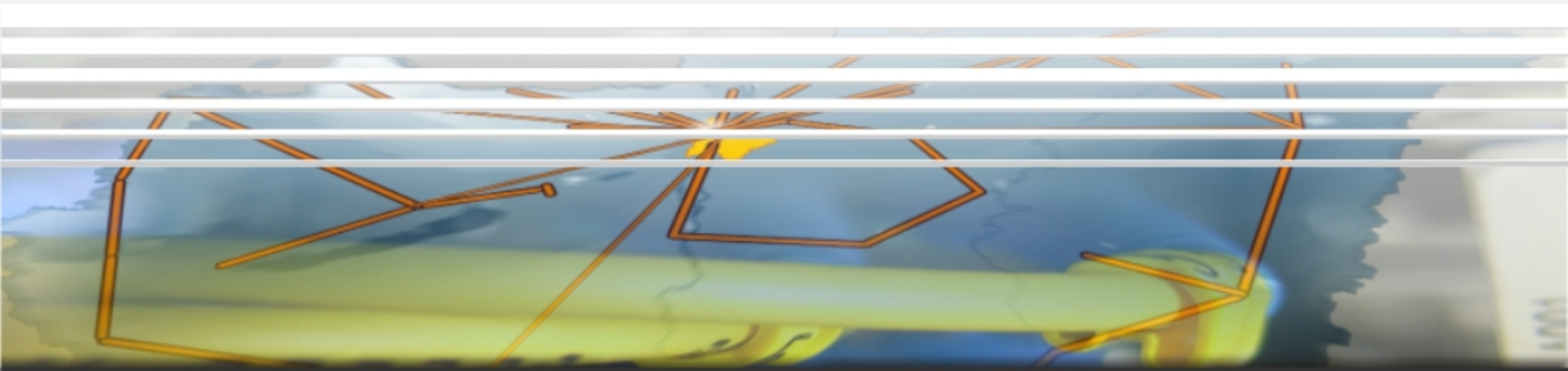


# Single Logout



TF-EMC2 2010

Vienna

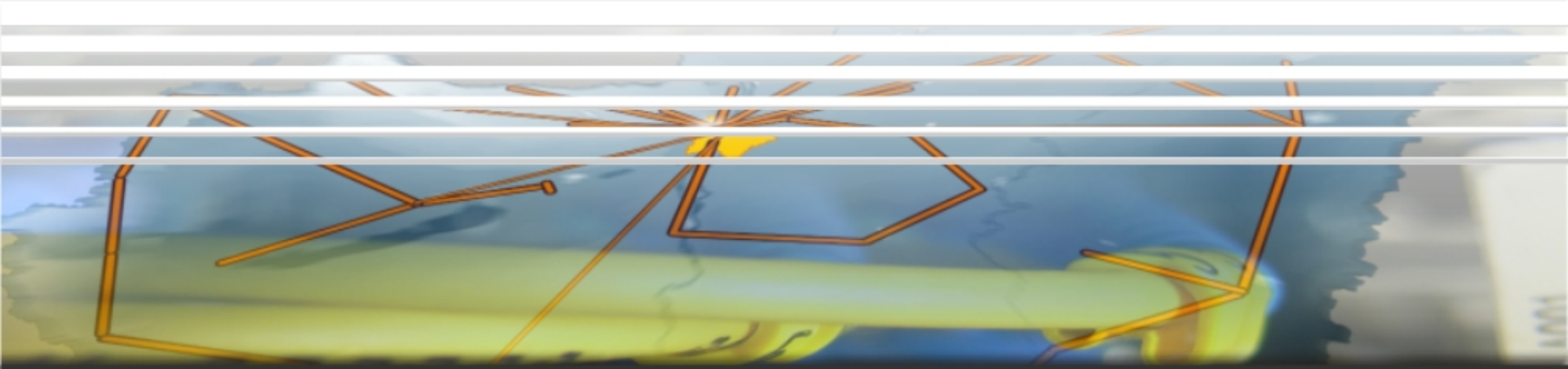
17<sup>th</sup> February 2010

Kristóf Bajnok

NIIF Institute



# Single Logout Sucking



TF-EMC2 2010

Vienna

17<sup>th</sup> February 2010

Kristóf Bajnok

NIIF Institute



# Everybody wants to logout...

- Single sign-on is a powerful toy
  - many want to be able to explicitly terminate the SSO session
  - they get disappointed if they're told to close their browsers
  - sometimes they can't quit from their browsers
    - user error: remaining download windows, OS/X behaviour, ...
    - kiosks, smart phones

