DARIAH-DE
Digital Research Infrastructure for the Arts and Humanities

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Access and Authentication Infrastructures Workshop

DARIAH-DE

JavaSP

Tobias Gradl
University of Bamberg

DARIAH-DE Java SP

1) **Use-case and goals**
2) **Frameworks**
3) **configuration**
4) **Prototypes & services**

Initial use case

- DARIAH-DE Schema Registry
  - Spring MVC based Java application
  - Running in Tomcat 7
  - Required access to the DFN-AAI service to integrate in the DARIAH-AAI model
  - Assign privileges to groups at runtime instead of hard-wiring in code or configuration

Implementation Goals

- Provide a native method for accessing for SAML-based AAI in Java Web Applications
- Remove the need for “workarounds” to integrate Shibboleth
- Adapt to the DARIAH AAI model to assign privileges to roles
- Build upon existing frameworks and implementations

DARIAH-DE Java SP

1) Use-case and goals
2) **Frameworks**
3) configuration
4) Prototypes & services

OpenSAML

- SAML is an OASIS Standard for the exchange of AAI details
- OpenSAML is the fundamental open-source implementation of SAML
  - SAML 1.0, 1.1 and 2.0 profiles
  - C++ and Java libraries
  - Base of various implementations such as Shibboleth, Apache WSS4J and others

https://wiki.shibboleth.net/confluence/display/OpenSAML/Home

Spring

- Open source Java Framework for development of JavaEE/Java applications
  - Facilitates implementation of persistence, message-bus, MVC, web services, security, etc.
  - Allows focusing on business logic development
  - Used by various services in DARIAH-DE
  - Generic Search,
  - Collection Registry,
  - Schema Registry, …

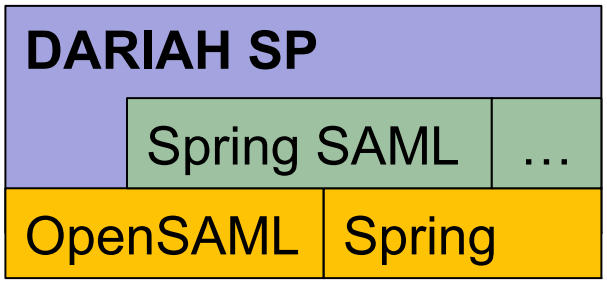
Spring Security – SAML extension

- Spring Security provides various security mechanisms as LDAP, Kerberos etc.
- Spring Security – SAML extension implements OpenSAML under Spring
  - Filter-based application of AAI
  - No influence on business logic development
  - Well documented

http://docs.spring.io/spring-security/site/extensions/saml/

DARIAH Java SP

- Largely build upon the frameworks of
  - Spring
  - Spring Security and the SAML extension
  - OpenSAML
- Some incompatibilities in the Spring SAML implementation were fixed
  - e.g. implementation of AttributeQuery Profile was missing



DARIAH-DE Java SP

1) Use-case and goals
2) Frameworks
3) **configuration**
4) Prototypes & services

DARIAH Java SP - Configuration

- Spring XML bean configuration (similar to Persistence, AOP etc.)

```
<?xml version="1.0" encoding="UTF-8" ?>
<beans xmlns="http://www.springframework.org/schema/beans"
      xmlns:security="http://www.springframework.org/schema/security"
          ...>
        ...
   <!-- Secured pages -->
   <security:http entry-point-ref="samlEntryPoint" access-decision-manager-ref="aDManager" >
      <security:intercept-url pattern="/locked" access="IS_AUTHENTICATED_FULLY" />
      <security:intercept-url pattern="/auth/**" access="IS_AUTHENTICATED_FULLY" />
      <security:intercept-url pattern="/admin_only" access="ROLE_ADMINISTRATOR" />
      ...
   </security:http>
```

DARIAH Java SP - Configuration

- Configure attribute query to be used to fetch DARIAH specific attributes

```
<bean id=„qryOptions" class="de.dariah.aai.saml.attributequery.SAMLAttributeQueryOptions">
      <property name="performAggregation" value="true" />
      <property name="attributeAuthorityIDP" value="https://ldap-dariah.esc.rzg.mpg.de/idp/sh...
      <property name="useOriginalSubjectNameID" value="false" />
      <property name="subjectIdAttributeName"
value="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"></property>
      <property name="subjectIdAttributeFormat" value="urn:oasis:names:tc:SAML:2.0:attrnam…
      <property name="noAggregationRequiredForEndpoints">
         <array>
           <value type="java.lang.String">https://ldap-
dariah.esc.rzg.mpg.de/idp/shibboleth</value>
         </array>
      </property>
      <property name="requiredAttributes">
            <array>
             <value type="java.lang.String">eduPersonPrincipalName</value>
             <value type="java.lang.String">mail</value>
```

