Shibboleth zum Mitmachen die AAR-Testumgebung

3ter AAR Workshop

Dr. Jochen Lienhard
E-Mail: lienhard@ub.uni-freiburg.de

AAR-Testumgebung- Was ist das?

- Identity Provider
- Service Provider
- Lokalisierungsdienst
- Metadatenverwaltung

- http://aar.vascoda.de/test/demo.php

Wie kann ich mitmachen?

- Jeder kann mitmachen.
- Was will man testen?
  - Identity Provider
  - Service Provider
- Wie kann ich mitmachen?
  - Beispiel: IdP
  - Beispiel: SP

Was muss ich tun? (IdP) (1)

- Tomcat (+ Apache) aufsetzen.
  - z.B. aus Linux-Distribution
- Shibboleth Software installieren.
  - Dokumentation auf der AAR Seite oder bei SWITCH oder bei Internet2
- Zertifikat erstellen/besorgen.
  - z.B. vom DFN

Was muss ich tun? (IdP) (2)

- Formular ausfüllen
  - http://aar.vascoda.de/test/idp.php
  - und abschicken.
- Zertifikat schicken
  - nur das Zertifikat, **nicht** den Key
- Bestätigung abwarten und überprüfen.

Was passiert bei AAR?

- Daten aus der Mail und Zertifikat werden in die Metadaten eingebunden.
- Metadaten werden signiert.
- Metadaten werden beim IdP, SP und WAYF aktualisiert.
- AAP.xml beim SP wird ergänzt.
- Metadaten werden dem neuen IdP geschickt bzw. mitgeteilt, wie und wo sie heruntergeladen werden können.

Was muss ich tun? (IdP) (3)

- Metadaten herunterladen und CRON-Job für das automatische Update (1mal täglich) einrichten.
  - metadatatool mit jks
- idp.xml konfigurieren
  - ProviderID, Zertifkatpfad, Relying Party, URLs, Loglevel
- arp.sites.xml konfigurieren
  - direkt aus der Bestätigungsmail übernehmen

Was muss ich tun? (IdP) (4)

- resolver.xml konfigurieren
  - LDAP, JNDI, Static
- security-constraint in Shibboleth-web.xml ergänzen und context in Tomcat-server.xml.
  - tomcat-users, LDAP, JNDI
- TESTEN und LOGFILES beobachten!

Was muss ich tun? (SP) (1)

- Apache aufsetzen.
  - z.B. aus Linux-Distribution
- Shibboleth Software installieren.
  - Dokumentation auf der AAR Seite oder bei SWITCH oder bei Internet2
- Zertifikat(e) erstellen/besorgen.
  - Server-Zertifikat für Apache, Client-Zertifikat für Shibboleth
  - z.B. vom DFN

Was muss ich tun? (SP) (2)

- Formular ausfüllen
  - http://aar.vascoda.de/test/sp.php
  - und abschicken.
- Zertifikat schicken
  - nur das Zertifikat, **nicht** den Key
- Bestätigung abwarten und überprüfen.

Was passiert bei AAR?

- Daten aus der Mail und Zertifikat werden in die Metadaten eingebunden.
- Metadaten werden signiert.
- Metadaten werden beim IdP, SP und WAYF aktualisiert.
- arp.sites.xml beim IdP wird ergänzt.
- AAP.xml für neuen SP erstellen.
- Metadaten und AAP.xml werden dem neuen SP geschickt bzw. mitgeteilt, wie und wo die Metadaten heruntergeladen werden können.

Was muss ich tun? (SP) (3)

- Metadaten herunterladen und CRON-Job für das automatische Update (1mal täglich) einrichten.
  - siterefresh mit AAR-Zertifikat
- shibboleth.xml konfigurieren
  - ProviderID, Zertifkatpfad, URLs, Loglevel
- AAP.xml konfigurieren
  - direkt aus der Mail übernehmen

Was muss ich tun? (SP) (4)

- apache(2).config konfigurieren
  - Ressource-Manager des Apache
    AuthType shibboleth
    ShibRequireSession On
    require REMOTE_USER demo

- zu schützende Datei anlegen
  - zum Auslesen der Web-Server-Variablen

- TESTEN und LOGFILES beobachten!

Typische Fehler

- Provider ID falsch eingetragen
- Firewall für Port 8443 geschlossen.
- http statt https (URL stimmt nicht)
- Kein client-Zertifikat (beim SP)
- arp.site.xml bzw. AAP.xml falsch konfiguriert.
- Falsche Relying Party
- alte Metadaten
- verschiedene Versionen von OpenSSL
- falsche Pfade in der Konfiguration
- Security Constraint und Context nicht ergänzt (IdP)
- falsche web.xml

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!