

Shibboleth Authentifizierung

Single Sign On
für Web Anwendungen
der Humboldt-Universität zu Berlin



Gliederung

- Hintergründe von Shibboleth
- Shibboleth – im Internet
- Funktionsweise Shibboleth
- Umsetzungsschritte
- Ausblick

Hintergründe von Shibboleth

- Das Wort 'Shibboleth'
 - Hebräisch ursprüngl. 'Getreideähre', jetzt aber Bedeutung Codewort
 - Altes Testament:

Gileaditer überführen Ephraimiten bei dem Versuch, unbefugt den Jordan zu überqueren durch das Codewort 'Shibboleth'.
 - Weitere Beispiele für Shibboleth's:
 - Für Ausländer: Eichhörnchen, Streichholzschächtelchen
 - Für Preußen: Oachkatzlschwoaf

Shibboleth – im Internet

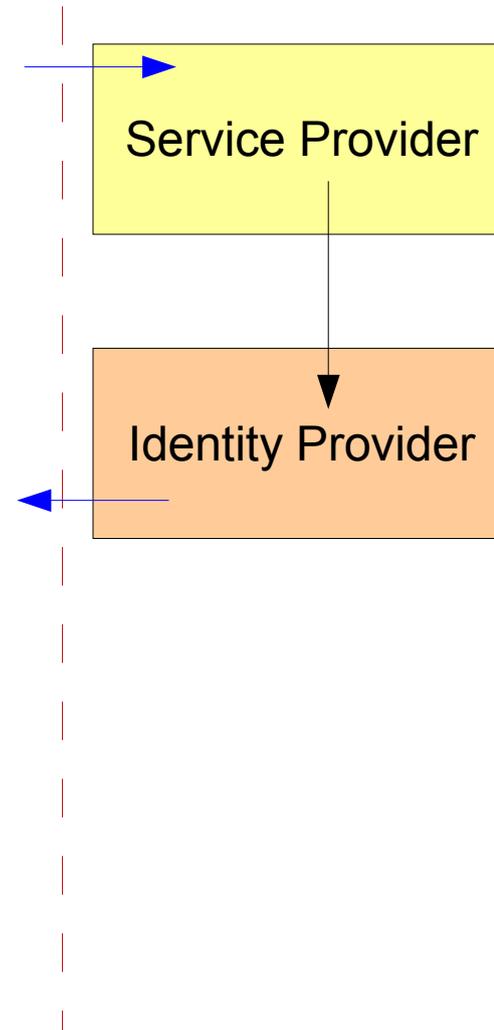
- **Single Sign On (SSO)** Verfahren für Web Anwendungen
 - Pro Sitzung (Arbeitstag) nur einmalige Authentifizierung des Nutzers
 - Alle unterstützten Web Anwendungen benutzen die selbe Authentifizierung
 - Die Authentifizierung ist zentral
 - Systempflege beschränkt sich auf ein System

Shibboleth – im Internet

- Funktionen von Shibboleth:
 - Authentifizierung
 - Besonderheit:
Gefilterte Übertragung von Attributen (Informationen über den Nutzer)
 - Bilden von Föderationen

Funktionsweise von Shibboleth

1. Nutzeranfrage über den Browser



Funktionsweise von Shibboleth

2. Eingabe von Nutzernamen und Passwort



Login - Humboldt-Universität zu Berlin

Humboldt-Universität zu Berlin

Attribute für Service: <http://shib2.cms.hu-berlin.de/shibboleth>

User: **usereins**

postalAddress	X Strasse 100, 10100 Test
uid	usereins
eduPersonEntitlement	urn:mace:dir:entitlement:hu-berlin:all
commonName	User Eins
eduPersonPrincipalName	usereins
postalCode	10100
eduPersonScopedAffiliation	staff

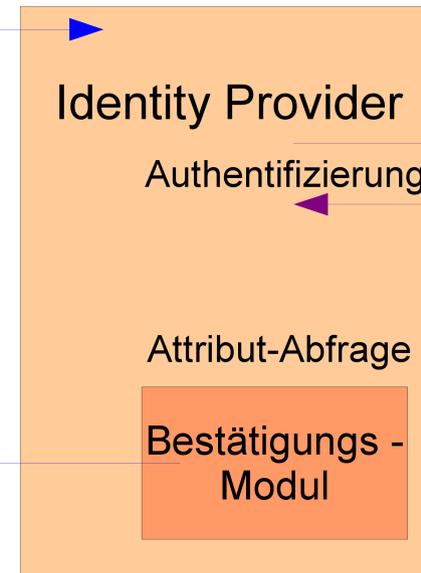
Diese Seite nicht mehr anzeigen. Ich bin mit der Übertragung der Attribute jetzt und in Zukunft einverstanden.*

*Je nach gefordertem Service können verschiedene Attribute übertragen werden. Die hier angezeigten Attribute beziehen sich auf den **aktuell** angeforderten Service.

