Aalto University
School of Science

Logout in Single Sign-on Systems

Sanna Suoranta, Asko Tontti, Joonas Ruuskanen, Tuomas Aura

IFIP IDMAN, London, UK, 8-9.4.2013

Logout in Single Sign-on Systems

- Motivation
- Single sign-on (SSO) systems
  - SSO in Finnish universities
- Logout in single sign-on systems
  - Problems in practice
- Suggestions for solution

Motivation

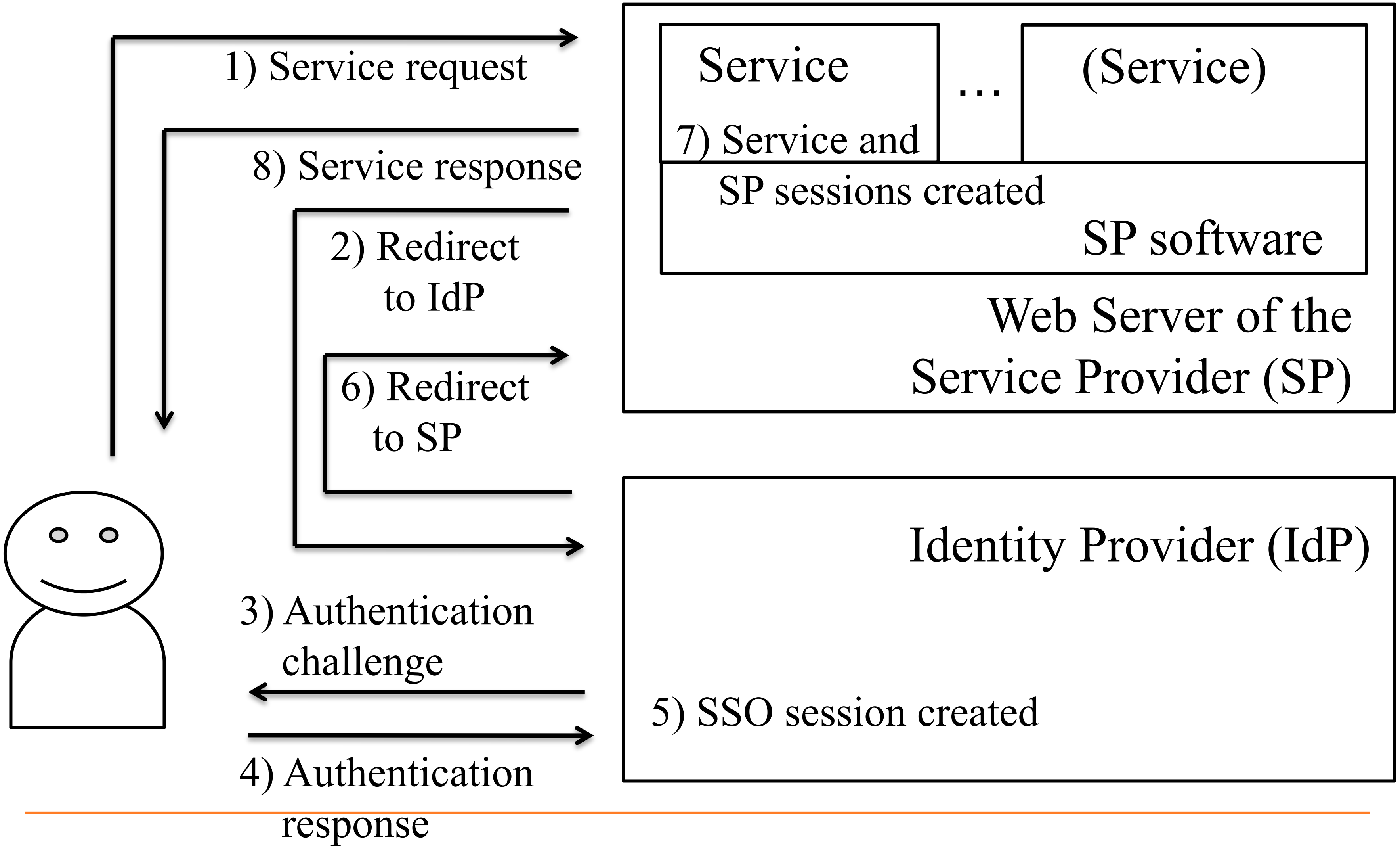
- Single Sign-on reduces the number of passwords user needs
  - Identity Provider authenticates the user on behalf of services
- If services are used with a shared computer, logging out is essential, or otherwise a next user of the computer can get in to the services with previous user's privileges
  - Not only the used service but also all other services that use the same SSO authentication
  - Logout is important part of authentication session in cases where timeout is not enough

