

# Shibboleth Single-Sign-On für Web-Anwendungen

**HRZ**  
Uni Marburg

Manuel Haim, Stand 10/2011



# Die Philipps-Universität Marburg

- gegründet 1527
- ca. 20.000 Studierende
- ca. 3.000 Mitarbeiter



# Warum Shibboleth?

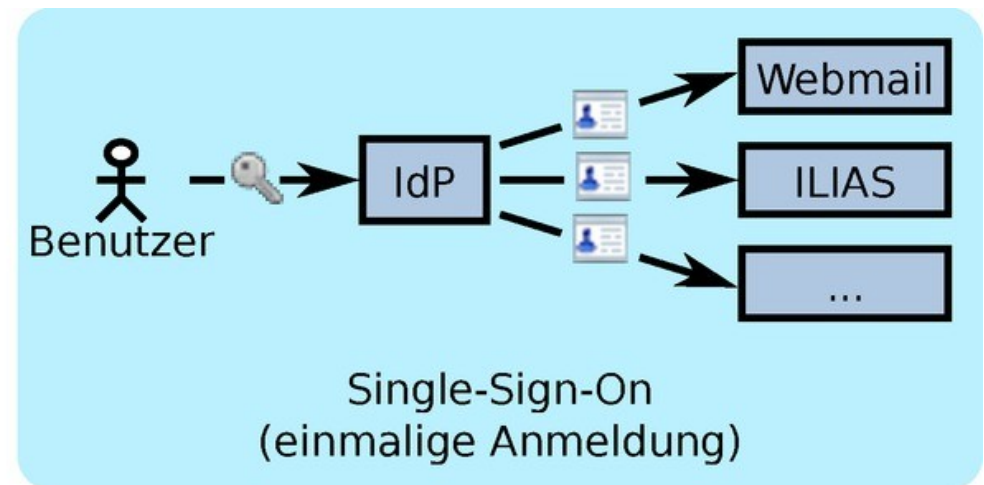
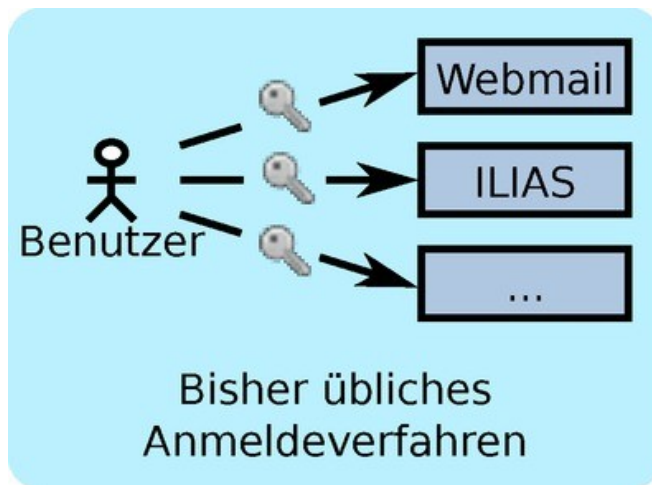


- **Authentifizierungsdienst:**  
zentrale Anmeldeseite für alle Web-Dienste (vgl. OpenID, Facebook, ...)
- **De-facto-Standard:**  
im Bibliotheksumfeld international verbreitet ← **Problem:**  
DFN-AAI fordert:  
Benutzerdaten max.  
zwei Wochen alt!
- **Nutzerfreundlich:**  
installationsfreie Alternative zu VPN-Zugang
- **Integration bestehender Web-Anwendungen:**  
einmal anmelden → alle Dienste nutzen ← **Unser Nahziel:**  
Shibboleth für lokale  
Web-Anwendungen



# Was kann Shibboleth?

- nimmt einmalig Anmeldung entgegen und erhält sie aufrecht
- übermittelt als „Identity Provider“ eine anwendungsabhängige Liste von personenbezogenen Daten an die jeweilige Web-Anwendung



## Anwendungsbeispiel:

ILIAS-Nachrichten gehen an Webmail, aber der Seitenwechsel erfordert ein erneutes Login.

ILIAS-Test

Angemeldet als Manuel Haim » Abmelden

Persönlicher Schreibtisch Magazin Suche Mail Administration Zuletzt besucht

Persönlicher Schreibtisch

Übersicht Persönliches Profil Nachrichten Kalender Notizen und Kommentare Bookmarks Kontakte

Webmail :: Willkommen bei Home.HRZ - Mozilla Firefox

uni-marburg.de https://home.hrz.uni-marburg.de/imp/login.php?imapuser=haimm

Philipps-Universität Marburg

Home.HRZ

- Anmeldung
- Bedienungsanleitung
- Terminverwaltung
- Zertifikatsprobleme
- Problem?