# Ultimate job of implementing logout

- Do everything to achieve logout
- Never give the users false sense of security

# SLO profile in SAML2

- Initiator
  - SP or IdP
- IdP notifies each session participant
- Bindings
  - front-channel + back-channel
    - initiating SP should prefer front-channel
    - IdP can use arbitrary binding which is claimed to be supported by the SP in the metadata
    - [administrative logout is only possible with back-channel]
- Transport and signing requirements

# Problems with SLO

- User interface, usability
- Interoperability
- Session management

# User interface, usability

- Avoid daisy-chains of redirects
- Prepare for a session participant
  - not responding
  - providing invalid answer and not redirecting back to the IdP properly
- Provide detailed information about the logout process
  - let the user decide to terminate all sessions or not
  - display what's going on
  - display the results

# IFrame-based UI (Shibboleth implementation)

- Idea from UNINETT / SimpleSAMLphp
- AJAX + IFrame
  - each IFrame has a GET to the local `SLOServlet`
  - can use GET/POST/SOAP bindings
  - status polled by JavaScript
- Send final `LogoutResponse` via `iFrame`
  - and don't give control to the initiating SP
- Fallback to a clumsy interface if JavaScript / Frames are not supported

Credits: Adam Lantos, Tamas Frank @ NIIF

## Logging out

### You have logged out from

(Not-so) Old Release

### You are logged in on these services

Good Guy Speaking Ancient Greek

The Pretender

Bright Shining Star

## Logging out

Bright Shining Star ✓

(Not-so) Old Release ✓

Good Guy Speaking Ancient Greek [Logout from this SP](#)

Use The Backdoor, Please! ✓

The Pretender [Logout from this SP](#)

Refresh

<https://www.aai.niif.hu/SLODemo/sloDemo.php>

### Do you want to logout from all the services above?

Yes, all services

No, only from (Not-so) Old Release

## Logging out

Bright Shining Star ✓

(Not-so) Old Release ✓

Good Guy Speaking Ancient Greek ✓

Use The Backdoor, Please! ✓

The Pretender ✓

You have successfully logged out

Bright Shining Star ✓

(Not-so) Old Release ✓

Good Guy Speaking Ancient Greek ✓

Use The Backdoor, Please! ✓

The Pretender ✓

You have successfully logged out

Finish logout

out



# IFrame + cookies

- Cookies are needed by the SPs to terminate session (front-channel)
- If the request is made in an IFrame, the browser treats the SP as a **third party**
  - some policy settings block third party cookies
    - usually not by default
    - some browsers block only Set-Cookie
  - unless they share a common domain
    - the meaning of which varies between browsers and versions

