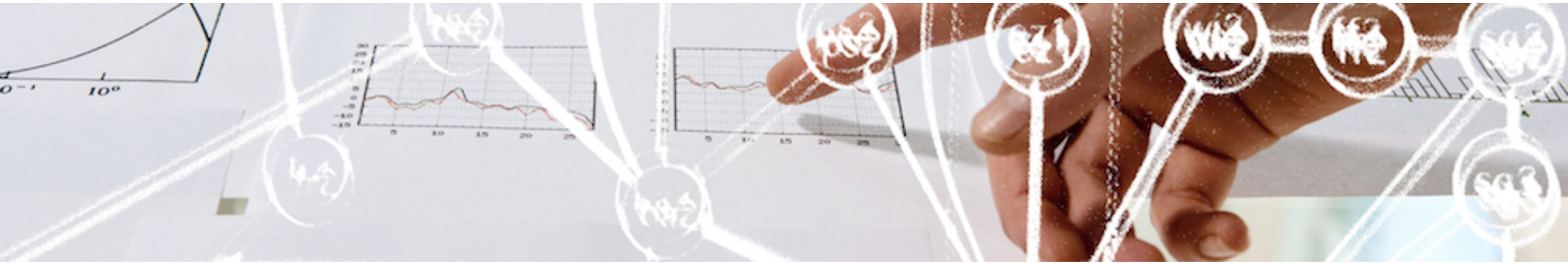
SAML Single Logout

with the Shibboleth IdPv3



SWITCH

Etienne Dysli-Metref
etienne.dysli-metref@switch.ch

Sessions, sessions, sessions!

- IdP session
- SP1 session
- application1 session
- SP2 session
- application2 session
- etc.

SLO is harder than SSO

- *Single*: terminate all sessions in one operation
- Does it make sense for the user?
- What happens when only one session is terminated?
- How do you cleanly terminate all those sessions?


NUKE IT FROM ORBIT
ITS THE ONLY WAY TO BE SURE
memegenerator.net

Availability with Shibboleth

- Already implemented in SP (simplified configuration since 2.4)
- SP can notify protected application
- Available since IdP 3.2.0, with some bugs in logout flow and view: IDP-956 (https://issues.shibboleth.net/jira/browse/IDP-956), IDP-924 (https://issues.shibboleth.net/jira/browse/IDP-924)
- Works on IdP 3.2.1 with those fixes applied
- Bindings: *front-channel* (HTTP-Redirect, HTTP-POST) and *back-channel* (SOAP)

Availability with Shibboleth

- Back-channel propagation not yet available on IdP, but planned for 3.3 (https://issues.shibboleth.net/jira/browse/IDP- 964)

