Shibboleth 2 und Interoperabilität

Herbsttreffen 2009 des ZKI-Arbeitskreises Verzeichnisdienste, Dresden

5. Oktober 2009

Peter Gietz

DAASI International GmbH

peter.gietz@DAASI.de

DAASI International

Directory Applications for Advanced Security and Information Management

DAASI International – mehr als ein „Mittler“

- Lieber: „externer Dienstleister“
- Vermittelt lieber Open-Source-Produkte
  - z.B.: OpenLDAP, Shibboleth, SimpleSAMLphp, OpenSAML, OpenXPKI, etc.
- Schreibt auch selbst Open-Source-Software
  - z.B.: OpenRBAC, XML-basierte IdM-Konnektoren, SPML-basiertes Provisionierungssysteme
- Schreibt auch für Sie spezielle Software (z.B. Tool zum Controlling von Studiengebühr-Projekten)
- Berät Sie u.a. in den Bereichen IdM, FidM, UCIdM
- Analysiert und bewertet Ihre IT-Infrastruktur, plant entsprechende Architekturen
- Nimmt aktiv an der Forschung teil (insbes. AAI und Grid-Computing)

DAASI International

Directory Applications
for Advanced Security
and Information Management

Agenda

- Föderationen im Hochschulbereich
- Shibboleth
- simpleSAMLphp
- Interoperabilität in SAML-basierenden Föderationen
- User Centric Identity Management
- OpenID, Motivation und technischer Überblick
- Interoperabilität SAML/OpenID
- Umfrage zu OpenID

DAASI International
Directory Applications for Advanced Security and Information Management

Motivation für domainübergreifende AA-Infrastrukturen

- Studenten werden immer mobiler (gefördert durch Bologna-Prozess)
  - Grundsätzlich wird hierdurch der Austausch von Studierendeninformationen zwischen Hochschulen wichtiger
  - Studiengänge der verschiedenen Hochschulen müssen kompatibel sein
  - Es gibt gemeinsame Studiengänge mehrerer Hochschulen
- Forschung funktioniert immer vernetzter
  - eResearch und Grid-Computing
  - Forscher aus verschiedenen Hochschulen benötigen Zugriff auf im Netz verteilte Ressourcen
- Verlagslizenzen für Datenbanken verlangen Autorisierungsattribute (anstelle von IP-basierter Autorisierung)
  - Lizenzen auch für Hochschulverbünde
  - Nationallizenzen

DAASI International
Directory Applications for Advanced Security and Information Management

Föderationen

- Federated Identity Management (FIdM)
  - stellt über die Grenzen einer Organisation hinweg Identitätsinformationen zur Verfügung
  - nutzt Authentifizierung und Autorisierung im Rahmen von Föderationen
  - baut auf die lokalen IdM-Systeme bzw. Authentifizierungs-dienste auf, sodass nicht jeder Benutzer in jeder Organisation einen Account benötigt
- Es kommen beim FIdM moderne Standards zum Einsatz, insbesondere SAML (Security Assertion Markup Language)
- Technologien sind z.B.: Liberty Alliance, Shibboleth, WS-Security

DAASI International
Directory Applications for Advanced Security and Information Management

Komponenten des FIdM

- Es werden folgende Funktionalitäten unterschieden
- Identity Provider (IdP), die an der lokalen Benutzerverwaltung der „Heimatorganisation“ ansetzt und Authentifizierungsstatus und Autorisierungsattribute weitergeben kann
- Service Provider (SP), die vor Ressourcen geschaltet sind, und über Informationen vom IdP Zugriffsentscheidungen vorbereitet
- Discovery Service, über den der Benutzer seine Heimatorganisation (Heimat IdP) auswählen kann
- Zentrale Metadatenverwaltung, über die alle Komponenten die Zertifikate und URIs der anderen Komponenten beziehen

DAASI International
Directory Applications for Advanced Security and Information Management

Vertrauen

- SP vertraut dass die IdPs der Heimatorganisationen korrekte und aktuelle Daten liefern
- IdPs vertrauen, dass SPs mit den übermittelten personenbezogenen Daten korrekt umgehen
- Das Vertrauen wird innerhalb der Föderation
  - über Verträge hergestellt
  - über digitale Signaturen implementiert
- Ein zentraler Betreiber der Föderation erleichtert die vertraglichen und technischen Aspekte des Vertrauens

