UNIVERSITÄT DUISBURG ESSEN

ZIM Zentrum für Informations- und Mediendienste

OpenID Service an der Universität Duisburg-Essen - Use-Cases und Implementierung

Burkhard Wald

September 2016

Was ist das Problem?

- Anhaltender Trend:
  - Immer mehr Prozesse des Uni-Lebens werden auf Web-Anwendungen abgebildet.
- Zwei Welten:
  - Zentral organisierte IT vs. Graswurzel-IT
- Alles schreit nach Authentifizierung
- Durchschleifen von Passworten ist tabu
- Suche nach weiteren Angeboten neben Shibboleth

Was ist OpenID?

- Die ID ist einen URL
- Jeder kann einen Identity-Provider anbieten.
- Jeder Service kann die OpenIds nutzen
- Es ist ein technisches Protokoll
- Es gibt keine Spielregeln
- ID-Provider und Serviceanbieter müssen keine Vereinbarung untereinander treffen

Typisches Szenario

- Ein personlisierter Web-Dienst, den jeder nutzen kann und bei dem man sich aber registrieren muss.
- Jede OpenID irgend eines Providers wird akzeptiert.
- Die Authentifizierung soll den persönlichen Zugang zu dem Dienst für den Nutzer schützen.
- Der Service-Anbieter hat kein eigenes Interesse an dem Zugangsschutz
- Es geht uns nicht darum dieses Szenario zu bedienen, obwohl es nicht ausgeschlossen ist, die Ids dafür zu verwenden.

Was ist bei unserem Szenario anders?

- Die OpenIDs müssen nicht generiert werden.
- Jede OpenID ist eine Aussage über die Person
  - https://openid.uni-due.de/student/1234567 (der authentifizierte Nutzer ist Student und hat die Martrikelnummer 1234567)
- Wir bestätigen dem Service-Anbieter die Wahrheit der Aussage
- Der Service-Anbieter muss uns vertrauen

OpenID-Service der Benutzerverwaltung

Openid:	https://openid.uni-due.de/mitarbeiter/burkhard.wald@uni-due.de
zu prüfende Behauptungen:	Ich bin Mitarbeiter der Universität Duisburg - Essen Ich habe die Mailadresse burkhard.wald@uni-due.de
Unikennung:	
Password:	
Nach erfolgter Authentifizierung:	Zurücklenken an https://openid1.zim.uni-due.de/
	Submit Cancel

Was ist anders als bei der DFN-AAI

- Kein bürokratischer Overhead einer Föderation
- Ein Service-Anbieter kann unsere OpenIDs nutzen, ohne uns zu fragen.
- Wir übermitteln keine Daten
- Der Nutzer gibt z.B. selbst seine Matrikelnummer an, in dem er die entsprechende OpenID verwendet.

Realisierung des OpenID-Providers

- http://www.packetizer.com/security/openid/
- Perl
- gut durchschaubar
- anpassbar und integrierbar, wenn man ein Perl-basiertes Selfcare-Portal für das IDM hat.

Realisierung des Service-Providers

- Apache
- Libopkele (c++ Library)
- mod_auth_openid
- Kofiguration:

```
AuthType  OpenID
require valid-user
AuthOpenIDLoginPage /login.html
```

- REMOTE_USER
  (Aus dieser Umgebungsvariablen kann die Web-Anwendung die akzeptierte OpenID lesen)

Andere Consumer

- http://www.janrain.com/openid-enabled/
  - verschieden Varianten, z.B. bei Ilias mit PHP
- https://github.com/stevelove/Dope-OpenID
  - PHP, z.B. bei TYPO3
- Für unseren Use-Case könnten die Consumer verschlankt werden.