Bundesministerium
für Bildung
und Forschung

Ausblick auf Shibboleth 2.0

4. Shibboleth-Workshop

Berlin, 28. Februar 2007

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

Übersicht

- OpenSAML 2.0
- Stand der Entwicklung
- Shibboleth 2.0 und SAML 2.0 Konzepte:
  - Authentication Context
  - Authentication Request
  - Single Logout
- Shibboleth 2.0 Komponenten:
  - Identity Provider
  - Service Provider
  - Discovery Service
- Ausblick auf Shibboleth 2.x

OpenSAML 2.0

- SAML 2.0 ist eine gemeinsame Weiterentwicklung der SAML 1.1-Spezifikation durch die Liberty- und Shibboleth-Community
- OpenSAML 2.0
  - „complete rewrite“
  - unterstützt SAML 2.0, 1.1 und 1.0
  - unterstützt XML Signing und Encryption
- Lizenz: Apache 2.0
- „as open as things get these days“

Stand der Entwicklung

- OpenSAML 2.0: Entwicklung ist weitgehend abgeschlossen
- Identity Provider (IdP), Service Provider (SP) und Discovery Service (WAYF) 2.0:
  - Spezifikationen liegen komplett vor
  - erste Komponenten sind in der Entwicklung (siehe ShibTwoRoadmap)
  - Java-Komponenten mit Spring 2.0
- Entwicklung ist „reasonably on track“ (Zitat Scott Cantor)
- Release-Datum ist noch unklar!

Shibboleth 2.0

- Interoperabilität mit Shibboleth
  - 1.3: uneingeschränkt
  - 1.2: voraussichtlich nur eingeschränkt
  - 1.1: sehr eingeschränkt, wenn überhaupt
- Unterstützung für SAML 2.0
  - Authentication Request und Context Classes inklusive Reauthentication, Passiv-Modus, NameIDPolicy, verschiedene NameID-Formate, ...
  - Single Logout (SLO)
- Browser/POST mit Attribute-Push als Default-Profil – erfordert XML Encryption und damit Inline-Zertifikate in den Metadaten!

Authentication Context

- XML Schema zur Beschreibung des gesamten Authentifizierungsprozesses inklusive der organisatorischen und technischen Verfahren
- Vergleichbar mit Level of Assurance
- Sehr komplex, deshalb werden üblicherweise vordefinierte Authentication Context Classes verwendet
- Beispiele für Authentication Context Classes:
  - Internet Protocol
  - PasswordProtectedTransport
  - SmartcardPKI
  - MobileTwoFactorContract

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 (minimal/maximal) verwendet werden dürfen
  - verlangen, dass der Benutzer sich erneut authentifiziert (ForceAuthn)
  - verlangen, dass keine Interaktion mit dem Benutzer erfolgt (IsPassive)

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, d.h, Anwendungen mit eigenem Session-Management müssen angepasst werden!

IdP 2.0 Komponenten

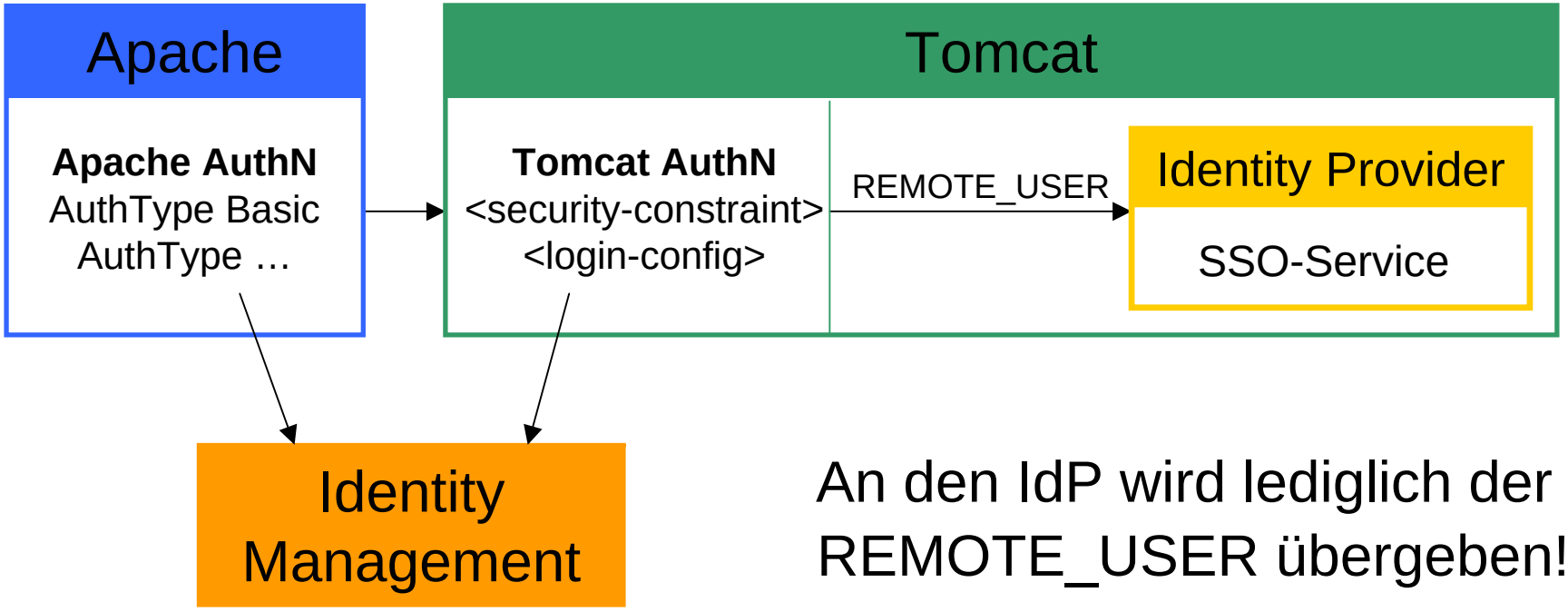
- Profile Endpoints
- Profile Handler
- Session-Manager
- Authentication Handler
- Attribute Resolver
- Attribute Filtering Engine
  (Shibboleth 1.3: ARP-Engine)

