Anforderungen und Konzepte bei Identitätsbeständigkeit und Identitätsmapping

Sebastian Karius[1], Marlies Gollnick[2], Robin Kopitz[3], Meiko Lips[4], Hermann Strack[5]

1 Hochschule Harz, skarius@hs-harz.de
2 Hochschule Harz, mgollnick@hs-harz.de
3 Hochschule Harz, rkopitz@hs-harz.de
4 Hochschule Harz, mlips@hs-harz.de
5 Hochschule Harz, hstrack@hs-harz.de

Abstract

Die Digitalisierung im Bildungswesen erfordert zunehmend die Verknüpfung verschiedenster Identitäts- und Serviceprovider. Im Nationale Bildungsplattform (NBP)-Infrastrukturprojekt „Kommunikation, Open Source, lebenslanges Lernen in Bildungseinrichtungen durch rechtssichere Integration – KOLIBRI“ (BMBF-Förderung) wurde u.a. die Verknüpfung verschiedenen Identitätsprovider von Schulen und Hochschulen mit verschiedenen Serviceprovidern praktisch demonstriert. Dabei wurden verschiedene Anforderungen und mögliche Lösungskonzepte zur Weitergabe, Beständigkeit und dem Mapping von Identitäten zwischen verschiedenen Identitätsprovidern untersucht und evaluiert. Besondere Anforderungen ergaben sich im Bezug zu eID gestützten Identitäten.

1. Einleitung

Digitalisierung in verschiedenen Bereichen wie dem Bildungswesen, der öffentlichen Verwaltung, dem Gesundheitswesen und in der Wirtschaft erfordern digitale Identitäten. Dabei gibt es verschiedene Verfahren um die eigene Identität nachzuweisen. Immer häufiger werden dabei sichere Verfahren wie zertifikatsbasierte- oder eID-Authentifizierungsverfahren (eID-Online-Ausweisfunktion des Personalausweises) nach eIDAS-Verordnung verwendet. Eine Person erhält so im Laufe ihres Lebens verschieden Identitäten mit verschiedenen Authentisierungsmethoden und entsprechenden Merkmalen. In vielen Fällen, insbesondere der Weitergabe von Dokumenten oder bestätigten personenbezogenen Daten, ist ein Mapping der Identitäten sinnvoll.

Im NBP-Infrastrukturprojekt „KOLIBRI“ für die Entwicklung eines Prototypen für eine Metaplattform zur Verbindung verschiedenen Bildungsnutzenden und Bildungsanbieten über eine zentrale „Verbindungsplattform“, gefördert im Rahmen von Forschungsprojekten zur Nationalen Bildungsplattform (BMBF-Förderung im Rahmen des BIRD Projektes) (Strack, 2022a, 2022b) wurden verschiedenen Authentisierungsmethoden, bis hin zu eID, implementiert und u.a. Anforderungen und Konzepte für das Mapping von Identitäten untersucht.

2. Anforderungen an Indentitätsmanagement und –mapping

Das NBP-Infrastrukturprojekt „KOLIBRI“ hat einen Plattform-Prototyp für die NBP in Deutschland implementiert. Diese Plattform ermöglicht, die Verbindung verschiedener Arten von Bildungseinrichtungen. Ein zentraler Bestandteil ist ein Identity Provider (IDP) der Satellitensysteme der Bildungsträger ermöglicht. Die entwickelte Plattform bietet

den Nutzenden die Möglichkeit nach einer Anmeldung verschiedene Dienste der angeschlossenen Bildungsanbieter zu nutzen ohne sich hierbei für jeden Bildungsanbieter neu anmelden zu müssen, ein sogenanntes Single Sign-On (SSO). Eine weitere Aufgabe war die Anbindung von sogenannten User Wallets zur Verwaltung selbstbestimmter Identitäten (Self-Sovereign Identity, SSI) sowie die Kopplung zu Bildungsträgersystemen mittels sogennater Metadaten-Konnektoren, wobei Wallets und Metadatenkonnektoren vom BMBF-Projekt BIRD zur Verfügung gestellt wurden.

