Shibboleth Authentifizierung

Single **S**ign **O**n
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 Ephraimiter 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.

Shibboleth – im Internet

- **S**ingle **S**ign **O**n (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

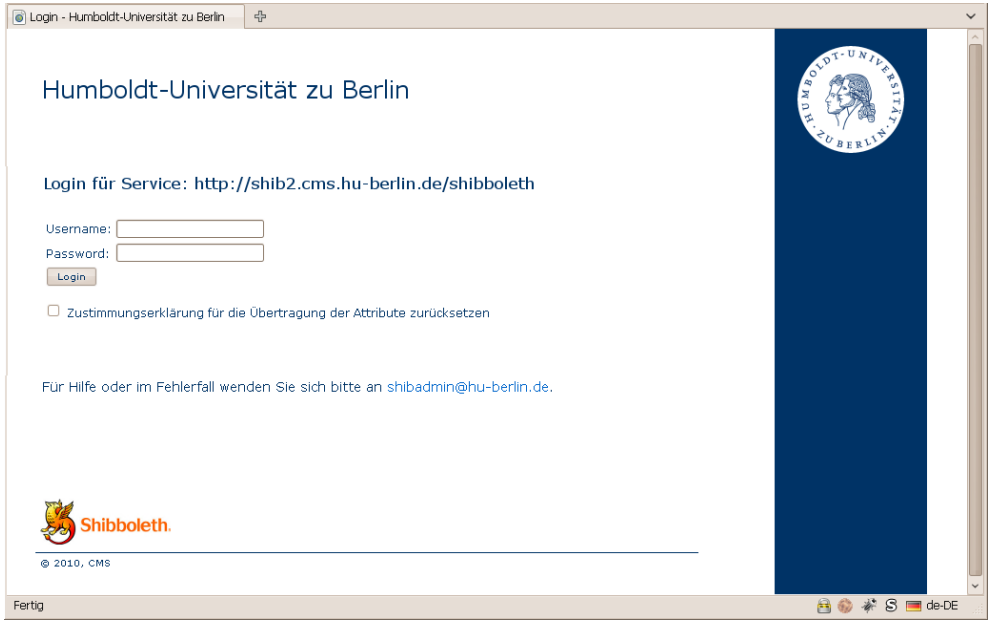
Shibboleth.

