SLODemo

!!! warning

```
For more complete description please go and see [how Single Logout is
implemented](https://help.edu.hu/books/aai/page/single-logout-in-shibboleth-idp) in Shibboleth
IdP.
```

To demonstrate the features we have prepared a demo application. The main purpose of the demo is to test the UI and various error conditions.

Preparing

- Metadata (unsigned)
- IdP: Based on Adam's Git repository

!!! info

```
This version is **still unreleased**.

You can grab a snapshot from the web-basedGit repository by selecting the latest commit and
clicking on the `snapshot` link
```

Authentication

There are 100 demo users from `demo1..100`, all users have the password 'demo'.

!!! info

```
It was necessary to use more than one demo account because IdP sessions mix if two testers
(browsers) share the same userid.

So if you face strange results (like trying to log out from SP's you were not logged in),
please first try it with another demoXX account to sort out possible IdP session mixing
problem.
```

The IdP uses the UsernamePassword Login Handler. **IdP logout is not possible with container-based authentication (like HTTP / X.509 / Kerberos)**.

Service Providers

SP1: (Not-so) Old Release

SP software	Shibboleth 2.2.1 (Debian backports)
Front channel logout	supported
Back channel logout	supported
Notes	This was a 2.1 SP which used to report partial logout on backchannel. Now it's working OK.

SP2: Bright Shining Star

SP software	Shibboleth 2.2.1 (Debian SID)
Front channel logout	supported
Back channel logout	supported
Notes	Both front- and back-channel logout should work properly

SP3: The Pretender

SP software	SimpleSAMLphp SAML2 SP
Front channel logout	supported
Back channel logout	not supported
Notes	SimpleSAMLphp does not support back-channel bindings, therefore the metadata does not contain it

SP4: Use The Backdoor, Please!

SP software	Shibboleth 2.2.1 (Debian SID)
Front channel logout	not supported

SP software	Shibboleth 2.2.1 (Debian SID)
Back channel logout	supported
Notes	The metadata of this SP does not contain front-channel bindings for logout

SP5: Old Slowhand

SP software	Shibboleth 2.2.1 (Debian backports)
Front channel logout	not working (times out)
Back channel logout	not working (times out)
Notes	Metadata points to a fake logout service that is not answering in time. Actually this is a PHP script that returns a `500 Internal Server Error` after 20 seconds of delay, similarly to an overloaded webserver. Actually there is a big difference: usually an overloaded server can not complete TCP connection establishment in time. This test only delays the sending of responses

SP6: Shibboleth Neanderthalensis

SP software	Shib 1.3 (IRL: Shibboleth 2.2.1 Debian backports)
Front channel logout	not supported
Back channel logout	not supported
Notes	The metadata of this SP does not contain any logout services, just like a normal Shib1.3 SP

SP7: Good Guy Speaking Ancient Greek

SP software	Shibboleth 2.2.1 (Debian SID)
Front channel logout	supported
Back channel logout	supported
Notes	This is a 2.x SP but it uses Shibboleth 1.3 SSO protocol. I'd expected a logout failure because of the Shibboleth-specific NameID format, however it turned out to be working.

SP8: Blitzkrieg

SP software	Shibboleth 2.2.1 (Debian SID)
Front channel logout	not working (if timed out)
Back channel logout	not working (if timed out)
Notes	This is a special SP that has a very short session lifetime (30 sec). If you hit the logout button within 30 sec, it should work but it should fail afterwards, because the principal is no longer known to the SP.

SP9: Knight Without Armour

SP software	Shibboleth 2.2.1 (Debian SID)
Front channel logout	supported
Back channel logout	supported
Notes	This SP only supports HTTP for both SSO and SLO. Presumably, it would not work if the SSO was using HTTPS (not checked).

How this demo works

The SLO Demo runs in a separate machine from all the SPs and IdP. So it has no information if the login is succeeded or not, it just hopes, everything goes as expected.

