Personalisierung mit Shibboleth

6. Shibboleth-Workshop

Frankfurt am Main, 8. Mai 2008

Bernd Oberknapp
Universitätsbibliothek Freiburg
E-Mail: bo@ub.uni-freiburg.de

Inhalt

- Personalisierung
  - Überblick
  - Bisher übliche Lösung
- Personalisierung mit Shibboleth
  - Pseudonyme (persistente NameIDs)
  - Implementierung im Identity Provider
  - Implementierung in Anwendungen
- Fazit

Was ist Personalisierung?

- Personalisierung ist laut Wikipedia die „Anpassung von Programmen, Diensten oder Informationen an die persönlichen Vorlieben, Bedürfnisse und Fähigkeiten eines Benutzers“
- Anbieter elektronischer Zeitschriften, Datenbanken und Bücher bieten häufig:
  - Suchhistorie
  - Merkliste
  - Alerts
  - RSS-Feeds
  - Voreinstellungen

Bisher übliche Lösung

- Einmalige Registrierung und Einrichtung eines „Personal Account“ (pro Anwendung…)
- Um die Personalisierung nutzen zu können, muss der Nutzer sich mit dem Personal Account einloggen (bei jeder Sitzung…)
- Der Personal Account ist dabei ein eindeutiges Merkmal für den Nutzer, unter dem die für die Personalisierung notwendigen Informationen gespeichert werden und anhand dessen der Nutzer wiedererkannt wird
- Demo: OvidSP

Lösung mit Shibboleth

- Mit Shibboleth kann das eindeutige Merkmal zur Wiedererkennung des Nutzer vom Identity Provider (IdP) geliefert werden
- Als eindeutiges Merkmal könnte im Prinzip die Benutzerkennung (eduPersonPrincipalName) oder E-Mailadresse (mail) verwendet werden
- Das ist aber nicht zu empfehlen, weil damit
  - die Identität des Nutzer offengelegt wird
  - alle Service Provider (SP) denselben Attributwert bekommen, so dass SP übergreifend Informationen über den Nutzer gesammelt werden könnten

Pseudonyme

- Diese Probleme lassen sich vermeiden, indem ein Pseudonym für den Nutzer verwendet wird – und zwar für jeden SP ein anderes
- Pseudonyme gehören in Shibboleth/SAML zu den persistenten Name Identifier (NameID)
- Shibboleth 1.3: eduPersonTargetedID
- Shibboleth 2.0:
  - eduPersonTargetedID wie bei Shibboleth 1.3
  - SAML2NameID
  - NameID Management Protokoll (bisher nur im SP implementiert)

Default-Implementierung im Shibboleth 1.3 IdP

- PersistentIDAttributeDefinition
- Die eduPersonTargetedID wird mit einem Key aus einem Java-Keystore berechnet als: SHA1(entityID(SP)+'!'+Principal+'!'+key(IdP))
- Laut Shibboleth-Wiki „for experimentation and not suitable for production use“, weil
  - kein NameID Management unterstützt wird
  - der Principal nicht aus dem NameID ermittelt werden kann (aus Datenschutzsicht ein Vorteil!)
  - NameIDs sich nicht ändern sollten, nur weil sich ein anderer Idenitifier (z.B. entityID des SP) ändert

Anforderungen

- Für das Generieren persistenter NameIDs ist ein dauerhaft gültiges, eindeutiges Merkmal für den Nutzer notwendig
- Die Benutzerkennung (uid) ist dafür nicht geeignet, falls wie in der Uni Freiburg
  - Kennungen nach Ablauf neu vergeben werden oder
  - Nutzer ihre Kennungen ändern können
- In bestimmten Fällen sollte derselbe NameID für mehrere SPs verwendet werden, z.B. wenn ein Anbieter mehrere Anwendungen betreibt (wie Elsevier mit ScienceDirect und Scopus)

Implementierung in myLogin

- Der myLogin-IdP der Uni Freiburg unterstützt Shibboleth 1.3/eduPersonTargetedID
- Die uid (Principal) ist in der Uni Freiburg nicht als Basis für das Generieren von NameIDs geeignet, deshalb wird ein anderes dauerhaft gültiges, eindeutiges Attribut „uniqueID“ auf Basis weiterer/anderer Daten generiert
- Für Accounts, die von mehreren Nutzern verwendet werden (z.B. Gruppen- und Kurs-Accounts), wird keine uniqueID und damit auch keine eduPersonTargetedID generiert

