

Logout Support on SP and Application

Possibilities and Limitations



SWITCH

SWITCHaai Team
aai@switch.ch

Single Logout: Is it possible?

Single Logout will work only in some cases reliably!

The only safe ways to log out from all applications are:

- **to delete all session cookies**
 - Have fun explaining an average user how to do this with his browser
 - Won't log you out if authenticated via Basic Auth, X.509 certificates, ...
- **or the recommended way: exit the web browser!**
 - Quickest, most reliable and easiest way to explain
 - Also logs users off from Facebook etc. :-)
 - But: Some modern browsers even restore transient sessions on restart (depending on the settings)

Agenda

- Single Logout in Federation
- Single Logout Issues
- Single Logout for SP
- Single Logout for IdP
- Support Resources

Single Logout in Federation

- Users access multiple services, but need to login once only
- They might be logged in to multiple services
- ... but how do they logout again from all services?
- The solution seems to be easy:
 - The user initiates the single logout process
 - The user is logged out from all services and the IdP in turn
- But:
 - Where does the user start the single logout process?
 - Who knows all of the services the user is currently logged in?
 - Should the user be logged out from all services in the federation, or also from Google Mail, Facebook, etc.?
 - What happens if an error occurs during the whole logout process?
- **Logout will be possible but it has a lot of limitations!**

SAML 2 SLO Messages and Flow

- SAML 2 SLO may be initiated by either the Identity Provider (IdP) or the Service Provider (SP)
- SP-initiated SLO:
 - An SP sends a logout request to the IdP
 - At the IdP, for each SP to which the user has authenticated:
 - The IdP sends a logout request to the SP
 - The SP attempts to destroy its session for the user and sends back a logout response indicating if this was successful
 - The IdP destroys its session for the user
 - The IdP sends a logout response to the initiating service provider, which then destroys its session
- It is the responsibility of the SLO initiator to provide the user with information about whether SLO has succeeded or failed.

SLO Issues: User Experience

What does a user expect when clicking on logout?

- Logout only from this single application?
 - Is of little use because of Single Sign On
- Logout from all applications where logged in? Which?
 - Also from Google Mail, eBay and other non AAI applications?

Therefore:

- Users must understand the consequences of logout
 - Must know that they currently are signed in to a single sign-on (SSO) system and what will result from clicking on logout
- Users must always know if logout has completely succeeded
 - Otherwise they may assume that it has and leave the computer, allowing someone else to erroneously access a service

SLO Issues: Logged in vs. Logged out

What defines if a user is logged in via AAI/application?

- 🍪 Shibboleth session cookie
- 🍪 Application session cookie (optional)
 - Some applications only check if user was authenticated via AAI

What is necessary to log out a user?

- Delete Shibboleth and application cookies (front-channel)
 - Only possible when user's browser is involved
 - Administrative logout not possible
- Or delete session information on server (back-channel)
 - Only possible if user's Shibboleth sessionID is known in application
 - Implies adaptation of application

SLO Issues: Technical Difficulties (1)

Front-Channel vs. Back-Channel problems

- Front-Channel: Protocol flow via browser
 - Process might break
 - User might get confused
- Back-Channel: Direct communication between SP and IdP
 - User's session cookie is not available

SAML 2 vs. SAML 1

- Only SAML 2 supports single logout
- There are still some Service Providers in SWITCHaai that support SAML 1 only (e.g. some publishers)
 - The user will not get logged out from SAML 1 services

SLO Issues: Technical Difficulties (2)

SP session vs. application session

- The SP and the web application often manage separate sessions
- SLO must make sure that both sessions are destroyed

The two flavors of logout

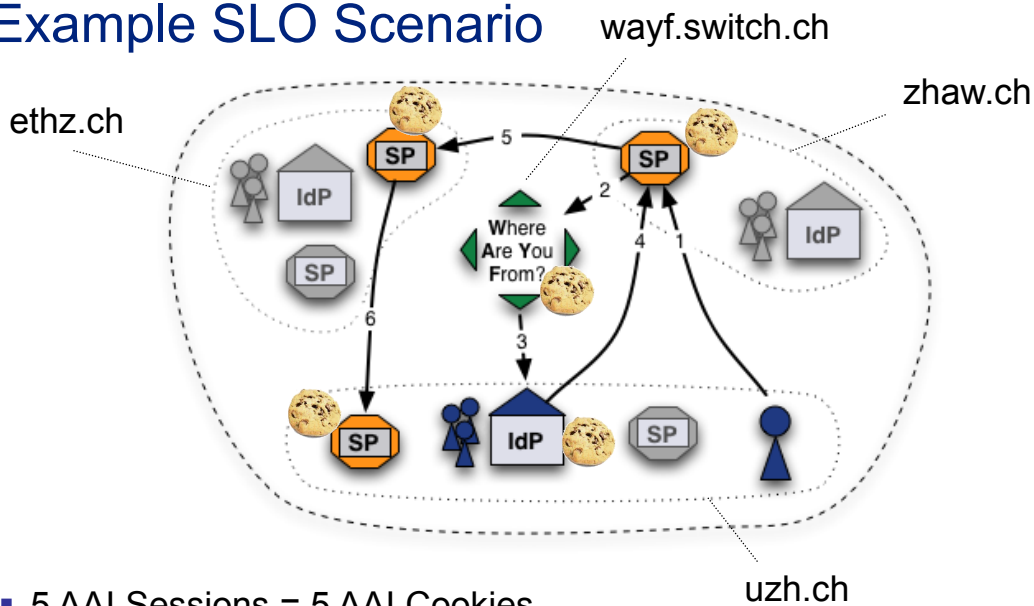
Local logout

- User's session is deleted only for one Service Provider
 - Not of much use due to Single Sign-On (SSO)
 - Or "egoistic" if IdP session also is bilaterally deleted but all other SP's session are still intact.

