iisys
Institut für
Informationssysteme
der Hochschule Hof

hochschule
hof
University of Applied Sciences

Approaches and challenges for a SSO enabled extranet using Jasig CAS

Florian Holzschuher

René Peinl

10.09.2013

iisys - Institut für Informationssysteme

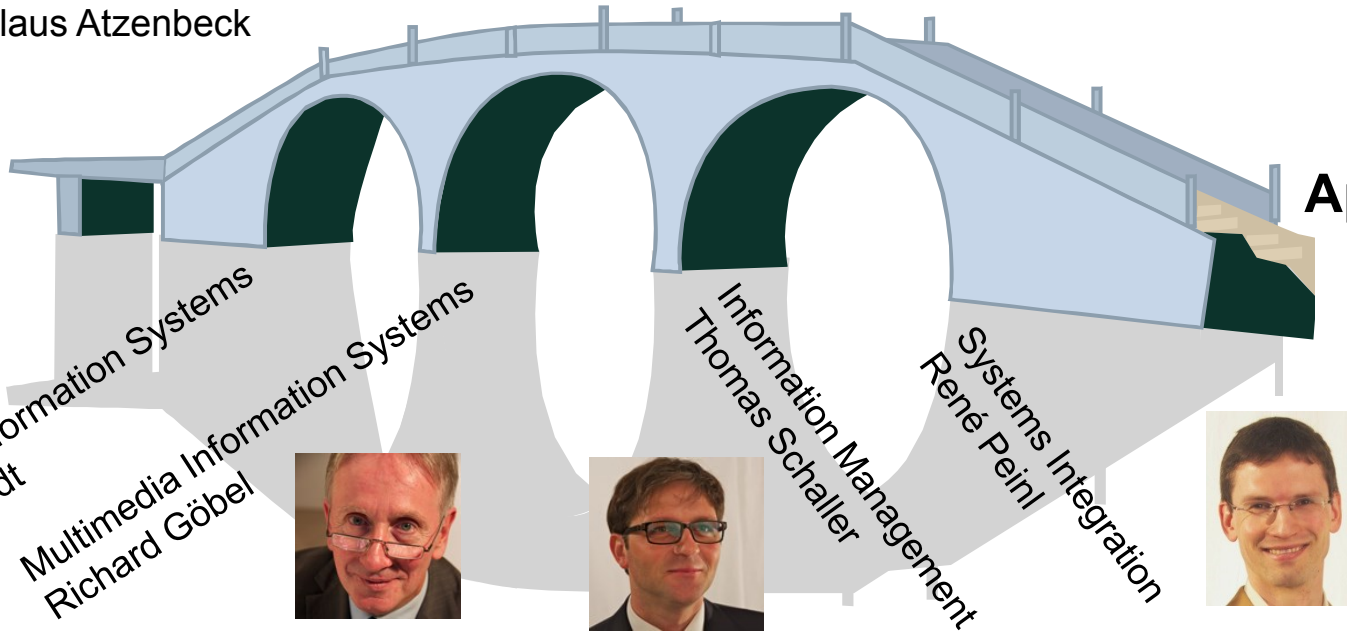
iisys
Institut für Informationssysteme der Hochschule Hof

Mission: „The institute is a competence centre for the application of information systems in companies. It is the bridge between international research and development and actual application in companies.“

Managing Director
Claus Atzenbeck

Research

Application



Agenda

iisys
Institut für
Informationssysteme
der Hochschule Hof

- Environment for Open Source SSO
- SSO scenarios
  - Intranet, Extranet, Cloud
- SSO protocols
  - Kerberos, SAML, OAuth, …
- SSO solutions
  - Shibboleth, CAS, JOSSO, …
- SSO experiences with CAS
- Conclusion

Environment for Open Source SSO

iisys
Institut für Informationssysteme der Hochschule Hof

- **Desktop**
  - Windows still market leader with ~ 90% share

- **Mobile**
  - Chrome for Android similar capabilities like Desktop Chrome

- **Server**
  - Microsoft Active Directory is prevalent even in OSS environments
    - SSO for all Microsoft products out of the box (NTLM, Kerb
  - OSS server-side applications mostly only with LDAP
  - SSO solution for OSS applications is needed

SSO scenarios

iisys
Institut für Informationssysteme der Hochschule Hof

- **Intranet**
  - Everything under control, can be a homogenous landscape

- **Extranet**
  - Reverse Proxy, two URLs, firewalls, less control over clients

- **Cloud SaaS**, esp. hybrid cloud
  - Maybe without reverse proxy, instead load balancing, caching, geo replication
  - Upload of user accounts
  - SSO solution should be integrated with usage monitoring

