Enhancing shibboleth to access Web Educational Resources more securely

Prof. Hatem Hamad

Islamic University – Gaza (IUG)
Palestine

Agenda

1. Introduction
2. Problem Definition
3. Proposed solution
4. Implementation
5. Conclusion

Web Educational Resources

- student portal
- Llibraries
  - Student services
  - Complex Web applications such as Learning management System

Federated Identity

Federated Identity is a single sign-on (SSO), in which a user's single authentication ticket, or token, is trusted across multiple IT systems or even organizations.

Federated Identity

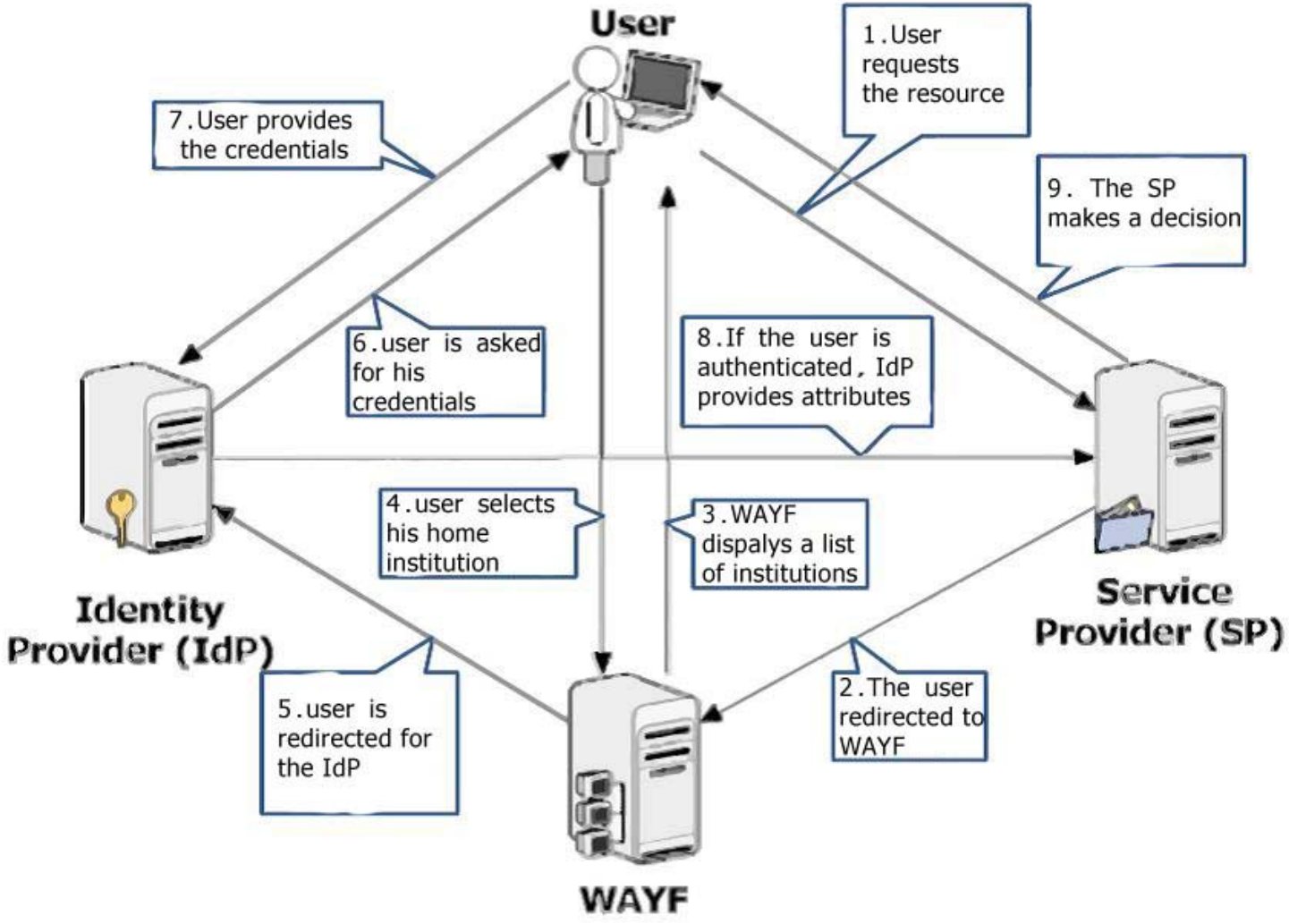
- Set of agreements, standards and technologies
- Trust relationships between organizations

