USING ESPRESSO [ESTABLISHING SUGGESTED PRACTICES REGARDING SINGLE SIGN ON] TO STREAMLINE ACCESS

Andy Ingham (UNC-Chapel Hill)

NASIG Annual Conference, June 4, 2011

What I hope to cover

- Problem statement
- Goals
- Challenges
- Assumptions
- A detour
- Sample use cases
- ESPRESSO deliverables
- ESPRESSO recommendations
- The future
- Questions ?

Problem statement

- What changes can be implemented to effectively and efficiently get ALL (but ONLY!) the "right" users to licensed external resources (even from the "open web"), utilizing single sign-on (SSO) technologies ?
  - **Currently, libraries and their users are forced to work in a mixed auth environment, that is still predominantly IP-based and requires proxying**
  - **Likewise, Service Providers ("SPs", such as resource vendors and publishers) must support multiple authentication mechanisms**

Goals

- Create Recommended Practices that will improve the user experience by providing consistency, simplicity, familiarity, improved usability, and will provide a path toward phasing out IP-centered authentication in favor of an SSO experience across a set of distributed service providers.
- Recommend an environment that is feasible for both libraries and vendors to implement and that provides security, privacy, manageability, and flexibility.

Challenges

- Can a vendor correctly associate a user with a current license? (sometimes called the "Discovery problem")
- Can various entry PATHs all be accommodated gracefully? (from library website, "open web", etc)
- Can various entry LEVELs all be accommodated gracefully? (top-level vendor page, "deep link", etc)
- Is use of resources accommodated properly regardless of the user's physical location?

Assumptions

- Institutional licenses are in scope, licenses for individuals are NOT.
- Institutions will have an identity management infrastructure in place (and generally leverage a federation, e.g., InCommon).
- Content suppliers will have standards-compliant "service providers" (SPs).
- Shibboleth is the current best-of-breed for providing an SSO environment.
- EZproxy (due to high market saturation) is prominent in this presentation.

A detour…

…to cover some background

Architectural shift

	Primary structural element	Secondary structural element
Proxy	LOCATION (IP address)	User attributes (via proxy server authn / authz)
SAML (Shibboleth)	User attributes (via IdP)	LOCATION (in order to accommodate ANONYMOUS “walk-ins”)

Proxy versus SAML (Shibboleth)

Benefit	Proxy	SAML
Provides SSO for LIBRARY resources	X	X
Provides SSO (also) for other "campus" resources		X
Eliminates IP range management for LIBRARY		Only if force authn even ON-CAMPUS
Eliminates IP range management for VENDOR(S) (including need for library to keep list sync-ed across all vendors)		X
Allows possibility for PERSONALIZATION streamlining across multiple vendors		X

Current situation (EZproxy)

REMOTE USE (current EZproxy environment)