SSO protocols

- **Windows environments**
  - NTLM
  - Kerberos
- **Web Service environments**
  - SAML
  - XACML
- **Web 2.0 environments**
  - OpenID
  - OAuth
  - OpenID connect

Open Source SSO solutions

iisys
Institut für Informationssysteme der Hochschule Hof

Shibboleth

- Internet 2 consortium, federated scenarios, Web Services, SAML

jasig CAS (Central Authentication Service)

- Uses own SSO protocol, but supports standards as well

Atricore™ JOSSO

- Java-based, but with .NET and PHP support, graphical SSO definition

ForgeRock OpenAM
Authenticate - Authorise - Federate

- Successor of the Sun Identity Manager

WSO2 Identity Server

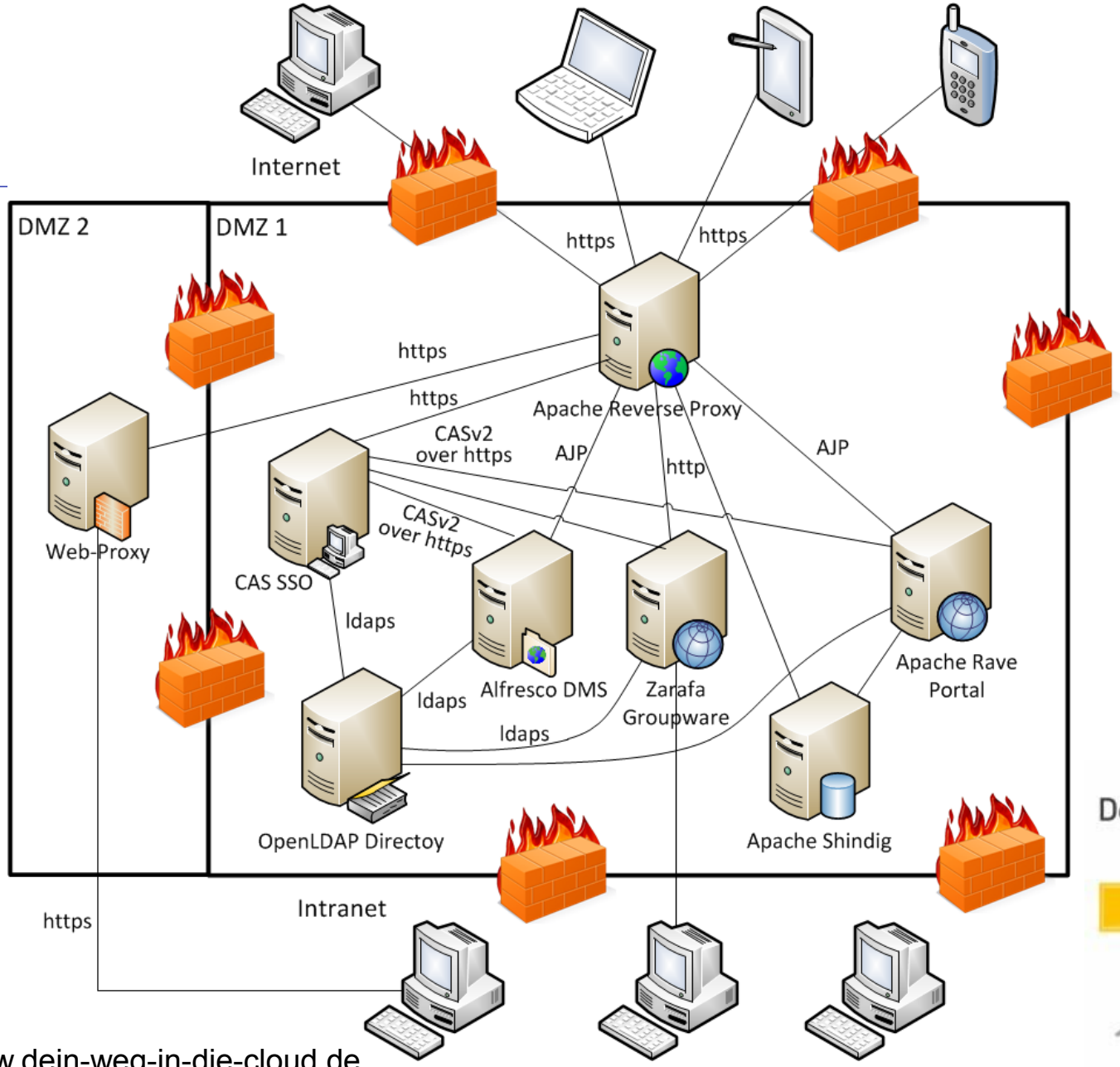
- Plays nicely together with the remaining WSO2 infrastructure