Webmail, Terminplaner, ...

» Universität » Home.HRZ

Bitte anmelden

Benutzername: haimm

Passwort:

Sprache: Deutsch

Modus: Traditionell

Anmelden

!!!-----!!!

Vorsicht: Immer wieder sind betrügerische E-Mails im Umlauf, in denen Sie dazu aufgefordert werden, Ihre Zugangsdaten (Benutzername, E-Mail-Adresse, Passwort) per E-Mail oder über eine externe Web-Seite preiszugeben. Bitte reagieren Sie nicht auf solche E-Mails. Die Preisgabe Ihrer Zugangsdaten kann erhebliche Folgen für alle Nutzer aus der Universität Marburg haben, insbes. die generelle Ablehnung des

Angebote | Meine Mitgliedschaften

Kalender

< September 2011 >

KW	Mo	Di	Mi	Do	Fr	Sa	So
35	29	30	31	1	2	3	4
36	5	6	7	8	9	10	11
37	12	13	14	15	16	17	18
38	19	20	21	22	23	24	25
39	26	27	28	29	30	1	2

Details: [Icon]

Mail

E-Mail-Postfach (5) »

ILIAS-Mails werden an die eingetragene E-Mail-Adresse weitergeleitet.

Bitte überprüfen Sie in regelmäßigen Abständen Ihr E-Mail-Postfach.

Details: [Icon]

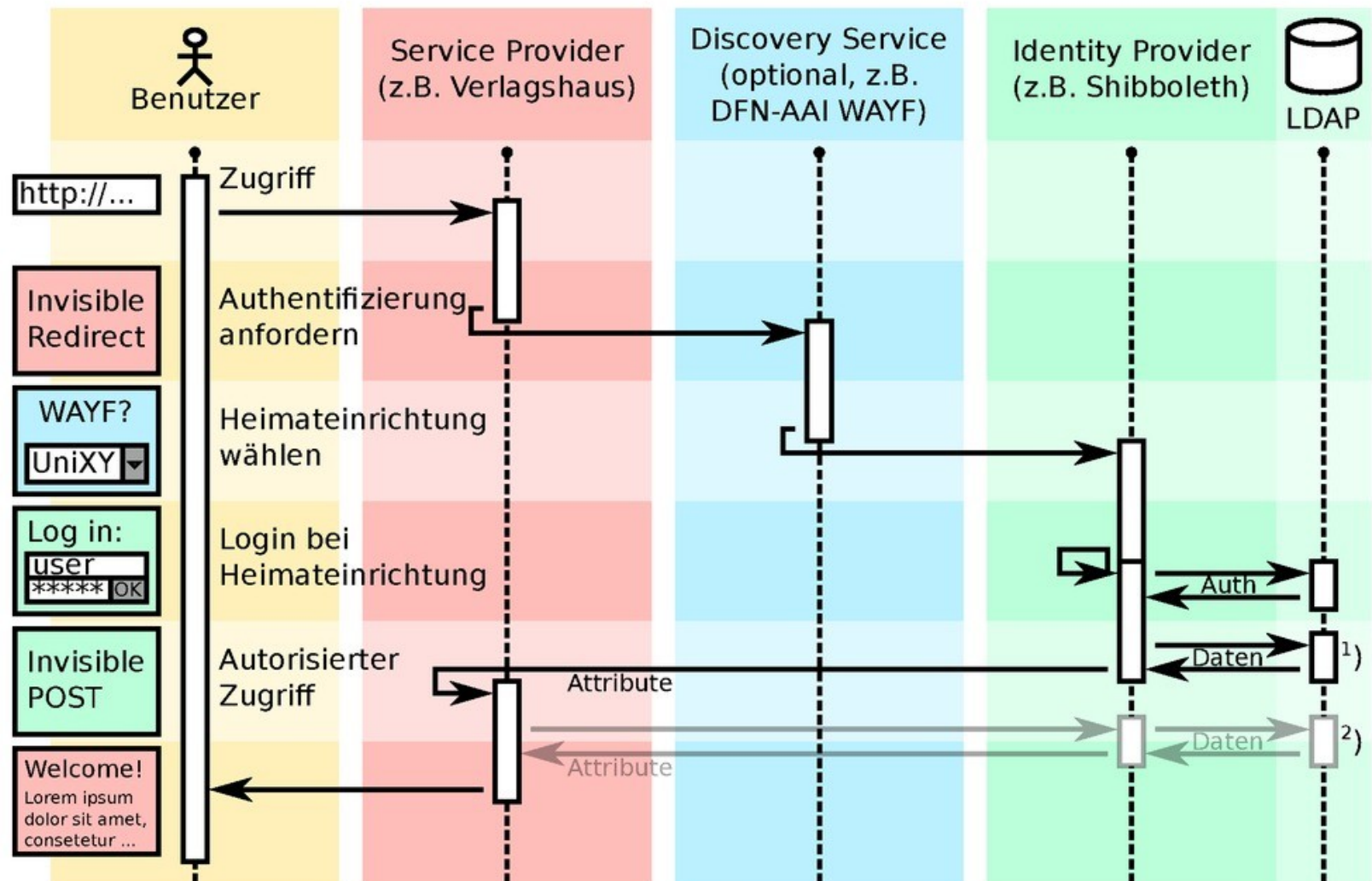
Die Lösung: Shibboleth!