Single Sign-on Systems

- OpenID – open federation
  - Several widely used services such as Google and Yahoo provides OpenID identities to services
  - But anyone can create an OpenID account without verification of identity
- Shibboleth (based on SAML)
  - Software freely available
  - But requires forming of a federation for cross-organizational SSO
- Facebook Connect and other similar services offer authentication
  - Centralized authentication for third party applications available

…

Single Sign-on



Single Sign-on at Aalto University

- In Finland, universities have formed a federation called HAKA; and that is joint together with Nordic SSO federation
  - Shibboleth SSO is used to authenticate both staff and students
  - CSC – IT Center for Science operates the HAKA federation and provides the metadata files needed
- Each university has its own identity provider
- Some services are common (e.g. library service Nelli),
- Others are university specific (e.g. study register Oodi that is used by half of the Finnish universities).
- Moreover, any new service can added to be used within the federation (e.g. CSE department’s own service where students return their assignments)

Logout in SSO

- Service session usually ends either when user logs out or a timeout logs her out
- Logout in SSO systems is not so straightforward – where the user logs out?
  - Only from the service at hand
  - From all services belonging to the same federation and form the Identity Provider (== global logout, single logout)
  - From the service at hand and the IdP, without ending other service sessions

Logout in SSO in practice

In practice, logout in SSO system can lead to several outcomes:

- Logout in the service application
- Logout in service provider (SP)
- Local logout
  - logout in the service and SP

service side logout

- Logout in identity provider (IdP)
- Local logout with IdP logout
- Global logout (single logout)
  - Requires that IdP know to which SPs the user has logged in
- Partial logout
  - Error situation where some sessions remain active

Logout Problems

- User does not know where she has logged out
  - Architectural knowledge of SSO is required to understand logout
  - Expectations affects: does the user want to log out from a single service or from all services?
- Implementation problems in service side
  - Either service's own session or SP's session is left behind – either one is enough to let user back in
- Cookie management
  - If user really want to log out, she has to close the web browser

Logout in SSO in Practice at Aalto

Logout in practice	Consequence	Example
Only service session removed	SP session allows user to get back in	Oodi (study register)
SP session removed but service session remains	Service session allows user to get back in, no possibility to contact IdP	Nelli (library service)
"You have been succesfully logged out"	From where? If local logout, user can get back in because IdP session is still active	Wiki (all kind of groups)
Local logout with IdP logout	Other services are still active but new services require re-authentication	Noppa (course information)
Choosing between local and IdP logout	Allows user to decide but requires knowledge of SSO	

What users want today?

- Linden et al. (2005) claim that users of SSO want Single Logout (SLO)
  - However, SSO was new in those days and users were not familiar with the concept
  - Shared computers in libraries should still execute SLO
- Unclear if this is the case today
  - Users today are more familiar with SSO
  - Users have personal devices such as smart phones and typing in credentials again after logout can be annoying

Suggested Solutions

- Unified and standardized process for ending sessions
  - E.g. order of removing the sessions
- Improving the cookie management in browsers
  - Ending the sessions without closing the browser
  - Allowing the IdP to access SP and service cookies
- Creating a mechanism to check the existence of an IdP session
  - SPs should be able to poll IdP to check if the IdP session is still active
- Unified user interface for logout
  - Federation should give guidelines for UI and its terminology

Questions?

Sanna.Suoranta@aalto.fi,
Asko.Tontti@csc.fi,
Joonas.Ruuskanen@aalto.fi,
Tuomas.Aura@aalto.fi