Neuerungen bei Shibboleth 2

Shibboleth-Workshop BW

Stuttgart, 7. Februar 2008

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

Übersicht

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

Aktueller Status

- Nach über einem halben Jahr Alpha- und Betatestphase gibt es seit Ende Januar den ersten Release Candidat (RC1)
- RC2 soll in Kürze folgen und eine ganze Reihe von Fehlern und Problemen im RC1 beheben
- Nicht im RC1 und damit wohl auch nicht in der ersten Shibboleth 2.0 Release enthalten sind:
  - Single Logout (soll bald nachgereicht werden)
  - Java Service Provider (wird noch länger dauern...)

Kommunikation IdP–SP

(Protokolle und Bindings)

Authentication Request

- In Shibboleth 1.3 einfacher Redirect zum IdP, in Shibboleth 2/SAML 2 XML-Request (über SSL 3.0 oder TLS 1.0, optional signiert)
- SP kann
  - vorgeben, welche Authentication Context Classes (z.B. PasswordProtectedTransport oder Mobile-TwoFactorContract) 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

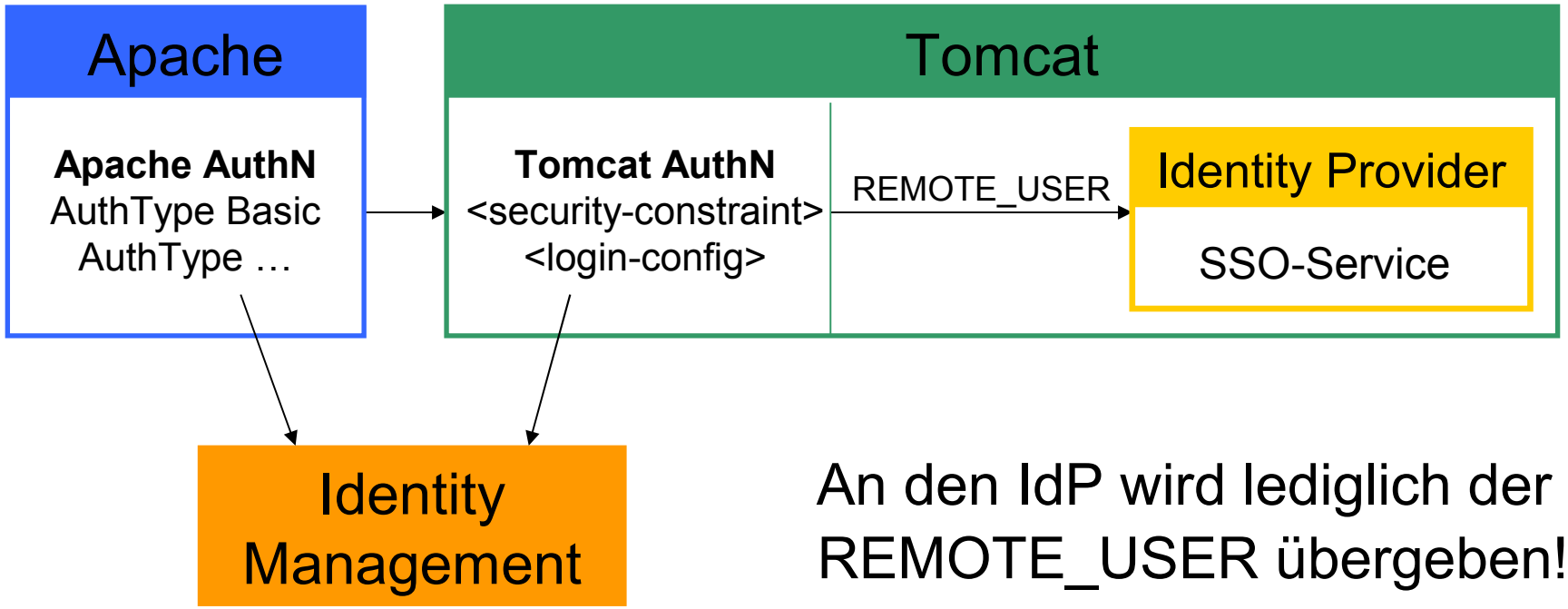
Single Logout

- 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)
  - 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)