# Wie funktioniert Shibboleth?

M. Haim, 12/2010



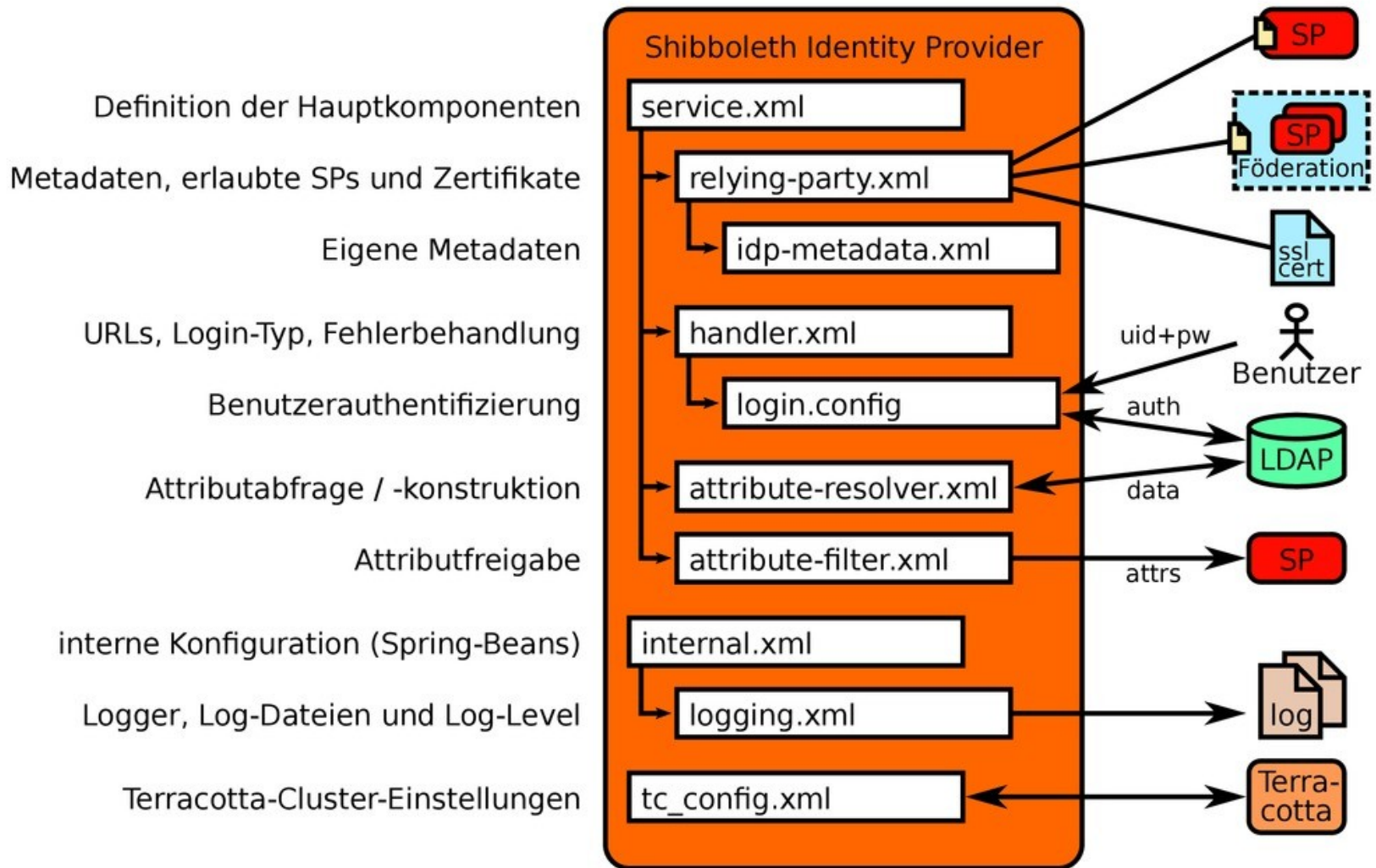
1) SAML2: Attribute werden XML-verschlüsselt & signiert mittels Benutzer-Client übertragen