Session-Manager

- SSO/Authentication Context- und SLO-Unterstützung bei Shibboleth 2.0 stellen im Vergleich zu Shibboleth 1.3 deutlich höhere Anforderungen an das Session-Management
- Session-Manager führt Buch über:
  - UserID (Principal Name)
  - verwendete Authentifizierungsverfahren (Authentication Context Classes)
  - Logins in SPs inklusive der verwendeten NameIDs und Authentication Context Classes
  - Zugriffszeiten und Timeouts

IdP 1.3 Architektur

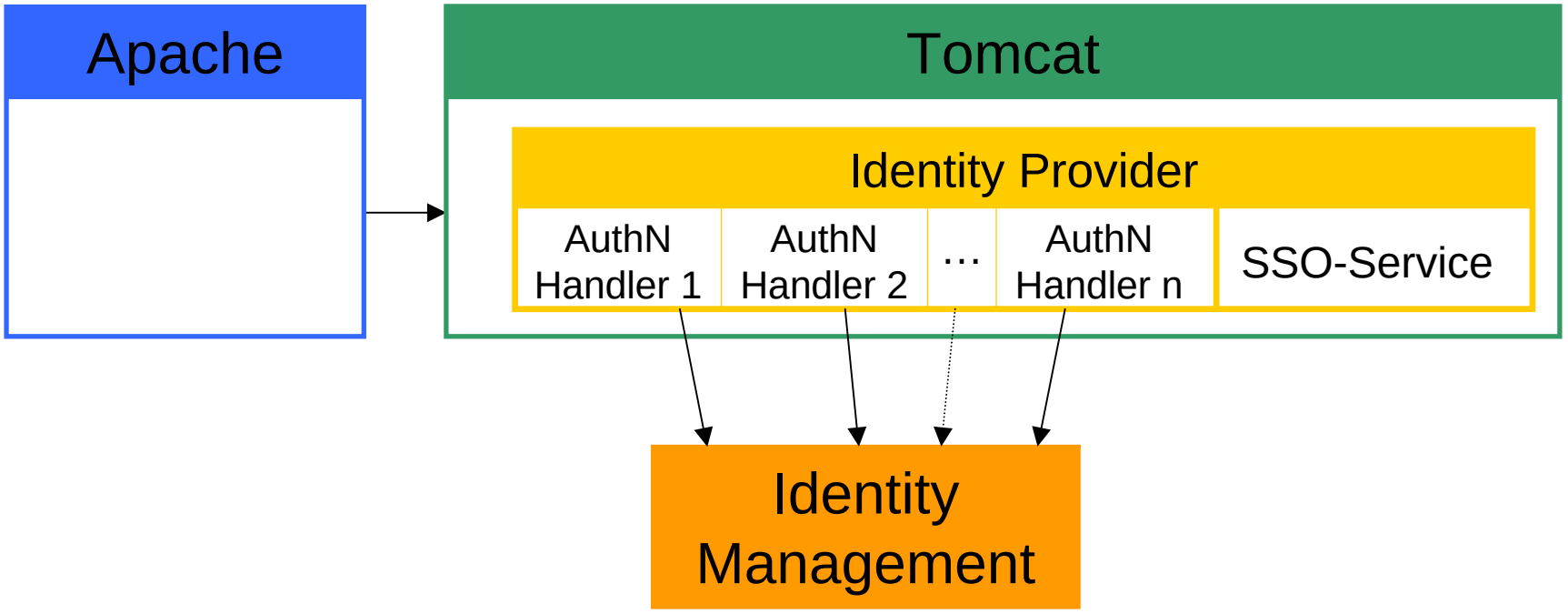
Bei Shibboleth 1.3 muss der SSO-Service des IdP durch eine Authentifizierung geschützt werden, z.B. über den Apache oder Tomcat:



