Stand der Entwicklung von Shibboleth 2

5. Shibboleth-Workshop

Berlin, 17. Oktober 2007

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

Übersicht

- Offizieller Status
- Kommunikation IdP–SP:
  - Authentication Request
  - Bindings
  - Single Logout
- Identity Provider:
  - Architektur
  - Authentication Handler
  - Attribute Resolver und Filtering Engine
- WAYF/Discovery Service
- Fazit

Offizieller Status

- Seit Ende Juli Alpha (ausgewählte Tester)
- Seit Mitte September Beta (allgemeiner Test)
- Komponenten im Betatest:
  - C++ Service Provider (SP)
  - Java Identity Provider (IdP)
- WAYF/Discovery Service: Technical Preview
- Java SP: Erst nach der 2.0 Release…
- Release-Datum ist immer noch unklar!

Kommunikation IdP–SP

(Protokolle und Bindings)

Authentication Request

- In Shibboleth 1.3 einfacher Redirect zum IdP, in Shibboleth 2.0/SAML 2.0 XML-Request (über SSL 3.0 oder TLS 1.0, optional signiert)
- SP kann
  - vorgeben, welche Authentication Context Classes (z.B. PasswordProtectedTransport) verwendet werden dürfen
  - verlangen, dass der Benutzer sich erneut authentifiziert (forceAuthn)
  - verlangen, dass am IdP keine Interaktion mit dem Benutzer erfolgt (isPassive)

Bindings

- Folgende Bindings werden unterstützt:
  - SAML1-Bindings wie bei Shibboleth 1.3
  - SAML2-Varianten der SAML1-Bindings
  - SAML2 HTTP Redirect (GET, IdP/SSO)
  - SAML2 HTTP POST (IdP/SSO)
  - SAML2 HTTP POST „SimpleSign“ (IdP und SP)
- SAML2-Bindings werden bevorzugt
- Beispiel: HTTP Redirect für den Authentication Request des SP an den IdP und HTTP POST (mit Attribute Push) für die Antwort

Single Logout

- Single Logout (SLO) beendet die Session im IdP und die zugehörigen Sessions in allen SPs, in die der Nutzer eingeloggt worden ist
- SLO kann erfolgen:
  - asynchron (Front-Channel) über den Browser (HTTP Redirect, POST oder Artifact, empfohlen)
  - oder synchron (Back-Channel) über SOAP
- SLO kann im SP oder im IdP initiiert werden
- Anwendungen-Sessions müssen ebenfalls beendet werden (erfordert Anpassungen bei Anwendungen mit Session-Management)

