Protokoll des Treffens der U-AG „Technische Infrastruktur“ der FID zum Thema Authentifizierung/Autorisierung am 20.02.2018 an der Staatsbibliothek zu Berlin

Sitzungsleitung: G. Gragert

Moderation: G. Gragert

Protokoll: K. Keßler

Teilnehmer/innen: 25 Teilnehmer/innen aus 19 Einrichtungen

1: Begrüßung / Single-Sign-On im FID Asien (G. Gragert)

Zusammenfassung

- „Die FIDs schießen quer“ vs. „The world as we know it“ → Ziel sollte die Vereinigung der Zugriffsberechtigungen sein.
- „FID Asien geht in Deckung“ → Shibboleth ein Weg. Vorstellung Workflow CrossAsia, Demonstration und Konfigurationsbeispiele. Auch Darstellung der Probleme mit eduPersonUniqueId, z.B. Datenschutz, technische Gründe.
- Wie geht es weiter? Andere Ansätze:
    - Schweiz: eine nationale Implementierung der eduPersonUniqueId → Wollen/können wir das?
    - ORCID: Authentifizierungsdienste möglich → Nutzbar im FID-Kontext?
    - WebID/TLS?

Anmerkungen und Hinweise

- Voraussetzung für die Nutzung von Schibboleth: Heimateinrichtung bietet dies an.
- eduPersonUniqueId ist mit Account verbunden, nicht mit einer Identität. Dies kann bei mehreren Identitäten zu Problemen führen. Wenn das IDM der Heimateinrichtung mehrere eduPersonUniqueId für eine Person enthält und somit unter Umständen unterschiedliche herausgibt.

Fragen und Antworten

F: Schweizer eduPersonUniqueId: Was passiert, wenn ein Wissenschaftler die Wissenschaft verlässt?

A (Zusammenfassung von Antworten mehrerer Teilnehmer/innen): Unterscheidung zwischen Authentifizierung (lebenslang) und Autorisierung (temporär) muss gemacht werden. In diesem Fall könnte sich der Wissenschaftler noch authentifizieren, hätte aber vermutlich keine Autorisierung für

einen Zugriff auf Ressourcen. Dies ist auch abhängig von den Lizenzbedingungen für Ressourcen. Am Ende muss immer eine Prüfung stattfinden, ob die Autorisierung vorliegt.

F: Wenn ein Nutzer auch z.B. die Rolle Mitarbeiter der Fernleihe hat. Wie sieht das mit der Berechtigung aus?

A (Zusammenfassung von Antworten mehrerer Teilnehmer/innen): Die Autorisierung/Berechtigung wird hinzuaddiert. Es werden weitere Attribute/Entitlements mitgegeben.

F: Erfahrung bei CrossAsia: Wie viele Einrichtigungen liefern eduPersonUniqueId?

A (G. Gragert): Schätzung ca. die Hälfte der Einrichtungen. Der Start war etwas holprig und erforderte viele Erklärungen gegenüber Nutzer/innen. Nach 3 bis 4 Monaten eingespielt. Wertung von keinen Beschwerden als gutes Zeichen. Am Anfang oft die Frage „Warum?“.

F: Anschlussfrage: Attribute Authority auf DFN-Ebene verankern um diese für alle nutzbar zu sein?

A (G. Gragert): Im Pilot wird eine Attribute Authority für das KfL aufgebaut.

2: Nutzerkreise für den Zugang zu FID-Lizenzen beim KfL (M. Huber)

Zusammenfassung

- Übersicht über die Aktivitäten des KfL und die Aufteilung über die verschiedenen Standort: Göttingen, Berlin und München sowie den Dienstleister VZG
- Übersicht über verschiedene verhandelte und abgeschlossene Lizenzen sowie Zugangswege
- Vorstellung der Abläufe, auch Darstellung der Probleme (weitere Identität, zu viele Klicks)
- Ausblick: Pilot mit Attribute Provider um weitere Identität zu vermeiden

Fragen und Antworten

F: Ist es notwendig die an den Lizenzen beteiligten Einrichtungen zu melden?

A (M.Huber): Ja, im Rahmen der Lizenzverhandlungen muss der FID dies festlegen.

F: Was bedeutet einwählen, was ist ein selektiver Nutzerkreis vs. Opt-in?