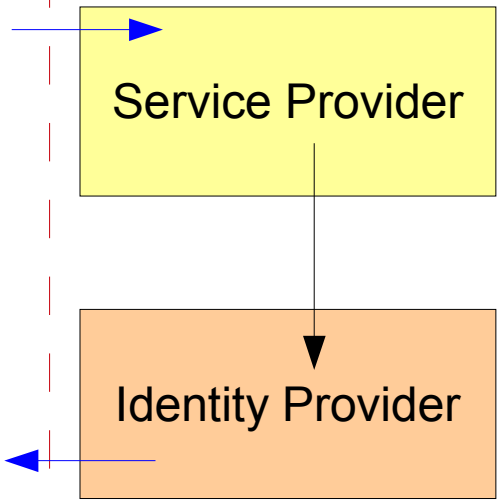
Shibboleth – im Internet

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

Funktionsweise von Shibboleth

1. Nutzeranfrage über den Browser

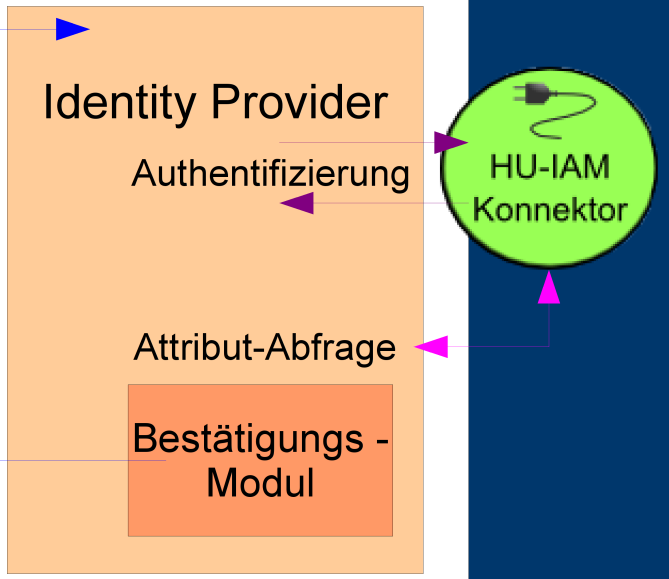




Shibboleth

Funktionsweise von Shibboleth

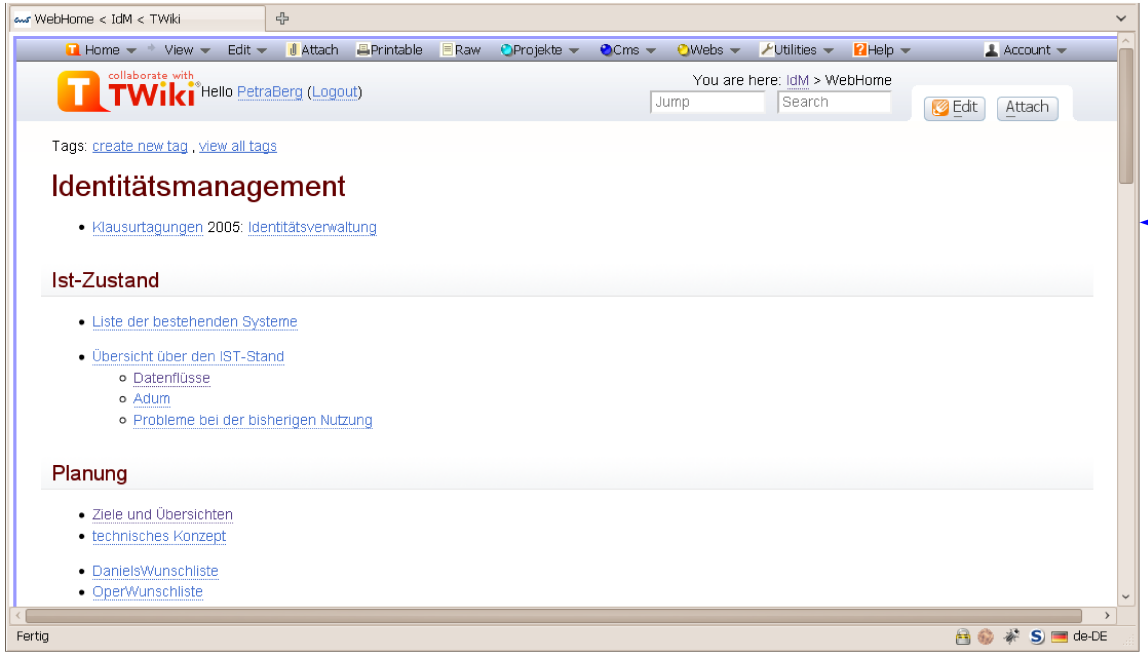
2. Eingabe von Nutzername und Passwort



Shibboleth.

Funktionsweise von Shibboleth

3. Bestätigung der Attribute



Identity Provider

Erstellen der Antwort mit Attributen

Service Provider

4. Autorisierter Web-Dienst

Shibboleth.

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

Shibboleth.

