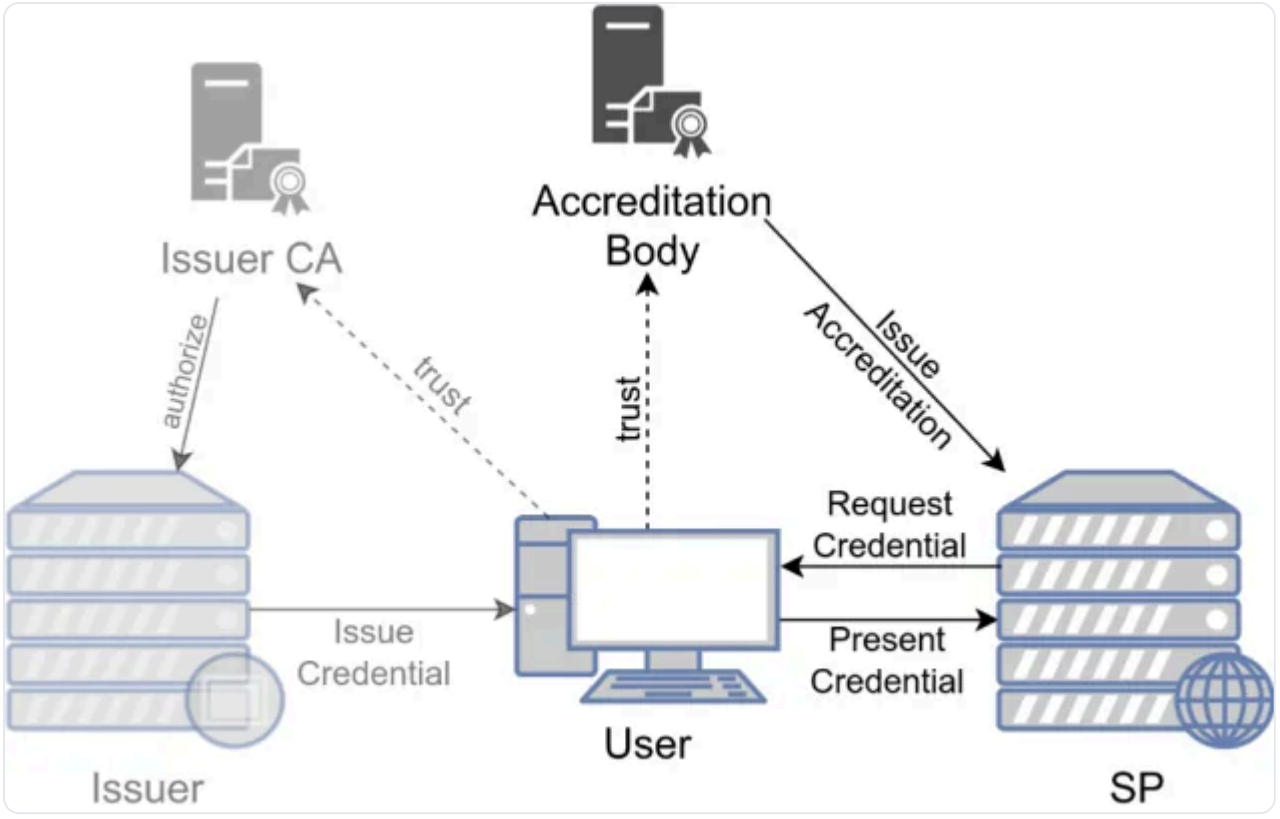



Abbildung 1: Überblick über die Entitäten mit Schwerpunkt auf dem Prozess der Credential-Präsentation

## 2.2. Pseudonyme

Pseudonyme dienen als datenschutzfördernder Mechanismus, indem sie Benutzern ermöglichen, mit Service Providern zu interagieren, ohne ihre wahre Identität oder eine dauerhafte Kennung preiszugeben.

Ein verbreiteter Ansatz zur Pseudonymität sind Pairwise Pseudonymous Identifiers. [1] Pairwise Pseudonymous Identifiers beruhen auf der Erzeugung eindeutiger Kennungen für jede paarweise Beziehung zwischen einem Benutzer und einem Service Provider. Das bedeutet, dass jeder Benutzer für jeden Service Provider, mit dem er interagiert, ein neues Pseudonym erzeugt und das Pseudonym eines SP nicht bei einem anderen SP wiederverwendet. Diese Kennungen werden bei Interaktionen als temporäre oder einmalige Pseudonyme verwendet und verhindern, dass SPs Benutzer über verschiedene Dienste oder Sitzungen hinweg verfolgen können (Linkability).

Eine weitere besondere Form von Pseudonymen (z.B. ABC4Trust-Pseudonyme [4]) ermöglicht eine anonyme bzw. pseudonyme und unverknüpfbare Nutzung eines Dienstes, erlaubt aber einer vertrauenswürdigen Stelle (Inspector) oder einer Gruppe von Stellen, die Identität hinter einem Pseudonym später aufzudecken.

