CASE STUDY

GÉANT ist ein Zusammenschluss europäischer nationaler Forschungs- und Bildungsnetzwerke (NRENs) und ein zentraler Teil der gesamteuropäischen Forschungsgemeinschaft. Dabei stehen GÉANT und dessen Dienste für wissenschaftliche Exzellenz, Forschung, Bildung und Innovation. GÉANT vernetzt über 10.000 akademische Institutionen und mehr als 50 Mio. Benutzer*innen miteinander und ist damit das größter R&E-Netzwerk der Welt.

ORGANISATION
GÉANT Association

BRANCHE
Forschung und Bildung

WEB
www.geant.org

DAS PROJEKT

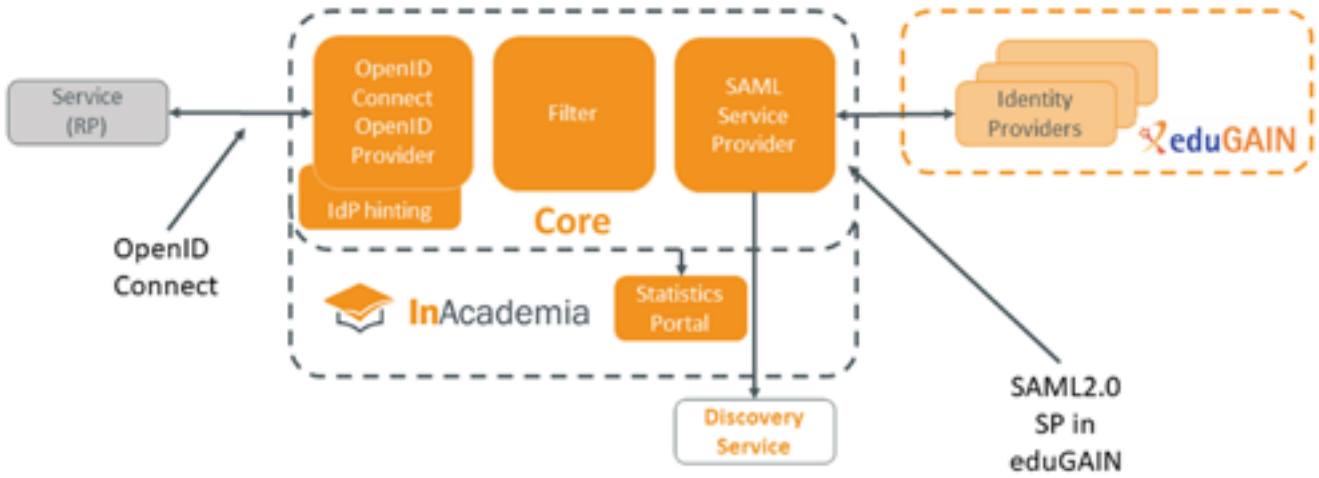
Mit InAcademia bietet GÉANT eine Lösung für gewerbliche und private Dienstleister an, die darauf spezialisiert sind, akademischen Nutzer*innen Leistungen und Rabatte und anzubieten. InAcademia kann in die Webpräsenz der Dienstleister integriert werden, so können die Nutzer*innen ihre Anspruchsberechtigung für bestimmte Angebote nachweisen. Damit entfällt für die Dienstleister die Notwendigkeit, große Mengen personenbezogener Daten zu erfassen und zu verarbeiten oder sich mit der Komplexität von föderierter Identitätsverwaltung im akademischen Umfeld befassen zu müssen.

InAcademia nutzt die durch SAML-Identity-Provider, wie der Shibboleth IdP, bereitgestellten Informationen der Heimatorganisation, um den Studierendenstatus zu validieren. Alle Informationen werden in Echtzeit überprüft und die Daten durch die etablierte Infrastruktur edu-GAIN gesichert.

InAcademia basiert auf den Standards SAML und OpenID Connect (OIDC) und hat als Kern einen SATOSA-Proxy. Der Dienst wird ständig erweitert.

Auf technischer Ebene „spricht" InAcademia OIDC in Richtung der Relying Partys (RPs, Dienste, die die Verifizierung anfordern) und SAML in Richtung der Identity Provider (IdPs, Herkunfts-Institutionen, hier Universitäten) die an eduGAIN teilnehmen. Aus diesem Grund wird SATOSA als Proxy zwischen den beiden Standards eingesetzt.

SATOSA lagert die Authentifizierung an den IdP der Herkunftsinstitution aus. Eine zusätzliche Ebene über SATOSA vergleicht die vom IdP erhaltene Zugehörigkeit mit der vom RP angeforderten und gibt eine pseudonymisierte Antwort an den Dienst zurück, die bestätigt, ob die Nutzerin einer Institution angehört. Alle überflüssigen Daten werden dabei verworfen. Die DAASI International hat eine Reihe von Microservices programmiert, etwa für die Fehlerbehandlung, die Protokollierung und die Zustimmung, und spielte eine Schlüsselrolle bei der kontinuierlichen Verbesserung des Dienstes.



BEITRAG

Zwischen 2020 und Ende 2022 wurde DAASI International beauftragt, an der kontinuierlichen Verbesserung des Codes zu arbeiten und zum OIDC-Frontend und anderen Microservices beizutragen, wie die Implementierung der Unterstützung für den OIDC-Genehmigungs-Codeflow und die Gewährleistung einer optimalen Anpassung an die Fehlerbehandlung und Fehlerprotokollierung des Codes. Die verbesserte Protokollierung wird etwa zur Analyse von Nutzerströmen und zur Identifizierung inkompatibler IdPs verwendet, was wiederum zu einer Verbesserung der Erfolgsquote bei der Validierung von Studierenden durch InAcademia geführt hat. So konnten schließlich erhebliche Fortschritte an der Codebasis erzielt werden, ganz ohne Nutzungsbeeinträchtigung für Bestandskunden.