- Integrity and privacy perserved
- Independance of organizations

Federated Identity Participants

- Service Provider (SP):
  - Provides one or more services within a federation
  - Access control policy
- Identity Provider (IdP):
  - Creates, maintains, manages identity information
  - user must authenticate at an IdP recognized by a SP
- Users:
  - wish to access services and consume resources

Federation System



SSO and SLO

- Single Sign On (SSO):
  - Sign on once at a site (single account)
  - Seamless signed-on for other sites
  - No extra authentication
  - SP both within and across circles of trusts
- Single Log Out (SLO):
  - Synchronized session logout
  - All sessions authenticated by an IdP closed !!

The Logout Process in Shibboleth Federation system

1. The logout in shibboleth specification is defined as a ***local logout***.
2. The solution introduced by shibboleth community was the second logout case ***Local logout with browser close***.
3. Researcher works on that problem and some of them introduces the third case with a partial solution to the global logout ***with forcing re-authentication***

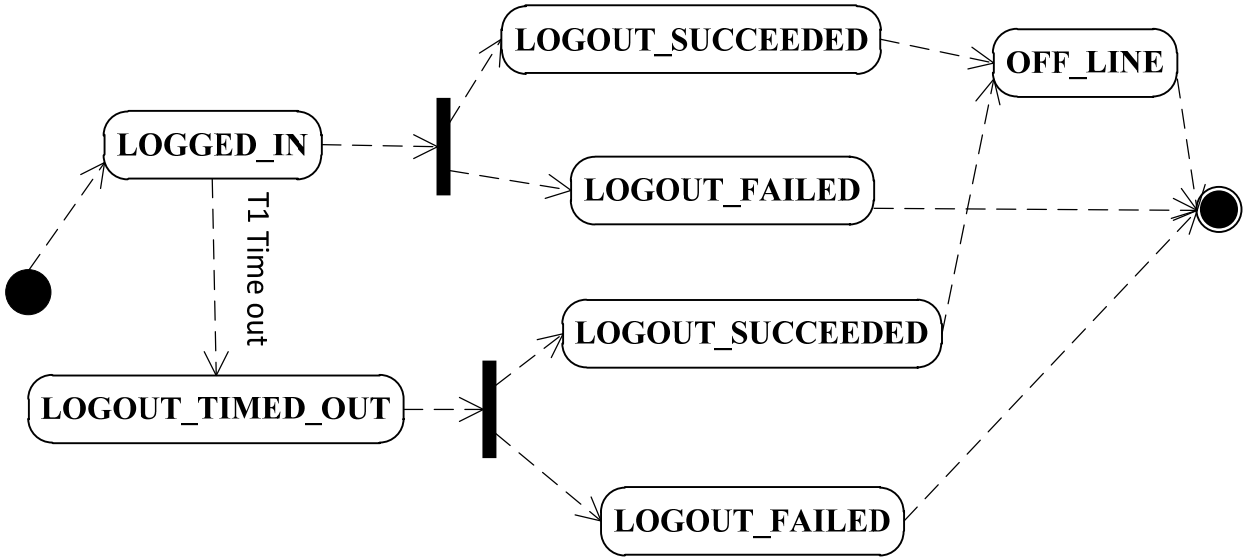
The Logout Process in Shibboleth Federation system

Logout	Description	Adv.	Dis.
Local logout	• Basic implementation in shibboleth community. • Logout the user from the SP whiteout the IdP.	Simplicity	• Loophole in the security system. • Sessions still alive while users logged out.
Local logout with browser close	• First solution by the shibboleth community. • Depend on the user.	More secure than first case	• The complexity of writing code at every SP. • The Varity of browsers face the capability of the response to the closing code at SP logout page.