2) SAML1: Attributanfrage erfolgt ohne XML-Verschlüsselung über verschlüsselten Rückkanal



# Konfiguration

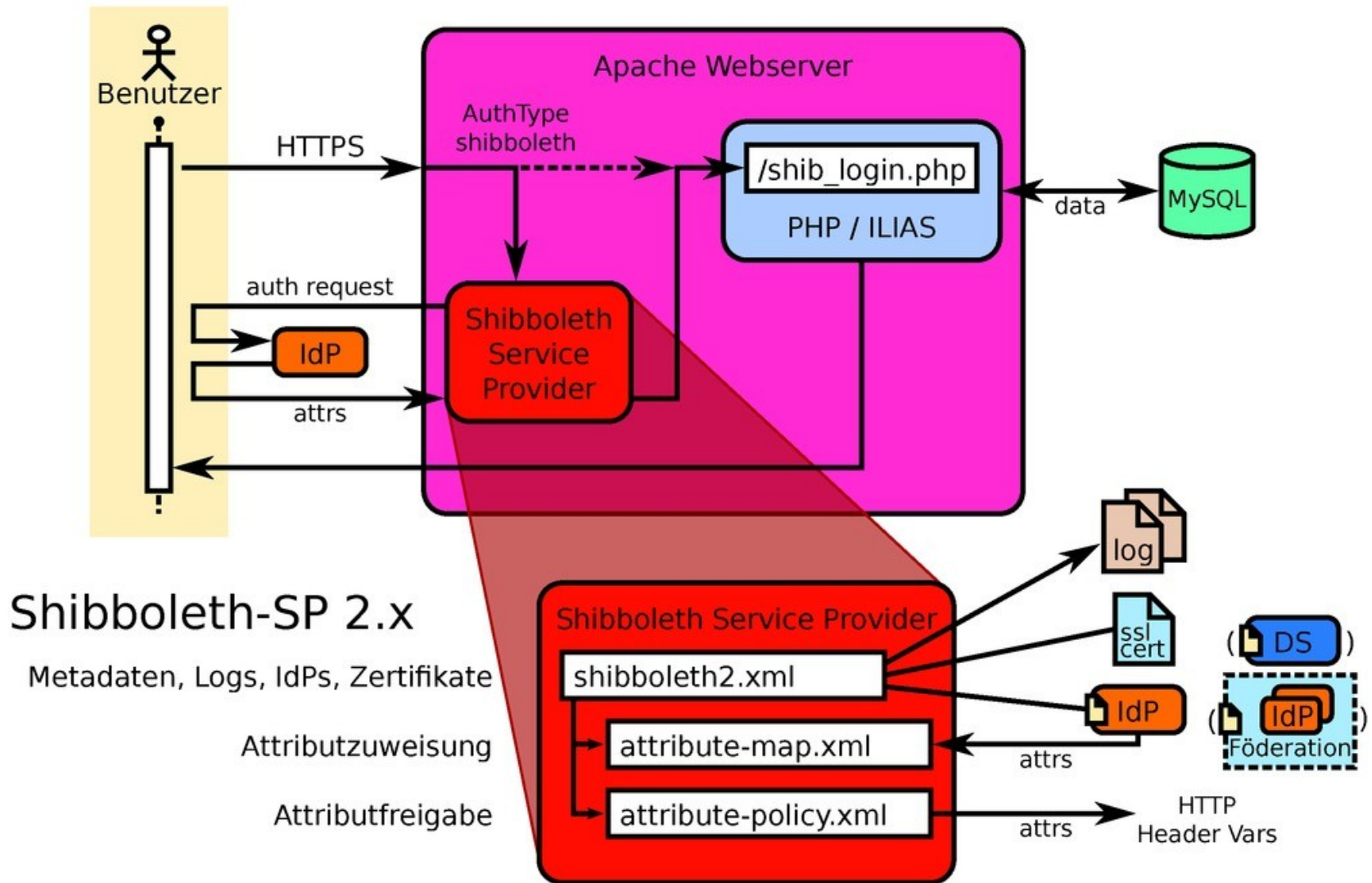




+ Webapplikation

war/idp.war bzw. src/main/webapp/





# Ausbau zum hochverfügbaren Service



# Lastverteilung + Ausfallsicherung = High Availability

- **Grundidee: Mehrere Server bilden einen Cluster**
  - Die Gesamtlast verteilt sich auf die Knoten (Lastverteilung)
  - Kein Dienstaussfall bei Ausfall eines Knotens (Ausfallsicherung)
- **Knoten müssen Zustands-Informationen teilen**
  - Shibboleth-IdP speichert alle Zustandsdaten im StorageService
  - Problem: Java-Map (Objektänderungen ohne Zurückschreiben)
  - Standardlösung: Java-VMs per Terracotta abgleichen