A: Entweder Vorauswahl des Nutzerkreises, aus dem sich dann die Personen anmelden/einwählen können, durch FID oder Angebot an Wissenschaftler/Institutionen und diese entscheiden welche Produkte sie nutzen

3: Single Point Authentifizierung am Beispiel von Pollux (D. Opitz)

Zusammenfassung

- Ursprüngliche Version der Authentifizierung mit HAN (doppeltes Login)
- Aktuelle Version der Authentifizierung mit HAN (SSO)

- Künftige Möglichkeit der Authentifizierung der Nutzer aus anderen FIDs (via Shibboleth etc.)

Fragen und Antworten

F: Welche fremde Software hat Zugriff auf Nutzerdaten?

A (D.Opitz): Korrekt ist, dass bei einer SPA keine Fremdsoftware Zugriff auf die Nutzerdaten erhält. Der HAN-Server hatte nur in der ersten Ausbaustufe Zugriff auf die Daten, weil die alte Version keine SSO-Unterstützung hatte und gezwungenermaßen auf die DB zugreifen musste, damit die Nutzer/innen nicht noch mehr Accounts brauchen.

F: Wie verhält es sich mit Passwortänderungen und der Handhabung dieser bei externem Dienst?

A (D.Opitz): Externer Dienst gibt nur Rückmeldung über Zugriff ja oder nein. Wir müssen noch einige Informationen separat erfragen, z.B. zugehörigen Institution, bei Premium-Account Klarnamen als Grundlage der Bestätigung für Nutzung von Lizenzen. Berechtigungen sind bei POLLUX gespeichert.

F: Wie ist der HAN-Server in externe Authentifizierung integriert?

A (D.Opitz): Gar nicht, dies geschieht separat.

F: Wie wird Autorisierung sichergestellt?

A: Autorisierung läuft nach einem Jahr aus und muss dann erneuert werden.

Diskussionsrunde

Erkennung von Nutzern und deren Zugehörigkeit zu Institutionen bzw. Nutzerkreisen

- Man sollte sich als neuer Service Provider nicht bei allen IDPs manuell eintragen müssen(Vorstellung, Prozesse, Formulare). Eine zentrale Stelle für die Registrierung wäre vorteilhaft. Das wäre ein erster Schritt. Eine Clearing-Stelle wäre gut. (O. Brandt/D. Opitz) → Ansätze Code of Conduct. Aber weiterhin sehr müsam. (G. Gragert)
- Aus Nutzersicht wäre das gut. Aber nicht nur Datenschutz, sondern auch Lizenzmodelle beachten. Autorisierung/Berechtigung muss pro Institution verwaltet werden, vermutlich riesiger Verwaltungsaufwand. (B. Gilitzer)
- Wichtig ist auch, dass die Person, die eine ID anlegt, nachweislich diese Person ist. (D. Opitz)
- Es ist auch noch schwierig einzuschätzen, wie Attribute Provider bei Verlagen akzeptiert werden. Eine Instanz für die Attribute wäre daher besser. (G. Gragert)
- Wenn es nur um Authentifizierung geht, warum baut man quasi ORCID nach? Berechtigungen müssen so oder so noch bei Institutionen liegen. (O. Brandt)
- ORCID ist nicht vertrauenswürdig. Personen können imitiert werden. (D. Opitz)
- Als ID wohl ok, aber natürlich nicht für Autorisierung. Interessant was mit der neuen Organization ID passiert. Hier sollte eine Überprüfung stattfinden. (G. Gragert)
- Wie sieht es mit Zertifikaten aus? (B. Bauer)
    - Sind sicher, aber nicht sehr nutzerfreundlich. (G. Gragert)

- Nicht nutzbar. (O. Brandt)
- Zu komplex, sowohl auf Nutzer- und auch auf Service-Seite. (D. Opitz)
- Man vergleiche es mit E-Mail. Zertifikate haben sich nicht durchgesetzt. (S. Farrenkopf)
- Ein weiterer Account ist eigentlich nicht das Problem. (D. Opitz)
- Wer stellt Zertifikate aus? (H. Miersch)
- Das ist auch das Problem bei WebID. Nur etwas für „Nerds“. (G. Gragert)
- Ist das nicht auch das gleiche Problem bei Nationaler ID. (H. Miersch)
- Ja, das müsste die Institution machen. Ein Riesenverwaltungsaufwand. (A. Dörrer)
- Ja, einfacher über Institution. Dennoch ein Aufwand. (D. Opitz)
- An der Institution wird die Identität in jedem Fall festgestellt. Eine weitere zentrale Institution hätte nur einen kleinen Zusatznutzen, würde aber viel Aufwand mit sich bringen. (B. Gillitzer)
- Technisch vermutlich gar nicht so aufwändig, aber vermutlich organisatorisch wegen Datenaustausch. (O. Brandt)
- Das scheint zu kompliziert. Wie machen das die Schweizer genau? (nicht notiert)
    - Vielleicht mal die Schweizer einladen. (O. Brandt)
    - Ich nehme mal Kontakt auf. (G. Gragert)
    - Hat die Schweiz etwas wie FIDs und wenn ja, wird sie hier genutzt? (M. Seyder)
        - Die ID wird allgemein für alle wissenschaftlichen Tätigkeiten genutzt (G. Gragert)
        - Ich habe auf die Schnelle eine Vortragsfolie gefunden: Erst wird die eduID angelegt, dann die lokale ID und die Attribute. (S. Farrenkopf)
        - Dies funktioniert also genau andersherum als bei CrossAsia. Ich stelle den Kontakt her. (G. Gragert)