DAASI International
Directory Applications for Advanced Security and Information Management

Shibboleth

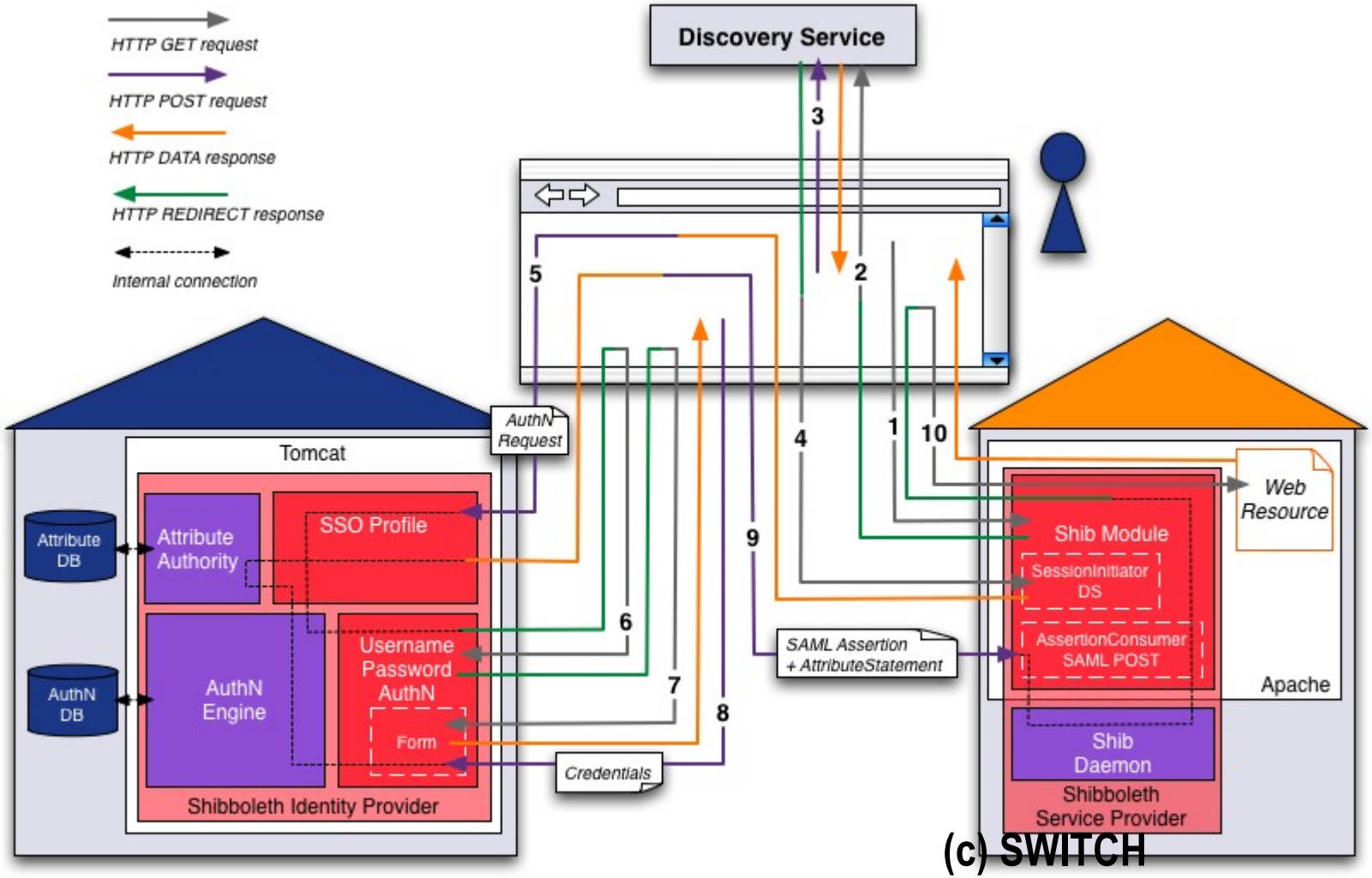
- Föderationssoftware vom US-amerikanischen Internet2-Konsortium
  - http://shibboleth.internet2.edu
- Basiert wie Liberty Alliance auf SAML
- Open Source Software, aktuell Version
  - 2.1.3 (IdP) und
  - 2.2.1 (SP)
- viele Anwendungen werden „shibbolethisiert“
- zusätzlich eine Single Sign On-Lösung: nach einmaliger Authentifizierung hat der Nutzer für eine bestimmte Zeit föderationsweit Zugriff auf verschiedene Anwendungen

Shibboleth.