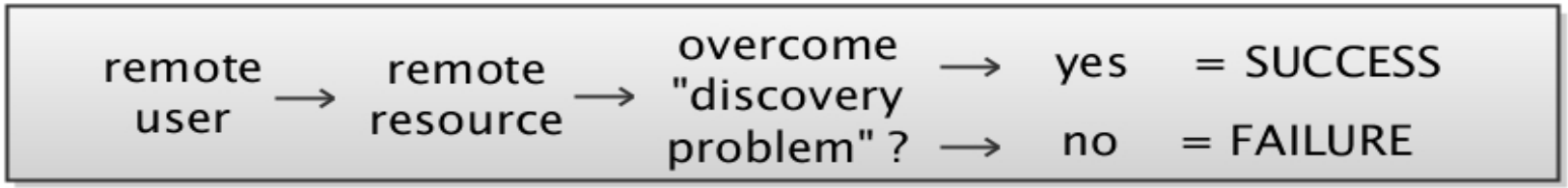
case 1 = un-mediated access

case 2 = mediated access

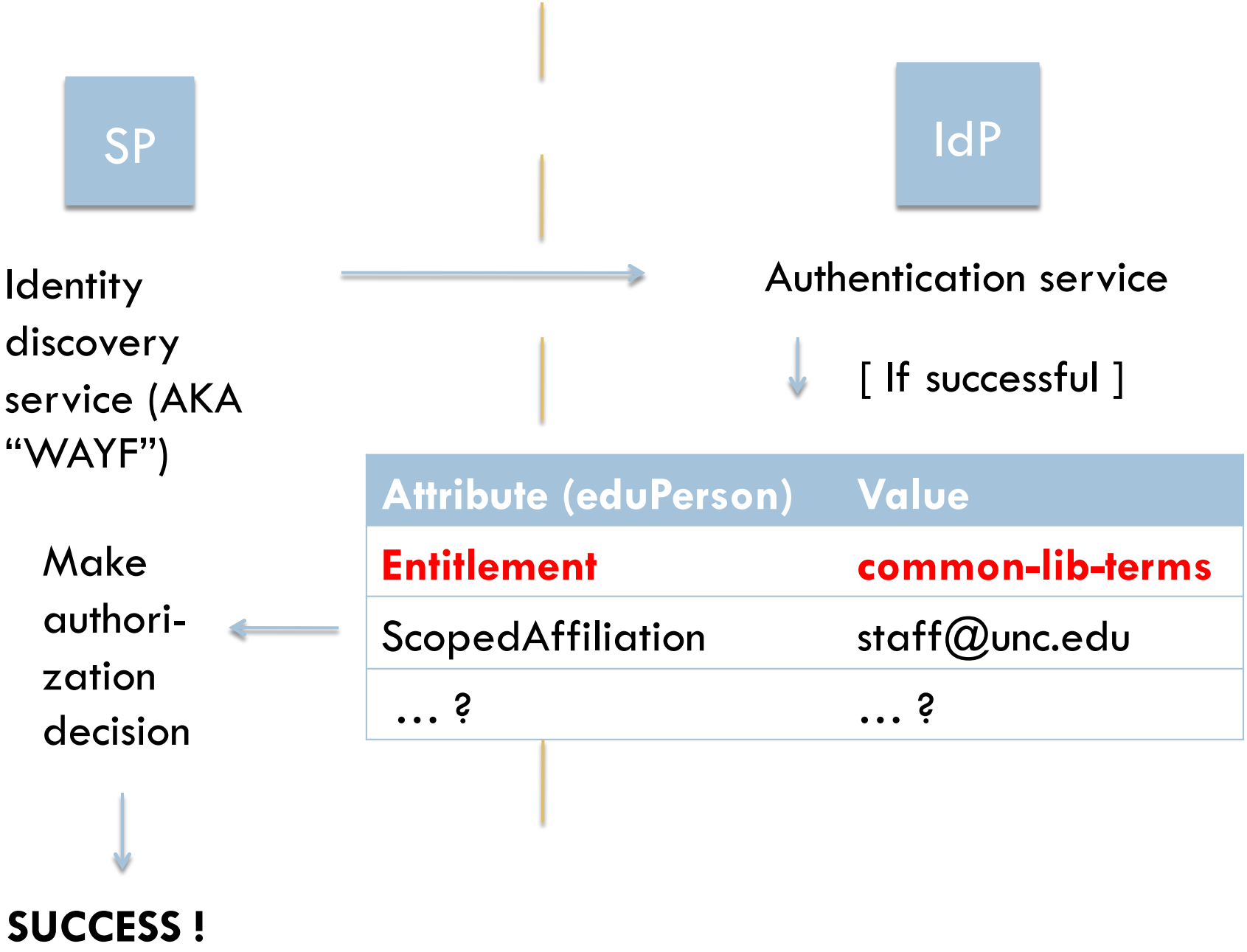
Current situation (Shibboleth)