The Logout Process in Shibboleth Federation system

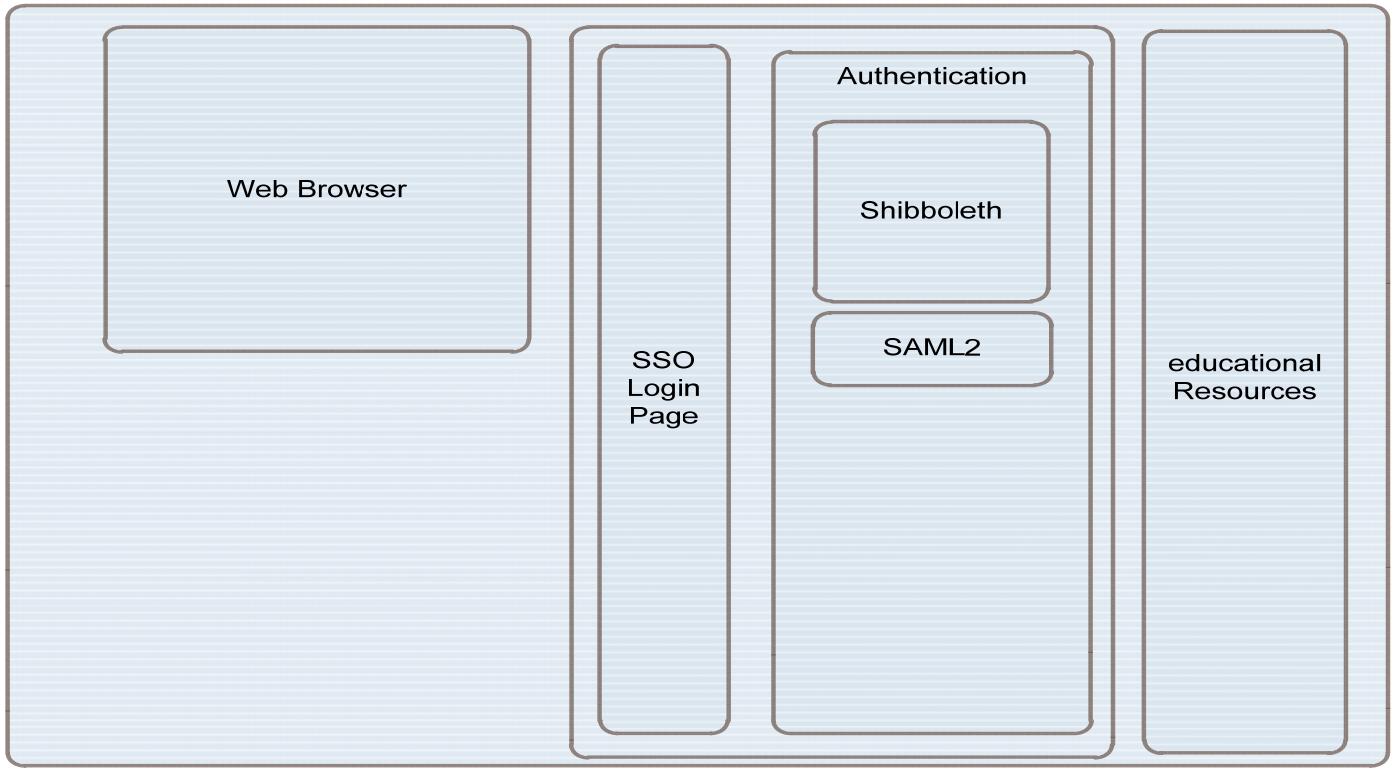
Logout	Description	Adv.	Dis.
re-authentication at every request	• Forcing to authenticate every time the user. perform a request	Intense security	• This Type of logout is not ideal in a “portal” environment • Destroy the concept of Single Sign-On.