Durch die beschriebenen Anforderungen und das Anwendungsgebiet selbst ergaben sich Fragestellungen zur Identitätsbeständigkeit und zum Identitätsmapping. Eine Person kann im Laufe ihres Lebens verschiedenste Bildungsinstitute besuchen. Dabei wird üblicher Weise eine eigene Identität für diese Person in jedem Bildungsinstitut erstellt. Beispielsweise erhält man an Hochschulen eine Matrikelnummer. In den seltensten Fällen ist es möglich die Identität von einem Bildungsinstitut an ein anders zu übergeben und so ohne zusätzlichen Nachweis der eigenen Person dort Bildungsangebote wahrzunehmen. Um dies zu ermöglichen ist entweder die Weitergabe, das Mapping oder eine externe vertrauenswürdige Anmeldung notwendig. Bei der Weitergabe werden die personenbezogenen Daten einer Person von einem Bildungsinstitut an ein anderes, mit der Zustimmung der Person, übergeben. Das Mapping von Identitäten ist notwendig, falls beide Bildungsinstitute bereits eine Identität angelegt haben, oder eine externe Identität wie die eID zum Abgleich personenbezogener Daten verwendet werden soll. Dabei muss die Person nachweisen, dass beide Identitäten zu dieser Person gehören, anschließend werden die Identität verknüpft. Bei externen Anmeldungen, auch SSO, wird der Anmeldung an einer externen Identitätsverwaltung vertraut und die benötigten personenbezogenen Daten weitergegeben.

Die Weitergabe von personenbezogenen Daten zu einem weiteren Identitätsprovider stellt technisch keine Herausforderung dar. Protokolle und Standards wie SAML 2.0 (OASIS, 2008), OIDC oder oAuth (OpenID Foundation, o. D.), ermöglichen SSO und sind praktisch bereits weit verbreitet, und auch im Rahmen des NBP-Infrastrukturprojekts „KOLIBRI“, eingesetzt wurden.

Die Verknüpfung verschiedener Identitäten stellt, besonders im Rahmen des NBP-Infrastrukturprojekts „KOLIBRI“ eine Herausforderung dar. Das grundlegende Problem besteht darin, dass verschiedene IDPs verschiedenen Identitätsmerkmale verwenden. Beispielsweise kann eine Identität durch den vollständigen Namen, die E-Mail-Adresse, einen Nutzernamen, ein Pseudonym oder bei Hochschulen durch eine Matrikelnummer dargestellt werden. Diese Identifikationsattribute können in zwei Klassen aufgeteilt werden, personenbezogene und providerspezifische erzeugte Attribute. Beide Klassen haben Vor- und Nachteile. Die personenbezogenen Attribute sind direkt einer Person zuordenbar, das hat den Vorteil, dass über verschiedenen IDPs hinweg die gleiche Person die gleichen Identifikationsattribute besitzt, allerdings wird die Person dadurch nachverfolgbar, was dem Datenschutz entgegensteht. Providerspezifisch erzeugte Attribute haben den Vorteil, dass sie üblicher Weise von jedem IDP unabhängig erzeugt werden und daher die identifizierte Person nicht nachverfolgbar ist, was jedoch das Mapping über die IDPs hinweg erschwert.