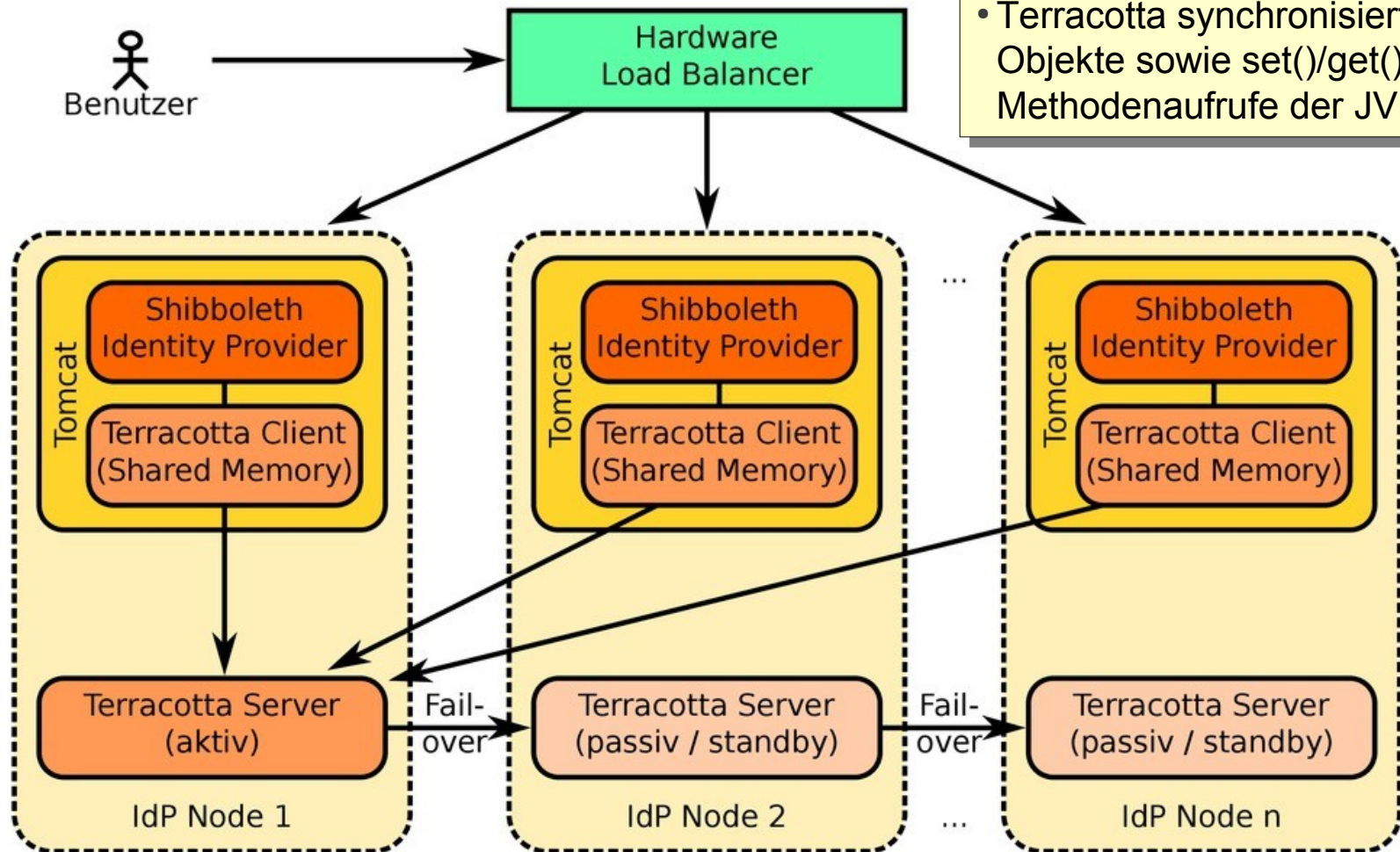
# Aufbau eines Shibboleth-Clusters

M. Haim, 12/2010

(gemäß Shibboleth-Wiki)

Funktionsweise:

- Terracotta synchronisiert alle Objekte sowie set()/get()-Methodenaufrufe der JVMs.