## 2.3. Datenschutzfördernde Technologien

### 2.3.1. Selective Disclosure

Selective Disclosure bezeichnet die Möglichkeit der Benutzer, die Informationen zu kontrollieren und zu begrenzen, die sie bei Authentifizierungsprozessen gegenüber Service Providern preisgeben. Durch den Einsatz datenschutzfördernder Technologien wie attributbasierter Credentials oder SD-JWTs [2] können

Benutzer bestimmte Attribute aus einem Credential selektiv offenlegen, ohne die übrigen Attribute preiszugeben. So kann ein Benutzer beispielsweise ein Reisepass-Credential verwenden und nur sein Geburtsdatum offenlegen, während alle anderen Attribute des Reisepasses verborgen bleiben. Dadurch wird sichergestellt, dass nur relevante und notwendige Informationen weitergegeben werden, was das Risiko von Datenschutzverletzungen und unbefugtem Zugriff auf sensible Daten minimiert. Gleichzeitig versetzen Selective-Disclosure-Mechanismen Benutzer in die Lage, die Kontrolle über ihre personenbezogenen Daten zu behalten und dennoch an Authentifizierungsverfahren teilzunehmen, wodurch Vertrauen in das Authentifizierungssystem gefördert wird.

#### 2.3.2. Zero-Knowledge-Beweise

Zero-Knowledge-Beweise (Zero-knowledge Proofs, ZKPs) sind eine kryptographische Technik, mit der die Gültigkeit einer Aussage nachgewiesen wird, ohne sensible Informationen preiszugeben. Im Kontext von Authentifizierungssystemen ermöglichen Zero-Knowledge-Beweise Benutzern, sich gegenüber Service Providern zu authentifizieren, ohne ihre zugrunde liegenden Credentials oder personenbezogenen Daten offenzulegen. Mit Zero-Knowledge-Protokollen können Benutzer den Besitz bestimmter Attribute oder Credentials nachweisen, ohne die Attribute selbst preiszugeben, und so ihre Privatsphäre schützen. Dies stärkt die Kontrolle der Benutzer über ihre Daten und gewährleistet zugleich die Integrität und Sicherheit des Authentifizierungsprozesses. Die Einbindung von Zero-Knowledge-Beweisen in Authentifizierungssysteme verstärkt die Datenschutzmaßnahmen und das Vertrauen der Benutzer in die Sicherheit des Systems.

Im Kontext dieses Berichts können Zero-Knowledge-Beweise und -Protokolle eingesetzt werden, um Selective Disclosure einen Schritt weiterzuführen und einen SP dazu zu berechtigen, nur Prädikate über Benutzerattribute anzufragen. Besitzt ein Benutzer beispielsweise ein Reisepass-Credential mit dem vollständigen Geburtsdatum, kann der SP berechtigt werden, nur das aus dem Geburtsdatum berechnete Alter des Benutzers abzufragen. In diesem Beispiel werden dem SP weder das Geburtsdatum selbst noch andere Attribute offengelegt, eine Altersverifikation ist aber dennoch möglich.

# 3. Ziele und Motivation

## 3.1. Datenschutzerwartungen

Um die Akzeptanz der Benutzer für ein Credential-System zu erhöhen und die Datenschutzerwartungen der Benutzer zu erfüllen, werden einige grundlegende Datenschutzziele [1] als Grundlage für den Umfang dieses Berichts verwendet. Diese Erwartungen sind an Interaktionen des Alltags in der Offline-Welt angelehnt. Weitere Aspekte dieser Ziele werden in den folgenden Abschnitten behandelt.

- Confidentiality (Vertraulichkeit): Wenn ein Benutzer ein Credential gegenüber einem Service Provider präsentiert, erwartet er, dass sein Credential nur für diesen konkreten Service Provider zugänglich ist. [3] Um diese Erwartung zu erfüllen, muss ein System den Service Provider authentifizieren, diese Information dem Benutzer präsentieren und sicherstellen, dass die Daten direkt (und z.B. verschlüsselt) an diesen Anbieter übertragen werden.

- Data Minimization (Datenminimierung): Benutzer erwarten, dass ein Service Provider nur die Daten erhält, die er zur Erbringung eines Dienstes benötigt, sowie Daten, die der SP von Gesetzes wegen erheben oder verarbeiten muss (z.B. aufgrund von KYC-Anforderungen). Benutzer können der Weitergabe weiterer Daten für eine weitere rechtmäßige Verarbeitung zustimmen, z.B. für Personalisierung oder Marketing.

- Anonymity and Pseudonymity (Anonymität und Pseudonymität): Viele Interaktionen im Alltag sind anonym. Benutzer erwarten, dass sie Dienste nutzen können, ohne ihre Identität preiszugeben. So argumentiert beispielsweise der Oberste Gerichtshof der USA sogar, dass es ein verfassungsmäßiges Recht auf Anonymität gibt, [4] und führt aus, dass die „Entscheidung für Anonymität durch die Furcht vor wirtschaftlicher oder behördlicher Vergeltung, durch die Sorge vor gesellschaftlicher Ächtung oder schlicht durch den Wunsch motiviert sein kann, die eigene Privatsphäre so weit wie möglich zu wahren". In manchen Fällen ist vollständige Anonymität nicht wünschenswert, beispielsweise wenn ein wiederkehrender Benutzer ein Online-Forum nutzen möchte. In diesem Fall erwarten Benutzer Pseudonymität, d.h. die Verwendung eines Pseudonyms, das nicht mit ihrer rechtlichen Identität verknüpft ist.