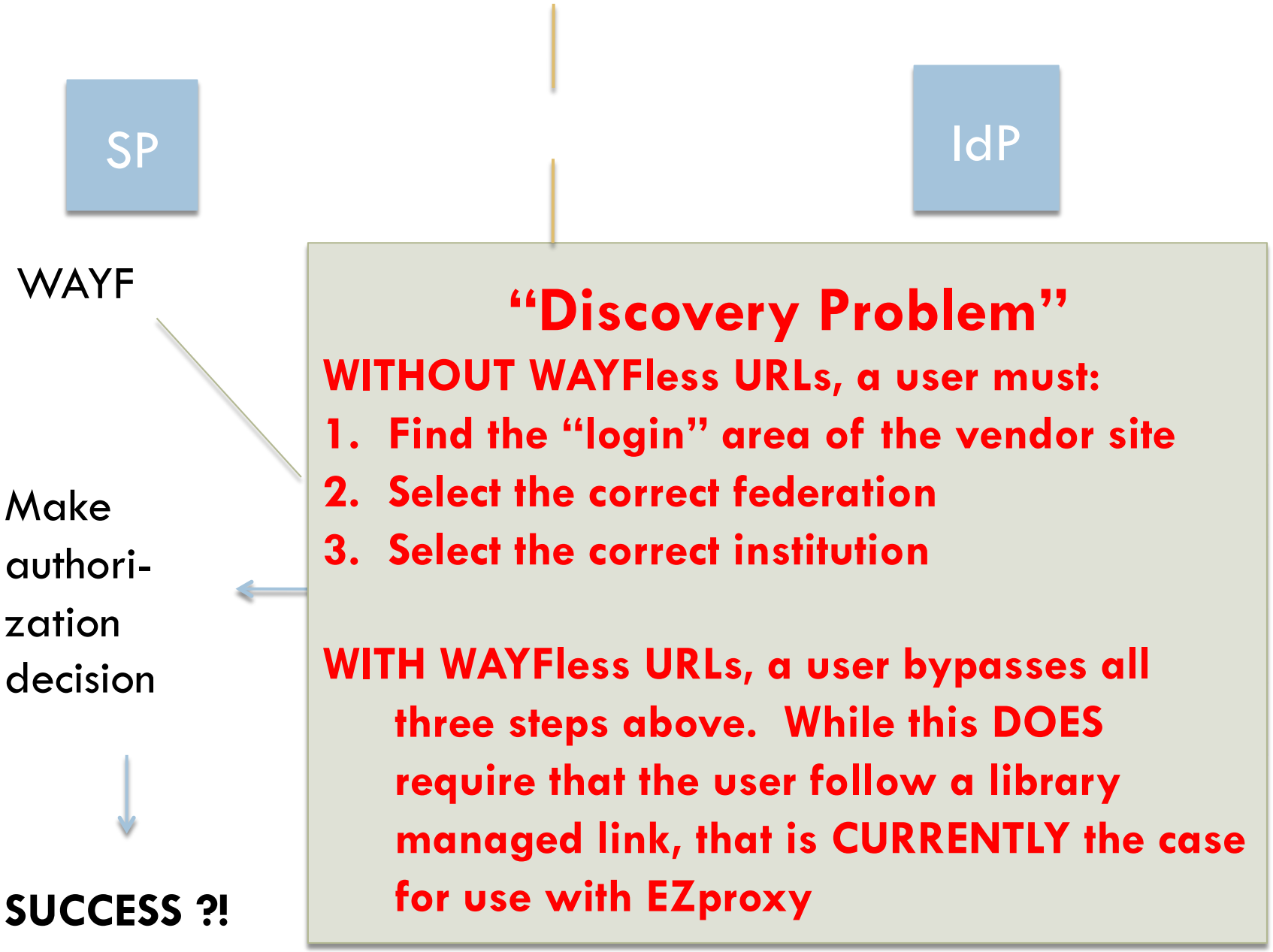
REMOTE USE (Shibboleth environment)

