Dezentrale Authentifizierung für Web-Anwendungen mit SAML und OpenID

Sebastian Rieger
sebastian.rieger@gwdg.de

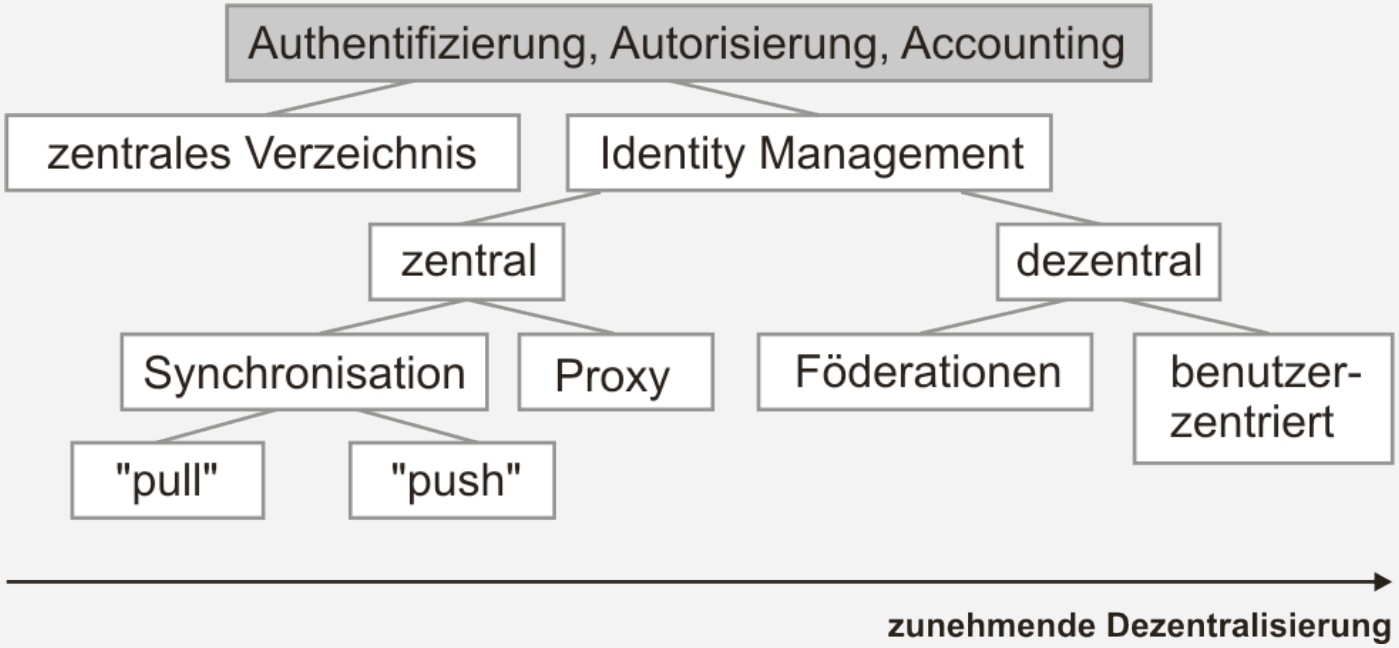
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen, Germany

25. DV-Treffen der MPG - 18.-20.11.2008, Göttingen

Evolution des Identity Managements (IDM)…

- **Ziel: Verminderung des Aufwands bei Authentifizierung, Autorisierung, Accounting**
  - einheitliche Authentifizierung, single password / username → Single Sign-On (SSO)
- **Früher zentrale Lösungen (NIS, Verzeichnisdienste, …) → "Silos", "Inseln"**
  - eingeschränkte Skalierbarkeit (für Externe, Kooperationen, ...), Problem Datenschutz
- **zunehmend dezentral (vgl. Kerberos, PKI, "federated identity", "user-centric"…)**
  - Fokus liegt derzeit auf Web-Anwendungen (Shibboleth bzw. SAML, OpenID, …)
- **Aktuelle Entwicklung: Föderationen (vgl. DFN-AAI, MPG-AAI, ...)**
  - Verbindung des IDM verschiedener Standorte (standortübergreifendes IDM)
  - Vertrauensstellung technisch: Zertifikate, juristisch: Policy