- Unlinkability (Unverknüpfbarkeit): Benutzer erwarten, dass sie ein Credential oder eine Gruppe von Credentials bei verschiedenen Service Providern verwenden können, ohne dadurch an Privatsphäre einzubüßen. Insbesondere sollten die beteiligten Service Provider die Interaktionen nicht miteinander verknüpfen können, da dies die Profilbildung des Benutzers ermöglichen würde. Bei anonymen bzw. pseudonymen Interaktionen möchten Benutzer dasselbe Credential (z.B. für die Altersverifikation) in zwei Interaktionen zweimal verwenden. Erwartet wird, dass der Dienst die beiden Interaktionen nicht miteinander verknüpfen kann, d.h. nicht weiß, dass derselbe Benutzer zweimal mit ihm interagiert hat (Multi-Show-Unlinkability).

- Unobservability (Unbeobachtbarkeit): Ebenso erwarten Benutzer, dass keine Partei außer den unmittelbar an einer Interaktion Beteiligten (d.h. dem Benutzer und dem Service Provider) erfährt, dass die Interaktion stattfindet. Insbesondere erwarten Benutzer, dass der Issuer oder eine andere Autorität (z.B. der Staat) nicht erfährt, bei welchem SP der Benutzer seine Wallet verwendet, oder auch nur, dass der Benutzer seine Wallet verwendet.

## 3.2. Benutzbarkeit und Rechtmäßigkeit

Dieser Bericht erkennt die Komplexität an, der Benutzer bei der Bewertung jeder Authentifizierungsanfrage gegenüberstehen. Insbesondere entstehen Probleme bei der Fähigkeit der Benutzer, die Legitimität des Service Providers und den Zweck der Datenoffenlegung einzuschätzen. In Parallele zu den Herausforderungen mit Extended-Validation-Zertifikaten (EV-Zertifikaten) in der Web PKI (HTTPS), bei denen Benutzer häufig Schwierigkeiten haben, legitime und 3 Dies bedeutet nicht zwingend, dass es keine rechtmäßigen Wege gibt, die Daten an weitere Parteien weiterzugeben, da die DSGVO beispielsweise erlaubt, dass Service Provider die Verarbeitung von Daten (unter bestimmten Bedingungen) an Dritte delegieren. Sie bleiben jedoch bei Verstößen oder Missbrauch rechenschaftspflichtig. 4 https://epic.org/issues/democracy-free-speech/anonymity/ bösartige Stellen zu unterscheiden, [3] erkennt das System die Notwendigkeit automatisierter Durchsetzungsmechanismen. Dies umfasst automatische Prüfungen, die sicherstellen, dass Datenanfragen den rechtlichen Anforderungen entsprechen. Benutzer können zwar die Möglichkeit behalten, automatisierte Entscheidungen zu übersteuern, doch solche

Handlungen könnten zu unbeabsichtigtem Übermaß an Datenweitergabe führen, z.B. bei einer Authentifizierung unter Stress oder wenn die Folgen nicht leicht abzuschätzen sind. Obwohl dieser Bericht auch Szenarien mit optionaler Datenoffenlegung betrachtet, besteht zudem selbst für nicht verpflichtende Informationen die Notwendigkeit eines legitimen Zwecks.

### 3.3. Haftbarkeit von SPs ermöglichen

Um die Haftbarkeit sich fehlverhaltender SPs zu ermöglichen, setzt das System Maßnahmen um, signierte Präsentationsanfragen zu sammeln, die effektiv als Nachweis für die Akkreditierung und den bei der Authentifizierung geltend gemachten Zweck dienen. Durch das Sammeln dieser Nachweise schafft das System die Grundlage, SPs für ihr Handeln zur Rechenschaft zu ziehen. Wird rechtlicher Rückgriff notwendig, versetzen überprüfbare Spuren und Nachweise die Inhaber von Credentials in die Lage, Behauptungen über Übergriffe oder Fehlverhalten von SPs zu belegen. Dadurch wird sichergestellt, dass SPs für jeden Vertrauensbruch haftbar gemacht werden können, was die Rechenschaftspflicht im Authentifizierungs-Ökosystem fördert.

### 3.4. DSGVO-Konformität

Die Einhaltung von Datenschutzvorschriften wie der DSGVO [8] ist für das Authentifizierungssystem jedes SP von größter Bedeutung. Beispielsweise betonen die Artikel 5 und 6 der DSGVO den Zweck und die Rechtmäßigkeit der Verarbeitung personenbezogener Daten. Es ist unerlässlich, den Zweck der Datenverarbeitung zu prüfen und die Übereinstimmung mit den Grundsätzen der DSGVO sicherzustellen. Zusätzlich muss das Framework bewerten, ob der Zweck den Zugriff auf qualifizierte Daten rechtfertigt oder ob der Zugriff auf unqualifizierte Daten ausreicht. In vielen Fällen genügt es, lediglich den Namen eines Benutzers zu erhalten, ohne dass ein behördlich ausgestelltes Credential nötig ist. Allgemeiner unterstreicht dies die Bedeutung, den Grundsatz „Privacy by Design“ und das „Need-to-know“-Prinzip einzuhalten und das Prinzip der minimalen Rechte (Least Privilege) umzusetzen. Indem der Zweck bewertet und der Datenzugriff strikt auf das für den beabsichtigten Zweck Wesentliche begrenzt wird, kann ein Akkreditierungssystem die DSGVO-Konformität verbessern, Datenschutzrisiken verringern und die Datenschutzrechte der Benutzer wahren.