DAASI International

Directory Applications for Advanced Security and Information Management

Shibboleth - schematisch



(c) SWITCH

Datenschutz

- Auch bei Filterung der Attribute am IdP werden nicht alle Datenschutz-Aspekte adressiert
  - zweckgebundene Verwendung der Daten?!
- Lösung 1: anonymisierte Benutzerprofile
  - eduPersonTargetedId
  - persistente ID wird vom IdP für jeden Benutzer an jedem SP erzeugt (Hash nicht invertierbar)
  - keine „Profilerstellung“ zwischen den SPs möglich)
- Lösung 2: Interface für Benutzereinwilligung
  - SWITCHaai ArpViewer bzw. uApprove (Servlet Filter)
  - Ermöglicht dem Benutzer Einwilligung vor Übertragung der Attribute zu neuem SP zu geben (auch wenn Attribute oder zugrunde liegende Policy sich ändert)

DAASI International
Directory Applications for Advanced Security and Information Management

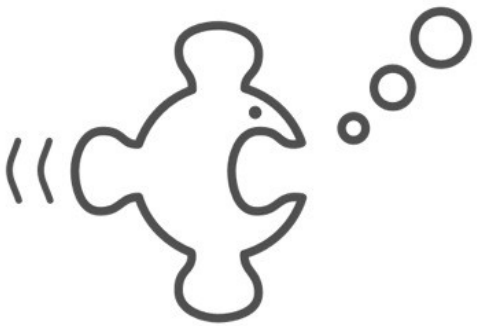
Shibboleth IdP: Zukunft

- Release 2.2:
  - Support für Jetty Servlet Container
  - Standalone configuration scripts, z.B. für SSL, Metadaten-Generierung, LDAP/Kerberos/Container AuthN, Datenbank/Connectors, Attribute Filter
- Release 2.3:
  - Bundle a clustering solution with the IdP
  - n-tier delegation („proxy AuthN“)
  - uApprove integration
  - Single Logout Support

DAASI International
Directory Applications for Advanced Security and Information Management

simpleSAMLphp

- Entwickelt für die norwegische SAML-Föderation FEIDE von UNINETT
- Unterstützt neben SAML2.0 IdP und SP noch weitere Protokolle (Shibboleth 1.3 IdP/SP, A-Select, WS-Federation, OpenID)
- Durch modulares Konzept einsetzbar als
  - SP für PHP-Anwendungen
  - IdP
  - Brücke zwischen verschiedenen Protokollen
- PHP-basierte Konfiguration
- PHP-basiertes Metadatenformat



DAASI International
Directory Applications for Advanced Security and Information Management

simpleSAMLphp Vor- und Nachteile

- Vorteile:
  - sehr einfache Installation
  - etwas einfachere Konfiguration als Shibboleth
  - nativer Schutz von PHP-Anwendungen (SP)
  - kein Servlet Container benötigt (IdP)
  - Brückenfunktion
  - simpleSAMLphp IdP unterstützt SLO bereits jetzt schon
- Nachteile:
  - Logging nur rudimentär konfigurierbar, debugging erschwert
  - Interoperabilität in Shibboleth-Föderation prinzipiell (s. nächste Folie)

DAASI International
Directory Applications for Advanced Security and Information Management

SimpleSAMLphp und Interoperabilität

- SimpleSAMLphp Metadatenformat nicht SAML-kompatibel
  => Konvertierungsroutinen werden aber angeboten
- SimpleSAMLphp SP in Shibboleth-Föderation unterstützt keine NameID-Encryption in Assertions vom IdP
  => kann im Shibboleth IdP abgeschaltet werden
- Interoperabilität erfolgreich im DAASI-Labor getestet
  - SimpleSAMLphp SP mit Shib 2.0 IdP
    - NameID-Encryption abstellen
    - Attributmapping OID-URNs->Namen
  - Shib 2.0 SP mit SimpleSAMLphp IdP
    - Anbindung an einen LDAP-Server
    - Attributmapping

