Sicherheit für Web-Anwendungen mit SAML2 und OAuth2

13. Tagung der DFN-Nutzergruppe Hochschulverwaltung

„Campus 4.0“

Westfälische Wilhelms-Universität Münster,
Münster 17.05.2017

Peter Gietz, DAASI International
Peter.gietz@daasi.de

Agenda

- Kurzvorstellung DAASI International
- Begriffe Identity Management und Föderiertes IdM
- SAML2 für Web Single Sign-On mit Shibboleth
- OAuth2/OpenID Connect für Non-Web-Fall (SOAP und RESTlike Services)
- Vor- und Nachteile von SAML2 und OAuth2/OIDC
- Erfolgreiche Kombinationen der beiden Technologien

Geschichte

Gründung: 2000 in Tübingen mit 4 Mitarbeitern als Spin-Off des ZDV der Universität Tübingen aus DFN-Projekten zu X.500/LDAP heraus

2003: Vortrag zu LDAP bei der DFN Nutzergruppe Hochschulverwaltung in Potsdam

2017: 20 Mitarbeiter, ca. 13 FTE,
ca. 1 Million Jahresumsatz

Weiter an Forschungsprojekten beteiligt zu:

- LDAP
- PKI
- Grid-Computing
- Virtuellen Forschungsinfrastrukturen
- Digital Humanities
- Föderiertes Identity Management

DAASI International GmbH

Kernkompetenzen

Identity & Access Management

- Verzeichnisdienste, Authentifizierungs- und Autorisierungsinfrastrukturen, Zugriffskontrolle, Single Sign-on, Provisionierung
- LDAP, PKI, SAML, OAuth2, OIC, SCIM, SPML, RBAC

Open-Source-Software

OpenLDAP, Shibboleth, didmos, midPoint

Digital Humanities

- AAI, digitale Forschungsinfrastrukturen, Datenbankanwendungen in den Geisteswissenschaften

DAASI International GmbH

Leistungen

- Consulting
- Integration
- Software-Entwicklung
- Support
- Schulung
- Projektmanagement und Gutachten