Dezentralisierung des Identity Managements

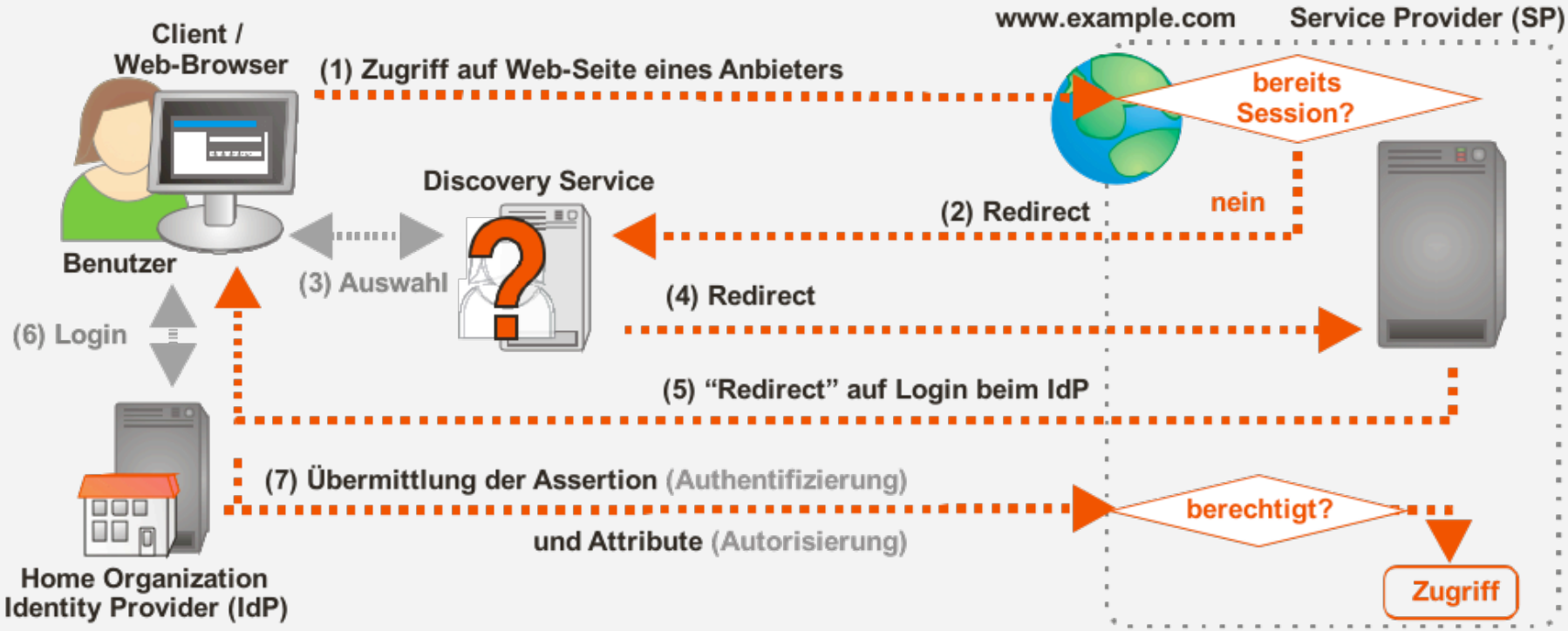


- zentrale Verzeichnisse z.B.: NIS, LDAP, Passport, …
- Synchronisation: Skript-basiert, Meta-Directory; Proxy: RADIUS, Virtual Directory, CAS…
- Föderationen: (Kerberos - Trusts), SAML: Shibboleth, simpleSAMLphp, ADFS, Liberty, …
- benutzerzentriert: OpenID, CardSpace, OAuth, sxip, higgins, …

Föderative Authentifizierung… mit SAML!