DAASI International
Directory Applications for Advanced Security and Information Management

SimpleSAMLphp und Shibboleth

- Shibboleth und simpleSAMLphp nebeneinander benutzbar (mit ein wenig Konfigurationsaufwand)
- Einsatzmöglichkeit:
  - simpleSAMLphp für PHP-Anwendungen
  - Shibboleth für andere Anwendungen
- Shibboleth ist vielseitiger und kann als Fallback ebenso für PHP-Anwendungen verwendet werden
- SimpleSAMLphp unterstützt OpenID

- Erste Frage der Umfrage: Wer hat schon einmal von OpenID gehört?

DAASI International
Directory Applications for Advanced Security and Information Management

User Centric IdM

- Die Benutzer bewegen sich auch außerhalb ihrer Hochschulidentität im Netz
  - „Web Identity Experience“
- Sie sind Mitglieder in verschiedenen Sozialen Netzwerken, z.B.:
  - Xing
  - LinkedIn
  - Facebook
  - StudiVZ
- Sie benutzen verschiedene Web 2.0-Dienste
  - Flickr
  - Twitter
  - Googleapps
  - Blogs
  - Wikis

DAASI International
Directory Applications for Advanced Security and Information Management

User Centric IdM und OpenID

- Die Benutzer müssen bisher immer wieder Ihre Identitätsdaten neu eingeben
- Hier setzt OpenID an:
  - OpenID ist ein dezentrales Identitätssystem
  - Anstatt sich für jede Webseite, bei der man sich anmelden muss, einen Benutzernamen und ein Passwort zu merken, wird ein zentrale OpenID und ein zentrales Passwort gespeichert
  - Man loggt sich dann mit diesen Daten einmalig beim OpenID-Server ein und kann dann verschiedene Webseiten nutzen
- Neue Terminologie:
  - OpenID IdP: OP
  - OpenID SP: „consumer“ oder „relying party“ (im Folgenden: SP)

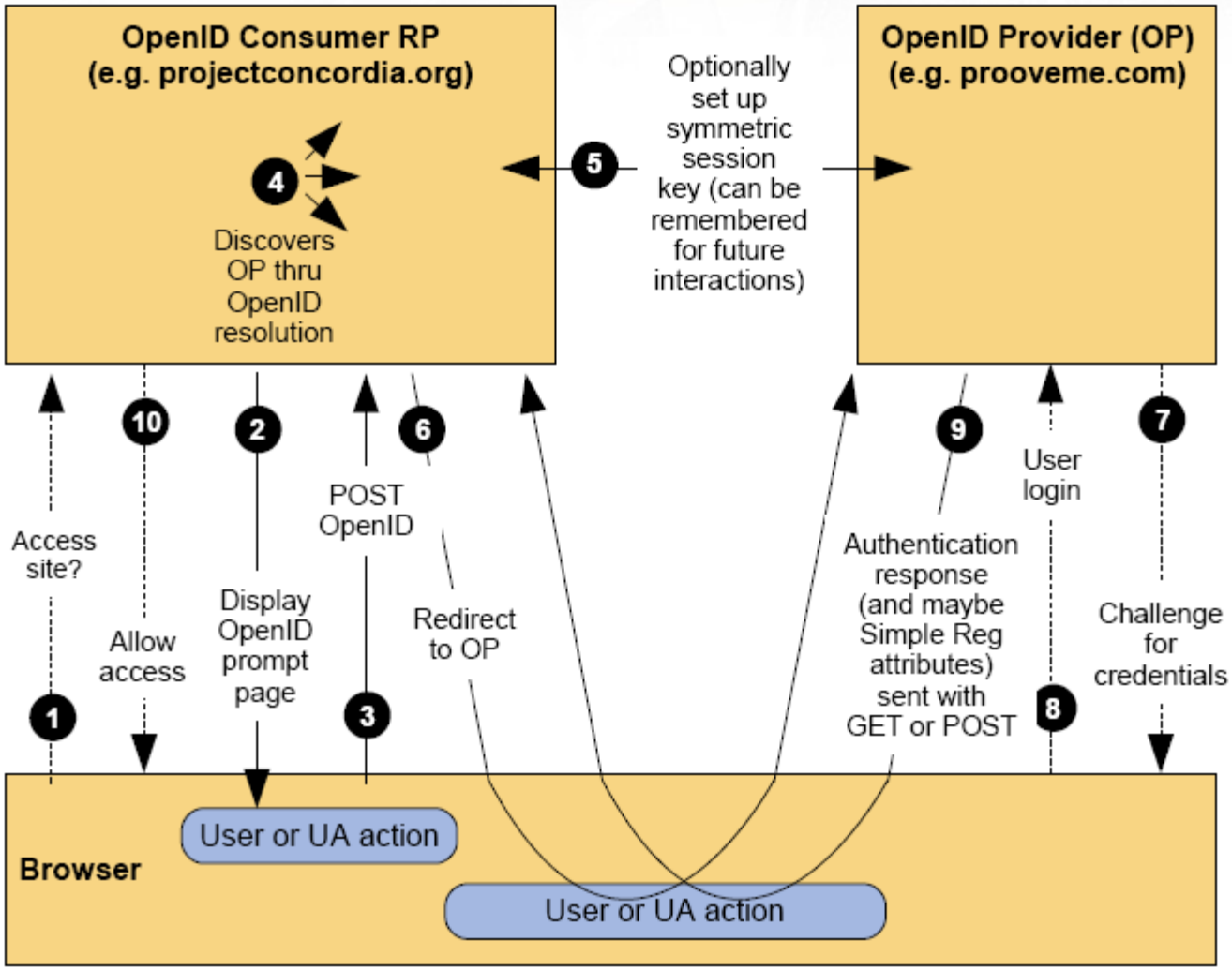
DAASI International
Directory Applications for Advanced Security and Information Management