Identity Provider

IdP 1.3 Architektur

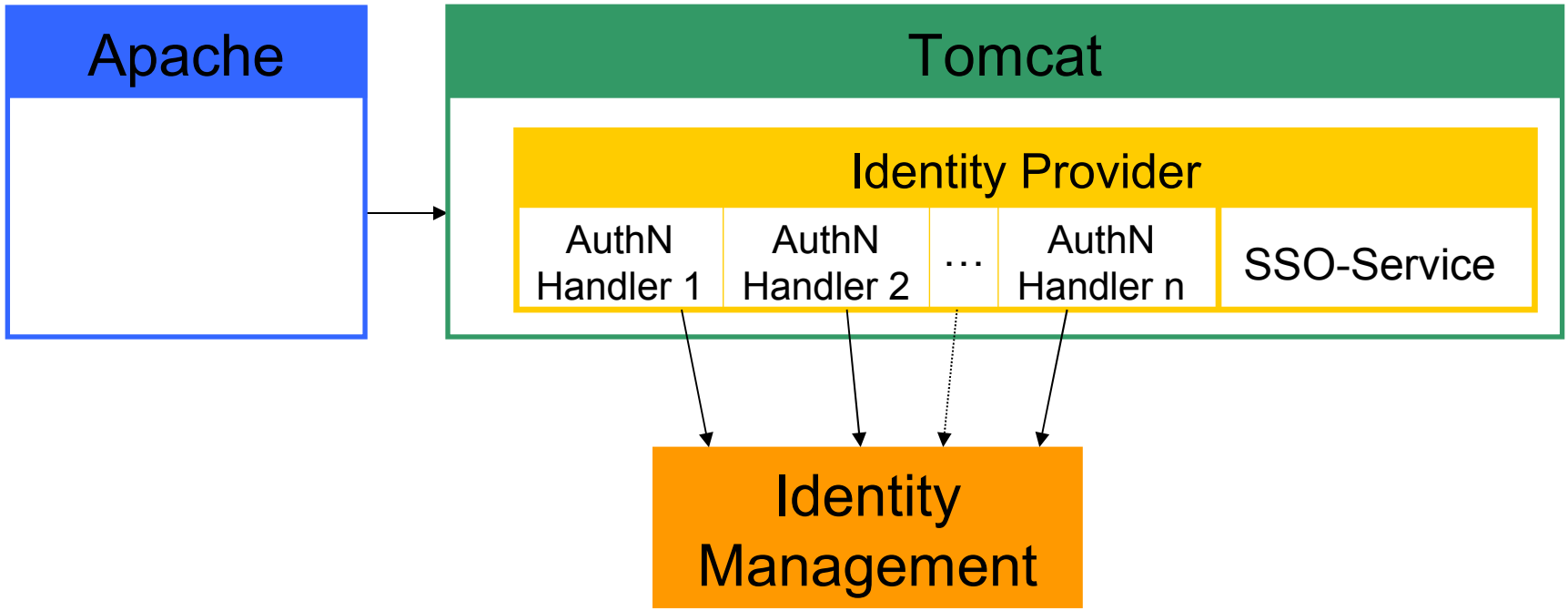
Bei Shibboleth 1.3 muss der SSO-Service des IdP durch eine Authentifizierung geschützt werden, z.B. über den Apache oder Tomcat:



An den IdP wird lediglich der REMOTE_USER übergeben!