Implementierung in myLogin

- Statt die entityID des SP direkt zu verwenden, wird ein vom SP abhängiges, in einer Datenbank gespeichertes Token verwendet
  - kann bei Bedarf für mehrere SPs gleich sein
  - Änderung der entityID eines SP wäre kein Problem
- Die Berechnung erfolgt per Stored Procedure: MD5(id(IdP)+uniqueID(Principal)+token(SP))
- Die berechneten eduPersonTargetedIDs werden nicht in der Datenbank gespeichert

Default-Implementierung im Shibboleth 2.0 IdP

- StoredIDDataConnector (der ComputedID-DataConnector ist veraltet!)
- Benötigt wird eine JDBC-fähige Datenbank
- NameIDs können für ungültig erklärt und neue generiert werden (für NameID Management)
- NameIDs werden zusammen mit dem Principal in der Datenbank gespeichert, so dass der Principal sich leicht anhand des NameID ermitteln lässt
- Aus Datenschutzsicht ist das problematisch – und ob diese Funktionalität zukünftig wirklich benötigt wird, ist noch unklar.

Implementierung in der Anwendung

- Die Anwendung kann auf NameIDs wie üblich über HTTP-Header oder Environment-Variablen (Shibboleth 2.0) zugreifen
- Default-Attributname ist eduPersonTargetedID oder persistent-id (Shibboleth 2.0)
- Der NameID könnte direkt als Merkmal zum Speichern der für die Personalisierung benötigten Informationen verwendet werden
- Alternativ könnte wie bisher üblich eine Registrierung erfolgen und der Personal Account mit der NameID „verlinkt“ werden

Implementierung in der Anwendung mit Registrierung

- Der Nutzer muss sich wie bisher üblich einmal registrieren, er kann aber mit Hilfe des NameID beim Zugriff automatisch in den Personal Account eingeloggt werden
- Wechselt der Nutzer zu einer anderen Einrichtung und damit einem anderem IdP, kann der Personal Account mit seinem neuen NameID verlinkt werden – der Nutzer kann seinen Personal Account so „mitnehmen“!
- Die Personalisierung kann auch wie bisher genutzt werden, wenn der IdP für den Nutzer keinen persistenten NameID liefert

Beispiele

- Suchportal der UB Freiburg
- vascoda
- ScienceDirect
- MetaPress (Springer und 173 weitere Verlage, voraussichtlich ab Q3/2008)
- ... und hoffentlich zukünftig viele weitere Anbieter/Anwendungen

Fazit

- Die Personalisierung mit Hilfe von persistenten NameIDs ermöglicht „Single-Sign On auch für Personal Accounts“ und damit eine deutliche Verbesserung für die Nutzer
- Für jeden SP ein anderes Pseudonym zu verwenden ist im Hinblick auf den Datenschutz die bestmögliche Lösung
- Anwendungen müssen damit rechnen, nicht für alle Nutzer persistente NameIDs geliefert zu bekommen – die Bindung der Personalisierung an einen NameID sollte optional sein

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

AAR ist ein Projekt der UB Freiburg
Gefördert vom BMBF (PT-NMB+F)

http://aar.vascoda.de/
bo@ub.uni-freiburg.de

Bibliothekartag 2008

- UB Freiburg/AAR und DFN sind auf dem Bibliothekartag 2008 (3.-6. Juni in Mannheim) mit einem Stand (Nr. 218) vertreten, gemeinsam mit dem GBV (Nationallizenzen) und der DFG (Knowledge Exchange)
- Vortragssessions:
  - Einsatzmöglichkeiten und Beispiele des SSO-Verfahrens Shibboleth im Rahmen einer föderativen Umgebung: Praxisberichte (Dienstag, 3.6. 10 Uhr)
  - Europaweite Infrastruktur zur Authentifizierung und Autorisierung in einem föderativen Umfeld. Ein Statusbericht (Mittwoch, 4.6. 13 Uhr)