Weiterführende Schritte

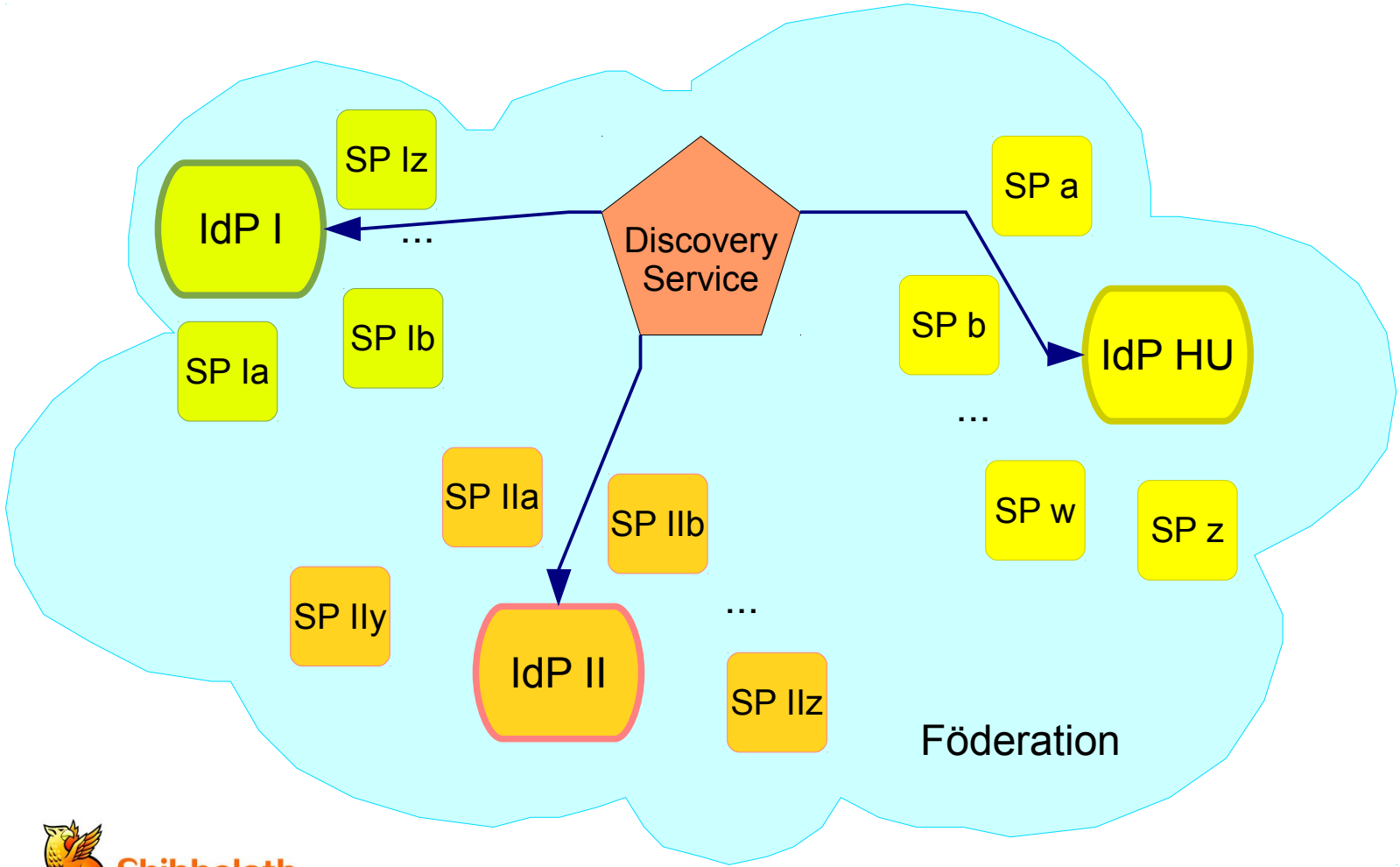
- Einbinden externer Web-Dienste
  - Prüfen von Föderationsverträgen
  - Einholen der Zustimmung des Datenschutzbeauftragten
  - Mitbestimmung der zuständigen Personalräte
  - Beitritt zur Föderation (Berliner Universitäten, DFN)
  - Gesonderte Verträge mit Dienstanbietern der entsprechenden Föderation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

Shibboleth.