State diagram of global logout

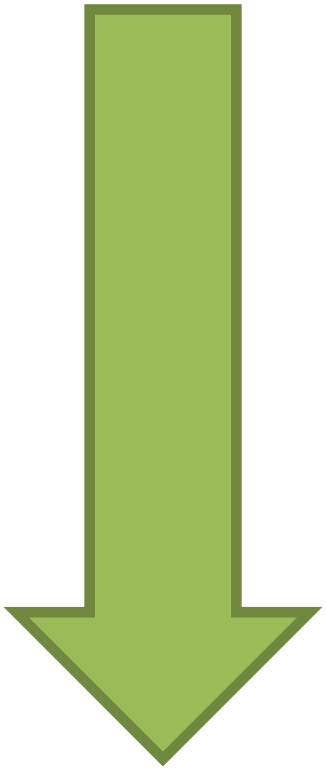


User Logout Status
LOGGED_IN
LOGOUT_SUCCEEDED
LOGOUT_FAILED
LOGOUT_TIMED_OUT
OFF_LINE

Proposed Model

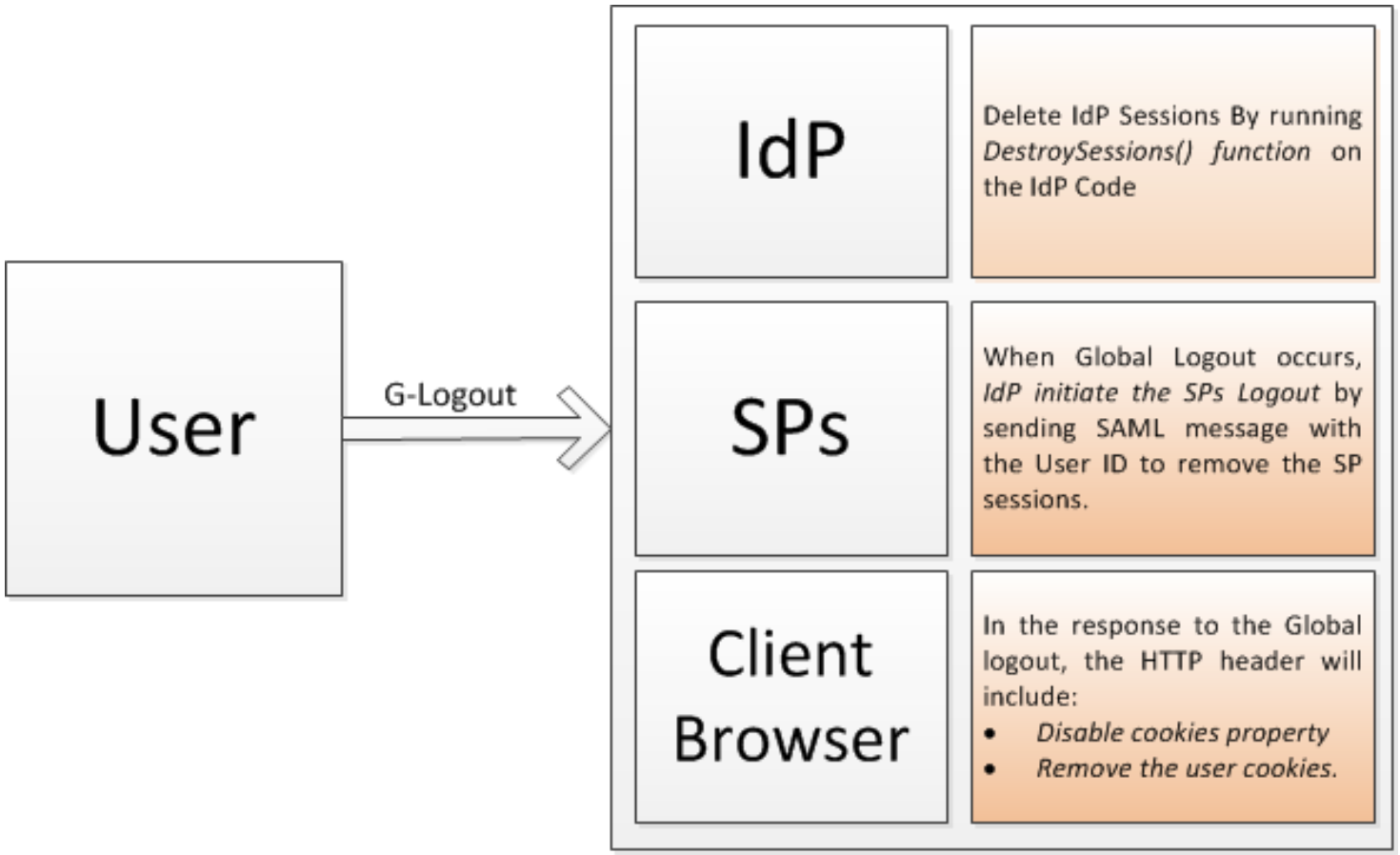


User Sessions



Sessions
IdP authentication session
IdP session
SP session
Application session

Global Logout mechanism



Global Logout Servlet Parameter

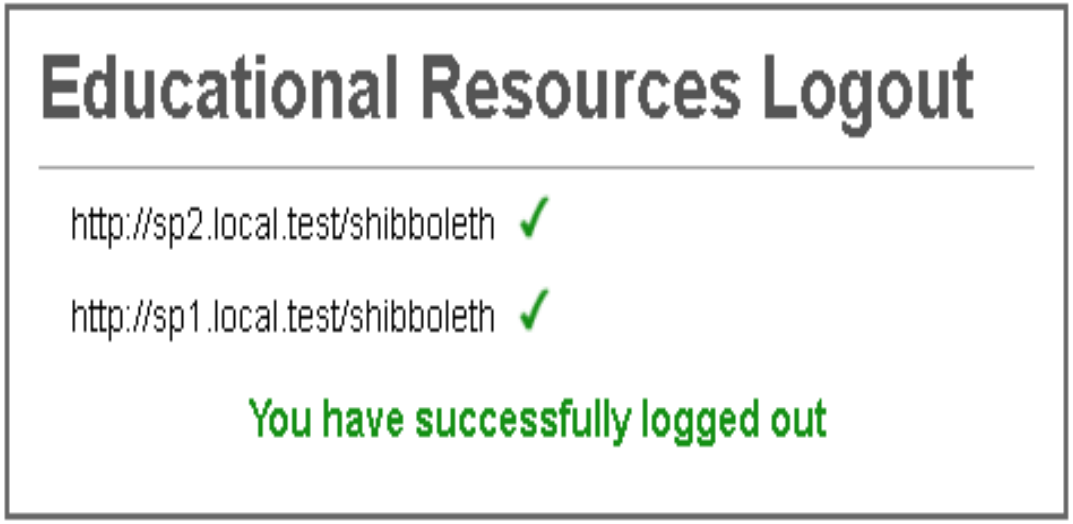
- **The IdP destroySession**

```
private void destroySession(SingleLogoutContext
sloContext) {

getSessionManager().destroySession(sloContext.getIdpS
essionID());
   }
```

Global Logout

- Logout information
  - SPs, where logged out correctly.
- The Status of the user is the OFF-LINE shibboleth state.



OFF-LINE shibboleth state

- Caching is required to maintain the status of the user.
- User status within the Shibboleth federation system is logged-in or logged-out, but to apply the visibility requirement a third state must be added 'off-line status'.
- *Off-line status* is the status when the user logged out of the Shibboleth federation system, while retaining the open-content sources in advance.

Caching

Where to Cache?

- By the service provider (sp)
- Or by identity provider (IdP)

Implementations

- Java coded Identity Provider (IdP) was Compiled using *NetBeans 7.1 IDE* installed on *Ubuntu 10.04* Linux distribution.
- C++ Coded Service Provider (SP) was managed by IIS and installed on *Microsoft Server* 2003 Enterprise Edition .
- The web interface of the educational services was created using Active Server Pages (ASP.NET) technology.

Conclusion

- Global logout is managed by the IDP
- User Off-line state (Caching)

Thanks for your attention

Questions ?