Neben den beiden Klassen von Identifikationsattributen gibt es zwei grundlegend verschiedene Ansätze Identitäten zu verwalten. Die erste ist die Identität bei einem IDP zu hinterlegen und sich gegenüber diesem zu authentisieren, um die eigene Identität einem

Serviceanbieter (SP) bereitzustellen. Die zweite Variante beruht auf einer Wallet. Dabei verwaltet der Nutzende seine Identitätsdaten selbstsouverän, auf einem von ihm kontrollierten Gerät, nachdem diese von einem IDP in die Wallet übertragen wurden. Die Identitätsdaten können dann direkt vom Gerät zum SP übertragen, die Authentisierung erfolgt dabei durch den Nachweis des Besitzes und des Zugriffs auf das Gerät. Diese Variante wird u.a. im Rahmen des BMWi Fördervorhaben „Schaufenster Sichere Digitale Identitäten“, unter dem Namen ID-Wallet, untersucht. Wobei die ID-Wallet auf Standards und Konzepte des eIDAS 2.0 setzt (Schwalm et al., 2022). Diese Art der Identitätsverwaltung wird mit Self Souvereign Identity (SSI) bezeichnet. (Preukschat & Reed, 2021)

Weiter kann eine Person bei verschiedenen IDPs verschiedene Klassen von Identitäten haben und verwalten. Dies erschwert zusätzlich das Weiterreichen oder Mapping dieser Identitäten. Daraus ergibt sich die hauptsächliche Anforderung an Identitätsmapping: Für eine Person muss nachgewiesen werden, dass jede der zu mappenden Identitäten Identitäten dieser Person sind. Dabei ist darauf zu achten nur notwendige Daten, und wenn nur vertraulich, zu übertragen.

3. Mapping von Identitäten zwischen IDPs

Um das Mapping von Identitäten zu ermöglichen wird eine Vertrauensbasis zwischen den beiden IDP Systemen benötigt. Dies kann entweder direkt gegenseitiges Vertrauen sein, oder das Vertrauen in eine dritte Instanz. Diese Vertrauensverhältnisse müssen für ein digitales Identitätsmapping auch digital abgebildet werden. Direktes Vertrauen zwischen IDP Systemen wird beispielsweise bei SAML2.0 oder oAuth durch das Hinterlegen von Zertifikaten oder Token ausgedrückt. (Hühnlein et al., 2020) Hier wird für ein System ein Zertifikat oder Token erzeugt, welches in einem anderen als vertrauenswürdig hinterlegt wird. Die Abbildung von indirekten Vertrauensverhältnissen kann z.B. durch qualifizierte elektronische Signaturen (QeS) (Europäisches Parlament, 2014) erfolgen. Ist eine Vertrauensbasis geschaffen, können Identitätsdaten vertraulich und integritätsgeschützt ausgetauscht und abgeglichen werden, was die grundlegende Voraussetzung für das Mapping von Identitäten ist.

Eine Person kann in der EU eindeutig per Vor- und Nachname, Geburtsname, Geburtsort, Geburtstag, aktueller Wohnort und Geschlecht identifiziert werden. Sind diese Informationen in beiden IDPs vorhanden, können Personen eindeutig gemapped werden. Haben beispielsweise zwei Bildungsträger diese Identitätsdaten, können Identitäten, die bei verschiedenen Bildungsträgern vorhanden sind anhand dieser Identitätsdaten automatisch gemapped werden, wobei eben genannte Daten notwendiger Weise übertragen werden müssen.

Per eID erhaltene Identitätsdaten, unterliegen jedoch besonderem Schutz, sie dürfen explizit nur in der Domain verwendet werden, in der sie abgefragt wurden. Damit können sie nicht für ein automatischen Mapping wie eben beschrieben verwendet werden. Auch falls nicht alle Daten um eine Person eindeutig zu identifizieren vorhanden sind, ist ein automatisches Mapping nicht zweifelsfrei möglich. Dieser Fall kann durch ein Nutzermanuelles Mapping gelöst werden. Dabei muss sich die Person mit beiden Identitäten, bei beiden IDPs, anmelden die gemapped werden sollen. Technisch muss sich die Person zunächst bei einem IDP authentisieren, dieser wird mappender IDP genannt. Danach wird die Person an einen zweiten IDP weitergeleitet und muss sich dort ebenfalls

authentisieren, dieser wird bereitstellender IDP genannt. Nach der Authentisierung erzeugt der bereitstellende IDP einen Bereitstellungstoken das den Nachweis der Authentisierung und ein eindeutiges Identifikationsmerkmal der Person enthält und leitet den Nutzer zurück zum mappenden IDP. Dieser prüft den Bereitstellungstoken und extrahiert das Identifikationsmerkmal. Der mappende IDP kann nun der Person das Identifikationsmerkmal des bereitstellenden IDP zuordnen.

