SSO via Shibboleth als Service im Rahmen des KfL-Projekts

03.09.2021

Beim Zugriff auf lizenzierte Ressourcen kommen Single-Sign-on-Mechanismen wie z. B. Shibboleth immer mehr zum Tragen. Dies hat dazu geführt, dass ein Großteil der Wissenschaftler in Deutschland über einen Login verfügen, mit dem sie ortsunabhängig alle Angebote ihrer Heimateinrichtung nutzen können. An den Komfort, sich mit nur einer Kennung bei verschiedenen Diensten anmelden zu können, haben sich viele Wissenschaftler bereits gewöhnt.

Ein FID lizenziert jedoch einrichtungsübergreifend für den Bedarf seiner jeweiligen Fachcommunity. Wird ein Wissenschaftler nun Mitglied in einem Fachinformationsdienst, erhält er zusätzlich zu den Berechtigungen für den Zugriff auf lizenzierte Ressourcen von seiner Heimateinrichtung entsprechende Berechtigungen durch den FID. Da die Heimateinrichtung eines Wissenschaftlers i. d. R. keine Kenntnis über dessen Mitgliedschaft in einem FID besitzt, kann diese die zusätzlichen Berechtigungen nicht an ihren Login binden. Dies ist nur am zugehörigen Konto beim FID möglich.

Damit der Wissenschaftler deswegen nicht mit zwei Logins arbeiten muss und somit ein Single Sign-on nicht mehr möglich wäre, wird im KfL-Projekt die etablierte und sichere Shibboleth-Technologie genutzt, um für FID-Angehörige einen Weg anzubieten, wie sie mit dem Login ihrer Heimateinrichtung gleichzeitig auch die Ressourcen der FID nutzen können, für die sie berechtigt sind. Dazu wurde eine Infrastruktur geschaffen, über die Wissenschaftler ihre Berechtigungen seitens eines FID mit denen ihrer Heimateinrichtung verknüpfen können.

Nutzung des Logins der Heimateinrichtung

Wenn ein FID die Nutzerverwaltung, die im KfL-Projekt angeboten wird, verwendet (KfL-Nutzerverwaltung), sind für den FID keine weiteren Schritte notwendig, um Mitgliedern seiner Community die Möglichkeit zu bieten, ihren Login bei ihrer Heimateinrichtung mit ihrem FID-Konto zu verknüpfen. Alle Funktionen sind in die KfL-Nutzerverwaltung integriert.

Für die Verknüpfung wählt der Nutzer bei der Registrierung zunächst aus einer Liste seine Heimateinrichtung aus und meldet sich dort wie beim Shibboleth-Login gewohnt mit seiner lokalen Kennung an. Anschließend wird er auf die Seiten der KfL-Nutzerverwaltung zurückgeschickt, um hier durch die Eingabe seiner persönlichen Registrierungsdaten die Anmeldung am FID abzuschließen. Bei der einmaligen Anmeldung an der Heimateinrichtung während des Registrierungsprozesses wird im Hintergrund eine eindeutige, pseudonyme ID (die sog. *eduPersonUniqueID*) von der Heimateinrichtung an die Nutzerverwaltung des KfL übermittelt und dort gespeichert. Diese ID wird später bei der Nutzung von anderen Services des jeweiligen FID (z. B. Nutzung des FID-Proxys) ebenfalls an diese Services übertragen, die dann wiederum mit dieser ID bei der KfL-Nutzerverwaltung nach Berechtigungen anfragen. Liegen entsprechende Berechtigungen für die jeweilige ID vor, werden sie übermittelt und der Nutzer erhält Zugriff einzig mit der Kennung seiner Heimateinrichtung. Für den FID-Nutzer ist dieses Verfahren nicht sichtbar und läuft ausschließlich im Hintergrund mittels der Kommunikation zwischen den Systemen ab.

Besitzt der FID-Nutzer bereits ein Konto in der KfL-Nutzerverwaltung, kann dieses auch nachträglich verknüpft werden. Nach der Anmeldung findet sich dazu auf der persönlichen Seite des Nutzers unter dem Abschnitt „Weiteres“ die Möglichkeit, die Heimateinrichtung zu wechseln. Wählt er diese Option, wird der Benutzer von der Nutzerverwaltung abgemeldet und gelangt zur Auswahl seiner Heimateinrichtung. Ab diesem Punkt verläuft das Verfahren genau wie bei der Erstregistrierung. Nach Abschluss läuft die Authentifizierung des Nutzers zukünftig über seine tatsächliche Heimateinrichtung und nicht mehr über die virtuelle.

