

Wie kann ich meine Web-Anwendung an das WebSSO anschließen?

08.09.2024 02:01:22

FAQ-Artikel-Ausdruck

Kategorie:	RRZE: SSO	Bewertungen:	0
Status:	öffentlich (Alle)	Ergebnis:	0.00 %
Sprache:	de	Letzte Aktualisierung:	10:12:00 - 24.07.2023

Schlüsselwörter

WebSSO, Shibboleth, SAML

Symptom (öffentlich)

Problem (öffentlich)

Wie können sich die Anwender meiner Web-Anwendung mittels WebSSO authentifizieren?

Was muss ich tun, um diesen Dienst nutzen zu können?

Lösung (öffentlich)

Generell kann jede Webanwendung an das WebSSO angeschlossen werden. Dabei kommuniziert diese nicht direkt mit dem zentralen Identity Provider (IdP), sondern mit einem lokal installierten Service-Provider (SP).

Wir unterstützen im Moment zwei Implementierungen von SPn unter Linux:

- Shibboleth ["http://shibboleth.internet2.edu/"] von Internet2 und
- simpleSAMLphp ["http://rnd.feide.no/simplesamlphp/"] von Feide RnD

Der Shibboleth-SP kommt als Daemon inkl. Apache-Module. Diese Variante kann von allen Webanwendungen, welche den Apache-Webserver einsetzen, verwendet werden.

Der SP von simpleSAMLphp kommt als PHP-Anwendung. Einzige Voraussetzung ist somit ein PHP-fähiger Webserver, wobei wir Unterstützung für den Apache-Webserver anbieten können. Diese Variante kann allerdings nur von PHP-Webanwendungen genutzt werden, da die Nutzung nur über eine PHP-API möglich ist.

Beide Implementierung müssen nach erfolgreicher Installation entsprechend konfiguriert werden. Danach muss der neue SP beim zentralen IdP registriert werden. In dieser Phase müssen auch die zu übergebenden Attribute definiert werden.

Außerdem muss es sich bei dem WebSSO um ein datenschutzrechtlich genehmigtes Verfahren handeln. Um dies nachzuweisen, reichen Sie uns bitte eine Kopie der Genehmigung des Datenschutzbeauftragten ["https://www.fau.de/universitaet/leitung-und-struktur/gremien-und-beauftragte/beauftragte/datenschutzbeauftragter/"] sowie die Anlage 1 zur Verfahrensbeschreibung ein.

In der Zwischenzeit wird unser Team mit Ihnen die Systemanbindung realisieren und testen.

Sie können Ihr Interesse per E-Mail an sso-support@fau.de ["mailto:sso-support@fau.de"] bekunden.

Dabei benötigen wir folgende Daten:

- Name + Telefon + E-Mail-Adresse Ansprechpartner (=Administrator)
- Name des Systems:
- Die technischen Attribute des Systems (metadata URL, AssertionConsumerService URL, SingleLogoutService URL).
- Die Attribute, die Sie benötigen. Inwieweit diese Sinn machen, wäre dann noch in einem Beratungstelefonat zu klären.

Danach erhalten Sie alle weiteren Informationen.