- Administrative logout is *not supported*

Implementation in IdPv3

IdP- and SP-initiated logout sequences

Logout views

Configuration overview

Configuration details

Fixes for IdP 3.2.0 and 3.2.1

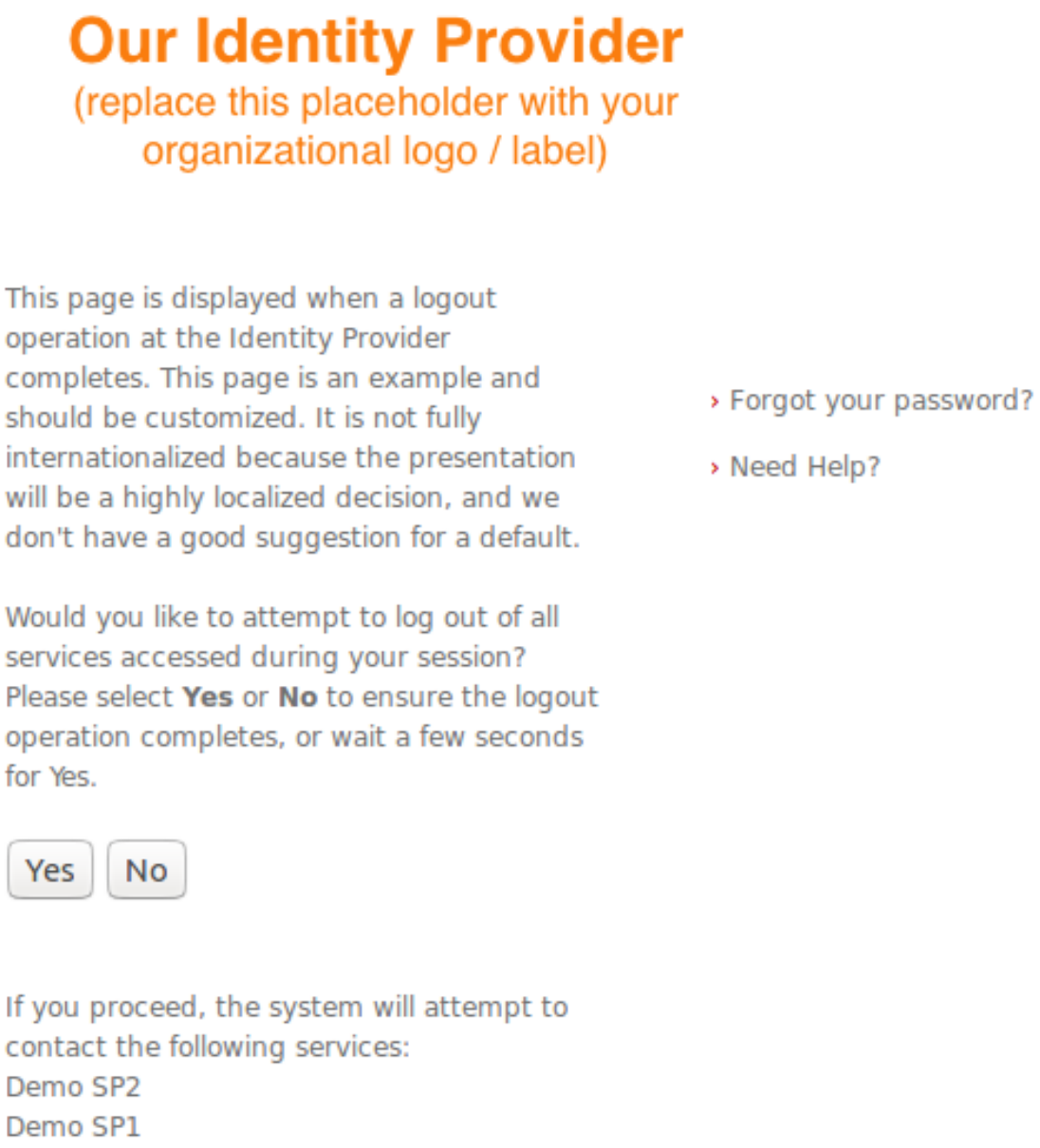
IdP-initiated (proprietary) logout

1. HTTP GET on `/idp/profile/Logout` with session cookie
2. End IdP session
3. Log out of other services? If yes, proceed
4. Propagate logout to accessed SPs
5. Display result (flow always ends at IdP)