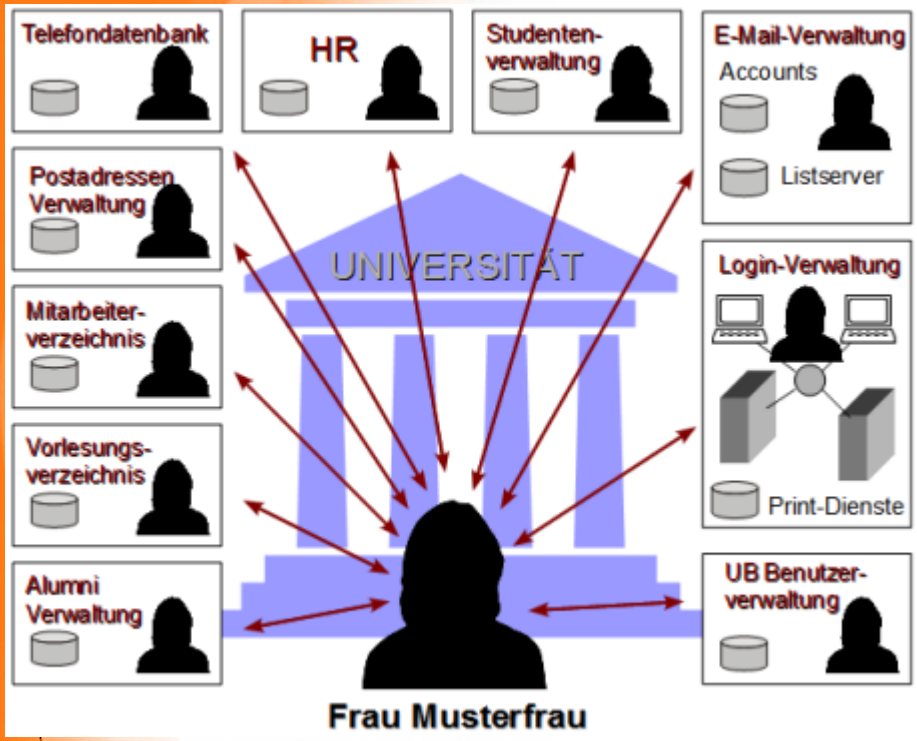
DAASI International GmbH

Begriffe
Identity Management
und
Federated Identity Management

Identity Management

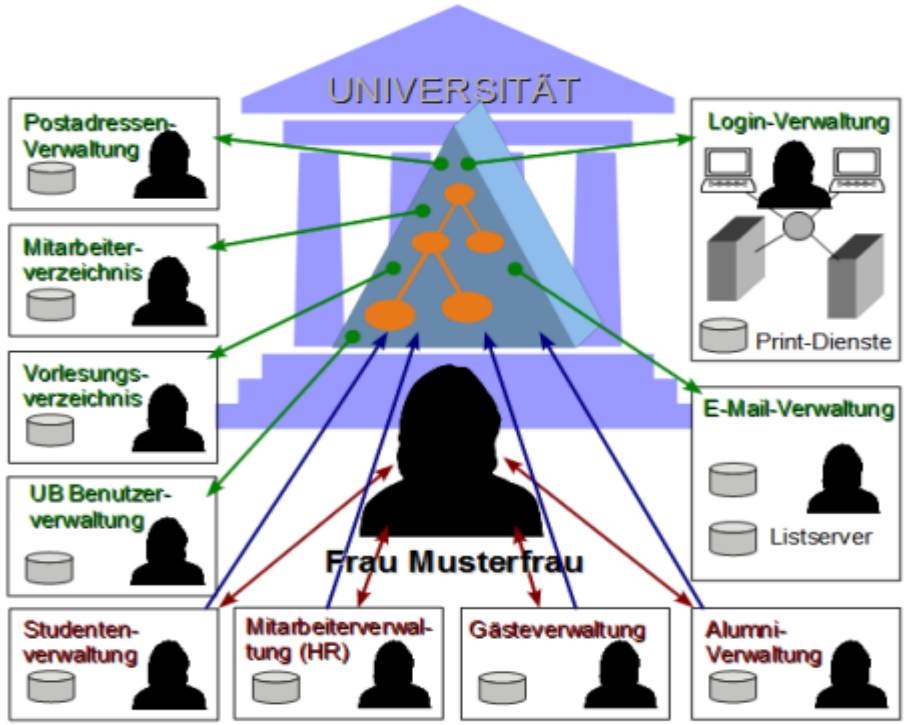
- Definition von Spencer C. Lee:
  - *Identity Management bezieht sich auf den Prozess der Implementierung neuer Technologien zum Verwalten von Informationen über die Identität von Nutzern und zur Kontrolle des Zugriffs auf Firmenressourcen.*
  - *Das Ziel von Identity Management ist es Produktivität und Sicherheit zu erhöhen und gleichzeitig Kosten der Verwaltung von Benutzern, ihrer Identitäten, Attribute und Berechtigungsnachweise zu senken*
- Erleichterungen für Nutzer und Administratoren
- Hier wichtig:
  - Identity Management ist Voraussetzung für Federated Identity Management da Zusagen über Aktualität und Richtigkeit der Identitätsdaten gemacht werden

DAASI International GmbH



Hochschule ohne IdM

Hochschule mit IdM



DAASI International GmbH

Federated Identity Management

- *FIdM-Definition von Peter Valkenburg, et.al (SURF):*
  - *Kollektiver Begriff für alle Prozesse, Standards und Technologien, die den Austausch von Identitäts-informationen über organisatorische Grenzen hinweg unterstützen*
- **FidM setzt eine Föderation voraus**
  - **Ein Vertrauensbund, der es ermöglicht, verteilte Ressourcen gemeinsam zu nutzen**
  - **Vertrauen wird durch Verträge und Einhaltung von entsprechenden Sicherheitspolicies gewährleistet**

DAASI International GmbH

Grundbausteine einer Föderation

- Eine Föderation besteht aus drei Bausteinen:
  - Föderationsverwaltung
    - zentraler Vertragspartner für Föderationsmitglieder
    - verwaltet Zugangsdaten zu den einzelenen Bausteinen (“Metadaten”)
    - betreibt zentrale Infrastrukturkomponenten
  - Identity Provider (IdP)
    - Benutzerverwaltung der Heimatorganisation
    - verantwortlich für Authentifizierung und Attribute
  - Service Provider (SP)
    - verantwortlich für Ressourcen
    - Entscheidet aufgrund von Aussagen des IdP

DAASI International GmbH

Vorteile von FIdM

- Identitätsdaten eines Benutzers müssen nur an einer Stelle gespeichert werden
  - Name, Kontaktdaten, Passwort, etc.
  - im IdP der „Heimatorganisation“
- Personenbezogene Daten
  - werden nur über gesicherte Verbindungen an Mitglieder des Vertrauensbunds geschickt
  - müssen aber gar nicht übertragen werden, da es oft nur auf Autorisierungsattribute ankommt
- Die Föderationstechnologien ermöglichen Single Sign On
- Föderation ähnelt einer PKI (Public Key Infrastructure), ist aber wesentlich einfacher zu implementieren:
  - nur Serverzertifikate notwendig
  - Passwort etc. anstelle der Benutzerzertifikate