- **Trennung in Service Provider (SP) und Identity Provider (IdP)**
- **Single Sign-On über SPs (innerhalb der Föderation)**
  - Vertrauen über Token / Assertion (Cookie) der Heimatorganisation (bzw. IdP)
- **Für Autorisierung: föderationsweit standardisierte Attribute**
  - z.B. eduPerson: eduPersonEntitlement (z.B. common-lib-terms) mittels URN
- **Vertrauen innerhalb der Föderation durch Zertifikate, Policy (metadata)**
  - Beispiel: MPG-AAI, DFN-AAI verwenden Zertifikate der DFN-PKI
- **Basis: Security Assertion Markup Language (SAML)**
  - SA
    M
    L 2.0, Organization for the Advancement of Structured Information Standards (OASIS)
- **Implementierungen: Shibboleth, simpleSAMLphp, ADFS, Liberty, …**

Beispiel für SAML: Shibboleth2.0



- "Single Sign-On" an SP und IdP mittels HTTP: Sessions, Redirects, Cookies…
- Discovery Service (vorher: Where are you from? WAYF Server), passive Auswahl durch SP möglich
- Attribute für Autorisierung können gefiltert werden, Benutzer kann Verwendung verweigern

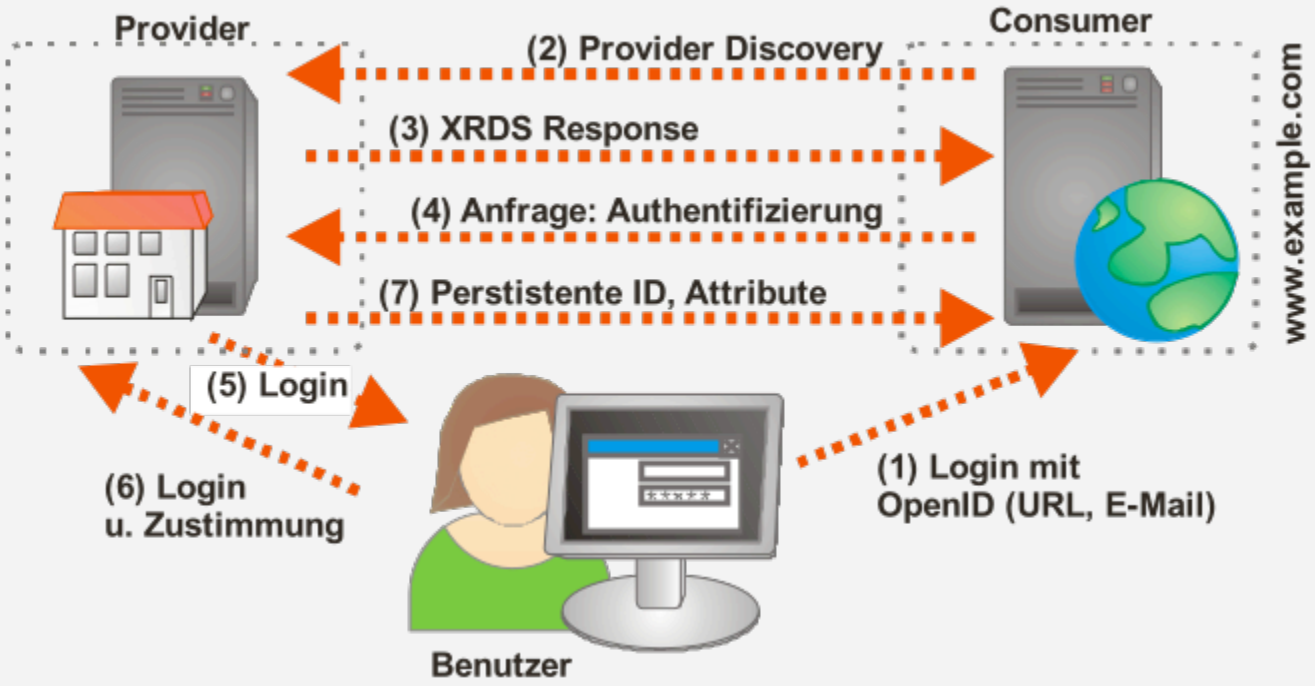
Probleme bei föderativer Authentifizierung

