Stockholms universitet

+

= Simple federated web apps

Tommy Andersson & Joakim Lundin, IT Services, Stockholm University

Stockholms universitet

What is GRAILS ?

Open Source

Web MVC

Runs on JVM

Builds on Spring

And much more

Apache, mod_shib, tomcat, grails

- AOP functionality through filters

```
<LocationMatch "/">
    AuthType shibboleth
    ShibrequireSession Off
    Require shibboleth
</LocationMatch>

JkMount   /*   ajp13_worker
```

```
JkEnvVar displayName
JkEnvVar eppn
JKEnvVar givenName
JkEnvVar mail
JkEnvVar norEduPersonNIN
JkEnvVar REMOTE_USER
JkEnvVar sn
```

```
def filters = {
  all(controller: '*', action: '*') {
    before = {
      if (!request.remoteUser) {
        try {
          session.invalidate()
        } catch (all) {}
        log.error "No request remoteUser attribute found, te
        redirect(url:'https://login.secure.su.se/logout')
        return false
      }
      if (request.remoteUser && !session.user) {
        session.user = [
                uid: request.remoteUser?.toUid(),
                displayName:request["displayName"]
        ]
      }
    }
  }
}
```

Are there no plugins?

Grails Spring Security Shibboleth Native SP Plugin

http://grails.org/plugin/spring-security-shibboleth-native-sp

Federated Grails

http://grails.org/plugin/federated-grails

Federated Role Delegation

Using gmai's we create and delegate roles through our LDAP. Scope is grabbed from eppn.

```
public final static String BASE_URN = 'urn:mace:swami.se:gmai:su-vfu:'
```

```
// Only SU scoped people (e.g. non-students and non-guestaccounts) have access to the role Sysadmin and SUPERVFUSEK.
if (request?.entitlement) {
  List<String> entitlements = (request?.entitlement as String)?.split(';')
  if (entitlements) {
    if (user?.class == User && scope == 'su.se') {
      role = (entitlements?.contains(BASE_URN + 'sysadmin')) ? Role.SYSADMIN : null
      if(!role){
        role = (entitlements?.contains(BASE_URN + 'supervfusek')) ? Role.SUPERVFUSEK : null
      }
    }
    if (!role) {
      ['vfusek':Role.VFUSEK, 'vfukontakt':Role.VFUKONTAKT].each { key, value ->
        // Will break as soon as a role is found, so use role hierarchy in the list above..
        if (!role) {
          role = (entitlements?.contains(BASE_URN + key)) ? value : null
        }
      }
    }
  }
```

Centralized Role And Access Delegation

Stockholms universitet

Through kontohantering.su.se.

(An application written in Grails.)

Systemrättigheter

SISU	Redigera
Wisum	Redigera
Polopoly	Redigera
Kontohantering	Redigera
Ladok på webb	Tentamenstjänsten - full behörighet : Avdelningen för IT och media(647) Tentamenstjänsten - begränsad behörighet : Avdelningen för externa kontakter(642) Redigera
Kontoaktivering	Redigera
IVS	Redigera
NyA	Rolladministratör **Okänd roll:** urn:mace:swami.se:gmai:nya-dw:base:o=SU Redigera
VFU-portalen	VFU-handläggare Redigera
TimeEdit Tool	Redigera
Sukatformulär	

Stockholms universitet

Future

Generalize and federate more applications

Build plugins for stuff others can use

Make the code available on GitHub

Stockholms universitet

Attributions

Shibboleth - http://shibboleth.net/

Grails - http://www.grails.org/

Groovy - http://groovy.codehaus.org/

SpringSource - http://www.springsource.org/

Stockholms universitet

Q

Contact info

Tommy Andersson
tommy.andersson@su.se

Joakim Lundin
joakim.lundin@su.se