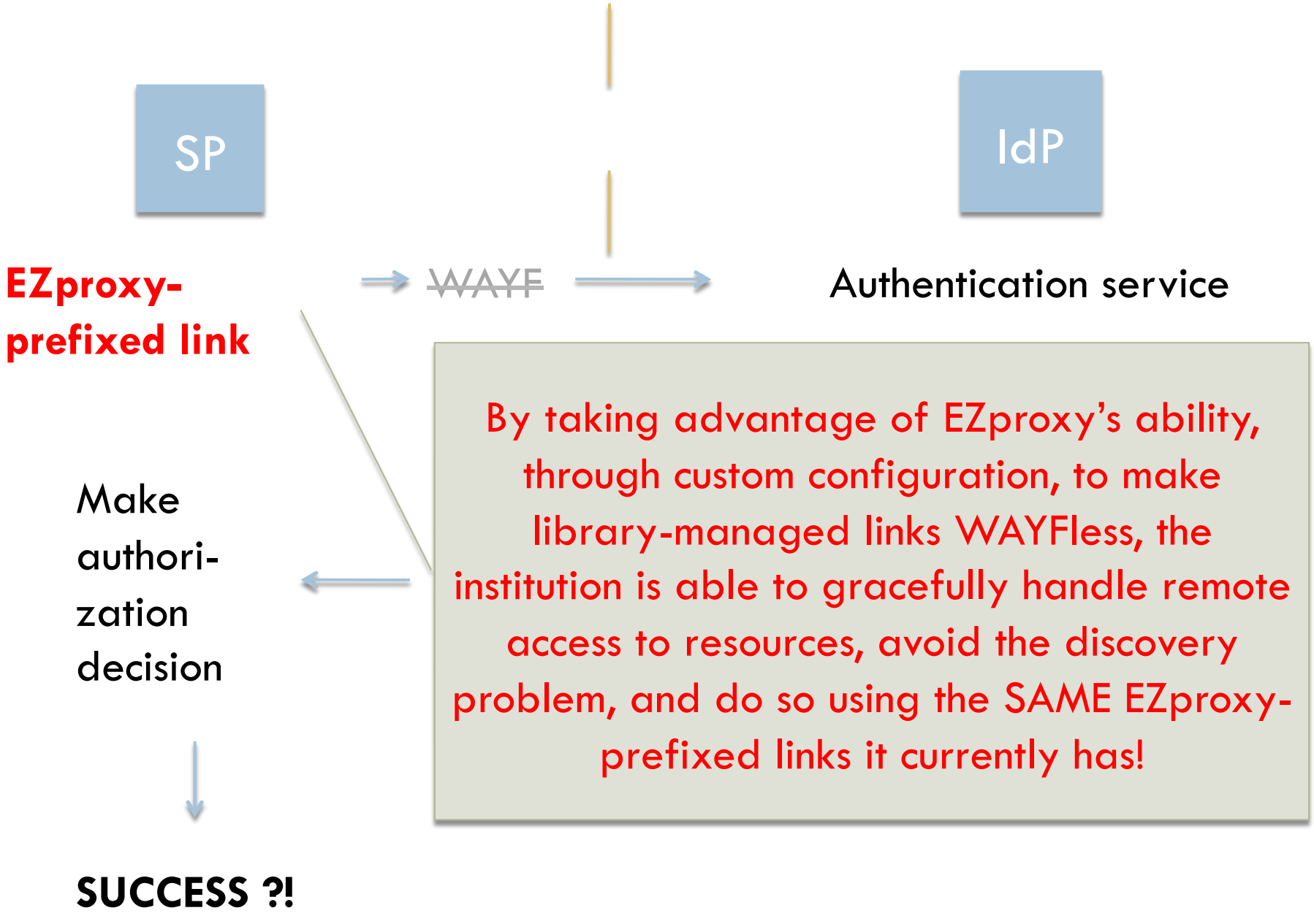
case 1 = un-mediated access



case 2 = mediated access


SP
IdP
Identity discovery service (AKA "WAYF")
Authentication service
[If successful]
Attribute (eduPerson)
Value
Entitlement
common-lib-terms
ScopedAffiliation
staff@unc.edu
… ?
… ?
Make authori-zation decision
SUCCESS !