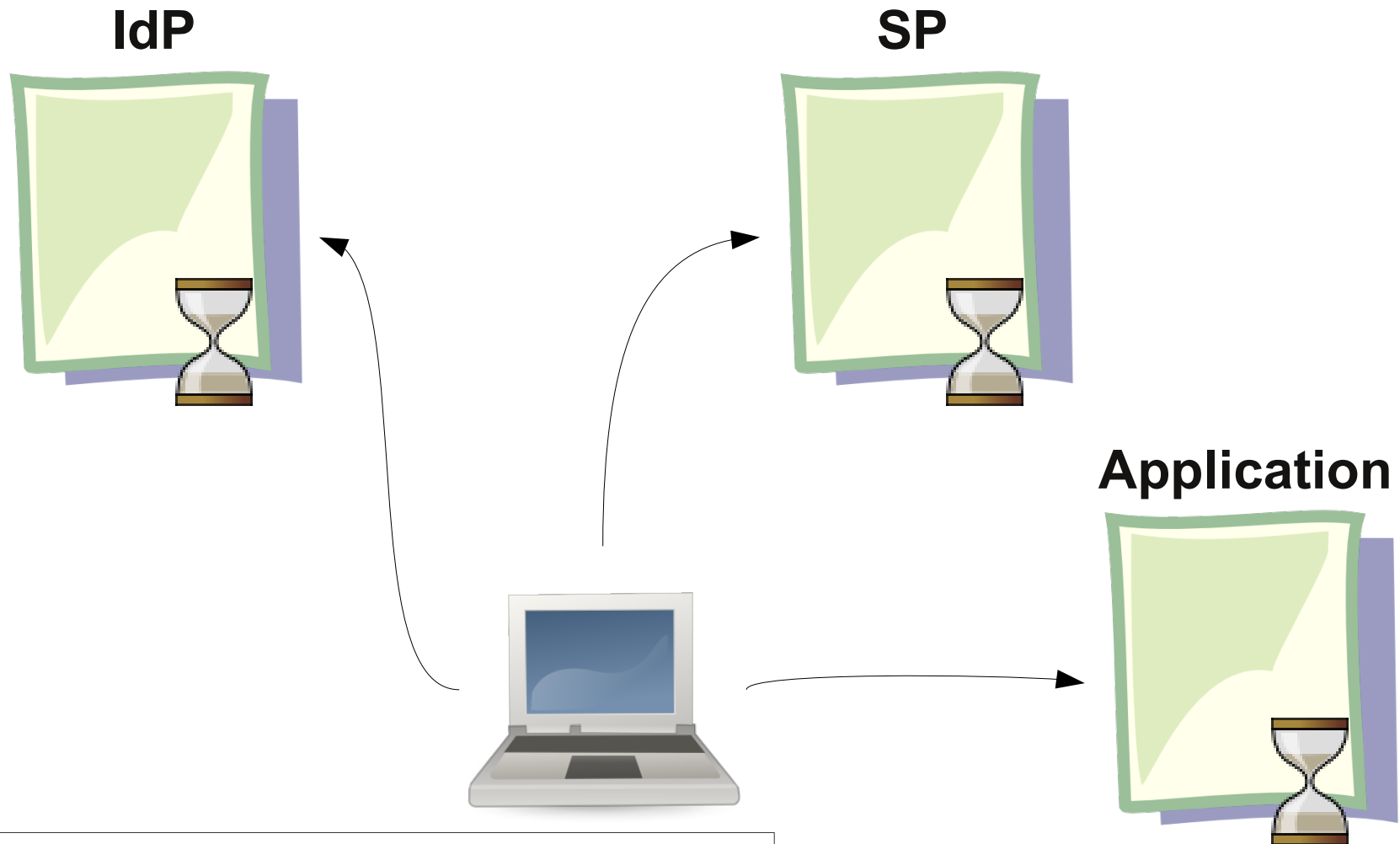
# Solving UI problems

- Either
  - users need to allow third-party cookies
  - or the SPs should be able to look up (and destroy) sessions based on the NameID
    - required for back-channel logout
    - required for cookie-less operation

# Interoperability

- SimpleSAMLphp does not support back-channel SLO bindings
- SSP does not sign logout messages
  - it's against the standard
    - Shib IdP implementation requires it by default
    - insecure unless the endpoint is HTTPS
  - neither does Shibboleth SP by default ;)
    - you can turn it on for all front-channel and back-channel messages (even for SSO)
- Oh... and Internet2 Shibboleth IdP does not support SLO ☹

# Session management



Independent sessions  
with independent *inactivity timeout*  
and session *lifetime*

# Session management: SP ↔ Application

- Stale application sessions should be avoided
- Check SP session validity on every page refresh
  - not possible to do real-time logout or tell the number of active sessions
- Alternative
  - Shibboleth SP Notify mechanism (*push*)
    - different for front-channel and back-channel

<https://spaces.internet2.edu/display/SHIB2/SLOWWebappAdaptation>  
<https://spaces.internet2.edu/display/SHIB2/NativeSPNotify>

# Session management: IdP ↔ SP

- The IdP must keep track of the active SPs for the user
  - SP session can expire before the IdP session
    - the user gets logout error
      - which is still much better than...
  - IdP session can expire before the SP session
    - SLO is not possible
    - after logging in again, **stale SP sessions remain**
      - even after doing 'proper' SLO
    - SP session lifetime **MUST** be limited by the `SessionNotOnOrAfter` attribute in the `AuthnStatement`

# Conclusion?

- It's not possible to implement true global logout in middleware generally
- It's possible to implement something that
  - conforms to the spec
  - can be used in certain cases
    - better-than-nothing
  - can be easily misused
    - who is responsible for not doing this?
- Non-SAML approaches can be viable
  - cookie removal by browser plugins
  - proprietary synchronisation of session data
    - like in enterprise products (eg. OpenSSO)

# What can federations do?

- Allow SLO endpoints in the metadata
  - disclaiming any warranty
- Push developers to solve interop issues
- Extend SSO requirements with `SessionNotOnOrAfter` and SP session lifetime-limiting
- Provide reference implementations for application notification mechanism
- **Educate admins**

# Recommended readings

- SAML2 SLO and SSO Profiles
- Front-channel SLO Deployment Profile  
<http://rnd.feide.no/content/front-channel-single-logout-deployment-profile>
- SLO issues  
<https://spaces.internet2.edu/display/SHIB2/SLOIssues>
- SLO implementation for Shibboleth IdP  
<https://wiki.aai.niif.hu/index.php/ShibIdpSLO>  
<https://www.aai.niif.hu/ShibIdPSLO> (binary build)