Vielen Dank für Ihre Aufmerksamkeit

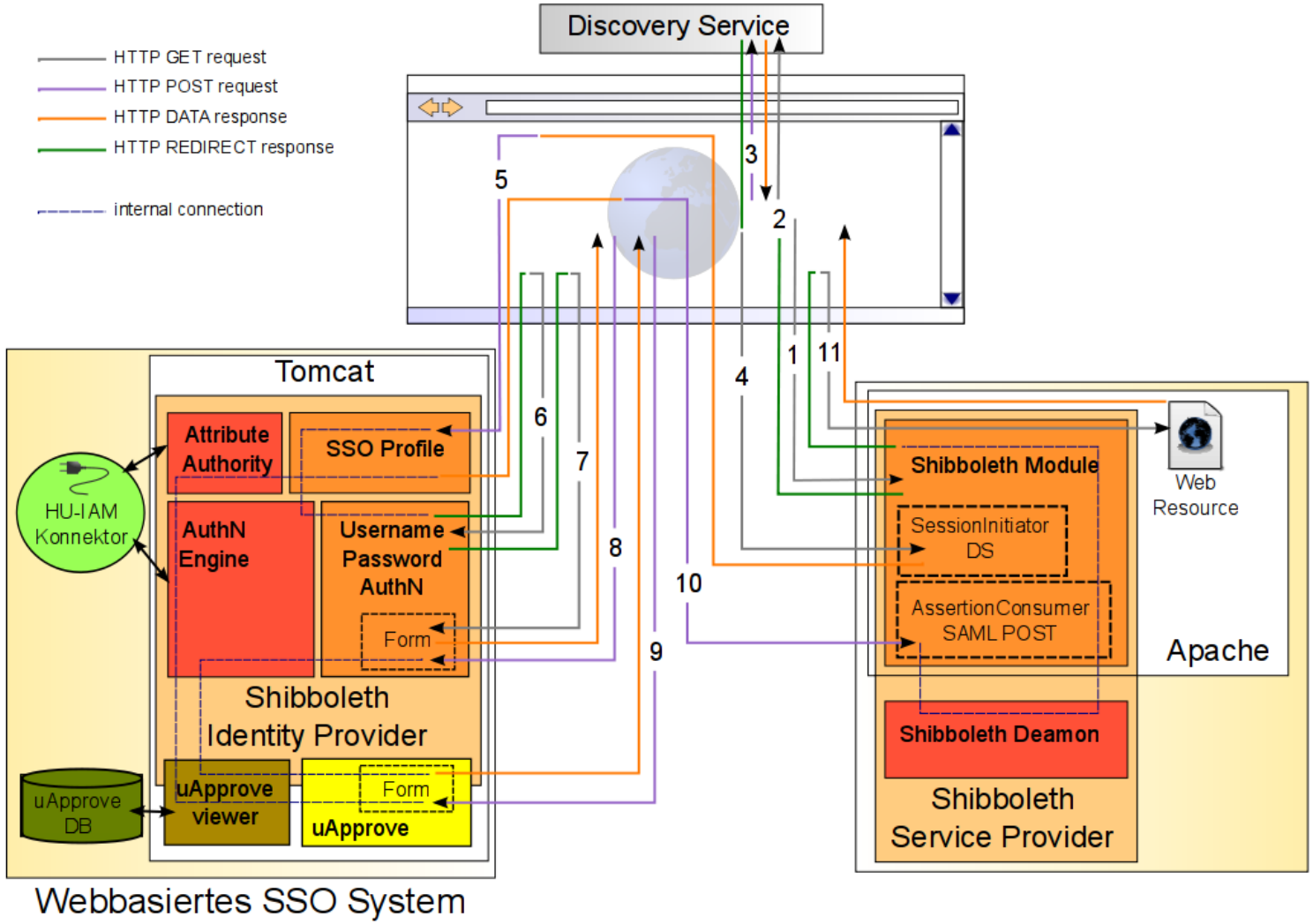
Shibboleth Föderation

- Mehrere Provider



Shibboleth.

Funktion im Detail



Shibboleth.