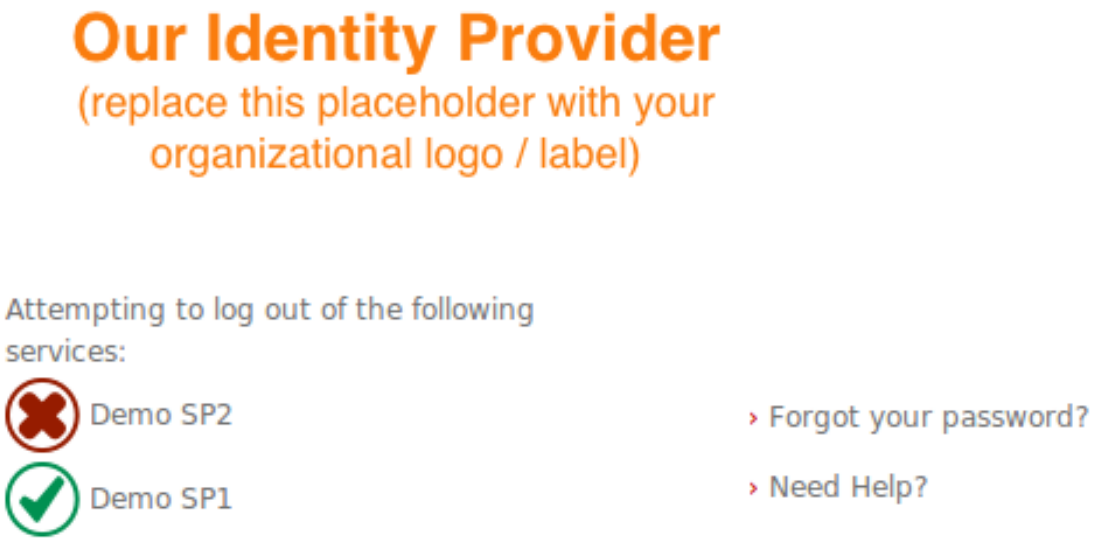
SP-initiated (SAML) logout

1. HTTP GET on `/Shibboleth.sso/Logout`
2. *(if notify)* Redirect to application logout notification endpoint
3. *(if notify)* Redirect to `/Shibboleth.sso/Logout`
4. Redirect to IdP with SAML LogoutRequest
5. Same as IdP-initiated logout (flow always ends at IdP)

IdPv3 logout views (1)

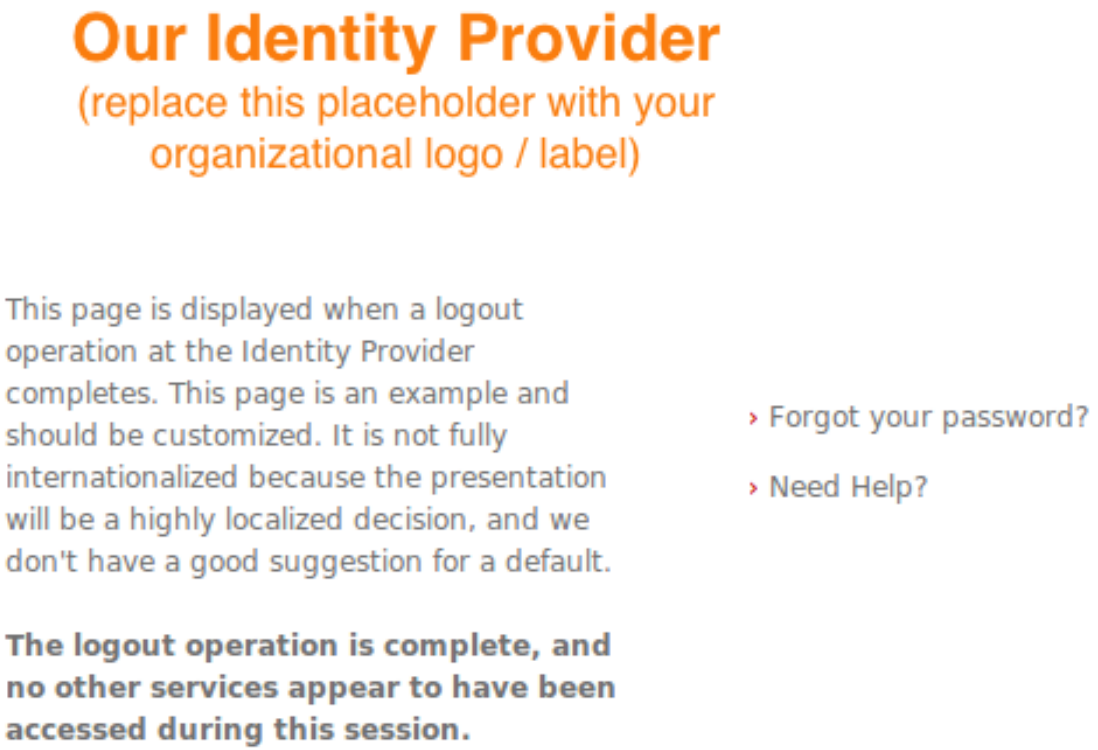


IdPv3 logout views (2)



- Shows list of SPs with logout status
- One hidden iframe per SP ⇒ each sends one SAML logout request
- Uses jQuery (https://jquery.com/)

IdPv3 logout views (3)



- No propagation question when the only SP in the session sends the logout request

Configuration overview

1. Enable SLO on your IdP (properties)
2. Publish IdP SLO endpoints in metadata (Resource Registry)
3. Enable SLO on your SP
4. If your SP-protected application has its own sessions:
   - Enable application notifications on your SP
   - Program your application to respond to logout notifications
5. Publish SP SLO endpoints in metadata (Resource Registry)
6. Test!

