
Shibboleth

Peter Steiner, in: New Yorker, Vol.69 (LXIX), No. 20, July 5, 1993, S. 61

Shibboleth: Überblick

- Shibboleth: Wozu?
- Was ist das?
- Wie funktioniert das?
- Was nützt das?
- Föderationen
- Anwendungsbeispiel: Nationallizenzen

Shibboleth: Wozu?

Es gibt Bedarf für Authentifizierung und Autorisierung über Einrichtungsgrenzen hinweg

Beispiele:

- Geldautomat bei fremder Bank
- Mobiltelefon im Ausland
- Benutzung des WLANs an fremder Uni
- Recherche in lizensiertem Angebot eines kommerziellen Anbieters

Shibboleth: Was ist das?

- Einrichtungsübergreifender SSO-Dienst
- „nur“ für Webdienste (HTTP mit Webbrowser)
- Setzt funktionierendes Identity Management vorraus (ist kein „IdM-System“!, aber eine tolle Erweiterung dafür)
- Open Source (Apache Software License 2.0)
- Middleware (es gibt nichts zu sehen)
- basiert auf SAML
- Entwickelt vom Internet2 Konsortium

Shibboleth

Altes Testament,Buch Richter, Kapitel 12, Vers 5ff: “Und die Gileaditer nahmen ein die Furt des Jordans vor Ephraim. Wenn nun sprachen die Flüchtigen Ephraims: Laß mich hinübergehen, so sprachen die Männer von Gilead zu ihm: Bist du ein Ephraiter? Wenn er dann antwortete: Nein, so hießen sie ihn sprechen: Schiboleth, so sprach er: Siboleth, und konnte es nicht recht reden. So griffen sie ihn und schlugen ihn an der Furt des Jordans, daß zu der Zeit von Ephraim fielen zweiundvierzigtausend.“

Szenario: Verteilte Authentifizierung und Autorisierung

Benutzerverwaltung:
Identity Provider (IdP)

Authentifizierung

Diensteanbieter:
Service Provider (SP)

Autorisierung

Informationsfluss mit Shibboleth

Benutzer

(1)

(3)

Lokalisierungsdienst

(2)

Benutzer bekannt?

nein

ja

(5)

(4)

(6)

Benutzer berechtigt?

Heimateinrichtung

(7)

(8)

(9)