DARIAH Java SP - Configuration

- Configure attribute query to be used to fetch DARIAH specific attributes

```
<bean class="org.springframework.security.saml.metadata.ExtendedMetadata">
    <property name="local" value="true"/>
    <property name="alias" value="dariah-javasp-sample3"/>
    <property name="securityProfile" value="metaiop"/>
    <property name="sslSecurityProfile" value="pkix"/>
    <property name="signingKey" value="demo2.dariah.eu"/>
    <property name="encryptionKey" value="demo2.dariah.eu"/>
    <property name="tlsKey" value="demo2.dariah.eu"/>
    <property name="requireArtifactResolveSigned" value="false"/>
    <property name="requireLogoutRequestSigned" value="false"/>
    <property name="requireLogoutResponseSigned" value="false"/>
    <property name="idpDiscoveryEnabled" value="true" />
    <property name="idpDiscoveryURL" value="https://wayf.aai.dfn.de/DFN-AAI-Test/wayf"/>
    <property name="idpDiscoveryResponseURL" value="https://demo2.dariah.eu/dariah-javasp...
</bean>
```

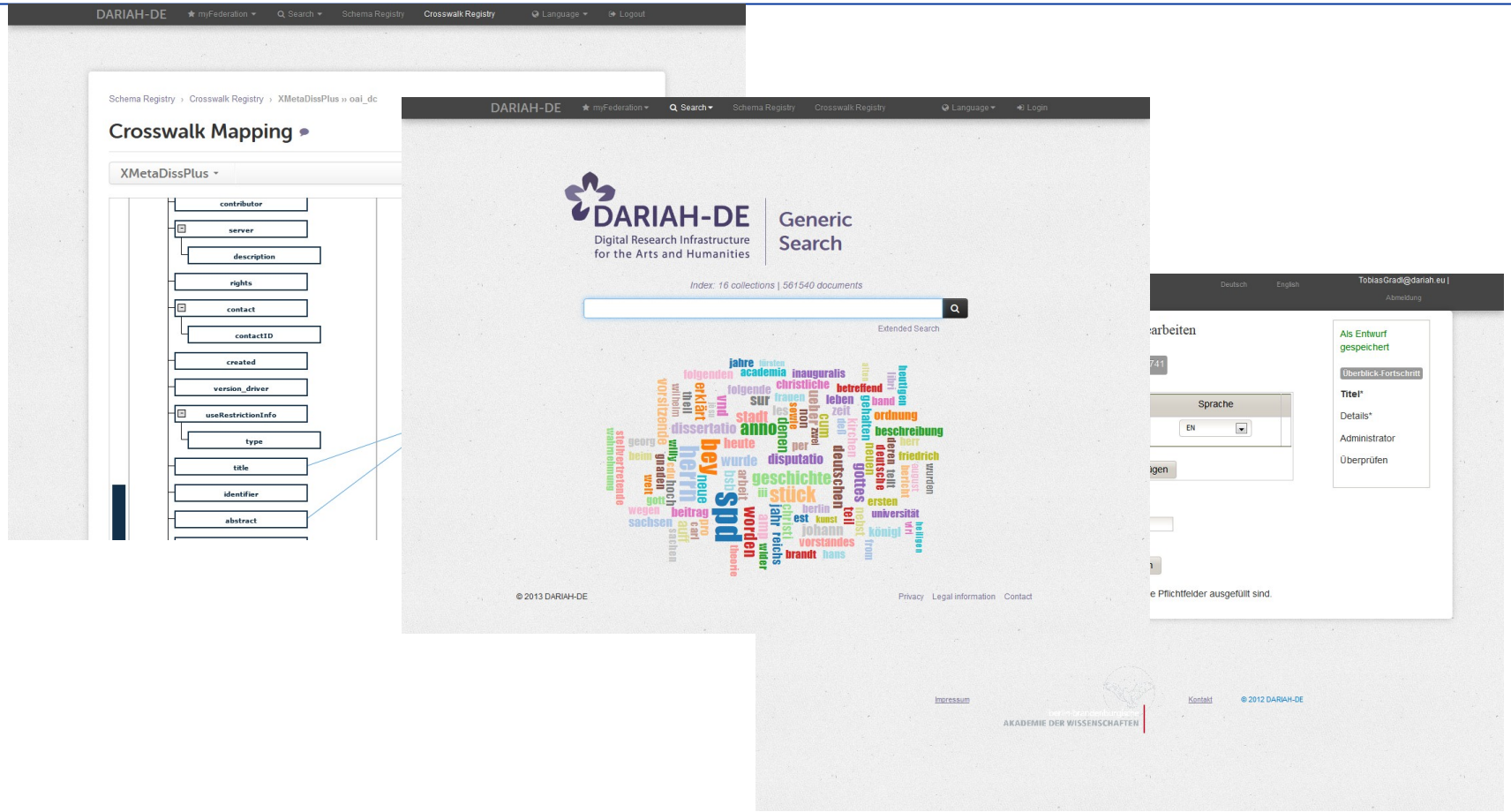
DARIAH-DE Java SP

1) Use-case and goals
2) Frameworks
3) configuration
4) **Prototypes & services**

Prototype

- http://demo2.dariah.eu/dariah-javasp-sample3

Services using the Java SP



DARIAH-DE

Services Links

- https://demo2.dariah.eu/colreg
- https://dev3.dariah.eu/search/
- http://dev3.dariah.eu/schereg

Thank you!

DARIAH-EU → http://dariah.eu
DARIAH-DE → http://de.dariah.eu

Contact → Tobias.Gradl@uni-bamberg.de