DAASI International GmbH

Motivation für Federated Identity Management in der öffentlichen Verwaltung

Motivation im Verwaltungsumfeld

- Erste Föderation im Verwaltungsumfeld war die Föderation der Hochschulen (DFN-AAI)
  - Studenten werden immer mobiler, wechseln die Hochschule öfters, bzw. belegen Kurse an anderen Hochschulen (E-Learning)
  - Forschung funktioniert immer vernetzter
    - Forschungsinfrastrukturen (eScience, Grid- und Cloud-Computing)
    - Forscher aus verschiedenen Hochschulen benötigen Zugriff auf im Netz verteilte Ressourcen („Virtuelle Organisationen“)
  - Verlagslizenzen erfordern Föderationen
    - z.B. für Datenbanken, die von Hochschulbibliotheken online gestellt werden
    - Verlage wollen Autorisierungsattribute (anstelle von IP-Ranges)
    - Lizenzen können auch an Hochschulverbünde erteilt werden

DAASI International GmbH

Motivation im Behördenkontext

- Viele Behörden sind dezentral organisiert, wollen aber zentrale Dienste anbieten, z.B.:
  - Bundesbehörden mit vielen Dienststellen im gesamten Bundesgebiet
  - Kultusministerien, die für alle Schulen Dienste anbieten
  - Alle Behörden eines Ministeriums
  - Behörden verschiedener Ministerien, die auf gleiche Anwendungen zugreifen
- In all diesen Fällen können die Benutzerdaten in der Heimatbehörde bzw. Heimatorganisation Schule bleiben