Die genannte ID ist dabei pseudonym, d. h., sie kann von den Diensten nicht direkt einer Person zugeordnet werden. Einzig die jeweilige Heimateinrichtung als ausgebende Stelle der ID könnte eine Zuordnung vornehmen. Ebenfalls ist durch die Eingabe von persönlichen Nutzerdaten im Zuge der Registrierung in der KfL-Nutzerverwaltung eine Zuordnung möglich. Dies muss an dieser Stelle gewährleistet sein, damit der FID die Zugehörigkeit der Person zu seinem Nutzerkreis prüfen und ihm entsprechende Berechtigungen erteilen kann.

Einzige Einschränkung ist bei diesem SSO-Verfahren momentan, dass nicht alle Heimateinrichtungen die benötigte pseudonyme ID liefern können. Zum einen kann dies an den lokalen Begebenheiten beim Identity Management liegen, so dass eine Person dort nicht eindeutig einer ID zuzuordnen ist. Bei anderen Einrichtungen erlaubt es evtl. der zuständige Datenschutzbeauftragte der Heimateinrichtung nicht, eine ID freizugeben, mit der das Nutzungsverhalten einer Person – wenn auch pseudonym – über verschiedene Systeme zusammengeführt werden kann. Um Verwirrung und Nachfragen durch Nutzer zu minimieren, werden in der Auswahlliste nur die Institutionen angezeigt, welche die ID auch liefern können. Die Projektpartner im KfL-Projekt stehen als Kommunikationspartner für alle Heimateinrichtungen zur Verfügung, um evtl. Frage hinsichtlich des Verfahrens zu klären.

Außer der Information, dass zu einer ID eine bestimmte, FID-bezogene Berechtigung besteht, gibt die KfL-Nutzerverwaltung keine weiteren personenbezogenen Informationen bei der Nutzung von FID-Lizenzen über den KfL-Proxy weiter.

Login bei der Nutzung von FID-Lizenzen

Hat ein FID-Nutzer den Login seiner Heimateinrichtung mit seinem FID-Konto verknüpft, kann er FID-Lizenzen, für die er berechtigt ist, direkt mit dem Login seiner Heimateinrichtung nutzen. Dazu wählt er wie gewohnt beim Shibboleth-Login seine Heimateinrichtung aus der Liste und meldet sich dann dort an. Hat er sich bereits vorher via Shibboleth bei seiner Heimateinrichtung authentifiziert, ist die Nutzung der FID-Lizenzen sogar nahtlos ohne weitere Anmeldung parallel zur Nutzung der Ressourcen seiner Heimateinrichtung möglich. Dies stellt einen hohen Komfortgewinn für die FID-Nutzer dar und integriert die FID-Lizenzen noch besser in ihre Arbeitsumgebung.

Ausbau des Verfahrens

Im aktuellen Stand funktioniert das Verfahren bei der Nutzung von FID-Lizenzen über den im Rahmen des KfL-Projekts betriebenen FID-Proxy. Die Projektpartner im KfL-Projekt sind jedoch bestrebt, die Proxy-Infrastruktur weitestgehend obsolet zu machen und die Möglichkeit zu schaffen, dass FID-Lizenzen direkt bei Verlagen genutzt werden können, die von sich aus bereits eine Shibboleth-Authentifizierung anbieten. Dazu sind jedoch bei den Verlagen gewisse technische Voraussetzungen zu schaffen.

Deswegen erfolgte im KfL-Projekt die Aufgabensetzung, alle für die Etablierung der Single Sign-on-(SSO)-Authentifizierung mit Shibboleth-Technologie im Rahmen des FID-Systems erforderlichen kommunikativen und organisatorischen Voraussetzungen im Dialog mit den FID und den Anbietern zu initiieren und zu koordinieren. Dabei soll ggf. auch auf neue technische Entwicklungen in diesem Bereich reagiert werden, um diese bei Bedarf den FID über die technischen Infrastrukturen, die im Rahmen des KfL-Projekts angeboten werden, zur Verfügung zu stellen.

Die Serviceteams der KfL-Partnerbibliotheken beraten die FID jederzeit gerne in allen organisatorischen und technischen Fragen der Single Sign-on-Authentifizierung via Shibboleth-Technologie.

Gerrit Gragert, Staatsbibliothek zu Berlin