ja

gestattet

nein

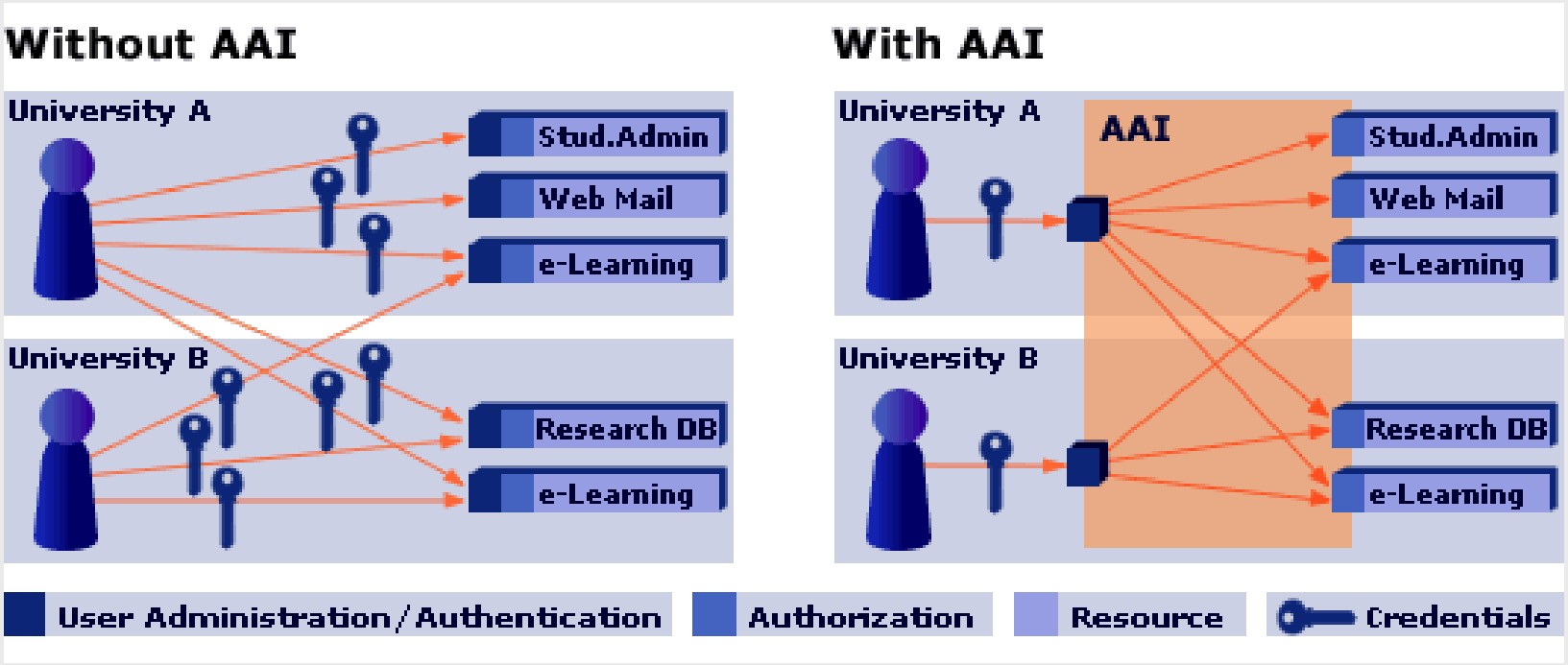
verweigert

Zugriff

Anbieter

Folie: verändert nach Ato Rupper, UB Freiburg, 2006

Shibboleth: Vorteile



Quelle: http://www.switch.ch/aai/about/

Vorteile für Nutzer

- nur noch eine digitale Identität
- SSO
- Zugriff unabhängig vom Aufenthaltsort/IP-Adressen
- Transparenz (wo sind meine Daten?)
- Benutzer kann ggf. selbst bestimmen, welche Daten weitergegeben werden („Visitenkartenmodell“)

Vorteile für „Einrichtungen“/IdP (z.B. Bibliothek oder Uni)

- Einfache Integration in bestehendes Identity Management
- Kein zusätzlicher Aufwand beim Anbieten neuer Dienste (Pflege von IP-Adressen, Verwaltung von Zugangsdaten, Einrichten von Benutzeraccounts...)
- Bessere Angebote für Nutzer: ortsunabhängige Dienste, Datenschutz...