DAASI International GmbH

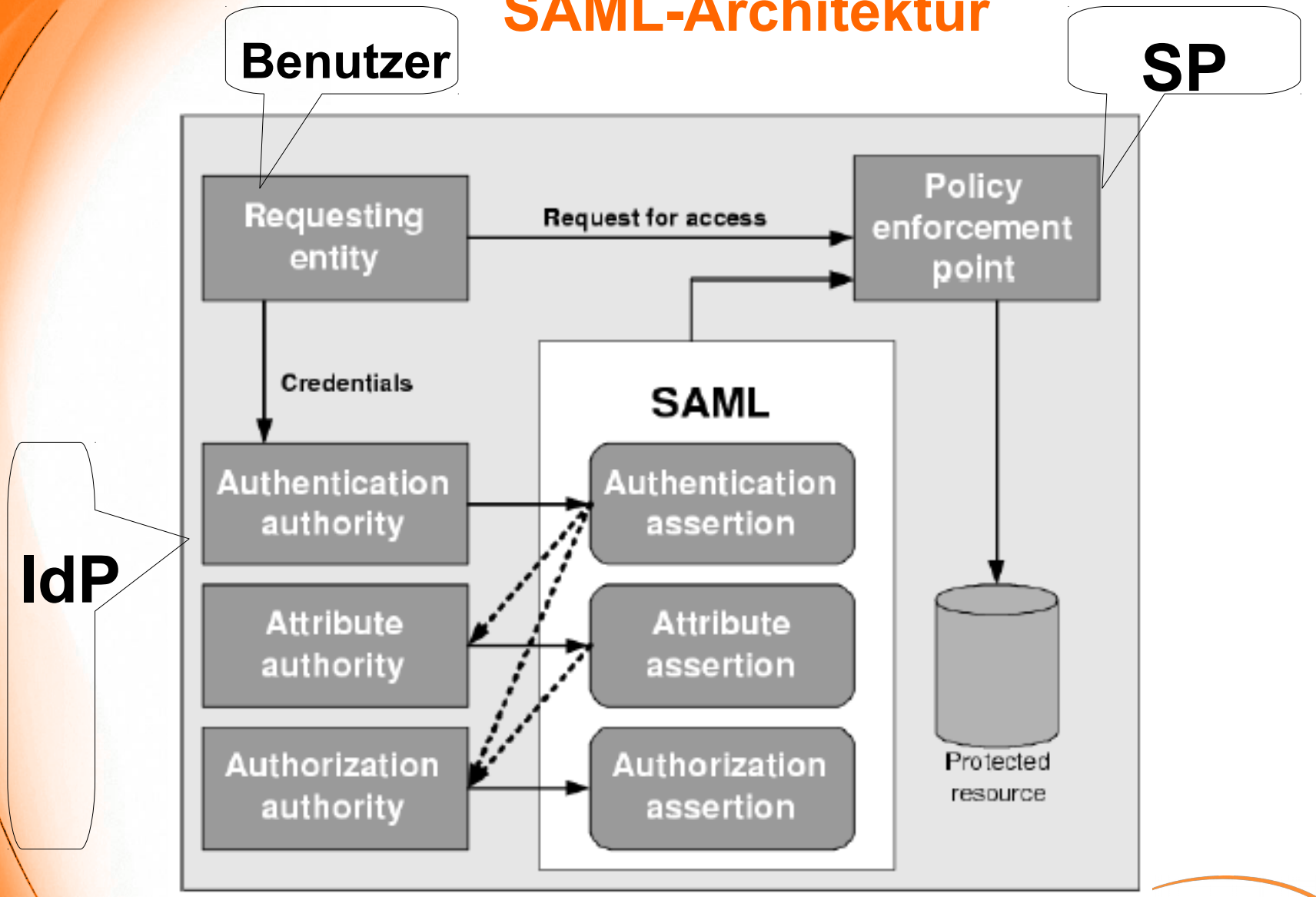
Der Standard SAML

SAML

- Security Assertion Markup Language
  - OASIS-Standard, aktuelle Version ist SAML2
- XML-Dokumente enthalten Zusicherungen (Assertions) die ein IdP über Benutzer macht:
  - Authentication Statements, Zusicherung, dass sich ein Benutzer authentifiziert hat
  - Authorization Statement, Zusicherung über bestimmte Zugriffsrechte
  - Attribute Statement, Zusicherung über bestimmte Eigenschaften eines Benutzers, die in Form von Attributen weitergegeben werden und den SP bei der Entscheidung über Zugriff unterstützen
- Profile spezifizieren welche Assertions wie zwischen IdP und SP ausgetauscht werden

