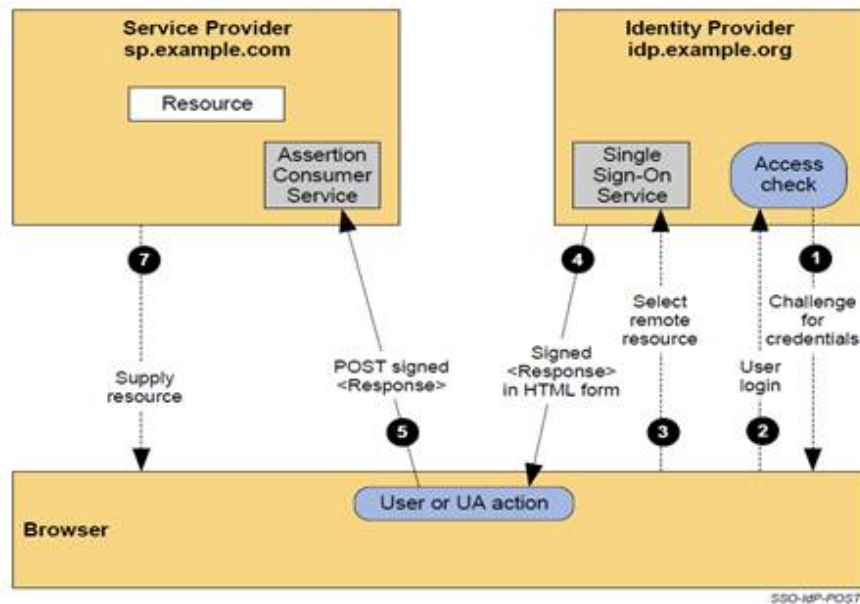On Wed, 19 Sep 2012, at 16:12 , Bing Chen <Bing.Chen@blackboard.com> wrote:
HI David,

Here's the info on Portal SSO.

1.1. Supported Business Use Cases

The Connect 5 Portal SSO utilizes the idP-initiated model to allow user access into the system. In this scenario, users will be visiting an idP page where they will be authenticated and click on a link to visit the Connect 5 Portal.

Upon accessing the Connect 5 Portal, the following scenarios are presented:
ü First time users will have a Portal login account created and automatically be associated with the contact data that has been previously uploaded into Connect 5, and be presented with the Portal home page
ü Returning users will be logged into the Portal and be presented with the Portal home page
ü Users who provided incorrect credential information and cannot be verified will be given an error message indicating that their login has failed

1.2. Rules

The following represents the types of Portal SSO scenarios required by Clients:

§ New Portal User at institution who has never visited Connect Portal (no Connect Global User aka CGU)
§ Existing Portal user who has an existing CGU created at the institution's Connect Portal

URL but now wants to log in using Portal SSO method via the institution's portal

Successful SAML Authentication response means the following:

§ Connect has verified Client signature within SAML
§ Look up Federation ID to locate Connect Global User (CGU)
§ If CGU is not found, display Connect Registration page
§ If CGU is found (aka returning user), take user to Connect Portal Home page
§ When association fails, user is informed as to why it failed
§ Admin will be informed of failure in order to then upload user contact data

Required fields for Portal SSO:

§ Need contact type, reference code; unique within institution

Required attributes within SAML are:

§ First Name
§ Last Name
§ Fed ID
§ Email address
§ Reference Code (closed portal only)
§ Contact type (closed portal only)
§ Logout URL (optional – default could be Connect portal URL)
§ If ReferenceCode and ContactType are not provided user will receive error message

URL:

§ Portal SSO URL can be created at each institution level
§ When Portal SSO URL is created at the higher institution level, it allows lower level users to log into their lower level account if that user has proper access into the lower level institution

New Portal User – No Connect GU:

§ We will be using a higher student as an example of a portal user visiting a school web site to access the Connect Access portal

2. Prerequisites

- Portal SSO will be available for Connect 5 and Connect 5 portals only
- Institution/school must have pre-load student contact data for Portal User to Connect to a contact association (student)
- Portal URL must be created; Portal SSO only applies to each Connect Portal URL
- New student User at institution who has never visited Connect Portal (no GU) must be allowed to connect with a created account
- Federation ID aka SSO Username provide by institution (must have and cannot change)
- Email Address aka Connect Portal Username (must have – either manual input or data capture from Federation ID; this can be changed)
- Password (optional)
- If a Student Portal User is allowed to de-associate from a Connect contact, they will have to be opted out from delivery preferences (if possible)
- Upon successful submission; new portal SSO URL is created and listed on Portal SSO list page
- Unsuccessful submission will keep Admin on current page with error message displayed on top navigation bar
- Error message should read "This is an invalid certificate file. Only .cer file type is allowed."
- Clicking on CANCEL button will return user to Portal SSO list page

Let's talk more later.

Thanks,
Bing

Bing Chen | VP Product Management
Blackboard Connect
Phone: 818-808-1736 | Fax: 818-808-1702 | Mobile: 818-913-8288
www.blackboard.com/connect