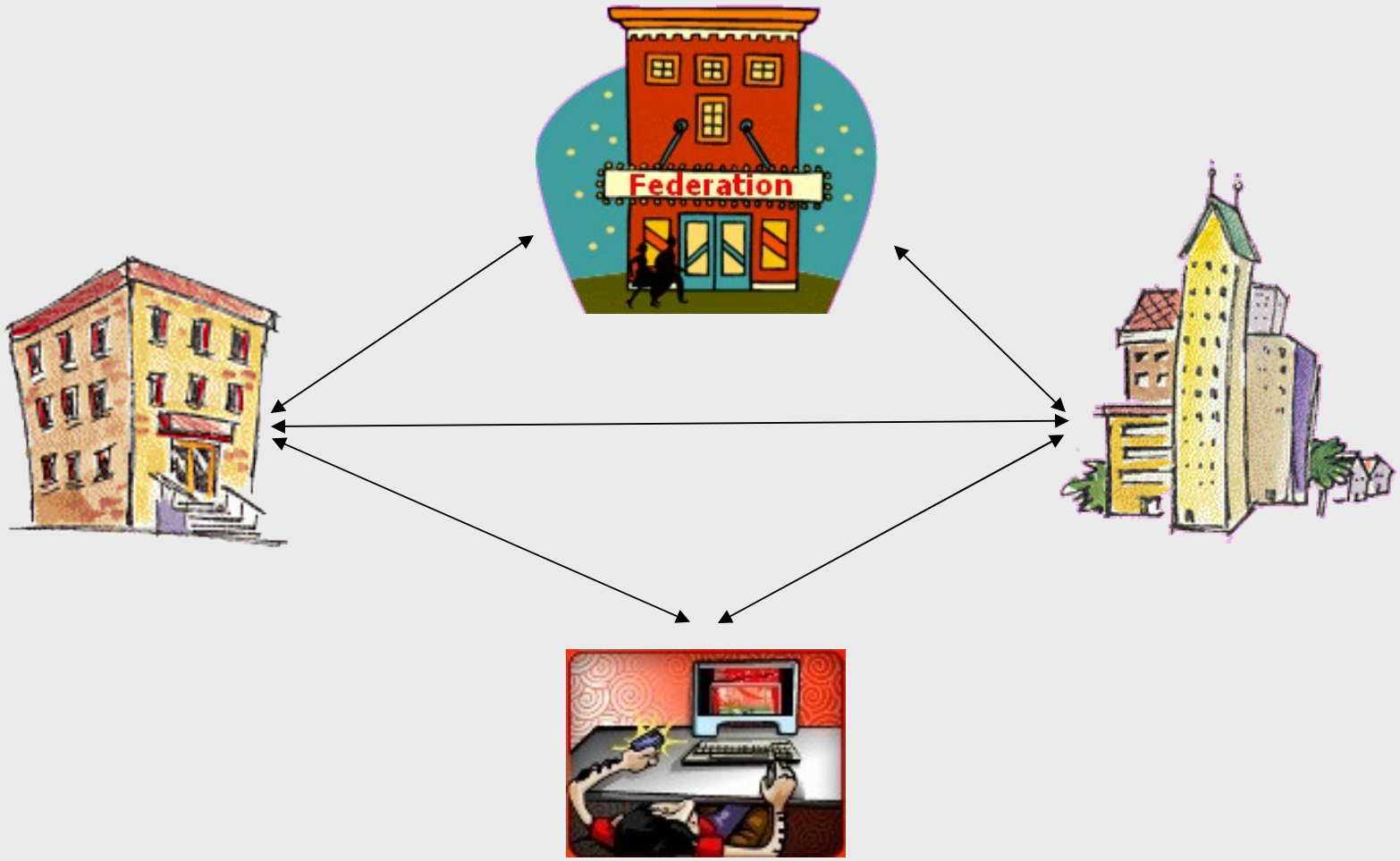
Vorteile für Dienstanbieter/SP

- Keine Verwaltung von Zugangs- und Benutzerdaten mehr
- Kontrolle der Nutzungsbefugnis (Autorisierung) anhand definierter Merkmale

Grundlagen für den Einsatz von Shibboleth

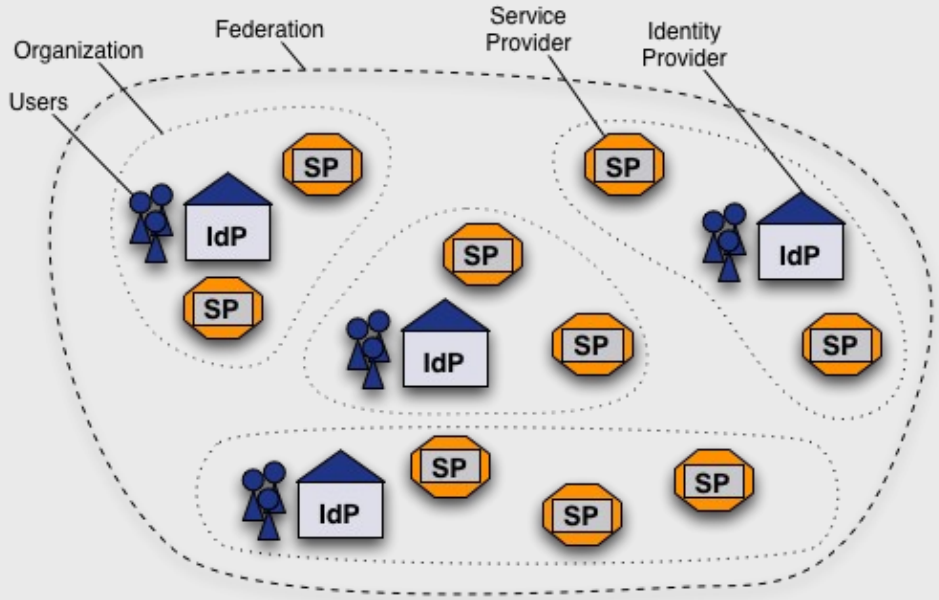
- Vertrauen
- Verträge
- Verschlüsselung

Beziehungsgeflecht



Föderationen

vertraglicher, organisatorischer und technischer Rahmen für verteiltes Identity Management mit Shibboleth



Quelle Grafik: http://www.switch.ch/aai/about/federation/

Föderationen

- Zusammenschluss von Identity Providern und Service Providern auf Grundlage von Vereinbarungen
- Durch vertragliche Fixierung der Vereinbarungen wird Vertrauen rechtlich abgesichert

Aufgaben einer Föderation

- Festlegung organisatorischer Rahmenbedingungen
- Festlegung technischer Rahmenbedingungen
- Überprüfung der Einhaltung der Bedingungen zur Teilnahme
- ggf. Betrieb eines WAYF-Dienstes

Anwendungsbeispiel: Nationallizenzen

Szenario:

- Viele Angebote von unterschiedlichen Anbietern
- Nutzer aus vielen unterschiedlichen Einrichtungen
- Nutzer, die keiner Einrichtung angehören (sogenannte Einzelnutzer)

Anwendungsbeispiel: Nationallizenzen

- Verbundzentrale betreibt Registrierungssystem für Institutionen
- Zugriffsberechtigte Einrichtungen registrieren IP-Adressen, Angehörige dieser Einrichtungen können aus diesen IP-Bereichen auf Angebote zugreifen
- Problem Einzelnutzer: keine festen IP-Adressen
- Adhoc-Lösung: Zugriff über verschiedene Proxies bei Verhandlungsführern, mehrmalige Registrierung, mehrere Logins, Intransparenz...

Anwendungsbeispiel: Nationallizenzen

Lösung:

- Registrierung der Einzelnutzer einmalig über System der VZG
- Benutzerdaten bilden eine Virtual Home Organization (VHO)
- VHO als Identity Provider für Shibboleth
- Übergangslösung: EZproxy zum Zugriff auf lizensierte Angebote bei der VZG als Shibboleth Service Provider (solange Angebote nicht Shibboleth-tauglich)