DAASI International GmbH

SAML-Architektur



Nach: RUBENKING, NEIL J.: Securing web services

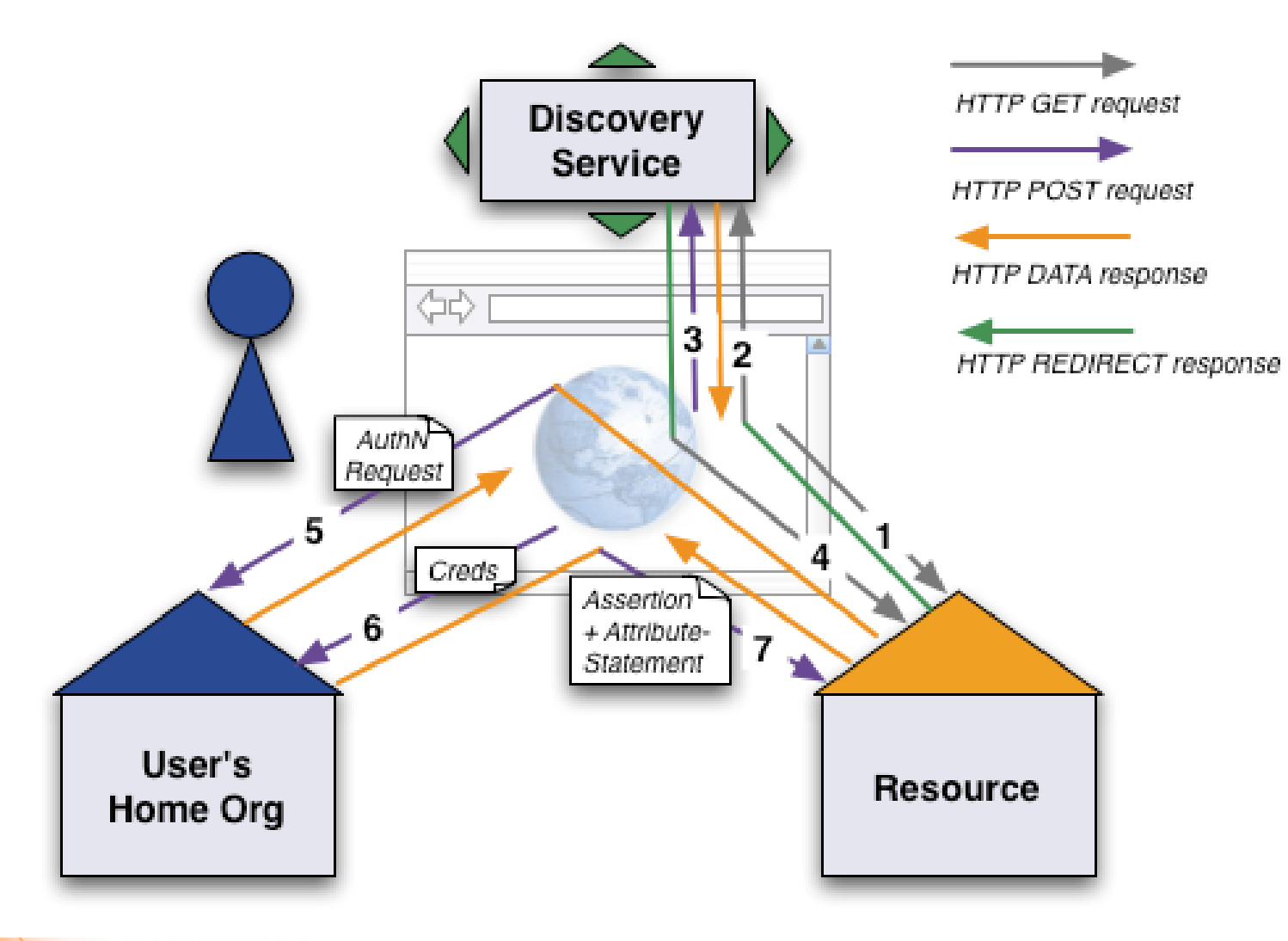
Open Source Implementierung Shibboleth

Shibboleth

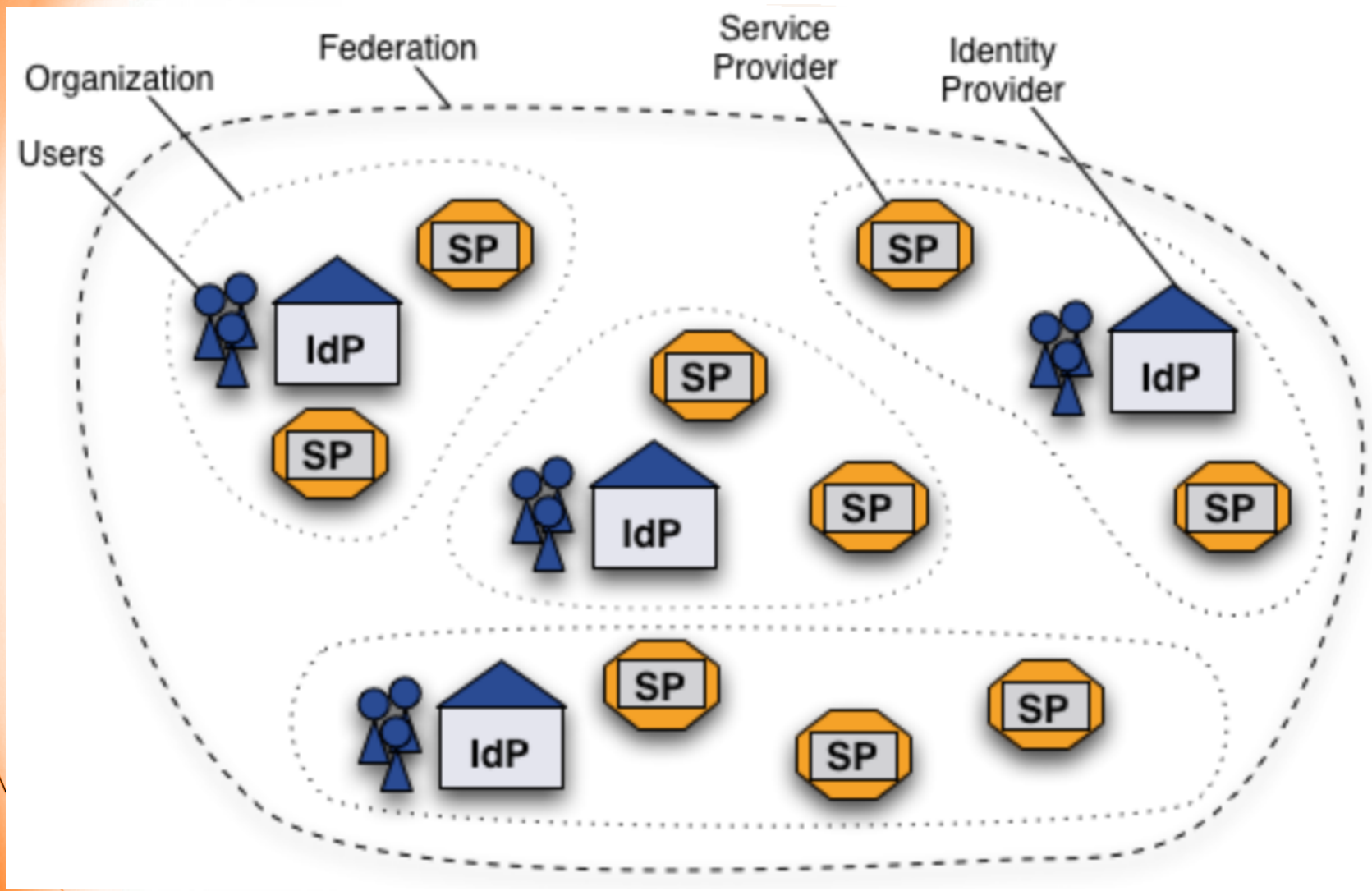
- Open Source Software vom US-amerikanischen Internet2-Projekt
- Implementiert das SAML-Profil WebSSO
  - nach einmaliger Authentifizierung hat der Nutzer für eine bestimmte Zeit föderationsweit Zugriff auf verschiedene Webanwendungen
- Viele Anwendungen sind bereits „shibboletisiert“
- Shibboleth baut im Wesentlichen auf zwei miteinander kommunizierende (Apache-)Module auf:
  - Identity Provider (IdP), der an die lokalen Benutzerverwaltungen angeschlossen wird
  - Service Provider (SP), der vor zu schützende Ressourcen bzw. Dienste gestellt wird.