OpenID

- Geht davon aus, dass ein Benutzer eine URL, oder XRI (Extensible Resource Identifier) hat
- Ein OpenID Identity Provider (OP) vertritt eine solche URL/XRI
- Funktionsweise:
  - Benutzer präsentiert einem SP die URL/XRI
  - SP ruft die URL auf, um den zuständigen IdP zu finden
  - SP tauscht mit IdP einen Schlüssel aus
  - Benutzer wird zum IdP redirected und authentifiziert sich dort
  - Benutzer wird zurück zum SP redirected zusammen mit einem Authentication Token
  - SP gewährt Zutritt zum Dienst
- OpenID 1.0 und 1.1 durch 2.0 obsolet

DAASI International
Directory Applications for Advanced Security and Information Management

OpenID Funktionsweise



OpenID vs. SAML

- OpenID ist einfacher
  - Spezifikationen dünner und leichter verständlich
  - Konkretes HTTP-Protokoll und nicht ein abstraktes Framework
  - Verschlüsselung einfach über SSL/TLS und nicht über XML-digital signatures und -encryption
  - Einfach implementierbar
  - Kein WAYF/Discovery-Service notwendig
- SAML ist flexibler
  - Verschiedene Möglichkeiten der Benutzeridentifizierung
  - Man könnte ein SAML-Profil und Protokoll-Binding spezifizieren, dass OpenId vollständig abbildet

DAASI International
Directory Applications for Advanced Security and Information Management

JISC-Studie zu OpenID

- JISC (nationales Forschungsnetz in GB) hat im Rahmen ihres eInfrastructure Programms eine Studie in Auftrag gegeben über die mögliche Verwendung von OpenID im Hochschulbereich
- Vgl. David Chadwick: Review of OpenID – Project Final Report, 3.12.2008
  - Sicherheitsanalyse
  - Entwicklung eines OpenID-Gateways
  - Nutzerumfrage

DAASI International
Directory Applications for Advanced Security and Information Management

Sicherheitsanalyse von OpenID

- Jeder, auch ein Spam-Roboter, kann sich eine OpenID registrieren, OpenID Provider sind alle gleich
- Es besteht keine Vertrauensbeziehung zwischen OpenID Providern und SPs
- IDs können (für andere Benutzer) wiederverwendet werden
- Provider können das Online-Verhalten ihrer Nutzer (bei welchem SP sie waren) nachverfolgen (auch bei SAML)
- Das Protokoll ist anfällig für Phishing (durch evil SP) und Cross Site Request Forgery (embeded scripts)
- Provider muss 24x7 verfügbar sein (auch bei SAML)
- Es existieren viele Provider, aber nur wenige SPs, die für die Interessenten von hohem Nutzen sind
- Das Protokoll sieht Diffie-Hellman und TLS (gegen MitM-Attacken) vor

DAASI International
Directory Applications for Advanced Security and Information Management

Wie könnte denn das zusammengehen?