Configuration: IdP properties

Required to enable SLO

- Track SPs logged into
  `idp.session.trackSPSessions = true [false]`
- Enable receiving SAML logout requests from SPs
  `idp.session.secondaryServiceIndex = true [false]`

Reference: LogoutConfiguration
(https://wiki.shibboleth.net/confluence/display/IDP30/LogoutConfiguration)

Configuration: IdP properties

Optional tweaks

- Display SP information from metadata

  `idp.logout.elaboration = true [false]`

- How long does the IdP remember SPs? It cannot know the real SP session duration!

  `idp.session.defaultSPlifetime = PT2H [PT2H]`

  `idp.session.slop = PT0S [PT0S]`

- Require logout requests/responses be signed/authenticated, better leave it enabled

  `idp.logout.authenticated = true [true]`

Configuration: IdP SLO endpoints

Publish `SingleLogoutService` endpoints in metadata

	Single Logout Service
SAML2 HTTP Redirect binding	https://xenos.switch.ch/idp/profile/SAML2/Redirect/SLO Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect **Only partially supported by Shibboleth Identity Provider.**
SAML2 HTTP POST binding	https://xenos.switch.ch/idp/profile/SAML2/POST/SLO Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST **Only partially supported by Shibboleth Identity Provider.**
SAML2 SOAP binding	https://xenos.switch.ch/idp/profile/SAML2/SOAP/SLO Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:SOAP **Only partially supported by Shibboleth Identity Provider.**

Configuration: SP logout service

Add “SAML2” inside the `Logout` element (in `shibboleth2.xml`)

```
<Logout>SAML2 Local</Logout>
```

Reference: NativeSPServiceLogout
(https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPServiceLogout)

Configuration: SP logout notifications

Add a `Notify` element (in `shibboleth2.xml`)

```
<Notify Channel="front"
        Location="https://sp.example.org/app/logout-notify"/>
```

and program your application to respond at the given URL

References: NativeSPNotify (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPNotify), SLOWebappAdaptation (https://wiki.shibboleth.net/confluence/display/SHIB2/SLOWebappAdaptation)

Configuration: SP SLO endpoints

Publish `SingleLogoutService` endpoints in metadata

Single Logout Service	
SAML2 SOAP binding	https://xenos.switch.ch/Shibboleth.sso/SLO/SOAP Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:SOAP
SAML2 HTTP Redirect binding	https://xenos.switch.ch/Shibboleth.sso/SLO/Redirect Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
SAML2 HTTP POST binding	https://xenos.switch.ch/Shibboleth.sso/SLO/POST Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
SAML2 HTTP Artifact binding	Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact

Fixes for IdP 3.2.0 and 3.2.1 (1)

```
--- system/flows/logout/logout-flow.xml    2016/01/20 19:57:55    8080
+++ system/flows/logout/logout-flow.xml    2016/04/01 14:23:58    8190
@@ -73,7 +73,7 @@
 <view-state id="LogoutView" view="logout">
-    <on-entry>
+    <on-render>
         <evaluate expression="WriteAuditLog" />
         <evaluate expression="environment" result="viewScope.environme
         <evaluate expression="opensamlProfileRequestContext" result="v
@3,7 +83,7 @@
         <evaluate expression="flowRequestContext.getExternalContext().
         <evaluate expression="flowRequestContext.getExternalContext().
         <evaluate expression="flowRequestContext.getActiveFlow().getAp
-    </on-entry>
+    </on-render>
     <transition on="proceed" to="LogoutCompleteView" />
     <transition on="end" to="LogoutCompleteView" />
     <transition on="propagate" to="LogoutPropagateView" />
```

original diff from svn.shibboleth.net

(http://svn.shibboleth.net/view/java-identity-provider/trunk/idp-conf/src/main/resources/system/flows/logout/logout-flow.xml?r1=8080&r2=8190&pathrev=8190&diff_format=u)