DAASI International GmbH

Ablauf SAML-Authentifizierung mit IdP Discovery



SAML-basierte (Hochschul-)Föderationen



Probleme mit SAML

SOAP und RESTlike Services

- Problem 1: Serviceaufrufe von nicht-Web-Browsern
- Problem 2: Delegierung von Credentials (z.B. geschütztes Web-Portal ruft Service auf)
- Lösung A: SAML Enhanced Client Or Proxy (ECP)
  - Ein ECP (-Client) ist fast ein Browser, nur ohne GUI (HTTP/HTTPS, GET/POST/Redirect, Cookies, etc.)
  - IdP fast unverändert (Basic Authn / X.509 Auth)
  - SP fast unverändert (Zugriff über REST)
- Probleme mit Lösung A:
  - Kaum gute Client-Libraries
  - Übergang von WebSSO zu ECP nicht gegeben

SOAP und RESTlike Services (2)

- Lösungen B, C und D:
  - Service-Accounts, ggf. kombiniert mit VPNs, SSH Tunnels, etc.
  - SAML STS - Plug-In für SOAP Web Services Security
  - Kerberos
- Lösung, die sich durchsetzt: OAuth2, IETF RFC 6749
  - Viele (Open Source)-Implementierungen für
    - Clients (weit weniger Anforderungen als an ECPs)
    - SPs (die hier Resource Server heißen, RS)
    - IdPs (hier Authorization Server, AS)

DAASI International

OAuth2 und OpenID Connect

OAuth2

- Protokoll zur Autorisierung von Zugriff auf eine Ressource
- Ein Client möchte im Namen des Nutzers (Resource Owner) auf dessen Ressourcen bei einem Resource Provider zugreifen
- Beispiel: "App (Client) verlangt Zugriff auf Profil-Informationen/Fotos/... (Ressource) des Nutzers (Resource Owner) bei Google (Resource Provider)" User muss diesen Zugriff autorisieren
- Aus technischer Sicht wird dem Client ein Access Token ausgestellt, mit dem er auf die Ressource zugreifen kann
- Access Token ist Bearer Token (= jeder der darüber verfügt, kann dann auf die Ressource zugreifen)
- Problem: OAuth 2.0 enthält keine Informationen über die Authentifizierung und ist damit nicht direkt für SSO geeignet

OpenID Connect (OIDC oder auch OIC)

- "simple identity layer on top of OAuth 2.0"
- Version 1.0 seit November 2014
- Erweitert OAuth 2.0 um
  - ID Token, das Informationen zur Authentifizierung enthält
  - UserInfo Endpoint zur Anforderung von Claims (Attributen)
  - Hinzufügen von "openid" als scope in der Anfrage an den OAuth2.0 Server
- Verschiedene "Flows", wie der Client an Access- und ID Token kommt: Authorization Code Flow, Implicit Flow und Hybrid Flow
- Für den klassischen Web SSO Fall ist Authorization Code Flow am weitesten verbreitet

SAML
vs./plus
OAuth2/OIDC

OAuth2/OIDC vs. SAML2

- Die beiden Protokollstacks kommen aus unterschiedlichen „Kulturen“ sozusagen IETF vs. OASIS
- SAML2 ist sehr etabliert, wird unterstützt von
  - CA, Entrust, ForgeRock, IBM, Microsoft, NetIQ, Oracle, Ping, SAP, etc.
- OAuth2/OIDC ist v.a. im Sozialen Netz etabliert, wird unterstützt von:
  - Amazon, Dropbox, Facebook, Google, Instagram, LinkedIn, Microsoft, Paypal, Twitter, Xing, etc.
- JSON Web Token (JWT) statt XML für das ID Token bzw. Assertion
- Die direkte Kommunikation zwischen OpenID Connect Provider (vgl. IdP) und Client erfolgt per REST-API statt per SOAP in SAML