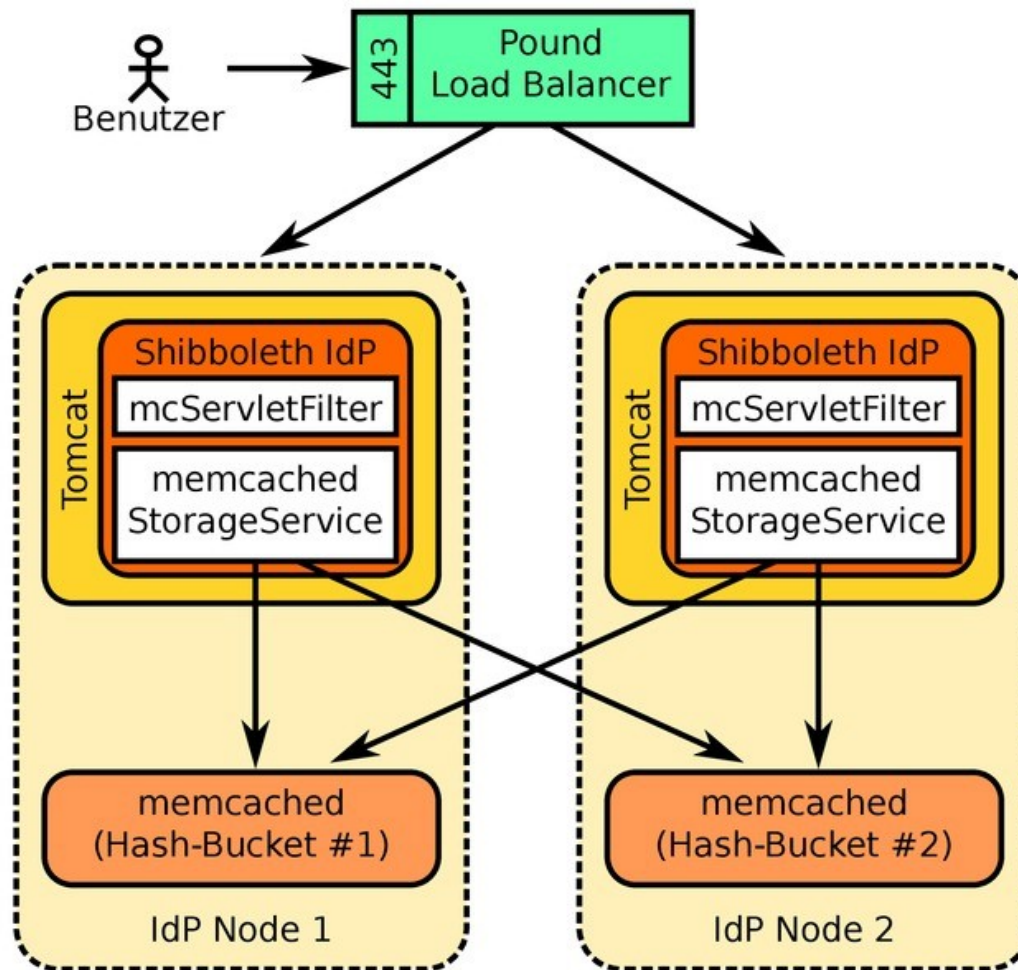




# Alternativer Aufbau eines Shibboleth-Clusters

(mit IdP Memcached StorageService)

M. Haim, 09/2011



## Funktionsweise:

- Pound mit „sticky session“.
- StorageService speichert alle Objekte immer in lokaler Map. (wg. Java-Objektreferenzen)
- StorageService wird bei get()- und set()-Operationen mit memcached abgeglichen. (BeanUtils.copyProperties())
- Ein ServletFilter wird nach jedem IdP-Servlet ausgeführt, um Änderungen am Session-Objekt explizit zurück in den StorageService zu schreiben.
- Daten werden per Hash-Funktion auf mehrere memcached-Instanzen verteilt.
- Bei Ausfall eines Servers ist schlimmstenfalls ein neues Login am IdP erforderlich.





# Lasttest mit „The Grinder“ – Ergebnisse

Anzahl Knoten	Cluster-Methode	-Xmx	RAM	Speicherverbrauch der jeweiligen Cluster-Methode pro Knoten	TPS*
2	—	1536m	3GB	—	65
2	Memcached (disjunkt)	1536m	3GB	10 MB RAM permanent, 13 MB RAM pro 5.000 Logins**	63
2	Terracotta 3.5.1	1536m	4GB	800 MB RAM permanent, 300 MB HD pro 5.000 Logins	22

\* Transaktionen pro Sekunde, hier: Anmeldungen pro Sekunde.