Below is a very brief description of the logout demo.

Selecting SPs

At first the user selects the SPs he/she wants to log in. The order of the login is currently sequential (not sure if it makes any difference).

Redirecting to SPs

1. all SP sessions are initiated by using `302 Redirect`s to the SPs SessionInitiator by specifying only the IdP entityID (https://sandbox.slotest.aai.niif.hu/idp/shibboleth).
   - the simpleSAMLphp login URL is somewhat similar but not the same
2. the SP initiates the session (the first one gets the user logged into the IdP)
3. the SP redirects to the homeURL

4. homeURL redirects back to the redirection point of the demo interface (by some trivial PHP script)
5. the demo interface starts over with the next SP or displays summary page

Summary page

The (supposedly) logged in SPs are displayed along with their logout urls. Logout opens up in a new window.

Logging out

User clicks on one of the logout URLs.

Start over

On page refresh you can start it over. If you are not asked for password by the IdP, it means that your IdP session was not cleared properly, therefore the logout is failed.

How to get your SP involved

1. Configure the SP as you wish
   - **Don't forget to set `signing="true"` or `signing="false"`**, as described in the SLO documentation
2. Configure the target application (or the page which is served on homeURL) to redirect to `[https://www.aai.niif.hu/SLODemo/sloDemoLoginRedirect.php](https://www.aai.niif.hu/SLODemo/sloDemoLoginRedirect.php)`.
3. Send SP details to **aai *at* niif *dot* hu**
   - Metadata
   - SessionInitiator URL
   - Optionally:
   - Front-channel logout initiator (if there's any)
   - Back-channel logout initiator (if there's any)
   - SP software & version
   - Session handler (attribute viewer) URL
   - Short description of what to test
   - A funny name, of course ;)
4. Configure your SP to trust slotest metadata (this will contain your SP metadata as well).
5. Please inform us when your test SP is no longer functioning

Setting up a back-channel only LogoutInitiator

See this Jira entry for background. If you have a pre-2.2.1 SP, you should use:

```
<LogoutInitiator type="Chaining" Location="/BackChannelLogout" relayState="cookie">
  <LogoutInitiator type="SAML2" outgoingBindings=" " />
  <LogoutInitiator type="Local"/>
</LogoutInitiator>
```

Expected results

SAML2

Single Logout profile is for SAML2 only. Therefore SP6 (Neanderthalensis) will always fail. Note that SP7 (Ancient Greek) actually *speaks* SAML2 although it initiates SSO with Shibboleth protocol. Therefore you cannot **initiate** SLO from SP7 but you can participate in SLO.

SP5 (Old Slowhand) will always fail unless the Logout request is initiated by it.

Front-channel, back-channel

The IdP can fallback to back-channel, if the logout is front-channel and the SP software does support only back-channel bindings. **Not the other way**, because front-channel bindings need the information held in browser cookies. Therefore front-channel SLO will work with SP4 (Backdoor) if initiated by some other SP's, but SP4 can only initiate back-channel SLO (which is not supported by many of the SP's above.)

Unexpected results

TODO

Support NoScript

!!! warning "TODO"

```
NoScript support has been added recently to front-channel logout, thorough testing is still necessary.

The user interface is a bit clumsy, because the daisy-chain of redirects is a no-go and some browser not even support frames. Ideas, tips are welcome for making it better.

The main rationale behind supporting noscript is to make it even possible to use logout with other clients than web browsers. Bach-channel is much more convenient for them, though.
```

Test with Application Notification

!!! warning "TODO"

```
Contribution is welcome!
```

Try it with various browsers

!!! warning "TODO"

```
Contribution is welcome!
```

Misc

- Publish shibd and IdP logs on a web page (real-time?)
- Add IPv6 addresses to the vhosts
- Add OpenSSO test SP

Változat #1
document-uploader hozta létre 2025-08-07 12:06:15 CEST
document-uploader frissítette 2025-08-07 12:06:15 CEST