### 3.5. eIDAS Identity Wallets (April 2024)

Die europäische eIDAS-2-Verordnung ändert die ursprüngliche eIDAS-Verordnung von 2016 und führt einen Rahmen für europäische digitale Identitäts-Wallets ein [9]. Die neue eIDAS-Verordnung führt zusätzlich zu den bestehenden Datenschutzregeln der DSGVO [5; 8] weitere Datenschutzregeln ein. Diese Regeln sind auf den Wallet-Kontext zugeschnitten. Für diesen Bericht sind die Artikel 5a, der die Identitäts-Wallet einführt, und 5b, der Service Provider behandelt, am relevantesten. Darüber hinaus begründet Artikel 5 ein Recht auf die Verwendung von Pseudonymen.

- SP Registration (SP-Registrierung): Ein SP muss sich in dem Mitgliedstaat registrieren, in dem er niedergelassen ist. SPs müssen sich gegenüber dem Benutzer identifizieren (Artikel 5b).
- Purpose Registration (Zweckregistrierung): Bei der Registrierung muss ein SP angeben, welche Daten von Benutzern angefordert werden sollen, und darf keine anderen als die angegebenen Daten anfordern (Artikel 5b).

- Purpose Information (Zweckinformation): Wallets müssen den Benutzer darüber informieren, ob der SP die Berechtigung hat, auf ein Credential zuzugreifen (Artikel 5a).
- Auditability (Prüfbarkeit): Die Liste der registrierten SPs und ihrer angegebenen Datenverarbeitung muss öffentlich und in einer für die automatisierte Verarbeitung geeigneten Form vorliegen (Artikel 5b).
- Unlinkability (Unverknüpfbarkeit): Der technische Rahmen muss Unverknüpfbarkeit gewährleisten (Artikel 5a).
- Selective Disclosure: Der technische Rahmen muss gewährleisten, dass die selektive Offenlegung von Daten möglich ist (Artikel 5a).
- Unobservability (Unbeobachtbarkeit): Der technische Rahmen darf Issuern oder anderen Parteien nicht erlauben, das Verhalten von Benutzern zu verfolgen, zu verknüpfen oder zu korrelieren (Artikel 5a).
- Pseudonyms (Pseudonyme): Die Verwendung von Pseudonymen, die vom Benutzer gewählt und verwaltet werden, darf nicht untersagt werden (Artikel 5). Wallets müssen dem Benutzer ermöglichen, Pseudonyme zu erzeugen und verschlüsselt und lokal zu speichern (Artikel 5a). SPs dürfen die Verwendung von Pseudonymen nicht verweigern, außer wenn die Identifizierung des Benutzers gesetzlich vorgeschrieben ist (Artikel 5b).
- Control (Kontrolle): Benutzer müssen die volle Kontrolle über die Nutzung der Wallet und über die Daten in ihrer Wallet haben (Artikel 5a).

### 3.6. Profilbildung durch SPs verhindern

Um der Gefahr der Profilbildung durch Service Provider zu begegnen, sollten Akkreditierungen auch die Verringerung der Verknüpfbarkeit berücksichtigen und Unverknüpfbarkeit ermöglichen. Nicht einvernehmliche Profilbildung ist ein zentrales Anliegen im Zusammenhang mit Verlust der Privatsphäre, Überwachungskapitalismus, Werbung und Überwachung. Um der Verknüpfbarkeit entgegenzuwirken, könnten Akkreditierungssysteme die Verwendung von Pseudonymen erlauben oder vorschreiben und so sicherstellen, dass Benutzeridentitäten weder eindeutig identifizierbar noch über die Zeit dauerhaft sind, um Tracking und Profilbildung zu verhindern. Ein weitergehendes Datenschutzziel ist Multi-Show-Unlinkability, bei der Benutzer Pseudonyme frei erzeugen können, ohne ihre Privatsphäre zu gefährden.

Ein offener Diskussionspunkt ist, ob eine unbegrenzte Anzahl von Pseudonymen erlaubt oder diese Anzahl pro Service Provider begrenzt werden soll. Einerseits unterstützt die Begrenzung der Pseudonymanzahl SPs bei der Überprüfung der Sybil-Resistenz und macht aufdringliche Maßnahmen wie die Verifikation von Telefonnummern überflüssig. Dies ist ein wichtiger Anreiz für SPs, ein Credential-System zu nutzen, und führt zu besserem Datenschutz für Benutzer. Andererseits schränkt es die Freiheit der Benutzer bei der Nutzung des Dienstes ein, wenn sie begrenzt werden, wie viele Pseudonyme (und damit Konten) sie anlegen können. Außerdem ist unklar, wie die Anzahl der Pseudonyme auf eine bestimmte Zahl größer als eins begrenzt werden kann.

### 3.7. Profilbildung durch Behörden und Infrastruktur verhindern

Um Überwachung und Profilbildung durch Behörden und Infrastrukturbetreiber zu verhindern, wird Unbeobachtbarkeit als grundlegendes Prinzip betont. Das Ziel ist sicherzustellen, dass Authentifizierungsprozesse für externe Stellen unbeobachtbar bleiben. Entscheidend ist, dass die Akkreditierungsstelle nicht direkt in den Akkreditierungsprüfprozess durch den Benutzer eingebunden ist.

### 3.8. Over-asking und Over-identification verhindern

Akkreditierungssysteme können Maßnahmen bieten, um sowohl übermäßige Identifizierung als auch die Übertragung unnötiger personenbezogener Informationen zu adressieren [5; 6; 7, Abschnitt 7.6].