Fixes for IdP 3.2.0 and 3.2.1 (2)

```
--- system/flows/logout/propagation/cas-flow.xml    2015/10/14 15:50:01
+++ system/flows/logout/propagation/cas-flow.xml    2016/04/01 14:23:58
@@ -3,12 +3,12 @@
       xsi:schemaLocation="http://www.springframework.org/schema/webflo

 <view-state id="ShowServiceLogoutView" view="cas/logoutService">
-    <on-entry>
+    <on-render>
         <set name="viewScope.logoutPropCtx"
              value="opensamlProfileRequestContext.getSubcontext(T(net.
         <set name="viewScope.messageID" value="T(java.util.UUID).rando
         <set name="viewScope.issueInstant" value="DateFormatter.print('
-    </on-entry>
+    </on-render>
     <transition on="proceed" to="proceed" />
 </view-state>
```

original diff from svn.shibboleth.net

(http://svn.shibboleth.net/view/java-identity-provider/trunk/idp-conf/src/main/resources/system/flows/logout/propagation/cas-flow.xml?r1=7822&r2=8190&pathrev=8190&diff_format=u)

Fixes for IdP 3.2.0 and 3.2.1 (3)

```
--- views/logout.vm    2016/01/05 12:57:59    8067
+++ views/logout.vm    2016/02/18 17:39:36    8095
@@ -65,10 +65,8 @@
 </ol>
 #else
 <p><strong>#springMessageText("idp.logout.complete", "The logout opera
-<!-- If SAML logout with no extra work to do, complete the flow by add
-#if ( $profileRequestContext.getProfileId().contains("saml2/logout") )
-<iframe style="display:none" src="$flowExecutionUrl&_eventId=proceed">
-#end
+<!-- Complete the flow by adding a hidden iframe. -->
+<iframe style="display:none" src="$flowExecutionUrl&_eventId=proceed">
 #end

 </div>
```

original diff from svn.shibboleth.net

(http://svn.shibboleth.net/view/java-identity-provider/trunk/idp-conf/src/main/resources/views/logout.vm?r1=8067&r2=8095&pathrev=8095&diff_format=u)

Fixes for IdP 3.2.0 and 3.2.1 (4)

```
--- views/logout-complete.vm    2015/10/28 16:17:35    7896
+++ views/logout-complete.vm    2016/02/18 17:39:36    8095
@@ -44,7 +44,7 @@

 <!-- If SAML logout, complete the flow by adding a hidden iframe. -->
 #if ( $profileRequestContext.getProfileId().contains("saml2/logout") )
-<iframe style="display:none" src="$flowExecutionUrl&_eventId=proceed">
+<iframe style="display:none" src="$flowExecutionUrl&_eventId=proceed">
 #end

 <footer>
```

original diff from svn.shibboleth.net

(http://svn.shibboleth.net/view/java-identity-provider/trunk/idp-conf/src/main/resources/views/logout-complete.vm?r1=7896&r2=8095&pathrev=8095&diff_format=u)

Fixes for IdP 3.2.0 and 3.2.1 (5)

```
--- system/views/logout/propagate.vm    2015/11/06 20:22:32    7958
+++ system/views/logout/propagate.vm    2016/02/18 17:39:36    8095
@@ -99,5 +99,5 @@

 <!-- If SAML logout, complete the flow by adding a hidden iframe. -->
 #if ( $profileRequestContext.getProfileId().contains("saml2/logout") )
-<iframe style="display:none" src="$flowExecutionUrl&_eventId=proceed">
+<iframe style="display:none" src="$flowExecutionUrl&_eventId=proceed">
 #end
```

original diff from svn.shibboleth.net

(http://svn.shibboleth.net/view/java-identity-provider/trunk/idp-conf/src/main/resources/system/views/logout/propagate.vm?r1=7958&r2=8095&pathrev=8095&diff_format=u)