IdP 2 Architektur

Bei Shibboleth 2 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 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

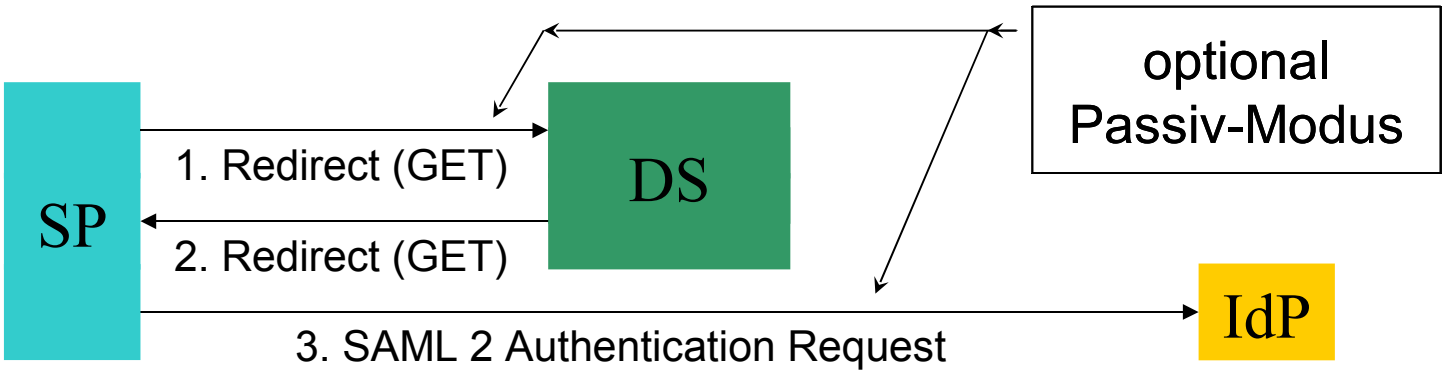
- Attribute Filtering Engine
  - erstellt die Liste der benötigten Attribute
  - filtert Attribute und Attributwerte
  - filtert NameIDs abhängig von der Relying Party
- Stark erweiterte Filtermöglichkeiten inklusive der Möglichkeit, eigene Filter zu definieren
- Attribute Release Policies (ARPs) für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

Discovery Service

IdP Discovery

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

- Bei Shibboleth 2 gibt ein neues Protokoll dem SP mehr Kontrolle über den Discovery Prozess:



Discovery Service

- Discovery Service, implementiert als Java Servlet, wird jetzt offiziell unterstützt
- Discovery Service unterstützt
  - SAML2 Discovery Service-Protokoll
  - Shibboleth 1.3 WAYF-Protokoll
  - mehrere Förderationen (MetadataProvider)
  - Plugins zur Filterung der IdP-Listen
- Integration in Anwendungen sollte vergleichsweise einfach möglich sein

Fazit

Zusammenfassung

- Shibboleth 2 bietet
  - viele neue Funktionen auf Basis der erweiterten Möglichkeiten von SAML 2
  - viele Verbesserungen, basierend auf den Erfahrungen mit Shibboleth 1.x, insbesondere
  - Vereinfachungen bei der Attribute-Abfrage (Attribute Push ist Default, kein Timeout und Refresh für Attribute)
- Single Logout wird in der ersten Shibboleth 2.0 Release noch fehlen, es wird aber hoffentlich bald nachgereicht

Empfehlungen

- Wenn Sie jetzt mit Shibboleth anfangen, nehmen Sie bitte gleich Shibboleth 2.0
- Wenn Sie schon mit Shibboleth 1.3 arbeiten, sollten Sie sich Shibboleth 2.0 möglichst bald anschauen
- Dies gilt insbesondere, wenn Sie einen IdP betreiben, da es beim IdP (im Gegensatz zum SP) umfangreiche Änderungen gegenüber Shibboleth 1.3 gibt
- Testen Sie möglichst auch gegen Shibboleth 1.3
- Die AAR-Testumgebung ist bereits auf Shibboleth 2.0 umgestellt

Vielen Dank für Ihre Aufmerksamkeit!