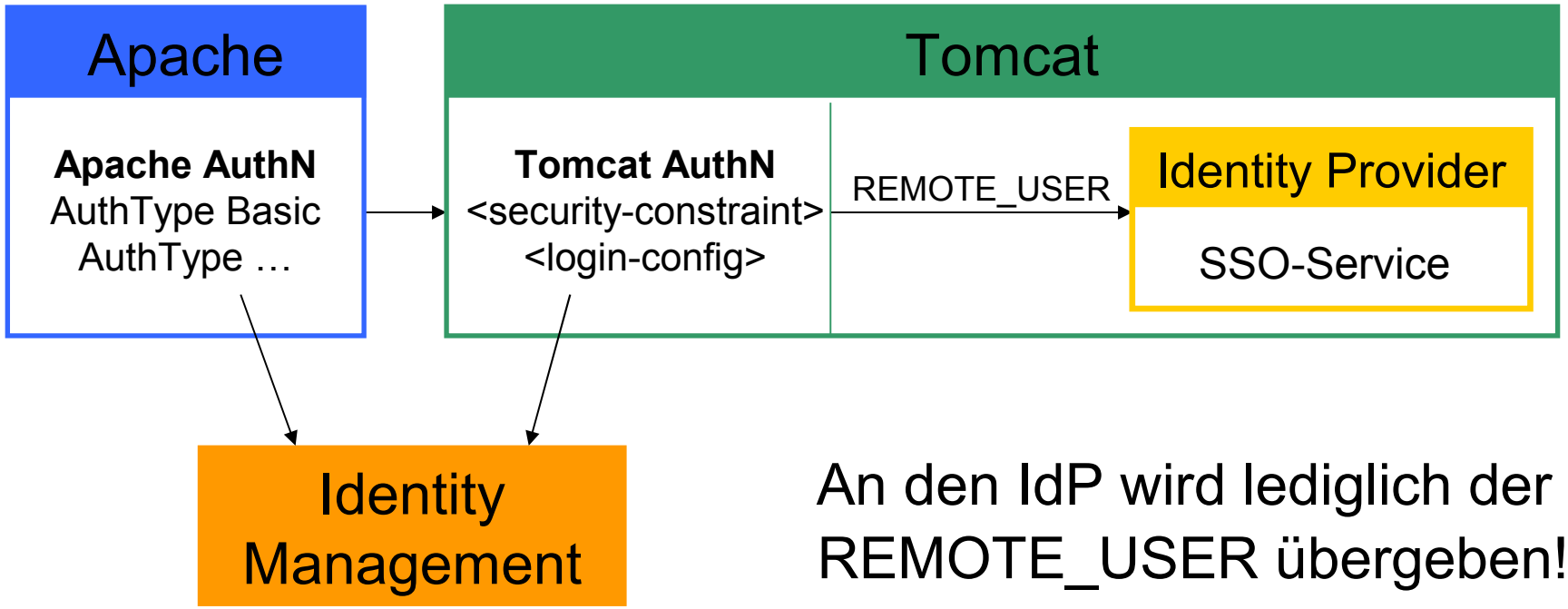
Status Kommunikation

- Authentication Request und SAML2-Bindings sind weitestgehend implementiert, aber noch nicht besonders gründlich getestet
- Single Logout ist momentan nur im SP implementiert und kann daher nur mit nicht-Shibboleth IdPs getestet werden
- Dokumentation lässt momentan noch zu wünschen übrig, was das Testen erschwert

Identity Provider

IdP 1.3 Architektur

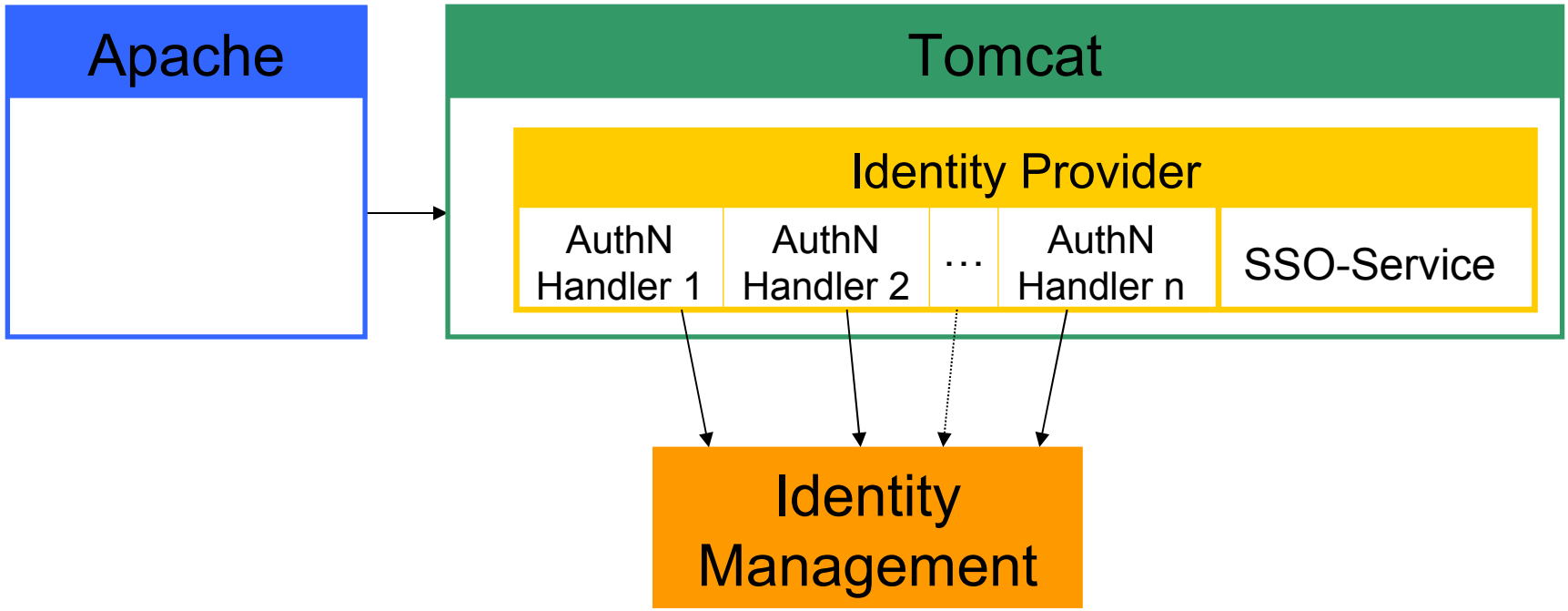
Bei Shibboleth 1.3 muss der SSO-Service des IdP durch eine Authentifizierung geschützt werden, z.B. über den Apache oder Tomcat:



An den IdP wird lediglich der REMOTE_USER übergeben!

IdP 2.0 Architektur

Bei Shibboleth 2.0 übernimmt der IdP die Kontrolle über die Authentifizierung. Die Authentifizierung erfolgt dabei über Authentication Handler:



Authentication Handler

- Authentication Handler werden abhängig von vorgegebenen Authentication Context Classes aufgerufen
- Authentication Handler erhalten zur Durchführung der Authentifizierung die vollständige Kontrolle
- Mitgeliefert werden bei Shibboleth 2.0 mindestens Authentication Handler für
  - Benutzerkennung/Passwort (über JAAS)
  - REMOTE_USER (ähnlich wie bei Shibboleth 1.3)
  - IP basierte Authentifizierung

Attribute Resolver

- Zusätzliche Attribute Connectors, u.a.
  - zum Extrahieren von Attributen aus SAML Attribute Statements und
  - zur Einbindung von Skripten
- Attribute Encoder zur Übersetzung der Attribute in Protokoll spezifische Darstellungen
- Principal Connectors zur Übersetzung von NameIDs in UserIDs und umgekehrt (NameIDs werden wie Attribute behandelt)
- Zugriff auf alle relevanten Informationen

Attribute Filtering Engine

- Attribute Filtering Engine
  - erstellt die Liste der benötigten Attribute
  - filtert Attribute und Attributwerte
  - filtert NameIDs abhängig von der Relying Party
- Stark erweiterte Filtermöglichkeiten inklusive der Möglichkeit, eigene Filter zu definieren
- Attribute Release Policies (ARPs) für
  - Benutzergruppen
  - Gruppen von SPs
- ARP Constraints