Comparison of Open Source SSO

iisys
Institut für Informationssysteme der Hochschule Hof

	Jasig CAS	Atricore JOSSO	WSO2 Id Server	Forgerock Open AM
Latest version	3.5.2 (22.02.13)	2.3.0 (31.08.12)	4.1.0 (11.02.13)	10.1.0 (20.02.13)
License	Jasigs own open source license	LGPL	APL v2	CDDL 1.0
Protocols	CAS, OAuth, OpenID, SAML, Kerberos	SAML, NTLM	OAuth, OpenID, XACML, SAML, … (18+),	OAuth, SAML, Kerberos
Authentication backends	JAAS, LDAP, AD, Radius, JDBC, X.509, Negotiate (Kerberos)	JAAS, LDAP JDBC, two factor auth with WiKID, X.509	LDAP, AD, JDBC, Cassandra	LDAP, AD, two-factor auth with HOTP, Negotiate (Kerberos)
Runtimes	Tomcat or other Servlet 2.4 container	JBoss, Tomcat, Websphere, Geronimo, Jetty	WSO2 Carbon server	Tomcat, JBoss
Agents	Spring, MS IIS, JEE, Apache 2.2, PHP, PAM	Apache 2.2, PHP 4+, MS IIS, Liferay, Alfresco, phpBB, Spring, Coldfusion	None found	Apache 2.4, MS IIS, Sun Web Srv, JBoss, Glassfish, Tomcat, Web Logic Websphere,

Test scenario



www.dein-weg-in-die-cloud.de

Experiences with CAS in an extranet

iisys
Institut für Informationssysteme der Hochschule Hof

- Single sign-on is working relatively well, single sign-out does not
- AJP solves most reverse proxy problems, but not all.
  Especially AJAX calls cause trouble
- Authentication on the reverse proxy instead of the application doesn't make a notable difference
- Local administrative accounts have to be prepared for SSO
- Fallback solution with an option to opt-out of SSO and use a manual local login would be desirable

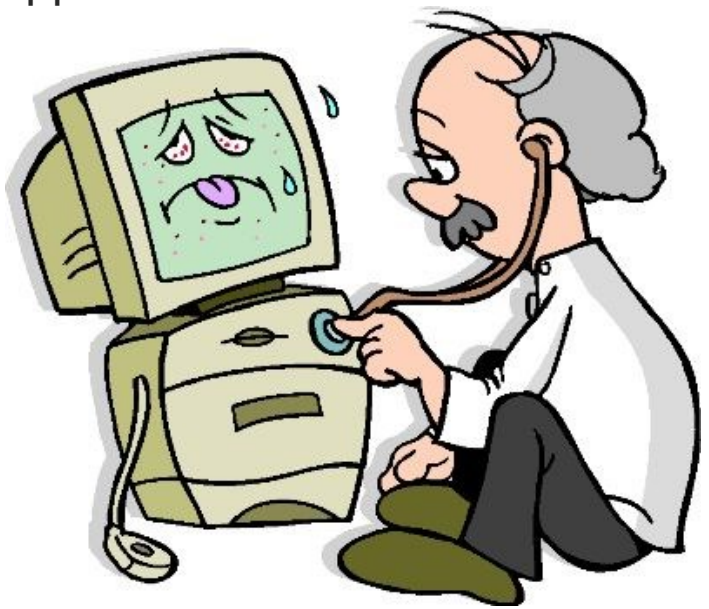


image source: www.empowernetwork.com/thorsband/basic-computer-troubleshooting-tips/

Experiences with CAS in an extranet #2

iisys
Institut für
Informationssysteme
der Hochschule Hof

- Inclusion of Apache Rave with Apache Shindig caused problems

  => CAS' ticket proxying feature could be a part of the solution

  again AJAX calls with problems

- SSO is especially ill-suited for infrastructure services

  => Apache Solr could not be used to index contents

  due to session problems

Image source: www.mostphotos.com

Conclusion

- Many Open Source applications are not well prepared for SSO (even well known ones like Alfresco)
- Besides SSO, you have to solve the identity management problem (synchronize user data between LDAP and application => IAM)
- Single sign-out is hard to implement, did only work well with Spring framework
- Complexity for SSO is rising from intranet, over extranet to (hybrid) cloud
- Gartner denoted SSO and IAM a "must have" for enterprises of all size and industry already 10 years ago
  => with open source software it's sadly not reality today,
  the same applies to Cloud applications in general

Thanks for your attention