Shibboleth.

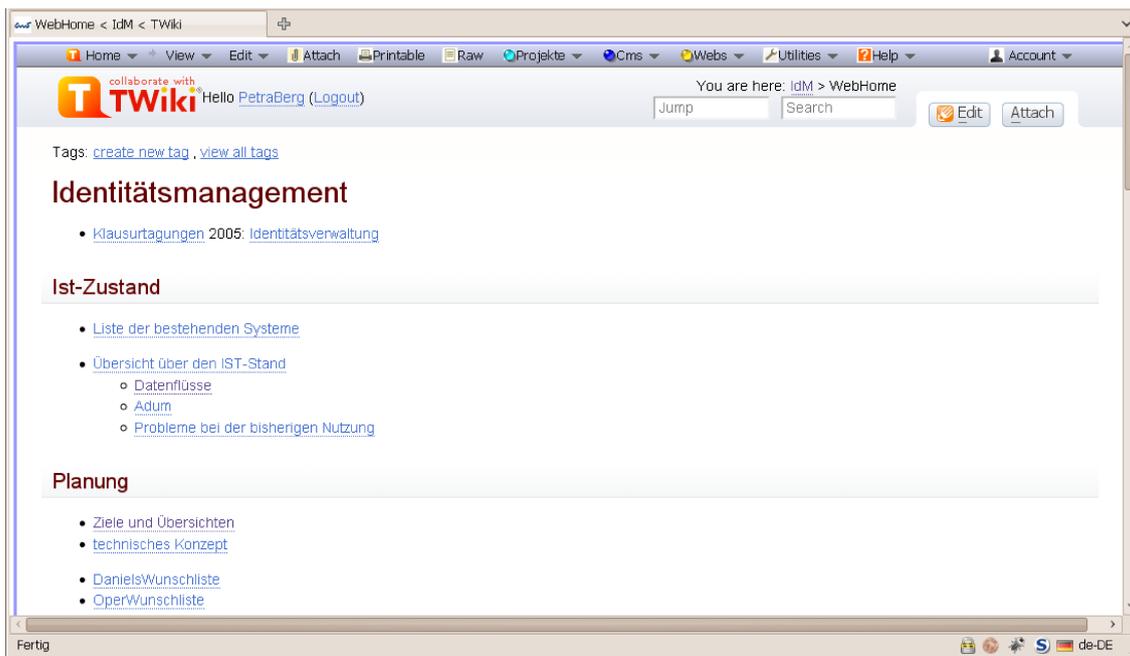
© 2010, CMS

Fertig



Funktionsweise von Shibboleth

3. Bestätigung der Attribute



Identity Provider

Erstellen der Antwort
mit Attributen

Service Provider

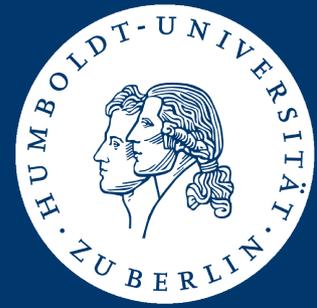
4. Autorisierter Web-Dienst

Umsetzungsschritte

- Nach Zustimmung von Datenschutz und Gesamtpersonalrat:
Produktivstellung des Shibboleth Identity Providers
- Schrittweises Anbinden der Web-Dienste der Humboldt-Universität
 - Sicherheitskonzept
 - Einholen der Zustimmung des Datenschutzbeauftragten
 - Mitbestimmung der zuständigen Personalräte
 - Produktivstellung des entsprechenden Web-Dienstes mit Shibboleth Authentifizierung
- **Ziel:** Schrittweise Ablösung des derzeitigen SSO-Systems (CAS) durch Shibboleth