Over-identification ist die übermäßige Identifizierung bei Interaktionen, die zuvor anonym stattfanden. Sie könnte verringert werden, indem die Offenlegung personenidentifizierbarer Informationen auf Anwendungsfälle beschränkt wird, in denen vertrauenswürdige Informationen wirklich benötigt werden (z.B. gesetzlich vorgeschrieben), und nur das geteilt wird, was für Authentifizierungszwecke wesentlich ist.

Ähnlich liegt Over-asking vor, wenn Service Provider von Benutzern mehr Attribute anfordern, als für ihren Anwendungsfall nötig sind. Durch die Durchsetzung strikter Zugriffsbeschränkungen und die Einhaltung des Grundsatzes der Datenminimierung könnte ein System sicherstellen, dass SPs nur die für die Authentifizierung mindestens erforderlichen Attribute erheben. Mit diesen Maßnahmen strebt das System einen Ausgleich zwischen der Erfüllung der legitimen Bedürfnisse von SPs und dem Schutz der Datenschutzrechte der Benutzer an.

Sowohl Over-identification als auch Over-asking stellen eine zusätzliche Herausforderung dar, da qualifizierte Daten in der Hand eines SP mehr Wert haben als nicht signierte Daten. Dies ist ein sehr attraktives Ziel für Angriffe, weshalb die Stellen mit Zugriff auf die Daten begrenzt werden müssen.

## 4. Einschränkungen

Akkreditierungen spielen zwar eine entscheidende Rolle, um die Vertrauenswürdigkeit von Service Providern sicherzustellen, es ist jedoch wichtig, ihre Einschränkungen zu erkennen.

Akkreditierungen können trotz ihres Werts nicht alle Probleme lösen, insbesondere nicht solche, die in rechtlichen oder Governance-Rahmenwerken wurzeln. So können beispielsweise bestimmte Rechtsordnungen die Offenlegung von Klarnamen oder Kennungen vorschreiben. Wird dies gesetzlich durchgesetzt, könnte ein staatlich kontrolliertes System SPs nicht daran hindern, diese Vorschrift umzusetzen. Akkreditierungsstellen würden dann insbesondere alle SPs für die Abfrage von Namen oder anderen identifizierbaren Daten akkreditieren. Benutzer können jedoch weiterhin die Weitergabe von Credentials verweigern, mit dem möglichen Effekt, keinen Zugang zu Diensten zu haben. Zusätzlich sind Akkreditierungen anfällig für Ausnutzung. Beispielsweise können Akkreditierungsstellen Akkreditierungen mit übermäßig freizügigen Beschränkungen ausstellen. Folglich ist das Vertrauen in die Akkreditierungsstelle von größter Bedeutung und erfordert Transparenzmaßnahmen wie öffentliche Logs von Akkreditierungen und Beschränkungen. Diese Logs ermöglichen es zuständigen Stellen, Akkreditierungsaktivitäten zu überwachen und die Einhaltung etablierter Standards sicherzustellen. Dies kann zwar aufdringliche Akkreditierungsbeschränkungen nicht verhindern, ermöglicht aber zumindest ihre Erkennung durch die Öffentlichkeit und kann die Autorität möglicherweise zur Rechenschaft ziehen.

Eine weitere Einschränkung liegt in der Natur digitaler Daten. Sobald Daten rechtmäßig weitergegeben wurden, wird es schwierig, Nutzungs- und Speicherbeschränkungen durchzusetzen: Der Benutzer hat keine Kontrolle darüber, was der SP tatsächlich mit den Daten macht und mit wem er sie teilt. Es gibt zwar Haftungsmechanismen, wie vom Benutzer gespeicherte Präsentations- bzw. Zugriffsprotokolle, diese verhindern jedoch von sich aus weder Missbrauch noch unbefugten Zugriff. Sie dienen aber als Nachweis der Datenweitergabe und können hilfreich sein, um Parteien für Verstöße zur Rechenschaft zu ziehen. Zusätzlich deckt die Akkreditierung vorrangig den Vorgang des Vorzeigens ab und erstreckt sich nicht auf den Schutz vor unbefugtem Zugriff auf die Wallet selbst. Beispielsweise können Akkreditierungsmechanismen in Szenarien, in denen eine Grenzbehörde das Telefon eines Benutzers beschlagnahmt, möglicherweise keinen direkten Schutz vor der Offenlegung von Daten bieten. [4]

# 5. Akkreditierung und Beschränkungen

## 5.1. Ausgangslage

Als Ausgangslage für diesen Bericht wird ein Credential-System betrachtet, in dem der Benutzer keine Informationen über den Service Provider (SP) hat, mit dem er interagiert. Selbst in Szenarien, in denen eine Form der gegenseitigen Authentifizierung ohne Akkreditierung stattfindet, d.h. der SP Informationen über seine Identität bereitstellt, hat der Benutzer keine Möglichkeit, den bereitgestellten Identitätsinformationen zu vertrauen. Ohne vertrauenswürdige Akkreditierungsinformationen fehlt dem Authentifizierungsprozess eine Ebene der Rechenschaftspflicht und Vertrauenswürdigkeit. Ohne Akkreditierung haben Benutzer keine Gewissheit über die Legitimität oder Zuverlässigkeit von SPs und sind potenziellen Risiken und Missbrauch ausgesetzt.

