Single Logout with the SWITCH edu-ID IdP

Daniel Lutz & Thomas Lenggenhager
aai@switch.ch

Berne, 14. March 2018
Overview

• SLO with the SWITCH edu-ID IdP
  • The scenarios with Screenshots

• Open issues with SLO and Shibboleth IdP v3.3

• How to make an SP SLO compliant

• What you should know about SP SLO
Single Logout Scenarios

The scenarios
a) Logged in at a single SP

b) Logged in at multiple SPs
   b1) All support SLO
   b2) Not all support SLO

Logout initiated at the SWITCH edu-ID My Account web application for all scenarios:
Case a) Logged in at a single SP

You have been logged out successfully.

You can now close your browser or the current tab.
Case b1) Logged in at multiple SPs (1/3)

You have been logged out successfully.

You're still logged in to the following services:

- AAI Attributes Viewer
- AAI Attributes Viewer Test

Log out of all services  Stay logged in
Case b1) Logged in at multiple SPs (2/3)

user picked: Stay logged in

You have been logged out successfully.

You're still logged in to the following services:

- AAI Attributes Viewer
- AAI Attributes Viewer Test

You can now close your browser or the current tab.
Case b1) Logged in at multiple SPs (3/3)

You have been logged out successfully of all SWITCH edu-ID services.

You can now close your browser or the current tab.
Case b2) Logged in at multiple SPs (1/3)

You have been logged out successfully.

You're still logged in to the following services:

- AAI Attributes Viewer
- SWITCH WWW

Log out of all services  Stay logged in
Case b2) Logged in at multiple SPs (2/3)

user picked: Stay logged in

You have been logged out successfully.

You're still logged in to the following services:

- AAI Attributes Viewer
- SWITCH WWW

You can now close your browser or the current tab.
Case b2) Logged in at multiple SPs (3/3)

user picked: Log out of all services

Logout failed for some services:

- SWITCH WWW

For security reasons, we recommend to close your browser. This is all the more important when working at a public computer (e.g. in computer pools or Internet cafés).
Open issues with SLO and Shib IdP v3.3 (1/3)

Default user experience has some deficiencies

Case a)

Our Identity Provider
(replace this placeholder with your organizational logo / label)

This page is displayed when a logout operation at the Identity Provider completes. This page is an example and should be customized. It is not fully internationalized because the presentation will be a highly localized decision, and we don’t have a good suggestion for a default.

The logout operation is complete, and no other services appear to have been accessed during this session.

Case b)

Our Identity Provider
(replace this placeholder with your organizational logo / label)

This page is displayed when a logout operation at the Identity Provider completes. This page is an example and should be customized. It is not fully internationalized because the presentation will be a highly localized decision, and we don’t have a good suggestion for a default.

Would you like to attempt to log out of all services accessed during your session? Please select Yes or No to ensure the logout operation completes, or wait a few seconds for Yes.

Yes  No

If you proceed, the system will attempt to contact the following services:
Demo SP2
Demo SP1

or wait a few seconds for Yes
Open issues with SLO and Shib IdP v3.3 (2/3)

text stays on screen, even after completion

Case b2)
Open issues with SLO and Shib IdP v3.3 (3/3)

• The modifications applied on the SWITCH edu-ID IdP are not forward compatible with future versions.

• No deployment instructions we could recommend for SLO with a Shibboleth IdP 3.3.
How to make an SP SLO compliant (1/4)

• Prepare your SPs for SLO
  • The SP will profit of local logout immediately and of SLO once the IdP is SLO capable
User initiates Logout from a page without frames

Replace in `shibboleth2.xml` the `<Logout>Local</Logout>` element with `<Logout>SAML2 Local</Logout>`

Terminate the web application session

Case a) web application has no session management
   → sufficient to terminate the SP session

Case b) web application has own session management
   • Application session timeout ≤ SP session timeout.
   • Application has a mapping: internal session ID ↔ SP session ID.
   • SP needs to be able to end the web application session.
   → Add a `<Notify>` element to `shibboleth2.xml`

This points to the web application’s logout link. At the end, the application must redirect to the return link provided as query parameter.
How to make an SP SLO compliant (3/4)

• Additional requirements for non-Shibboleth SPs
  • SP must support HTTP-Redirect binding.
  • SLO requests MUST be signed.
  • The `<saml:NameID>` element in `<samlp:LogoutRequest>` messages MUST NOT be encrypted.
  • SLO responses MUST be signed.

These requirements were derived from the draft
SAML V2.0 Interoperability Deployment Profile V1.0:
https://kantarainitiative.github.io/SAMLprofiles/saml2int.html
How to make an SP SLO compliant (4/4)

- **Behavioral requirements**
  - SPs MUST terminate a subject’s local session **before** issuing a `<samlp:LogoutRequest>` message to the IdP.
  - SPs MUST NOT issue a `<samlp:LogoutRequest>` message as the result of an idle activity timeout.
  - Only publish a SLO service location in the Resource Registry once all the requirements are met. ➔ This avoids bad user experience.

- **Virtual Hosting Limitations**
  - An SP that maintains distinct sessions across multiple virtual hosts SHOULD identify itself by means of a distinct `entityID` (with associated metadata) for each virtual host.
    ➔ A single entity can have **only one** `<SingleLogoutService>` endpoint per binding.
What you should know about SP SLO

Five independent sessions at IdP, SP1, app1, SP2 & app2

End of SP session does not necessarily imply end of Application session.

Each session has its own timeout. Ensure: $SP_{timeout} \geq App_{timeout}$

User has to initiate SLO. A timeout should never trigger SLO.
SP Single Logout in action (1/12)

1) User clicks Logout within **Application 1**
2) **Application 1** ends its session
3) **Application 1** redirects to **SP1 Logout**
4) **SP1** ends its session
SP Single Logout in action  (5/12)

5) **SP1 redirects to IdP Logout**

Diagram:

- **_idp_session: IdP**
- **_shibsession: SP_1**
- **session-cookie: appl**
- **SP1** connected to Application 1
- **SP2** connected to Application 2
- **_shibsession: SP_2**
- **session-cookie: app2**
6) **IdP** ends its session

**Diagram:**
- **IdP**
  - `_idp_session`: IdP
- **SP1**
  - `_shibsession`: SP_1
  - Session-cookie: appl1
- **SP2**
  - `_shibsession`: SP_2
  - Session-cookie: app2

© 2018 SWITCH | 25
7) **IdP** offers choice for **Logout all** or **Stay logged in**

- **Sp1**
  - _shibsession: SP_1
  - session-cookie: appl
  - Application 1

- **Sp2**
  - _shibsession: SP_2
  - session-cookie: app2
  - Application 2

- **Idp**
  - _idp_session: IdP

**Log out of all services**  **Stay logged in**
8) **IdP calls SP2 Logout in a frame**

User clicked on:

Log out of all services
9) **SP2** redirects within the frame to **Application 2** logout
10) **Application 2** ends its session and redirects to **SP2 Logout**
11) **SP2** ends its session and redirects back to **IdP**
12) **IdP** reports success
Single Logout Guide

• Initially it will be for SP only, based on the content of these slides.

• Once the issues are solved on the IdP side, an SLO guide for IdP will follow.

• Ensure a good user experience:

  Register a SLO Service Location only once you are sure that the entity is capable to handle SLO properly.