

InCommon Online Forum

InCommon Technical Advisory Committee

Thursday, February 25, 2010

Questions either via Adobe Connect chat or the conference call

Dial-in numbers:

+1-734-615-7474 Preferred (from any phone where long distance has no add'l cost)

+1-866-411-0013 (US/Canada only and only if above number costs user more than 800/866 calls)

Access Code: 0101010#

Forum: A public meeting place for the exchange of ideas.

“When, in some obscure country town, the farmers come together to a special town-meeting, to express their opinion on some subject which is vexing the land, that, I think, is the true Congress, and the most respectable one that is ever assembled in the United States.”

- Henry David Thoreau

InCommon Online Forum

InCommon TAC

Thursday, February 25, 2010

Agenda

1. SAML 2 roll-out (<https://spaces.internet2.edu/x/lg2p>)
2. Attribute Management and uApprove (<https://spaces.internet2.edu/x/TRWp>)
3. Technical priorities (<https://spaces.internet2.edu/x/8RSp>)
4. Your item here (as time permits)

SAML 2.0 Rollout

<https://spaces.internet2.edu/x/lg2p>

Initial Approach

- Extended existing web form to support SAML 2 bindings/endpoints
- Leave SP keys registered for both signing/encryption
- Defer additional features to XML submission process

Early Problems

- Overlooked implications of upgraded SPs not registering SAML 2 endpoints once IdPs started doing so
- No guidance on how/what to register, causing variance, strange endpoint choices
- Recent minor bug involving protocol support field in metadata, which led to major bug attempting to fix it

Clean up

- Sites with SAML 2 supporting software should register that support, and cleanup their metadata using web UI
 - IdPs should support at least HTTP-Redirect binding
 - IdPs should generally NOT include a SAML 2 SOAP attribute service
 - SPs should support at least HTTP-POST binding
- SPs using Shibboleth 2 that don't wish to support SAML 2 should disable/comment out the `<SessionInitiator type="SAML2">` element in their configuration

Discovery

- Federation "WAYF" application will be upgraded to support the latest "DS" protocol soon
- Keep an eye out for new tools for "embedding" discovery into SPs/applications

Better Attribute Management uApprove

<https://spaces.internet2.edu/x/TRWp>

Agenda

- Overview of uApprove
- Discussion of the Model
- Experiences of the Pioneers

Attributes: the Current State of the Art

- User/department contacts local IDP administrator to request policy for new SP
- Typically the IdP and SP administrators must communicate to work out the details of attribute exchange.
- The IDP Administrator manually configures an IdP to release the agreed upon user attributes to the designated SP
- Conclusion: the current process is too "heavyweight" to be effective

User consent and default policy

- IDP Administrator Creates Default Policy
 - For attributes in a standard set, release what the SP asks for, if the user agrees.
- What is User Consent:
 - At an IdP, after login and before attributes are sent to the SP, the user is asked, via a web form, to approve the release of his or her information to the SP.
 - If the user approves, login continues as normal and approved attributes are sent to the SP for access to the remote service.
- We believe that for many IdPs this may be a reasonable approach

Concerns

- In practice user consent has many issues that CAN make it complex.
 - Optional attributes
 - Some attributes are inherently hard to understand
- There are many legal and policy issues with release of personal information
 - Is approval necessary when a site is "necessary to use for a business or academic purpose"?
 - FERPA (addressed by "consent")
 - Concerns that users may not really be understanding "consent"
- User consent in the IdP is not a panacea, but we believe it is an important tool in the toolkit

The vision, in practice

- The IDP Site develops and configures a default attribute release policy
- IdP admins install enhanced IdP software
 - able to consume the SP's requested attributes and other characteristics from federation metadata and make it available to attribute release mechanisms.
 - IdP admins also install user-consent mechanisms in their IdPs
- An SP admin registers information with InCommon about the attributes their site requires

User Experience

- When a user goes to an SP for the first time, the attribute and consent machinery comes into play.
- If the SP is in the default policy category, the IDP software determines the requested attributes and asks the user to consent to their release, storing the decision for next time.