- **Integration in mehreren Föderationen**
  - Lösungsansatz: IdP in mehreren Föderationen / eduGAIN (Konföderation)
- **Usability**
  - Komplexität in Bezug auf Verwendung und Verwaltung (Benutzer, Betreiber)
  - auf Web-Anwendungen beschränkt (Entwicklung: GridShib, Desktop, …)
  - “Single Logout” ist schwierig realisierbar
- **Datenschutz (Attribute verlassen Heimatorganisation…)**
  - Lösungsansatz: Attribute Relea s e Policy (ARP), Zustimmung des Benutzers (ArpViewer der SWITCHaai, …)
  - Herausforderung für Accounting: Pseudonymisierung (durch persistente ID

Benutzerzentriertes IDM mit OpenID

- **Nächste Evolutionsstufe des IDM ("user-centric","Identity 2.0", …)**
  - Usability, ubiquitäre Nutzung, Vereinfachung, Datenschutz auf Nutzerseite
- **Selbstbestimmung, -verwaltung der Identitäten durch Benutzer**
  - Identity Selector: ideale Lösung für Integration mehrerer Föderationen (z.B. Auswahl einer "Karte" durch Benutzer) → I-Ca
    r
    ds: Managed (IdP), Personal (Self-Signed), Relationship (Social Networking)
  - bei OpenID: Login mittels **URL (http://mein-name.myopenid.com, http://muster.xyz.mpg.de), neuer Trend: E-Mail Adresse (z.B. bei Google)**
- **Implementierungen:** OpenID, CardSpace, sxip, OAuth, higgins, Bandit, Ping…
- **Große Player steigen als Provider und Consumer in den Markt ein:**
  OpenID (Provider): Google, IBM, Microsoft, VeriSign, Yahoo!
  CardSpace (Provider): Microsoft Windows Vista, Higgins, …

Beispiel: OpenID



- Discovery-Service entfällt bzw. Auflösung erfolgt durch: URL, E-Mail-Adresse
- Erweiterungen: unterschiedliche Identitäten pro Benutzer (Personas), Trusted Relying-Parties (digitale Signatur des Tickets / Attribute) z.B. in sxip, CardSpace, …

Grenzen von OpenID?

- Usability besser als bei SAML-basierten Verfahren! insbesondere Discovery!

…aber…

- Übermittlung von Attributen als Extension - noch nicht überall implementiert
- Datenschutz / Approval für die Übermittlung der Attribute dito
- Vom Standard abweichende Implementierungen wie E-Mail als OpenID

…außerdem…

- Phishing: z.B. Provider kein HTTPS oder Benutzer auf “gefälschten” Provider umgeleitet
- Replay Attacken, und Man-in-the-Middle Angriffe (da Standard nur Diffie-Hellman)
- Weitere Probleme z.B. XSS, CSRF siehe z.B. https://www.blackhat.com/presentations/bh-usa-07/Wysopal_and_Eng/Whitepaper/bh-usa-07-wysopal_and_eng-WP.pdf

ggf. noch entscheidender… Bindung an Provider…

- Wegfall des Providers, Erhöhung der Kosten → Abhängigkeit, Profilbildung
  Lösung: Delegation (OpenID in eigener Domain) bzw. eigener Provider…

Fazit und Ausblick

- Benutzerzentrierte Authentifizierungsverfahren sind ideal für die Benutzer: Usability, Discovery, … Sicherheitsprobleme werden momentan gelöst…
- Attribute, Datenschutz etc. als Extensions standardisiert durch OpenID Foundation
- Branchengrößen steigen in den Web-SSO Markt ein. z.B. Google, Yahoo!… aber fast alle bieten Provider keine Consumer! → Consumer stattdessen z.B. bei kleinen Startups!

OpenID und SAML lösen gleiche Probeme, unterschiedliche Nachteile → Integration

- SAML (insbesondere Shibboleth) derzeit de facto Standard für wissenschaftliche Anwendungen (Verlage, E-Learning, GridShib, …)
- Für MPG-AAI z.B. Shibboleth Erweiterung für Login per E-Mail Adresse (IdP Proxy)
  - vereinfachtes Discovery, Integration mit DFN-AAI bzw. weiteren Föderationen
  - Datenschutz durch Freigabe der Attribute durch Benutzer etc.
- Ideallösung Integration! OpenID / CardSpace in Shib… teilweise schon implementiert…

Vielen Dank für die Aufmerksamkeit!