## 5.2. SP-Akkreditierung

Um eine überprüfbare und vertrauenswürdige Identität des Service Providers (SP) einzuführen, werden Akkreditierungen verwendet. Akkreditierungen werden von Akkreditierungsstellen (Accreditation Bodies, AB) erstellt, Stellen, denen der Benutzer vertraut. Durch die Einführung von ABs in das System wird die Herausforderung, Vertrauen in jeden einzelnen SP aufzubauen, auf eine einzige Vertrauensbeziehung reduziert. Auf Grundlage dieser Vertrauensbeziehung zur AB wird Vertrauen an einzelne SPs delegiert. Indem Benutzer einer einzigen AB direkt vertrauen, können sie daher (indirekt) den Identitätsinformationen aller akkreditierten SPs im System vertrauen. Zusätzlich können ABs vor der Ausstellung von Akkreditierungen an SPs prüfen, ob diese Datenschutzvorschriften und andere Gesetze einhalten. Beispielsweise können sie prüfen, ob der SP einen legitimen Zweck für die Verarbeitung der personenbezogenen Daten des Benutzers hat.

In einem System, in dem die Akkreditierung einen Mechanismus zur Feststellung von Legitimität und Vertrauenswürdigkeit von Service Providern bietet, sind Benutzer in der Lage, Überprüfungen vorzunehmen und fundierte Entscheidungen zu treffen. Die Akkreditierung gibt Benutzern ein Mittel an die Hand, die Glaubwürdigkeit von SPs zu beurteilen, und stärkt dadurch Vertrauen und Zuversicht in den Authentifizierungsprozess. Zusätzlich führt die Akkreditierung eine Haftungsebene ein, die SPs bei Fehlverhalten für ihr Handeln und ihre Entscheidungen zur Rechenschaft zieht.

Es kann für Benutzer jedoch herausfordernd sein, anhand der Akkreditierungen fundierte Entscheidungen zu treffen. Die Komplexität der Akkreditierungsprozesse und die Beurteilung der Akkreditierungskriterien können Hindernisse für Benutzer darstellen. Ein Wallet-System kann den Benutzer zwar unterstützen, indem es Credentials nur an akkreditierte SPs weitergibt, doch muss der Benutzer weiterhin selbst beurteilen, welche Credentials und Attribute er an den SP weitergibt. Dies kann zu Over-asking und damit zu Over-sharing privater Daten führen.

### 5.3. Akkreditierungsbeschränkungen

Um den Benutzer weiter zu unterstützen und zu verhindern, dass zu viele Daten an einen SP weitergegeben werden, werden Akkreditierungen mit Beschränkungen gekoppelt. Akkreditierungsbeschränkungen führen eine entscheidende Ebene der Kontrolle und des Schutzes in das Authentifizierungssystem ein. Indem SPs bestimmte Beschränkungen auferlegt werden, etwa hinsichtlich der Art der Daten, die sie von Benutzern anfordern dürfen, verbessert das System Privatsphäre und Sicherheit der Benutzer. Solche Beschränkungen können begrenzen, welche Credentials ein SP anfordern darf, oder flexiblere Richtlinien sein, etwa den Zugriff auf bestimmte Attribute oder sogar Zero-Knowledge-Prädikate einzuschränken. Mögliche Arten von Akkreditierungsbeschränkungen werden in Abschnitt 7 weiter unten besprochen.

Indem nur Zugriff auf die Daten gewährt wird, die der SP rechtmäßig verarbeiten darf, helfen Akkreditierungsstellen (ABs) dabei, den Missbrauch der Daten der Benutzer zu verhindern.

Die Wallet des Benutzers spielt eine zentrale Rolle bei der Durchsetzung dieser Beschränkungen und stellt sicher, dass bei Authentifizierungsprozessen nur autorisierte Daten an SPs weitergegeben werden. Während die Wallet automatisch kontrollieren kann, dass keine Daten weitergegeben werden, für die der SP keine Berechtigung hat, hängt es vom Design des Systems ab, ob der Benutzer diese Entscheidung übersteuern kann.

Dieser proaktive Ansatz schützt nicht nur vor Over-asking und unnötiger Datenoffenlegung, sondern gibt Benutzern auch mehr Kontrolle über ihre personenbezogenen Informationen. Beschränkungen dienen als Schutzmaßnahme, die Authentifizierungsprozesse mit Datenschutzprinzipien und rechtlichen Anforderungen in Einklang bringt und letztlich Vertrauen und Zuversicht in das Authentifizierungssystem fördert.

## 6. Akkreditierungsformen

Um die automatisierte Überprüfung und Kontrolle durch Wallet-Software zu ermöglichen, müssen Akkreditierungen und Akkreditierungsbeschränkungen in maschinenlesbarer Form erstellt werden. Dies kann in vielen Formen geschehen. Die Hauptanforderung ist, dass die Informationen der Wallet bei der Interaktion mit dem SP letztlich auf vertrauenswürdige Weise zur Verfügung stehen. Beispielsweise kann die Veröffentlichung von Akkreditierungsinformationen folgende Formen annehmen:

- Accreditation Certificate (Akkreditierungszertifikat), ausgestellt an den SP: Nachdem SPs ihren Dienst beschrieben, den Zweck der Datenverarbeitung angegeben und die Akkreditierungsprüfung bestanden haben, erhalten sie von der Akkreditierungsstelle (AB) eine Form von Akkreditierungszertifikat. Dieses Zertifikat ist von der AB digital signiert und enthält Akkreditierungsinformationen und die Beschränkungen. Bei der Authentifizierung präsentiert der SP

dieses Zertifikat dem Benutzer. Der Benutzer prüft das Zertifikat anschließend mit seinem lokalen Trust Store und verwendet es dann, um den SP zu authentifizieren. Der Benutzer nutzt außerdem Standard-Widerrufsprüfungen (OCSP oder OCSP-Stapling), um sicherzustellen, dass die Akkreditierung noch gültig ist.