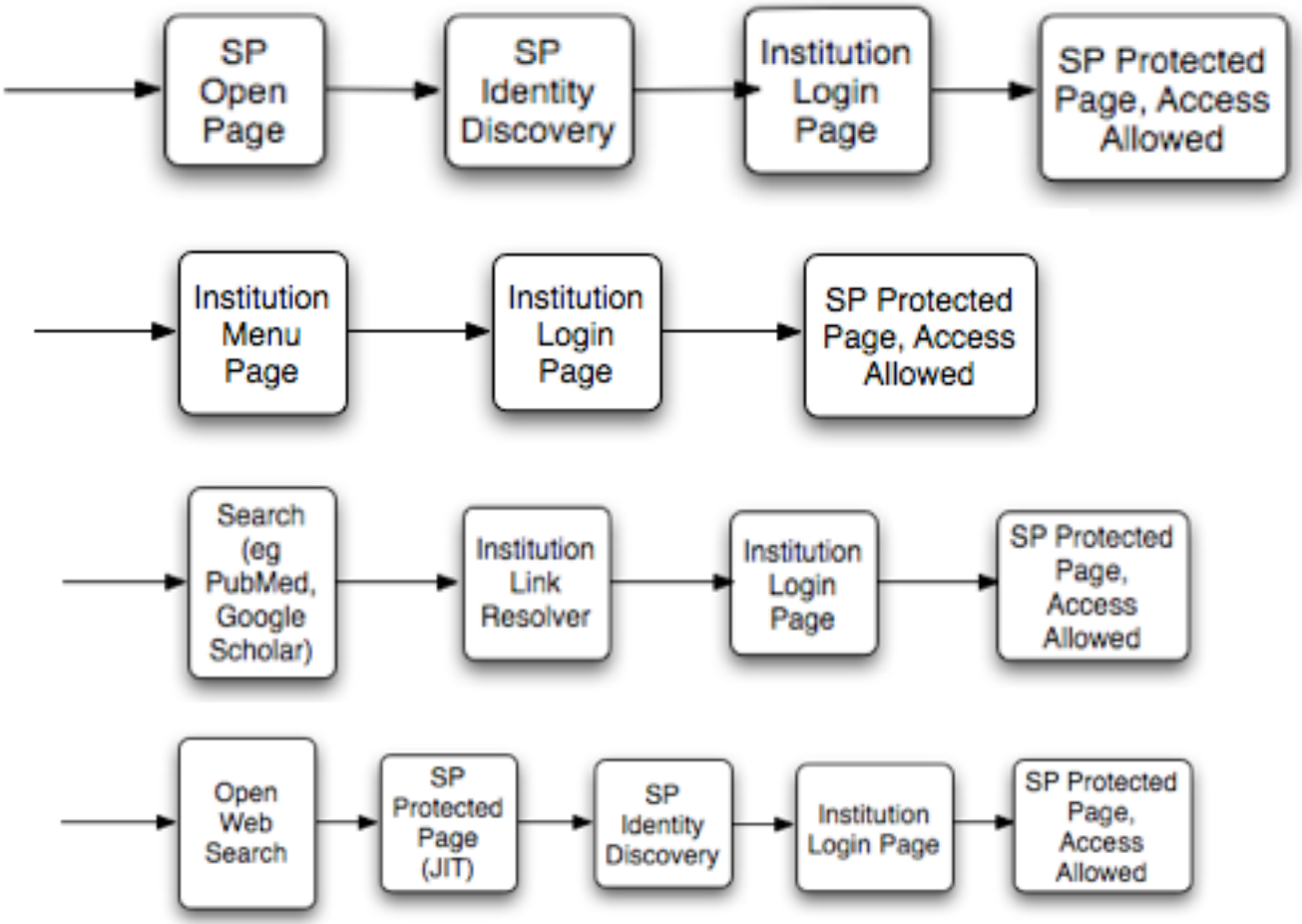

SP
IdP
WAYF
"Discovery Problem"
WITHOUT WAYFless URLs, a user must:
1. Find the "login" area of the vendor site
2. Select the correct federation
3. Select the correct institution
WITH WAYFless URLs, a user bypasses all three steps above. While this DOES require that the user follow a library managed link, that is CURRENTLY the case for use with EZproxy
Make authori-zation decision
SUCCESS ?!


SP
IdP
EZproxy-prefixed link
WAYF
Authentication service
By taking advantage of EZproxy's ability, through custom configuration, to make library-managed links WAYFless, the institution is able to gracefully handle remote access to resources, avoid the discovery problem, and do so using the SAME EZproxy-prefixed links it currently has!
Make authori-zation decision
SUCCESS ?!

End of detour and …

… back to the NISO Recommended Practice document.

Sample use cases



ESPRESSO deliverables

- Develop a standard vocabulary of technical, business and policy-related terms used by Web SSO and Federated Authentication products
- Describe use cases that indicate the ways in which a browser would arrive at a Service Provider, traverse a Discovery process, and arrive at the appropriate login mechanism. (E.g., from library home page; via federated searches; from the "open web"; to deep links, often via link resolvers / OpenURL)
- Develop a set of "best practice" recommendations for the relationships between customers, licensing bodies, federations, and service providers.

ESPRESSO deliverables

- Propose standardized user interface elements
  - Identify a preferred location for login links
  - Recommend to Service Providers a standard approach for guiding the user to the desired authentication method
    - Propose standardized GUI flows
    - Provide tips for easy identification of home site
    - Suggest guidelines for lists of federations and IdPs
    - Recommend judicious use of branding
  - Develop standardized approaches for handling "automatic" login when the URL presented at the SP identifies the user's preferred authentication method and/or authentication provider.

ESPRESSO deliverables