Linkresolver

- Einbindung FID Linkresolver bei eigener Institution. Der Nutzer weiß ja nicht welche Ressourcen er über den FID beziehen kann. Wie könnte der Workflow sein zu einer Datenbank, die vom FID lizenziert ist? (B. Bauer)
    - Zur Information: Wir bauen gerade einen Dienst auf in unserem Discovery System bei Campus-Lizenzen. (A. Gerlach, ULB Halle-Wittenberg)
    - Bei Campus-Lizenzen klar. Bei anderen Lizenzen schwieriger. (M. Huber)
    - Man könnte Indikatoren in den Katalogisaten vermerken. (D. Opitz)
    - Man bräuchte dann auf Linkresolver-Ebene Rollen. (J. Maas)
    - Haben wir mit EZB dann nicht schon eine Infrastruktur? (S. Farrenkopf)
    - Nicht ganz ausreichend. VZG baut eine Verbesserung auf. (J. Maas)
    - Am Ende entscheidet der FID wo und welcher der Eintrag vorgenommen wird. (S. Farrenkopf)
    - Grundproblem ist, dass nicht nur der Nutzer auf Basis der Institution identifiziert werden muss, sondern auch auf Basis der Einzel-FID-Lizenz. (B. Bauer)
    - Zur Klarstellung: Es gibt zwei Perspektiven über die gesprochen werden muss. Zum einen dass eigenem System. In diesem sollte die Anzeige, dass etwas eine FID-Lizenz

ist selbst unkompliziert implementierbar sein. Zum anderen ist dies bei anderen Systemen, z.B. Google Scholar, wohl generell nur über die IP möglich. (K. Keßler)
    - Es wäre ggf. möglich unterschiedliche Ansichten anzubieten, abhängig ob man über eine eigene IP oder über einen Proxy zugreift. (M. Huber/U. Casny)
    - Man kommt aber im Grunde immer wieder auf das Thema einer zentralen Stelle für die Autorisierung zurück, die sowohl IP- als auch nutzerabhängig Entitlements zur Verfügung stellen kann. (G. Gragert)

- LAS:eR
    - Erster Pilot soll in Kürze online gehen. Wir haben Berührungspunkte. Bei nächstem Termin Vorstellung von LAS:eR. (G. Gragert)
    - Unklar, wie die VZG darin involviert ist. Am besten auch Herrn Steilen einladen. (J. Maas)
    - Nehme ich mit für einen Folgetermin. (G. Gragert)