Global logout = Single Log Out (SLO)

- User's SSO session deleted on IdP and **all** SPs
 - For authentication methods like HTTP Basic Auth or some external authentication systems, the IdP cannot destroy the SSO session!
 - Only safe way for logout is to cleanly exit the web browser or even to logout from the system!

Example SLO Scenario



- 5 AAI Sessions = 5 AAI Cookies
 - 1 at IdP (uzh.ch)
 - 3 at SPs (zhaw.ch, ethz.ch, uzh.ch) but applications also have a cookie...
 - 1 at WAYF/DS (wayf.switch.ch)

How to get rid of sessions?

- SP "just" needs to delete all cookies that identify session
 - Impossible for Service Provider because cookies probably are for different domains or hosts
- Redirect browser to each SP, IdP and WAYF in order to delete cookies (front-channel logout)
 - What happens if one host is down? User is stranded
- Use IFRAMES to send browser to all components
 - Solves some of the technical issues but administrative logout (force logout of a malicious user) still is not possible

Current state of SLO in Shibboleth (1)

SLO requires:

- SAML 2 (Shibboleth 2)
- Built-in form-based username/password authentication method

Shibboleth Service Provider 2.5.x

- Supports local and global logout

Shibboleth Identity Provider 2.4.x

- Supports local and global logout
- Doesn't support "full" SAML 2 logout, i.e. doesn't support logout from multiple Service Providers

Current state of SLO in Shibboleth (2)

Adapted Applications:

- Worldwide there are less than 10 applications that already are ready to support SAML 2 logout (incl. Moodle, ILIAS, Resource Registry)

Enabling Single Logout on the SP

Enable SLO for SP to support global logout:

- Add "SAML2" to the existing <Logout> element in the Shibboleth SP configuration in /etc/shibboleth/shibboleth2.xml

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

- SAML 2 logout is initiated by accessing the following URL:
<https://ilias.example.com/Shibboleth.sso/Logout>
 - If the IdP supports SAML 2 logout, too, then SAML 2 logout starts.
 - Else, local logout is done.
- By default, the IdP doesn't return to the SP
 - SP can be configured to force returning (IdP possibly returns with "partial logout" status)

Enabling Single Logout in the web application

If the application manages its own session, it needs to be adapted or configured to support single logout


- The application needs to implement a "logout notification handler"
<https://wiki.shibboleth.net/confluence/display/SHIB2/SLOWWebappAdaptation>
 - SP notifies the application about logout through a "back-channel"
 - Application needs to destroy the session
- Some applications, like Moodle and ILIAS, have built-in support (see documentation)
- Notification must be enabled in the Shibboleth SP configuration in /etc/shibboleth/shibboleth2.xml

```
<Notify  
  Channel="back"  
  Location="https://ilias.example.org/.../shib_logout.php"/>
```


Enabling Single Logout on the IdP

- Requires Shibboleth IdP version 2.4.0 or higher
- Configure IdP to support SAML 2 SLO:
 - Relying Party SAML 2 Logout Request Profile in `relying-party.xml`
 - Configure SAML 2 SLO handlers in `handler.xml`
- Implement logout page in `logout.jsp`
 - Final landing page after SLO
 - Tells user the results of the logout

Example Landing Page on IdP



SWITCHaai

Abmeldung

Sie haben sich vom Anmelde-Dienst (Identity Provider) abgemeldet. Möglicherweise sind Sie aber noch bei einem oder mehreren der folgenden Dienste angemeldet:

- **AAI Attributes Viewer** (<https://aai-viewer.switch.ch/shibboleth>)
- **Resource Registry** (<https://rr.aai.switch.ch/shibboleth>)

Bitte beachten Sie folgendes:

Falls Sie an einem Computer arbeiten, der von mehreren Personen verwendet wird (z. B. Computer in Internet Café):
Bitte melden Sie sich ganz ab (Abmeldung von Mac OS X) und starten Sie evtl. den Computer neu. Ansonsten ist es möglich, dass fremde Personen später auf Ihre persönlichen Daten zugreifen können, da Sie möglicherweise trotzdem noch bei anderen Diensten angemeldet sind.

Falls Sie an Ihrem privaten Computer arbeiten, der nur von Ihnen verwendet wird:
Wenn Sie sicher sein möchten, dass Sie auch von anderen Diensten abgemeldet sind, empfehlen wir Ihnen, die Chronik des Browsers (insbesondere Cookies) zu löschen, oder den Computer neu zu starten. (Es reicht teilweise nicht aus, nur den Browser zu schliessen.)

Conclusion

- Single Logout is partially possible
- Works well if user is logged in to one application only
- It's still better to get logged out from the IdP than not to logout at all

Support Resources

- Single Logout Issues
 - <https://wiki.shibboleth.net/confluence/display/SHIB2/SLOIssues>
- Single Logout for Shibboleth SP
 - Configuration of SP Logout Initiator
<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPLogoutInitiator>
 - Adaptation of Web Application
<https://wiki.shibboleth.net/confluence/display/SHIB2/SLOWebappAdaptation>
 - Logout notification to application
<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPNotify>
- Single Logout for Shibboleth IdP
 - <https://wiki.shibboleth.net/confluence/display/SHIB2/IdPEnableSLO>