Das Nutzer-manuelle Mapping hat einen entscheidenden Vorteil gegenüber dem automatischen Mapping: Das vom bereitstellenden IDP übergebene Identifikationsmerkmal muss nicht dem intern genutzten Identifikationsmerkmal entsprechen. Das ermöglicht ein Vorgehen vergleichbar mit dem Pseudonymprinzip der eID. Dabei wird für jede eID-Domain, bei der sich eine Person per eID anmeldet ein neues Pseudonym erzeugt, sodass eine Wiedererkennung zwischen Anwendungen behindert bzw. zumindest erschwert wird. Im Mapping Fall, kann der bereitstellende IDP für jeden mappenden IDP ein eigenes neues Pseudonym für die Person erzeugen. Im Falle eines zentralen IDP, ist es einer Person mit dieser Vorgehensweise möglich, alle Identitäten zentral zu verwalten und SSO wird ermöglicht. Im Falle von SSI, kann eine Person verschiedenen Identitäten in der eigenen Wallet „sammeln“ und sich so gegenüber verschiedenen SP selbstsouverän authentisieren.

Fazit

Durch den Einsatz von eID- und anderen zentralen, wenn auch weniger gesicherten, Authentisierungsverfahren, den Einsatz von Wallets steigt die Zahl der Identitäten, die eine Person besitzt. Das Mapping von Identitäten ist technisch möglich, es sind jedoch die organisatorischen und rechtlichen Rahmenbedingungen zu beachten, die spezielle Vorgehensweisen wie bspw. das Verwenden von Pseudonymen erforderlich machen.

Quellen

Strack, H., Gollnick, M., Karius, S., Lips, M., Wefel, S., Altschaffel, R., Bacharach, G., Gottlieb, M., Pongratz, H., Radenbach, W. & Waßmann, A. (2022). Digitization of (Higher) Education Processes: Innovations, Security and Standards. EPiC Series in Computing, 86, 22–29. https://doi.org/10.29007/rrg4

Strack, H., Karius, S., Gollnick, M., Lips, M., Wefel, S. & Altschaffel, R. (2022). Preservation of (higher) Trustworthiness in IAM for distributed workflows and systems based on eIDAS. 1617-5468. https://doi.org/10.18420/OID2022_11

Strack, H., Gollnick, M., Karius, S., Lips, M. (to be published 2023). Schlussbericht für das Teilvorhaben „Gesicherte Hochschul- und Bildungsdigitalisierung mittels Identitäten und Trust Services (eIDAS)“ der Hochschule Harz im Rahmen der Initiative Nationale Bildungsplattform

OASIS. Security Assertion Markup Language (SAML) V2.0 Technical Overview. OASIS. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

OpenID Foundation. OpenID Connect specifications. OpenID Foundation. https://openid.net/developers/specs/

Schwalm, S., Albrecht, D. & Alamillo, I., (2022). eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI. In: Roßnagel, H., Schunck, C. H. & Mödersheim, S. (Hrsg.), Open Identity Summit 2022. Bonn: Gesellschaft für Informatik e.V.. (S. 63-74). DOI: 10.18420/OID2022_05

Preukschat, A. & Reed, D. (2021). Self-Sovereign Identity. Manning Publications.

Europäisches Parlament. (2014). Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung). http://data.europa.eu/eli/reg/2014/910/oj

Hühnlein, D., Hühnlein, T., Hornung, G. & Strack, H. (2020). Towards Universal Login. In Open Identity Summit 2020 (S. 193–200). Gesellschaft für Informatik e.V. https://doi.org/10.18420/ois2020_18