Weiterführende Schritte

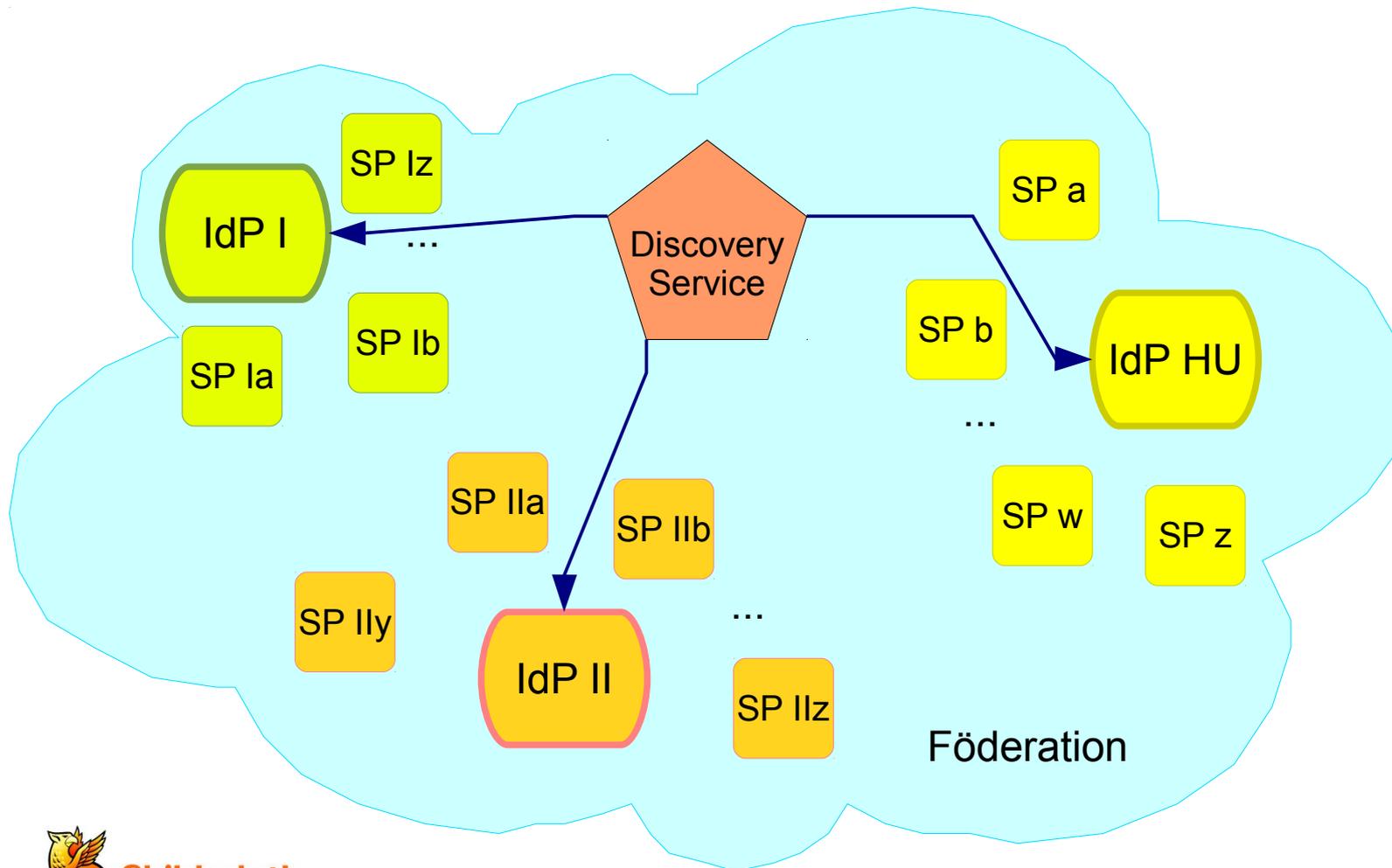
- Einbinden externer Web-Dienste
 - Prüfen von Föderationsverträgen
 - Einholen der Zustimmung des Datenschutzbeauftragten
 - Mitbestimmung der zuständigen Personalräte
 - Beitritt zur Föderation (Berliner Universitäten, DFN)
 - Gesonderte Verträge mit Diensteanbietern der entsprechenden Föderation (Vertragsprüfung Datenschutz, Personalräte)
 - Statt Einzelprüfung auch Abschluss einer Dienstvereinbarung möglich



Vielen Dank für Ihre Aufmerksamkeit

Shibboleth Föderation

- Mehrere Provider



Funktion im Detail

