Von der Testumgebung zum produktiven Einsatz von Shibboleth

3. Shibboleth-Workshop

Freiburg, 10. Oktober 2006

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

Kein „Kochrezept“?

- Die Strukturen in den Einrichtungen, insbesondere beim **Identity Management**, und die Struktur von **Anwendungen** sind sehr **unterschiedlich**.
- Die Einführung von Shibboleth ist entsprechend ein **individueller Prozess**, ein allgemein anwendbares „Kochrezept“ gibt es dafür nicht.
- Vorgestellt werden
  - **typische Fragestellungen** und
  - **Empfehlungen** basierend auf
  - **bisherigen Erfahrungen.**

Ausgangssituation

- Die **Ausgangssituation** nach dem ersten Test in der **Testumgebung** sieht typischerweise wie folgt aus:
  - Die Identity Provider (IdP) oder Service Provider (SP) **Software ist installiert** und
  - die grundlegende **Funktionsfähigkeit ist getestet**.
  - Die **Authentifizierung** erfolgt meist über die Apache oder Tomcat „Benutzerdatenbank“, vielleicht auch schon über einen LDAP-Server.
  - Einige Webseiten oder Skripte sind über mod_shib geschützt, aber die **Autorisierung** (Attributweitergabe, Zugriffskontrolle) ist meist nur grundsätzlich getestet.
- **Und wie geht es weiter?**

Grundlegende Fragen

- Wie soll Shibboleth **in die vorhandene Umgebung integriert** werden?
  - IdP: Konzept für ein **Single Sign-on** (in Intranet) und die Integration in das **Identity Management**
  - SP: Integration in die **Anwendung(en)**
  - IdP/SP: Integration in die **technischen und organisatorischen Workflows**
- Welcher Föderation oder **welchen Föderationen** tritt man bei?
  - IdP: Welche **Dienste** sollen genutzt werden?
  - SP: Welches sind die **nutzenden Einrichtungen**?

Welche Föderationen?

- Aus dem Betritt zu einer **Föderation** ergeben sich im Allgemeinen **(Mindest-)Anforderungen** an
  - das **Identity Management** (für IdPs),
  - die **Sicherheit**, insbesondere was
  - die verwendeten **Zertifikate** betrifft,
  - die **Attribute** für den Datenaustausch und
  - den **Datenschutz**.
- Föderationen unterstützen die Teilnehmer im Allgemeinen aber auch in diesen Fragen!

Webserver-Zertifikate

- Die Zertifikate für Webserver, die Dienste für die Nutzer anbieten, sind **unabhängig von Shibboleth**.
- Für **IdPs** ist ein Zertifikat **erforderlich**, um die Authentifizierung der Nutzer zu schützen.
- Für **SPs** ist ein Zertifikat **dringend zu empfehlen**, wenigstens um den Aufbau der Shibboleth-Sitzung und den Shibboleth Session-Cookie zu schützen!
- Die Zertifikate sollten idealerweise automatisch von den gängigen Browsern verifiziert werden können.

SP: Grundlegende Fragen

- Wie werden die **Ressourcen** bisher **geschützt** (Apache, Tomcat, eigenes Verfahren, ...)?
- Existiert ein **Sitzungsmanagement**?
- Kann dieses weiter verwendet werden, z.B. indem eine Sitzung über Shibboleth aufgebaut wird?
- Existiert eine **Rechteverwaltung**?
- Können die notwendigen Informationen über die Nutzer von den IdPs über **Attribute** bereitgestellt werden? Welche Alternativen gibt es, falls nicht?
- Welche **neuen Dienste** können mit Shibboleth angeboten werden? Personalisierung?

SP: Apache/mod_shib

- Wird bisher **IP-Kontrolle** oder **Apache Basic Authentifizierung** verwendet, kann dies meistens sehr **einfach durch Shibboleth ersetzt** werden!
- Benötigt die Anwendung den **REMOTE_USER**, so kann dieser über ein **Attribut** (zum Beispiel eduPersonPrincipalName) bereitgestellt werden.
- Es können **Kombinationen von Attributen** als Autorisierungskriterium verwendet werden.
- Beim IIS gibt es vergleichbare Möglichkeiten.

SP: Lazy Session

- Interessant für **komplexere Anwendungen**: Shibboleth stellt die vom IdP gelieferten Attribute der **Anwendung** zur Verfügung, die damit **selbst die Zugriffkontrolle** durchführen kann.
- **Lazy Session**: Die Anwendung stößt auch den Shibboleth-Prozess selbst an (per SessionInitiator).
- Shibboleth **zusätzlich** zu anderen Verfahren zu implementieren ist häufig unproblematisch.
- Alternative: Die Authentifizierung **komplett auf Shibboleth umstellen** und damit die Benutzer-verwaltung von der Anwendung entkoppeln!

Virtuelle Heimateinrichtungen

- Nutzer, die keiner Einrichtung zugeordnet werden können oder deren Einrichtung Shibboleth (noch) nicht unterstützt, können einer **virtuellen Heimat-einrichtung** (**VHO**) zugeordnet werden.
- Beispiele:
  - Zugriff auf **DFG-Nationallizenzen** durch Privatnutzer
  - Zugriff auf Bibliotheksanwendungen der UB Freiburg durch Mitarbeiter externer Bibliotheken (VHO Freiburg)
- Möglichkeit für **kommerzielle Anbieter**:
  VHO auf Basis der eigenen **Kundendatenbank**

SP: IdP Discovery

- **IdP Discovery-Problem**: Wie kommt der Nutzer vom SP zum IdP seiner Einrichtung?
- Antwort: Lokalisierungsdienst (WAYF), aber:

  „The **WAYF concept is broken by design** and **cannot handle multiple federations** in practice, although in many constrained situations it can appear to.“ (Scott Cantor)

- Wenn ein SP mehr als einer Föderation angehört, sollte er eine **eigene Einrichtungsauswahl** in die Anwendung integrieren!