Technologie

- Also keine technische Lösung für Berechtigung bei Nutzerkreisen? (U. Casny)
    - Ein Problem ist auch, dass viele Anbieter/Verlage in der Regel nur ip-basiert operieren. Es wird schwierig den Anbietern dies beizubringen. (A. Dörrer)
    - Kann HAN als Autorisierungsinstrument fungieren? (U. Casny)
    - HAN fragt Attribute Provider ab. (G. Gragert)
    - Also ein weiteres Autorisierungsinstrument? (U. Casny)
    - Bei CrossAsia: Der HAN-Server prüft die IP. Wenn keine Berechtigung vorliegt, dann erscheint normalerweise die Anmeldeseite des HAN-Servers, aber eigentlich sollte auf die Anmeldeseite der Heimateinrichtung umgeleitet werden. Bei uns gibt es ein Skript zur Prüfung, ob Shibboleth-Anmeldesession vorhanden. Aber dies ist mit einer einzigen URL nicht machbar. Ein Access Mode Switch könnte interessant sein. Aber es ist noch unklar wie genau dieser funktioniert. (G. Gragert):
    - Bei uns macht der HAN-Server gar keine dieser Prüfungen mehr, sondern das Front-End. Beschreibung verschiedener Szenarien. Ein interner Link-Resolver, der dies alles abhandelt. (D. Opitz)
    - Super, aber ist das nachnutzbar, kann man das generalisieren? Das müsste man überprüfen. (S. Farrenkopf)
    - Schwierig, da wir ein ganz anderes System haben. Zum Beispiel in der VuFind-Community könnte man das besser nachnutzbar machen. Dies in kleinem Umfang bei einem FID zu machen war schon nicht ohne. (D. Opitz)
    - Also wichtiger, dass man mehr über LAS:eR herausbekommt. Auf die Verlage können wir nicht hoffen. (O. Brandt)
    - Gerald Steilen sagte mal, dass die Verlage das doch gern machen würden, ein einfaches System, dass für Nachweise genutzt werden kann. (T. Pianos)
    - Kommt wahrscheinlich auf den Verlag an. (S. Farrenkopf)
    - So etwas erscheint als Henne-Ei-Problem. Nebenbemerkung: Problematisch bei Pollux erscheint: Man kann sich nicht einfach eine URL bookmarken. (G. Gragert)

  - Wäre es nicht sinnvoll die Rechteprüfung in eine Zwischenschicht auszulagern? Dann könnte man es einfacher generalisieren. Vielleicht wäre dies ein Weg um eine zentrale Prüfung aufzubauen. Dies könnte man kooperativ im FID-Kontext weiterverfolgen, ggf. zentral oder auch dezentral. (B. Gillitzer)
- Forschungsdaten:
  - Nutzung von Shibboleth für Forschungsdatenarchiv war bei uns im FID-Antrag im Rahmen der Prüfung für den Bedarf hinsichtlich des Forschungsdatenmanagement in der Community enthalten. Es war erstaunlich, dass dieser Punkt bei der Begutachtung herausgestrichen worden ist. Gibt es in dieser Hinsicht Erfahrungen bei anderen FIDs? (O. Brandt)
  - Zum Beispiel beim FID Pharmazie war in der 1. Förderphase eine kleine Bedarfsanalyse inkludiert. In der 2. Förderphase ist ein Pilot-Dienst inkludiert. (K. Keßler)
  - Bei uns kein Forschungsdatenmanagement, aber die Vermittlung. Sichtbarmachung und Autorisierung. Individuell zu betrachten in individuellen Kontexten. Gibt es dafür schon eine Zielstruktur? (S. Farrenkopf)
- Streaming: Im unserem FID besteht sehr viel Bedarf an Filmen und Serien. Viele Titel sind nicht mehr auf DVD erhältlich. Wie kann man Streaming-Dienste im Rahmen eines FID-Dienstes anbieten? (M. Seyder)
  - Wir haben VHS-Kassetten digitalisiert. Aber nur Streaming für einen Nutzer zulässig, entweder vom Campus aus oder authentifiziert. (H. Miersch)
  - In der Regel gibt es momentan nur Dienst für personengebundenes Streaming. (J. Kühne)
  - Also steht unserer FID vor einer schwierigen Herausforderung. (M. Seyder)

Abschluss

- Kommunikation zu technischen Fragen: Erster Anlaufpunkt über die Mailingliste, aber dann Vermittlung an entsprechende Kolleg/innen notwendig. Situative Koordinierung von Gruppen.
- Masterplan für einheitliche Plattform/Nachnutzung bestehender Lösungen: Ja, sinnvoll. Links zu Repositorien über Mailingliste abfragen. Sammlung an zentraler Stelle. → Unterstützung durch SuUB Bremen (D. Opitz) angeboten. → Sammlung wird hier stattfinden: https://github.com/suub/fid-resources
- Workshop zum Thema Software-Entwicklung (Tools, Methoden, etc.) → Tübingen (O. Brandt)/Kiel (T. Pianos) haben sich bereit erklärt bei der Organisation zu helfen.
- Protokoll/Präsentation → Diese werde zusammen an die AG-FID-Mailingliste und die Teilnehmer/innen des Workshops verschickt werden.
- Nächstes Treffen zum Thema Authentifizierung/Autorisierung
  - Ende des Jahres
  - Versuch der Einladung von Kolleg/innen aus der Schweiz und der VZG (G. Steilen hinsichtlich LAS:eR)