- Grundsätzlich ist es denkbar, dass einzelne OpenID IdPs eine strengere Sicherheits-Policy fordern.
- Schränkt man dann den Zugriff bei den Service Providern auf Nutzer ein, die bei solchen Providern registriert sind, kann ein höheres Sicherheitsniveau bewirkt werden.
- Irgendwann werden die Studierende eventuell OpenID-Unterstützung fordern (Studiengebühren).

DAASI International
Directory Applications for Advanced Security and Information Management

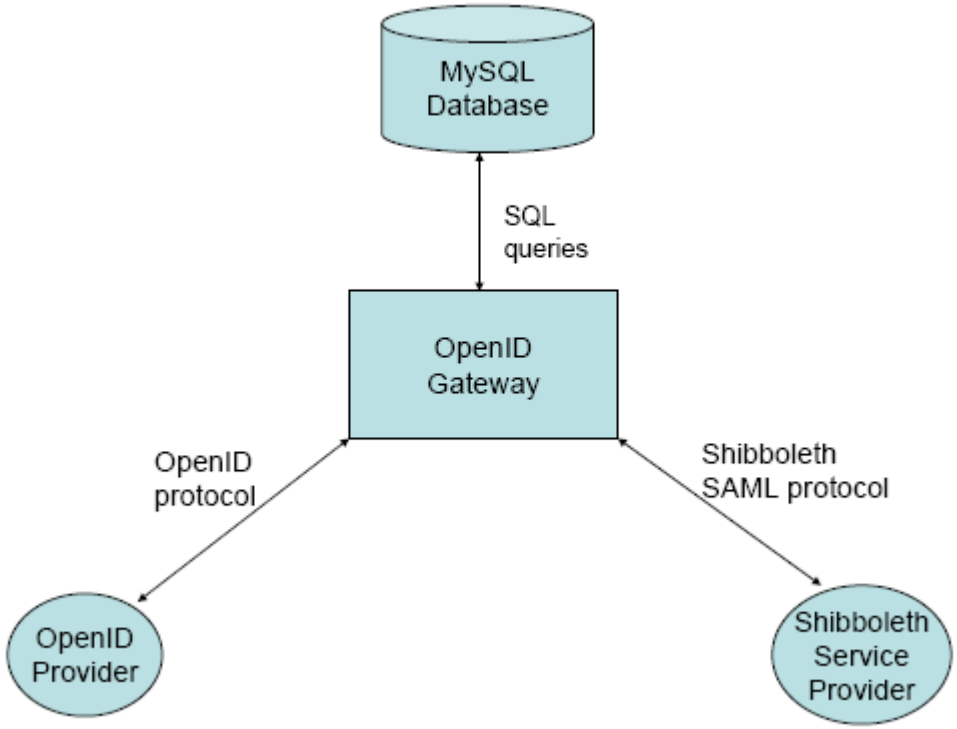
OpenID-SAML Gateway

- Erscheint in der britischen Föderation als Shibboleth Identity Provider
- Wählt man ihn aus, bekommt man eine Möglichkeit zur Eingabe einer OpenID-URL.
- Von dort wird der Benutzer wiederum zu seinem OpenID Provider weitergeleitet und kann sich dort einloggen.
- Die zurückgegebene OpenID wird dem ursprünglich anfragenden Service Provider der Föderation als eduPersonPrincipalName übergeben.
- Werden weitere Attribute benötigt, kann der Benutzer diese zu seiner OpenID direkt am Gateway eintragen.