Status Identity Provider

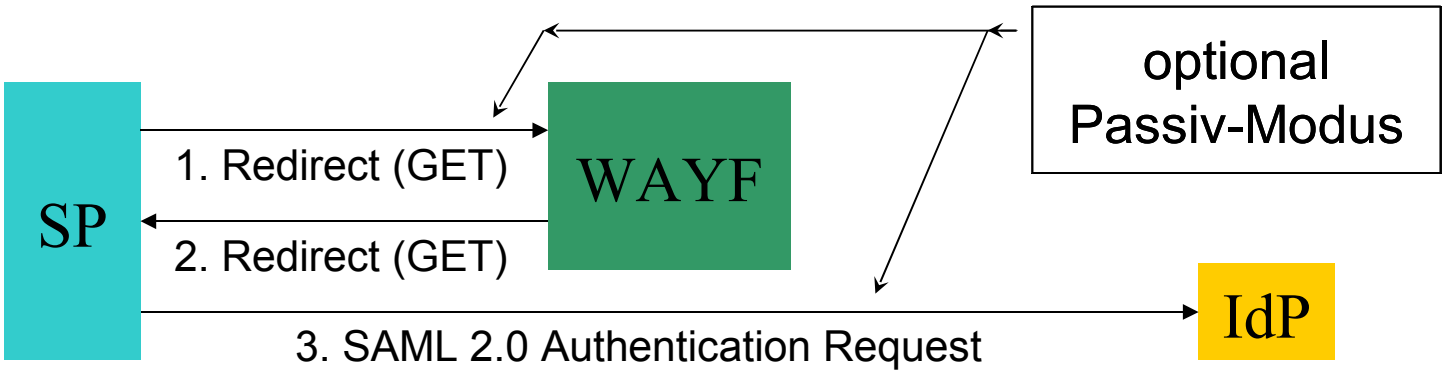
- Authentication Handler und Attribute Resolver und Filtering Engine scheinen weitestgehend implementiert zu sein
- Das Testen ist momentan noch schwierig:
  - die Dokumentation lässt noch zu wünschen übrig
  - es gibt umfangreichen Änderungen in der Konfiguration gegenüber Shibboleth 1.3
  - SAML2-Funktionalität erfordert SAML2-NameIDs
- Neben dem Single Logout fehlen angeblich noch weitere Funktionen im IdP, was genau ist aber unklar…

WAYF/Discovery Service

IdP Discovery

- Bei Shibboleth 1.3 wird der Nutzer vom SP über den WAYF zum IdP geleitet:

- Bei Shibboleth 2.0 gibt ein neues Protokoll dem SP mehr Kontrolle über den Discovery Prozess:



Discovery Service

- WAYF/Discovery Service wird offiziell unterstützt
- Implementiert als Java Servlet
- Unterstützung für mehrere Förderationen
- Plugins zur Filterung der IdP-Listen
- Integration in eine Anwendung sollte damit vergleichsweise einfach möglich sein

Status Discovery Service

- Bisher keine offizielle Beta, sondern nur eine Technical Preview (seit Anfang des Jahres)
- Aktuelle Entwicklungsversion (Subversion) funktioniert offenbar stabil und unterstützt unter anderem auch das neue Discovery Service Protokoll
- SP unterstützt das neue Protokoll ebenfalls (vollständig?)
- Für den Discovery Service erforderliche Metadaten-Extension ist auch implementiert

Fazit

Zusammenfassung

- C++ SP ist am weitesten fortgeschritten:
  - weitestgehend „Feature Complete“, teilweise aber noch nicht besonders gut getestet
  - Installation und Konfiguration sind vergleichsweise einfach, weitgehend identisch mit Shibboleth 1.3
- Java IdP ist leider noch nicht ganz so weit, einige Funktionen fehlen noch…
- Testen der SAML2-Funktionalität wird noch durch fehlende Dokumentation erschwert
- Interoperabilität mit Shibboleth 1.3 ist offenbar wie versprochen voll gegeben

Empfehlungen

- Warten Sie nicht auf Shibboleth 2, sondern fangen Sie jetzt mit Shibboleth 1.3 an!
- Wenn Sie den SP auf einer 64 Bit-Plattform betreiben wollen, sollten Sie sich allerdings gleich den 2.0 Beta SP anschauen
- Helfen Sie möglichst beim Testen der 2.0 Beta – je mehr testen, desto schneller wird es eine Release geben! Für einen Test des IdP sollte man viel Erfahrung mit Shibboleth 1.3 haben…

Vielen Dank für Ihre Aufmerksamkeit!