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 den 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-Authentifizierung
  - 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
- ARPs für
  - Benutzergruppen
  - Gruppen von SPs
- ARP Constraints

C++ SP 2.0

- Kein Timeout und Refresh für Attribute
- Support für Clustering über Schnittstelle für ODBC-fähige Datenbanken
- Übergabe der Attribute an die Anwendung über Environment-Variablen statt HTTP-Header (wegen Problemen mit der Längenbegrenzung bei HTTP-Headern)
- Schnittstelle zu Anwendungen für SLO?

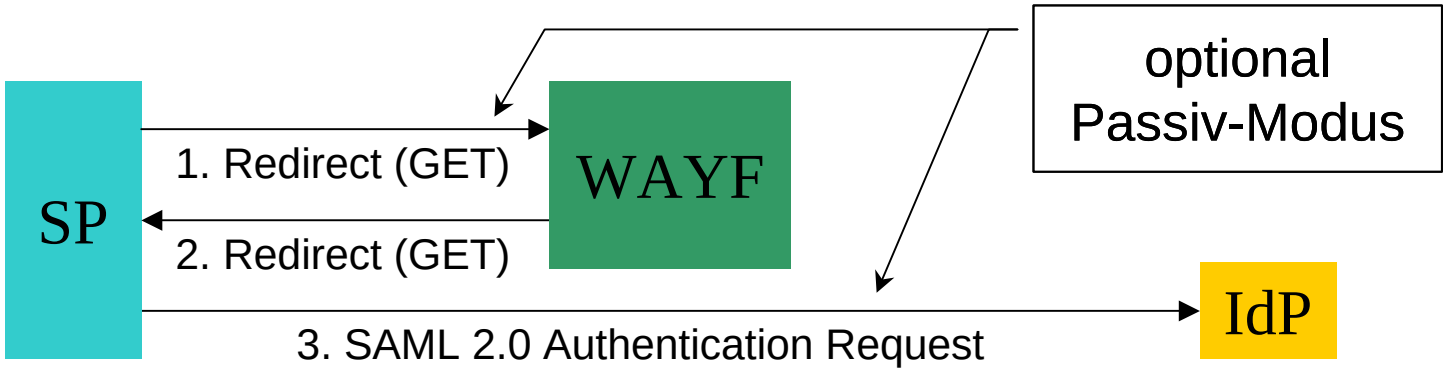
Java SP 2.0

- Es wird einen Java SP geben!
- Implementiert als Java Servlet Filter
- Attribute werden der Anwendung als Request- oder Session-Attribute zur Verfügung gestellt
- Java SP wird Attribute Resolver und Attribute Filtering Engine enthalten (wie der IdP, auf derselben Code-Basis)

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 2.0

- Discovery Service (WAYF), implementiert als Java Servlet, wird offiziell unterstützt
- Neues Protokoll gibt dem SP mehr Kontrolle über den Discovery Prozess
- Modus ohne Interaktion mit dem Nutzer (isPassive)
- Unterstützung für mehrere Förderationen
- Plugins zur Filterung der IdP-Listen
- Integration in eine Anwendung sollte damit vergleichsweise einfach möglich sein

Ausblick: Shibboleth 2.1

- NameID Management und Mapping
- SAML 2.0 angewandt auf Portale, Metasuche und Web Services (Multi-tier Anwendungen)
- Priorität werden Web Services (SOAP) haben
- Basis wird voraussichtlich Liberty ID WSF 2.0 sein, wesentliche Komponenten sind:
  - Delegation (modelliert über SubjectConfirmation)
  - SOAP Binding (WSF Security)
  - SAML Token Service (WSF Authentication)

Zusammenfassung

Shibboleth 2.0 bietet

- viele neue Funktionen auf Basis der erweiterten Möglichkeiten von SAML 2.0 und
- viele Verbesserungen, basierend auf den Erfahrungen mit Shibboleth 1.x

Warten Sie trotzdem nicht auf Shibboleth 2.0!

Vielen Dank für Ihre Aufmerksamkeit!