OAuth2/OIDC vs. SAML2

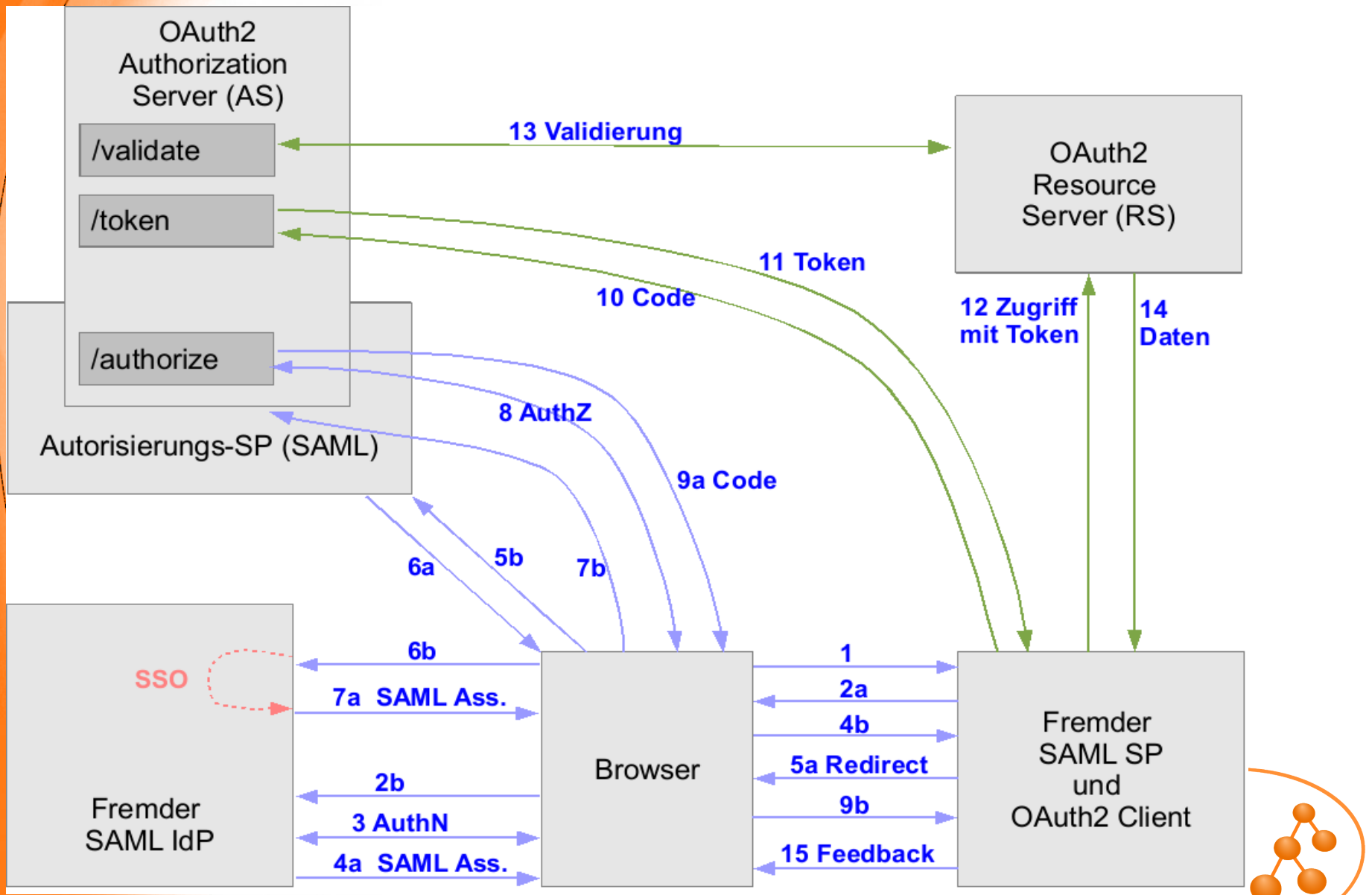
- Anwendungen (Clients) können per Design rein JavaSkript-basiert im Browser laufen (Implicit Flow)
  - Damit ist OIDC deutlich flexibler für mobile Anwendungen nutzbar
- SAML ist aber immer noch das etabliertere Protokoll, dessen Sicherheit bewiesen ist
- OAuth2 anfällig gegen Phishing-Attacken
- OIDC/OAuth2 kennt (noch) nicht das Konzept einer kontrollierten Föderationen, sondern geht von automatischer Client-Registrierung aus