- Identify approaches that allow Federated Search technologies and portals to leverage existing Web SSO authentication sessions of a user when contacting backend Service Provider sites.
  - Work with those package mechanisms that currently support “delegated authentication”.
  - Ensure that Service Providers have access to the documentation they need to support this feature.

ESPRESSO deliverables

- Provide plans for the promotion and adoption of these Recommended Practices to make the access improvements a reality
  - 1. Marketing plan
  - 2. Business case/justification will be developed as part of the marketing plan.

ESPRESSO recommendations

- SPs continue to support multiple authentication options during this time of transition.
- SPs and libraries move quickly to reduce reliance on IP-based access control.
- SPs and libraries move quickly to deprecate userids/passwords validated AT the service provider site.
- SPs and libraries move quickly to implement and use standards-based federated authentication.

ESPRESSO recommendations

- SPs should adopt standard placement/wording of the login link on all pages.
- SPs should utilize as many time-saving mechanisms as possible (and as economically as possible) for guiding the user to the appropriate authentication method (this is the “Identity Discovery Page”).
- SP and IdP web designers should utilize branding at appropriate places in the browser flow.

The future

- Seek feedback on the NISO Recommended Practice document at http://www.niso.org/workrooms/sso/
- Leverage a NISO standing committee?
  - Provide some mechanism for outreach, support, and engagement with both service providers and institutions
  - Update the guidelines and related resources
- Disseminate implementation guides?
- Provide webinars?

Questions for me ?

- SSO website: www.niso.org/workrooms/sso
- SSO Interest Group list: www.niso.org/lists/ssoinfo
- SSO Charge: www.niso.org/workrooms/sso/charge
- See also InC-Library information
  - https://spaces.internet2.edu/display/inclibrary/InC-Library
  - https://spaces.internet2.edu/display/inclibrary/Best+Practices

- Andy Ingham [andy_ingham@unc.edu]