- Accreditation Registry (Akkreditierungsregister): Bei diesem zentraleren Ansatz ist das Ergebnis des Akkreditierungsprozesses kein Zertifikat, sondern ein Eintrag in einem öffentlichen Register. Dieser Eintrag ist zwar mittels eines (selbstsignierten) Zertifikats mit dem SP verknüpft, die Akkreditierungsinformationen selbst werden aber direkt im Register gespeichert. Der Vorteil dieses Ansatzes ist, dass zuständige Stellen die Liste der akkreditierten SPs überwachen und prüfen können und dass die Informationen leichter aktualisiert werden können. Bei naiver Umsetzung besteht ein Nachteil dieses Ansatzes darin, dass das Register möglicherweise erfährt, wann eine Wallet mit einem bestimmten SP interagiert, was zu Beobachtbarkeit führt. Dies könnte durch das fortlaufende Herunterladen eines Schnappschusses des Registers oder durch andere datenschutzfreundlichere Architekturen verringert werden.

- Combination (Kombination): Eine Kombination aus Akkreditierungszertifikat und Register könnte potenziell sowohl Privatsphäre während des Authentifizierungsprozesses als auch Prüfbarkeit des Systems ermöglichen. Bei diesem Ansatz wird das Vertrauen in den SP durch die Verifikation des Zertifikats hergestellt (wie bei der ersten Option) und anschließend geprüft, ob das Zertifikat mit dem Register verknüpft ist (z.B. mit Mechanismen wie der Certificate Transparency der Web PKI [2]). Dadurch wird die Last, zu überprüfen, ob eine AB eine zu freizügige Akkreditierung ausgestellt hat, vom Benutzer auf zuständige Stellen verlagert.

# 7. Arten von Akkreditierungsbeschränkungen

## 7.1. Boolesche Beschränkung

Boolesche Akkreditierungsbeschränkungen stellen den oben beschriebenen Basisfall dar: Ein Service Provider (SP) ist entweder akkreditiert oder nicht. Für einen akkreditierten SP gewährt die Wallet Zugriff auf alle in der Wallet gespeicherten Credentials. In diesem Fall muss der Benutzer entscheiden, ob er den Zugriff auf die angeforderten Daten gewährt oder nicht.

## 7.2. Ordinale Beschränkung

Ordinale Akkreditierungsbeschränkungen stellen die Akkreditierung in Form einer numerischen Stufe dar. In diesem Fall wird entweder jede Stufe auf eine Menge fortgeschrittenerer Beschränkungen innerhalb der Wallet abgebildet, oder jedes Credential bzw. Attribut ist mit einer bestimmten Stufe verbunden. Der zweite Ansatz ähnelt dem Geheimhaltungsklassifizierungsansatz, der häufig bei Verschlusssachen angewendet wird, d.h. es muss eine Übereinstimmung zwischen der Akkreditierungsstufe des SP und der Stufe der Information bestehen. Beispielsweise könnte eine Akkreditierung für personenbezogene, aber nicht sensible Informationen einem SP die Berechtigung erteilen, Name, Adresse und Geburtsdatum des Benutzers abzufragen, während sensiblere Informationen wie gesundheitsbezogene Daten nicht zugänglich sind.

## 7.3. Erweiterte Beschränkungen

Die folgenden erweiterten Arten von Akkreditierungen ermöglichen eine flexiblere Zugriffskontrolle. Anstatt Alles-oder-nichts-Zugriff zu gewähren oder sich auf vordefinierte Stufen zu stützen, autorisieren Akkreditierungsstellen (ABs) den Zugriff auf bestimmte Credentials, Attribute oder Prädikate ausdrücklich.

### 7.3.1. Credentials

Akkreditierungszertifikate enthalten eine Liste aller Credential-Typen, auf die der SP zugreifen kann. Credential-Typen können beispielsweise mit Uniform Resource Names (URNs), Digital Object Identifiers (DOIs) und Credential-Schemas identifiziert werden.

### 7.3.2. Attribute

Um eine flexiblere Kontrolle zu ermöglichen, können Akkreditierungszertifikate als Beschränkungen auch eine Liste von Attributen enthalten. Wie bei Credentials können Attribute mit verschiedenen Schemata identifiziert werden, z.B. mit URNs [5] oder anderen Identifikationsschemata. [6]

### 7.3.3. Prädikate

Um datenschutzwahrende und -fördernde Technologien wie attributbasierte Credentials und Zero-Knowledge-Beweise zu unterstützen, können Akkreditierungszertifikate den Zugriff auf Daten auf bestimmte Prädikate über diese Daten beschränken. Ist der einzige vom SP angegebene legitime Zweck beispielsweise eine Altersprüfung seiner Benutzer, könnte die AB diesen SP nur für Altersprüfungs- oder Datumsdifferenz-Prädikate akkreditieren. Dadurch hat der SP keinen Zugriff auf andere Daten, nicht einmal auf das Geburtsdatum des Benutzers [3].

