OPEN SOURCE &
SINGLE SIGN-ON
SSO FOR 1.6 MILLION USERS WITH JBOSS PICKETLINK

DR. IR. RONALD MIDDELKOOP
Open Source Conference 2012
ABOUT ISAAC

• Started in 1999 at the Technical University Eindhoven
• 55 passionate employees
• ‘Full Service Internet Agency’
• Crazy about the Internet & Open Source
• Some of our partners:
THE ISAAC AMBITION

“TO BE THE BEST E-BUSINESS ENABLER IN THE WESTERN EUROPEAN REGION”

Innovative, high end technical solutions, proven technology, result driven
ABOUT RONALD

• Application Architect at ISAAC
• Java-based middleware with a focus on system integration
• Architect for Basispoort case
AGENDA

1. Use Case: Basispoort SSO
2. SSO: advantages
3. SSO: using SAML
4. Jboss Picketlink: open source SAML implementation
5. Beyond Jboss Picketlink
BASISPOORT SSO

USE CASE

GOALS:

• Single Sign-on to educational applications by primary school pupils and teachers
• Portal with the available applications
SO WHAT DOES IT DO?

Basispoort Single Sign-On
Go to e.g. a history application from one publisher …
...and you are redirected to the Basispoort login. There, you select the class you’re in...
...then you select yourself...
...and finally your password picture...
...and you are logged in.
Now go to any other application from any publisher…
...and you are logged in without providing credentials.
WHAT’S SO GREAT ABOUT SSO?
Basispoort Single Sign-On
SSO: ADVANTAGES

Ease of use for the End User:
- One login page with one password for all Service Providers
- Log in at 1 Service Provider, logged in at all Service Providers

Ease of use for the Company:
- Make central identity stores (e.g. Active Directory or database) available to all Service Providers, securely and uniformly

 Ease of use for Service Providers:
- Delegate authentication / authorization
BASISPOORT SSO

GOALS:
• Single Sign-on to educational applications by primary school pupils and teachers
• Portal with the available applications

CHALLENGES:
• Scale: 9000 schools with 1.6 million pupils
• Scale: 4 participating publishers with a large, dynamic set of some 120 educational applications
• Identity Store Management: Every school has a store
• Target Audience: young, not all are able to read
• SSO delegation: 4 participating network providers
SO HOW DOES IT WORK?
Basispoort Single Sign-On
ASSIGNING IDENTITIES
TO PUPILS AND TEACHERS IN BASISPOORT BACKEND

1. Obtain list of schools from central school file
2. Obtain pupil and teacher data from School Administration System through:
   1. Manual upload by ICT Coordinator of school, or
   2. Automatic nightly synchronization
3. Assign ID to every new pupil and teacher
SINGLE SIGN-ON
THROUGH BASISPOORT IDENTITY PROVIDER

Pupil / Teacher

Educational Application

BP Portal

BP IdP

BP Backend
SINGLE SIGN-ON
THROUGH IDENTITY PROVIDER OF NETWORK PROVIDER
AVAILABLE APPLICATIONS
SYNCHRONISATION

ALL PARTIES INVOLVED MUST AGREE ON THE BASISPOORT ID OF A PUPIL OR TEACHER
LET'S'S FOCUS ON SSO
THAT'S WHAT WE'RE HERE FOR, RIGHT?
SAML 2.0 PROTOCOL

SAML is an XML-based framework for communicating user authentication, roles, and attributes.

• Approved as an OASIS standard in 2005
• A set of 7 specifications (http://saml.xml.org/saml-specifications)
• Covers use cases like:
  • Login
  • Logout
  • Role / Attribute communication
• Using various ‘bindings’ that determine how parties communicate
WEB BROWSER SSO PROFILE WITH THE HTTP POST BINDING

1. Browser attempts to access some resource at Service Provider

2. Is there an existing authenticated user for this browser session?

3. Form containing SAML < AuthnRequest >

4. SAML < AuthnRequest > from POST

5. Login

6. Form containing SAML < Response > with Basliggpoor ID

7. SAML < Response > from POST

8. Is the authenticated user authorized to access the requested resource?

9. Return to resource
WEB
BROWSER
SSO PROFILE
WITH THE
HTTP POST
BINDING >
WEB BROWSER
SSO PROFILE
WITH THE HTTP POST BINDING

1. Browser attempts to access some resource at Service Provider

2. Is there an existing authenticated user for this browser session?

3. Form containing SAML < AuthnRequest >

4. SAML < AuthnRequest > from POST

5. Login

6. Form containing SAML < Response > with Basiskort ID

7. SAML < Response > from POST

8. Is the authenticated user authorized to access the requested resource?

9. Return to resource
WEB BROWSER SSO PROFILE WITH THE HTTP POST BINDING

1. Browser attempts to access some resource at Service Provider

2. Is there an existing authenticated user for this browser session?

3. Form containing SAML &lt; AuthnRequest &gt;

4. SAML &lt; AuthnRequest &gt; from POST

5. Login

6. Form containing SAML &lt; Response &gt; with Basiskaart ID

7. SAML &lt; Response &gt; from POST

8. Is the authenticated user authorized to access the requested resource?

9. Return to resource
WEB BROWSER SSO PROFILE WITH THE HTTP POST BINDING >
WEB BROWSER SSO PROFILE WITH THE HTTP POST BINDING
WEB BROWSER SSO PROFILE WITH THE HTTP POST BINDING

1. Browser attempts to access some resource at Service Provider

2. Is there an existing authenticated user for this browser session?

3. Form containing SAML <AuthnRequest>

4. SAML <AuthnRequest> from POST

5. Login

6. Form containing SAML <Response> with Basispoort ID

7. SAML <Response> from POST

8. Is the authenticated user authorized to access the requested resource?

9. Return to resource
WEB BROWSER SSO PROFILE WITH THE HTTP POST BINDING >
WEB BROWSER
SSO PROFILE
WITH THE HTTP POST BINDING >
WEB BROWSER SSO PROFILE WITH THE HTTP POST BINDING: ADVANTAGES

• Mature

• Simple

• Secure (signatures, encryption)

• Several off-the-shelf implementations available, including open source
JBoss Picketlink
An open source SAML implementation
**JBoss PicketLink**

**The Good**
- Open source!
- Part of JBoss EAP 6, so supported
- Basically, just works out of the box
- Works even for complex issues like signatures, despite different libraries used by partners

**The Bad**
- Not fully mature
BEYOND JBOSS PICKETLINK

- Login via Network Provider (IdP Proxy)
- Logout
  - Disable Global Logout
  - Add custom logout protocol
WRAP-UP

- SSO applicable in many cases. Great advantages for end-user, company and service providers

- SAML is a mature, robust and secure SSO communication protocol

- We have used JBoss Picketlink in a very large use case and it works well

- Custom extensions are almost always needed, but possible
THAT'S IT!
THANKS FOR YOUR ATTENTION

GO TO WWW.ISAAC.NL OR TALK TO US AT THE ISAAC BOOTH