\*\* Bei Verwendung von nur einem Memcached-Server: ca. 25 MB RAM pro 5.000 Logins.

- Der Speicherverbrauch des „geteilten“ Speichers entwickelte sich in den Tests linear.
- Memcached arbeitete auch nach 150.000 Anmeldungen munter weiter.
- Terracotta lief im Modus „permanent-store“ (wie im Shibboleth-Wiki vorgegeben) und wurde vermutl. durch die Festplattennutzung ausgebremst. Nur 5.000 Logins getestet.



# Tipps zur Optimierung der einzelnen Knoten

- Debian Linux: KVM, je 4 CPUs @ 2,5GHz, 3 GB RAM  
(RAM ist wichtig: Tomcat wird bei Nutzung der Swap-Partition sehr sehr langsam!)
- Tomcat 6: Java-Heap-Space erhöht (-Xmx 1536m)
- LDAP-Anfragen ohne :caseExactmatch:
- LDAP: Eigener dnResolver in login.config  
vt-ldap unterstützt noch kein LDAP Connection Pooling,  
vgl. <http://code.google.com/p/vt-middleware/issues/detail?id=118>
- ConnectionPool in attribute-resolver.xml  
(→ nicht zwingend nötig, macht Shibboleth bereits automatisch)
- Cluster-Lösung: memcached (-m 1024) statt Terracotta



# Ausbau von Shibboleth zum Single-Sign-On-Portal



# Unsere Login-Seite (mit Erweiterungen) im Corporate Design

Philipps-Universität  
Marburg

## Single Sign-On

Anmeldung (Login)  
Selbstauskunft  
Sitzung beenden (Logout)  
Hilfe

## Zugang für Mitglieder und Angehörige der Philipps-Universität Marburg

» Universität » HRZ » Single Sign-On

Nicht angemeldet!

Nach der Anmeldung  
werden Sie weitergeleitet zu:

### Lernplattform ILIAS (Testserver!)

Die Lernplattform der Uni  
Marburg bietet Funktionen für  
die online-gestützte Lehre  
unter einer einheitlichen  
Oberfläche.

## Bitte anmelden

Sie müssen sich anmelden, um den folgenden Dienst zu nutzen:  
» Lernplattform ILIAS (Testserver!)«

Benutzername:

Passwort:

Benutzergruppe: Professoren/Mitarbeiter und Studierende ▾

Single-Sign-On\*: ☒ Ja, ich möchte weiterhin angemeldet bleiben.

Anmelden

Gastzugang\*\*: Als Gast anmelden

## Wichtige Hinweise:

- Bitte achten Sie bei Ihrem Benutzernamen auf korrekte Groß- und Kleinschreibung!
- \*Single-Sign-On: Ihre Anmeldung bleibt erhalten und ist bis zu 8 Stunden lang gültig. Nach einmaliger Anmeldung haben Sie **Zugriff auf alle Web-Anwendungen** (wie ILIAS, Webmail, Bibliotheken und Verlage etc.), die eine Anmeldung über die Uni Marburg unterstützen, ohne dass Sie zwischendurch erneut Ihr Passwort eingeben müssen.
- \*\*Gastzugang: Innerhalb unserer Bibliotheken können Sie sich anonym als Gast anmelden. Bitte beachten Sie, dass manche Dienste und Web-Anwendungen jedoch nur registrierten Nutzern zur Verfügung stehen.
- Zur sicheren **Abmeldung** schließen Sie bitte Ihren Browser. Nur so können Sie verhindern, dass Sie bei einzelnen Web-Anwendungen angemeldet bleiben oder beim erneuten Aufruf einer Web-Anwendung wieder automatisch angemeldet werden.
- **Das HRZ und seine Mitarbeiter werden Sie zu keiner Zeit, weder persönlich, telefonisch noch per E-Mail, dazu auffordern, Ihre Zugangsdaten bzw. Ihr Passwort preiszugeben.**