DAASI International
Directory Applications for Advanced Security and Information Management

OpenID-SAML Gateway

- Das Gateway besteht aus einem Shibboleth Identity Provider, der als Remote User Authentication ein Apache OpenID Authentication Module verwendet und eine mySQL-Datenbank für die Speicherung der vom Benutzer gegebenen Attribute.



DAASI International
Directory Applications
for Advanced Security
and Information Management

SimpleSAMLphp und OpenID

- Die Verwendung von SimpleSAMLphp als OpenID Consumer ist relativ einfach möglich und konnte im DAASI-Labor erfolgreich getestet werden
- Der Betrieb von SimpleSAMLphp als OpenID Provider ist laut Dokumentation ebenfalls möglich, die Installation klappte aber nicht auf Anhieb. Wir arbeiten daran.
- Der SSP-Autor Andreas Akre Solberg hat auch eine Proof-of-Concept-Brücke zwischen OpenID-SP und SAML 2.0-IdPs implementiert (vgl. http://rnd.feide.no/content/bridging-saml-20-and-openid)
- Damit kann ein Nutzer der bei einem SAML IdP registriert ist, bei OpenID Service Providern eine entsprechende OpenID angeben

DAASI International
Directory Applications for Advanced Security and Information Management

Nutzerumfrage

- Im Rahmen einer Technologieförderung des Ministeriums für Wissenschaft und Kunst des Landes Baden-Württemberg Wurde DAASI von der Firma My3So, die im Bereich Social Networking tätig ist, beauftragt, eine Studie zu OpenID im deutschen Hochschulbereich durchzuführen
- Teile der JISC-Nutzerumfrage möchte ich deshalb heute hier bei Ihnen durchführen

DAASI International
Directory Applications for Advanced Security and Information Management

Nutzerumfrage (N=55)

1.) Kannten Sie OpenID vor diesem Vortrag?

- Sehr gut (0)
- Ziemlich gut (4)
- Ein wenig (28)
- Nie davon gehört (19)

2.) Gibt es in Ihrer Einrichtung Anwendungen, die sich auf OpenID stützen? (0)

3.) Gibt es in Ihrer Einrichtung Pläne für solche Anwendungen? (2: Wiki und Studentenportal)

DAASI International
Directory Applications for Advanced Security and Information Management

Nutzerumfrage

4.) eine vom Benutzer ausgewählte OpenID könnte bei der Registrierung an der Hochschule mit aufgenommen werden als zusätzlicher Login-Name, welcher sowohl innerhalb als auch außerhalb der Hochschule Bedeutung hätte

a) Sehen Sie hierin einen möglichen Nutzen? (5)
b) Wieviel Aufwand sähen Sie dies einzuführen?

- Geringer Aufwand (4)
- Größerer Aufwand mit Änderung an den Prozessen (20)
- Nicht rechtfertigbarer Aufwand (6)

c) Können Sie sich vorstellen, dass Ihre Einrichtung dies unterstützt?

- Nie und nimmer (1)
- Nur wenn andere Einrichtungen dies auch tun (7)
- Vielleicht (30)

DAASI International
Directory Applications for Advanced Security and Information Management

Nutzerumfrage

5.) Unter welchen Bedingungen würden Sie OpenIDs als Authentifizierung zu Ihren Diensten akzeptieren?

- Nie (11)
- Nur ausgewählte OpenID-Provider mit erhöhter Sicherheitspolicy (28)
- Jeden OpenID-Provider, vorausgesetzt, die Verbindung zwischen OpenID und Benutzer ist sichergestellt (0)
- Wirklich jeden OpenID-Provider (0)

6.) Würden Sie einen OpenID-Identity-Provider innerhalb der DFN-AAI-Föderation akzeptieren? (16)

6.a) Wenn ja, nur einen von einer Hochschule betriebenen OpenID-Provider? (1)

7.) Würden Sie zugriffsbeschränkte Dienste auch für Benutzer kommerzieller (nicht zur Föderation gehörenden) OpenID-Provider zulassen? (0)

DAASI International
Directory Applications for Advanced Security and Information Management

Vielen Dank für die Beteiligung und für Ihre Aufmerksamkeit!

- Fragen?
- Bei Interesse an der fertigen Studie, bitte Email an peter.gietz@daasi.de
- DAASI International GmbH
  - www.daasi.de
  - Info@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management