DAASI International

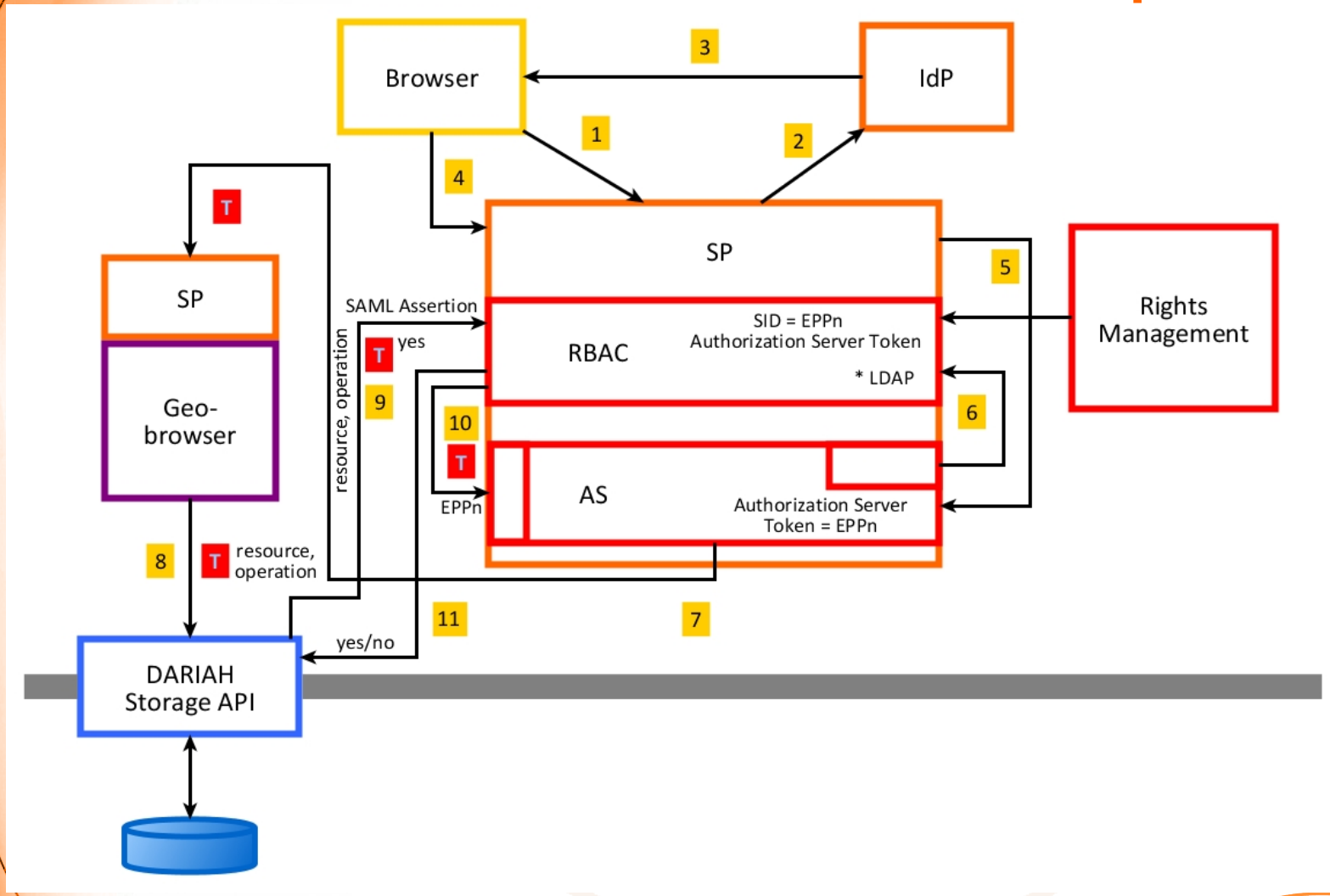
OAuth2/OIDC plus SAML2

- Man kann das Gute aus beiden Welten kombinieren
  - Authentifizierung in der Föderation über SAML2
  - WebSSO über SAML2
  - Non-Web und Mobile über OAuth2
- Auch Authentifizierung über OIDC lässt sich mit SAML kombinieren
  - Vgl. OIDC-Plugin für Shibboleth

oAuth2/SAML AuthzCode Set-Up 1



OAuth2/SAML AuthzCode Set-Up 2



Vielen Dank für Ihre Aufmerksamkeit!

DAASI International

Web www.daasi.de

Telefon 07071 / 407 109 0

E-Mail info@daasi.de