### 7.3.4. Pseudonyme

Eine weitere Art von Akkreditierungsbeschränkung betrifft den Umgang mit den identifizierbaren Informationen des Benutzers, d.h. Identitätskennung oder Pseudonymen. Beispielsweise könnte ein soziales Netzwerk lediglich dazu akkreditiert sein, das Wallet-System zur (erneuten) Authentifizierung von Benutzern zu verwenden (z.B. als bequemerer oder sicherer Ersatz für einen Passwortmanager oder ein Zweitfaktor-System). In diesem Fall hat das soziale Netzwerk als SP keinen Anlass, weitere Informationen über den Benutzer zu erfahren. Während der Zugriff auf Credentials und Attribute des Benutzers mit den oben besprochenen Beschränkungsarten leicht eingeschränkt werden kann, hat der SP weiterhin Zugriff auf die Kennung des Benutzers. Somit kann der SP mehrere Besuche desselben Benutzers verknüpfen und andere Profilbildungstechniken anwenden.

Um Benutzer bei der Wahl ihrer Identitäten zu unterstützen, können ABs SPs darauf beschränken, nur auf Pseudonyme der Benutzer zuzugreifen, und verhindern, dass für jeden SP nur ein einziges Pseudonym möglich ist. Dies ist das Wallet-Gegenstück zu einem Benutzer, der mehrere Konten bei einem SP anlegt, ohne eine Verknüpfung zwischen diesen Konten herzustellen.

Beispielsweise verhindern die Pairwise Pseudonymous Identifiers von OIDC systemweite Profilbildung durch zusammenarbeitende SPs, hindern einen SP aber nicht daran, mehrere Besuche des Benutzers zu profilieren. Im Gegensatz dazu wahren Pseudonyme, die von den Benutzern frei erzeugt werden (ob in

irgendeiner Weise mit ihrer Wallet-Identität verknüpft oder nicht), die Privatsphäre und Wahlfreiheit des Benutzers. Zwar liegt es grundsätzlich bei den Benutzern, wie viele Pseudonyme sie für jeden Dienst verwenden, es kann aber aufgrund von Sybil-Beschränkungen eine Obergrenze geben (siehe Diskussion in Abschnitt 3.6 oben).

## 8. Fazit

Akkreditierungen und Akkreditierungsbeschränkungen sind grundlegende Säulen in der Architektur Credential-basierter Authentifizierungssysteme. Diese Techniken spielen eine wichtige Rolle beim Aufbau von Vertrauen, bei der Sicherstellung von Rechenschaftspflicht und beim Schutz der Privatsphäre der Benutzer. Indem Service Provider (SPs) Akkreditierungsprozessen unterzogen werden, werden Benutzer in die Lage versetzt, die Legitimität und Vertrauenswürdigkeit der SPs zu beurteilen. Darüber hinaus fügen Akkreditierungsbeschränkungen eine Schutzebene hinzu, die Over-asking und unnötige Datenoffenlegung verhindert und Benutzern mehr Kontrolle über ihre personenbezogenen Informationen gibt. Die Wirksamkeit von Akkreditierungen und Beschränkungen hängt von der Sorgfalt der Akkreditierungsstellen bei der Prüfung der SPs und ihres Verarbeitungsbedarfs ab. Ziel bleibt es, einen Ausgleich zwischen reibungslosen Authentifizierungserlebnissen, der Ermöglichung von Innovation und der Wahrung von Datenschutzprinzipien zu finden. Mit der Weiterentwicklung der Authentifizierungstechnologien werden fortlaufende Bemühungen zur Verfeinerung der Akkreditierungsprozesse und zur Integration von Beschränkungsmechanismen entscheidend sein, um Integrität, Sicherheit und Benutzerzentrierung von Authentifizierungssystemen im digitalen Zeitalter zu gewährleisten.

## Referenzen


[*] OpenAI. ChatGPT (3.5) [Large language model] was used to edit parts of the text.

[1] A. Pfitzmann, M. Hansen. Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology (Version 0.28), 2006.

[2] D. Kales, O. Omolola and S. Ramacher, Revisiting User Privacy for Certificate Transparency, IEEE EuroS&P, 2019.

[3] S. More, S. Ramacher, L. Alber and M. Herzl, Extending Expressive Access Policies with Privacy Features, IEEE TrustCom, 2022.

[4] K. Rannenberg, J. Camenisch, A. Sabouri, Attribute-based credentials for trust. 2015.

[5] Epicenter Works, Analysis of Privacy-by-Design EU Legislation on Digital Public Infrastructures, 2024.

[6] Germany: eIDAS 2.0 Architecture Concept (Version 2), 2024.

[7] EUDI Wallet: Architecture and Reference Framework (Version 1.3), 2024.

[8] European Parliament and Council of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), 2016.

[9] European Parliament and Council of the European Union, Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2), 2024.

[10] S. More, J. Heher, E. Fasllija, M. Mathie, Service Provider Accreditation: Enabling and Enforcing Privacy-by-Design in Credential-based Authentication Systems, ARES EDId, 2024.

---

1. https://openid.net/specs/openid-connect-core-1_0.html#PairwiseAlg ↩
2. https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/ ↩
3. https://arstechnica.com/information-technology/2017/12/nope-this-isnt-the-https-validated-stripe-website-you-think-it-is/ ↩
4. Mechanismen wie App Attestation könnten den direkten Zugriff auf die Daten zwar erschweren, sie können jedoch unbefugten Zugriff durch Stellen mit physischem Zugriff auf das Gerät des Benutzers nicht vollständig verhindern. ↩
5. https://eid.egiz.gv.at/anbindung/uebersicht-der-personenmerkmale-attribute/ ↩
6. https://schema.org ↩