Was macht überhaupt WebSSO?

14.05.2024 19:30:44

FAQ-Artikel-Ausdruck

Kategorie:	RRZE: SSO	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	17:28:08 - 27.08.2009

Schlüsselwörter

SSO, Single-Sign-On, Web-SSO, WebSSO, Shibboleth, SAML

Symptom (öffentlich)

Problem (öffentlich)

Was ist eigentlich dieses Web Single Sign-On/WebSSO?

Was kann ich damit machen? Was bringt/hilft es mir?

Lösung (öffentlich)

Das Web Single Sign-On (kurz: WebSSO) ermöglicht eine zentrale Authentifizierung und Autorisierung von web-basierten Ressourcen. Das System besteht im Wesentlichen aus zwei miteinander kommunizierenden Modulen:

- dem Identity Provider (IdP) und
- dem Service Provider (SP).

Der IdP ist für die Authentifizierung und die Bereitstellung von Attributen verantwortlich. Um diese Aufgabe erfüllen zu können, ist er an die vorhandene Benutzerverwaltung, dem Identity Management (IdM) System, angeschlossen. Im vorliegenden Fall erfolgt dies über die Provisionierung eines LDAP-Servers, welcher als Authentifizierungs- und Attributquelle für den IdP dient. Dieser LDAP-Server enthält die von den SP benötigten Attribute.
Ein am IdP authentifizierter Benutzer, kann die Ressourcen aller angeschlossenen SPs nutzen, ohne sich erneut authentifizieren zu müssen. Vom IdP gibt es nur eine zentrale Instanz, diese ist unter www.sso.uni-erlangen.de ["https://www.sso.uni-erlangen.de/"] zu erreichen.

Die vom IdP weitergegebenen Attribute, werden für jeden SP einzeln festgelegt. Vorbedingung für eine Anbindung ist, das eine aktuelle und freigegebene Verfahrensbeschreibung vorliegt. Die Anbindung der SPs erfolgt unter Beachtung des Gebots der Datensparsamkeit. Der Zugriff auf den zentralen IdP von außen ist nur über den verschlüsselten HTTPS-Port erreichbar. Dieser dient zur Kommunikation mit den Benutzern, wie z.B. bei der Authentifizierung.

Der SP ist für die ihm zugeordneten Ressourcen (web-Anwendung) verantwortlich. Für jeden Server auf dem eine Webanwendung das WebSSO nutzen soll, muss also ein SP installiert sein. Die Entscheidung über einen erfolgreichen Zugriff, trifft der SP aufgrund der Aussagen des IdP. D.h. anhand der vom IdP erhaltenen Attribute, entscheidet der SP, auf welche Ressourcen der Benutzer zugreifen kann. Einem authentifizierten Benutzer kann natürlich auch der komplette Zugriff, aufgrund fehlender Attribute, verwehrt werden.