SP: Zertifikate

- SPs benötigen für Shibboleth 1.3 ein Zertifikat für **SSL Client** und **Signing** (Shibboleth 2.0: zusätzlich **Encryption** oder Encryption statt SSL-Client?)
- Einige Föderationen wie InCommon und HAKA verlangen (noch), dass **Zertifikate bestimmter CAs** verwendet werden. Ein SP, der an mehreren Föderationen teilnimmt, muss gegebenenfalls also **mehrere Zertifikate** verwenden!
- DFN-AAI: Es sollen **Zertifikate von allen CAs** akzeptiert werden, die die **Policyanforderungen der DFN-PKI** erfüllen.

IdP: Grundlegende Fragen

- Der **Aufbau eines IdP für eine Einrichtung** ist deutlich aufwendiger als die Implementierung von Shibboleth in einer Anwendung. Wer einen IdP aufbaut, plant meistens auch den Betrieb von SPs!
- Wie könnte ein **Konzept für ein Single Sign-on (SSO)** für die eigenen SPs im Intranet aussehen?
- Wie wird der **IdP in das Identity Management (IdM) integriert**?
- Wie wird die **Verfügbarkeit** (Ausfallsicherheit) des IdP gewährleistet? Wenn der IdP ausfällt, kann man sich in keinen SP mehr einloggen...

IdP: Single Sign-on Konzept

- Falls ein **SSO** (im Intranet) **vorhanden** ist: Soll es mit Shibboleth **integriert** oder durch Shibboleth **ersetzt** werden?
- **Analyse der eigenen Anwendungen**:
  - Welche davon kommen für ein SSO in Frage?
  - Welches sind die **Killerapplikationen**? Diese sollten zuerst umgestellt werden!
- Single Logout? Erst mit Shibboleth 2.0...
- **SSO** als eigenen **Dienst** positionieren?

IdP: Authentifizierung

- Welche **Quellen für Identitäten** gibt es?
- Auch wenn ein Identity Management vorhanden ist, gibt es **Problemfälle** wie
  - Universitätskliniken
  - Bibliotheken: **Walk-in User**
- **Authentifizierungsverfahren**:
  - Welche Verfahren kommen in Frage?
  - Welche **Anforderungen** gibt es seitens der Anwendungen? (Stichwort: Level of Assurance)

IdP: Autorisierung/Attribute

- **Welche Attribute kann das IdM liefern**?
- **Welche Attribute werden für Shibboleth benötigt**? Dies hängt von den Anwendungen ab und ist je nach Anwendungsbereich (Bibliothek, Grid, eLearning, ...) sehr unterschiedlich!
- Wie werden die Attribute aus dem IdM **eindeutig** auf die Attribute für Shibboleth **abgebildet**?
- Wie werden **eduPersonTargetedID** und andere Shibboleth spezifische Attribute gehandhabt?
- Eventuell ergeben sich daraus neue **Anforderungen an das IdM**!

Beispiel: Freiburger IdP

- Tomcat-Authentifizierung mit Anbindung an **drei Benutzerdatenbanken** über eigenen JAAS-Realm:
  - LDAP-Server des **Rechenzentrums**
  - LDAP-Server des **Klinikums**
  - Ausleihsystem der **Bibliothek**
- Lösung für **Walk-in User**: Mapping von IP-Adressen auf Pseudo-Accounts und Login über Ausleihsystem
- Autorisierung über **Attribute** aus den **LDAP-Servern**, dem **Ausleihsystem** und einer **eigenen Rechtedatenbank** (SQL)

IdP: Benutzerschnittstelle

- Die **Login-Maske** ist der zentrale Punkt, hier muss alles Wesentliche erklärt werden:
  - Was bedeutet es, wenn man sich einloggt?
  - Wie loggt man sich wieder aus?
  - Dokumentation und Support!
- Beispiel: University of Washington
- Kontrolle der **Attributfreigabe** durch den Nutzer bei personenbezogen Daten: **Autograph** mit sehr intuitivem Visitenkartenmodell.
- **SSO als eigenen Dienst positionieren!**

IdP: Zertifikate

- IdPs benötigen für Shibboleth 1.3 ein Zertifikat für **SSL Server** und **Signing** (Shibboleth 2.0: zusätzlich **Encryption** oder Encryption statt SSL Server?)
- DFN-AAI: DFN-Mitglieder können und sollten **Zertifikate der DFN-PKI** verwenden!
- Mit den Zertifikaten der DFN-PKI sollte sich in den meisten Fällen vermeiden lassen, dass verschiedene Zertifikate für verschiedene Föderationen (und damit verschiedene Kommunikationsendpunkte im IdP) verwendet werden müssen.

Noch ein paar Kleinigkeiten...

- Die Einführung von Shibboleth wirkt sich sowohl auf die **Technik** als auch auf die **Organisation** aus. Die Worksflows müssen angepasst werden!
- Technik:
  - Aktualisierung der Metadaten
  - Aktualisierung der APRs/AAPs
  - Security-Fixes
  - Logging?
- Dokumentation und Support
- Werbung für Shibboleth machen! 

...zum Schluss.

Das waren **jede Menge Fragen**...
...und zumindest **einige Antworten**.

Haben Sie noch Fragen?

Vielen Dank für Ihre Aufmerksamkeit!