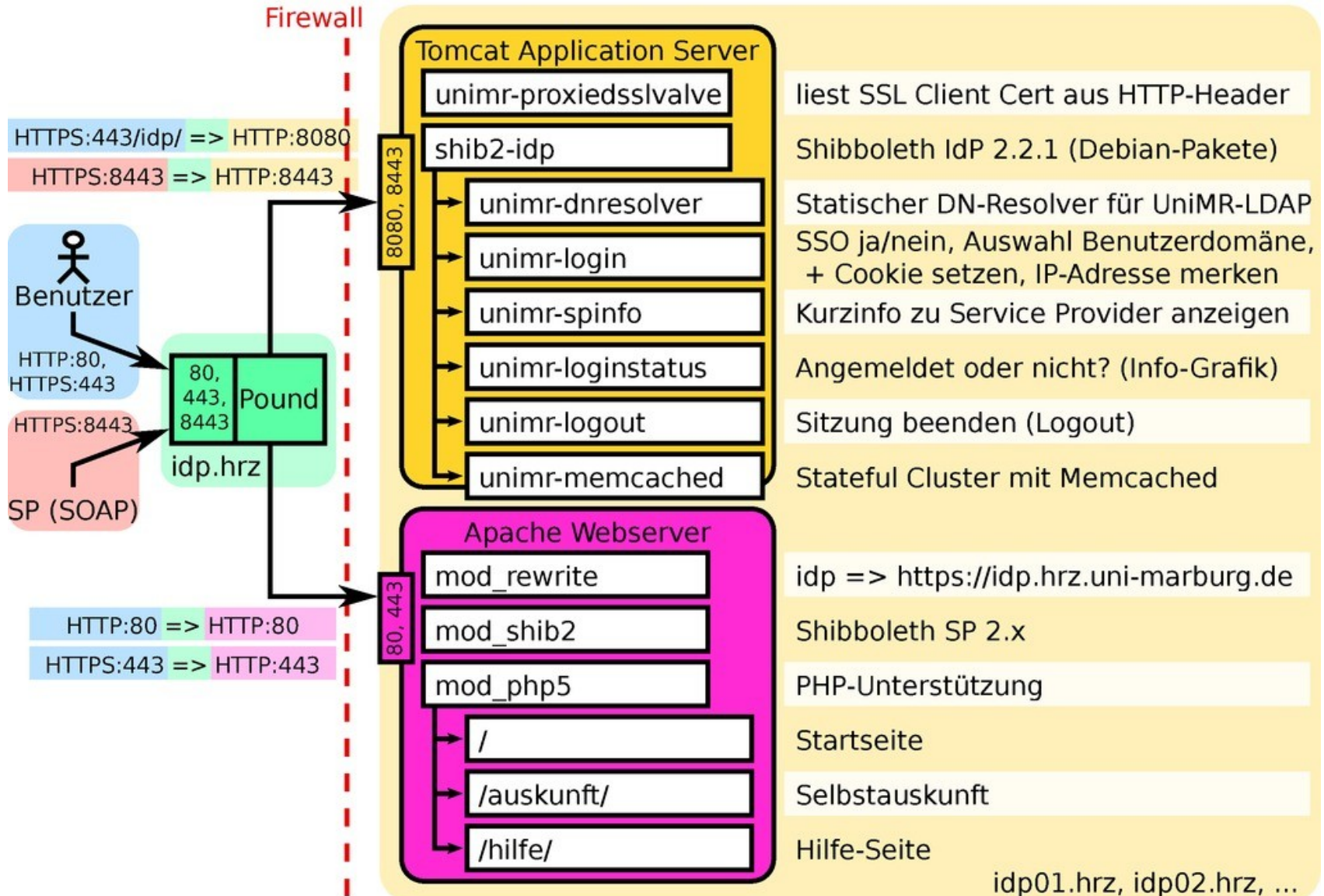
Host: ido01 - Zuletzt aktualisiert: 11.08.2011

Philipps-Universität  
Marburg

Hochschulrechenzentrum - Shibboleth, Hans-Meerwein-Straße, D-35032 Marburg  
Tel. 06421/28-28282, Fax 06421/28-26994, ✉ E-Mail



Impressum







## Weiterführende Links

- Shibboleth:  
<http://www.shibboleth.net>,  
<https://wiki.shibboleth.net/confluence/display/SHIB2/Home>
- Föderation DFN-AAI:  
<https://www.aai.dfn.de>
- Shibboleth Single Sign-On an der Uni Marburg:  
<https://idp.hrz.uni-marburg.de>
- IdP Memcached StorageService (Eigenentwicklung):  
<https://wiki.shibboleth.net/confluence/display/SHIB2/Memcached+StorageService>



# Danke für Ihre Aufmerksamkeit!

## Noch Fragen?

→ Gern jetzt im Anschluss :-)

→ sonst per E-Mail: Manuel Haim, [haim@hrz.uni-marburg.de](mailto:haim@hrz.uni-marburg.de)

Quellennachweis Icons: „Crystal Project“ (GNU LGPL).