Shibboleth at University of Michigan

uApprove Deployment

InCommon Attribute Release

- Had been operating in Pilot Mode
 - Opt-in required
 - Temporarily provided means to approve the release of identity data
- To move beyond Pilot
 - Remove barriers
 - Make more self-describing

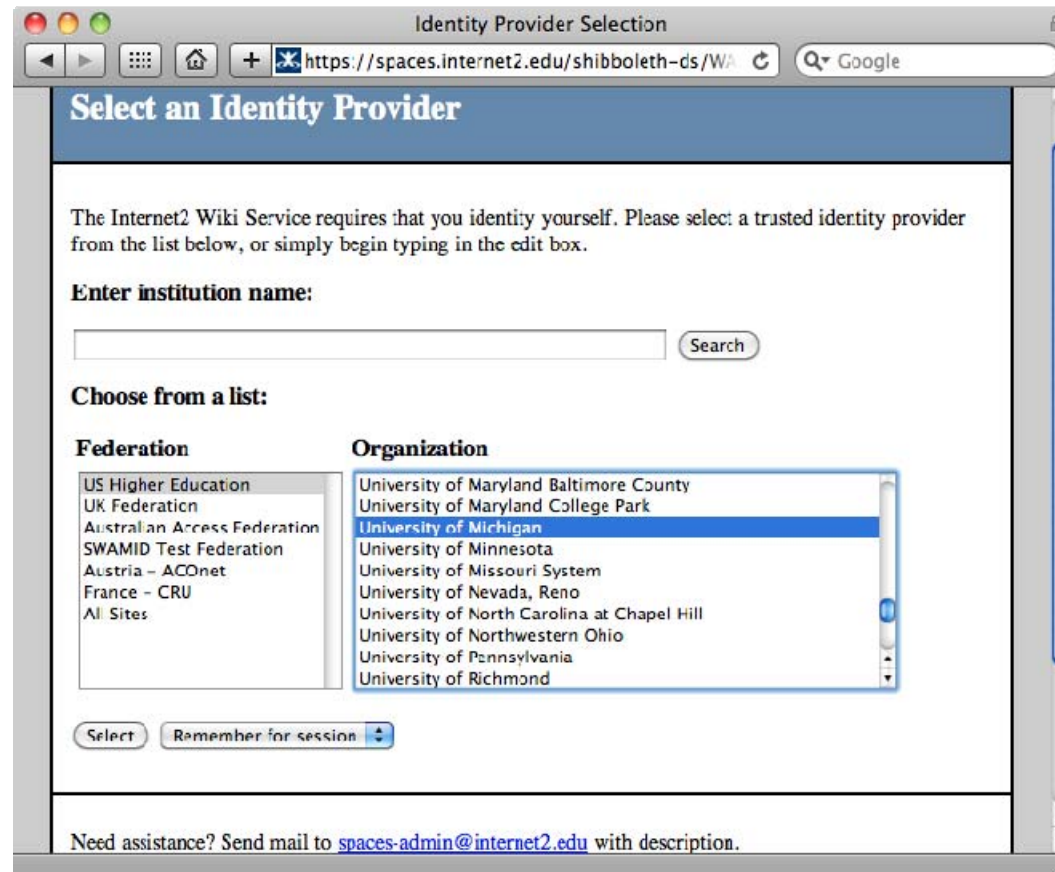
Governance Board

- Investigated how others were handling privacy concerns around attribute release
 - Found common desire existed to be able to have individuals approve the release of attributes
 - Saw mention of uApprove being used within SWITCH
- Demonstrated uApprove to IDM Governance Board
 - Liked it, but had issues with changes to data and privacy settings after approval to release
 - Looked into methods of detecting state changes and forcing re-approval

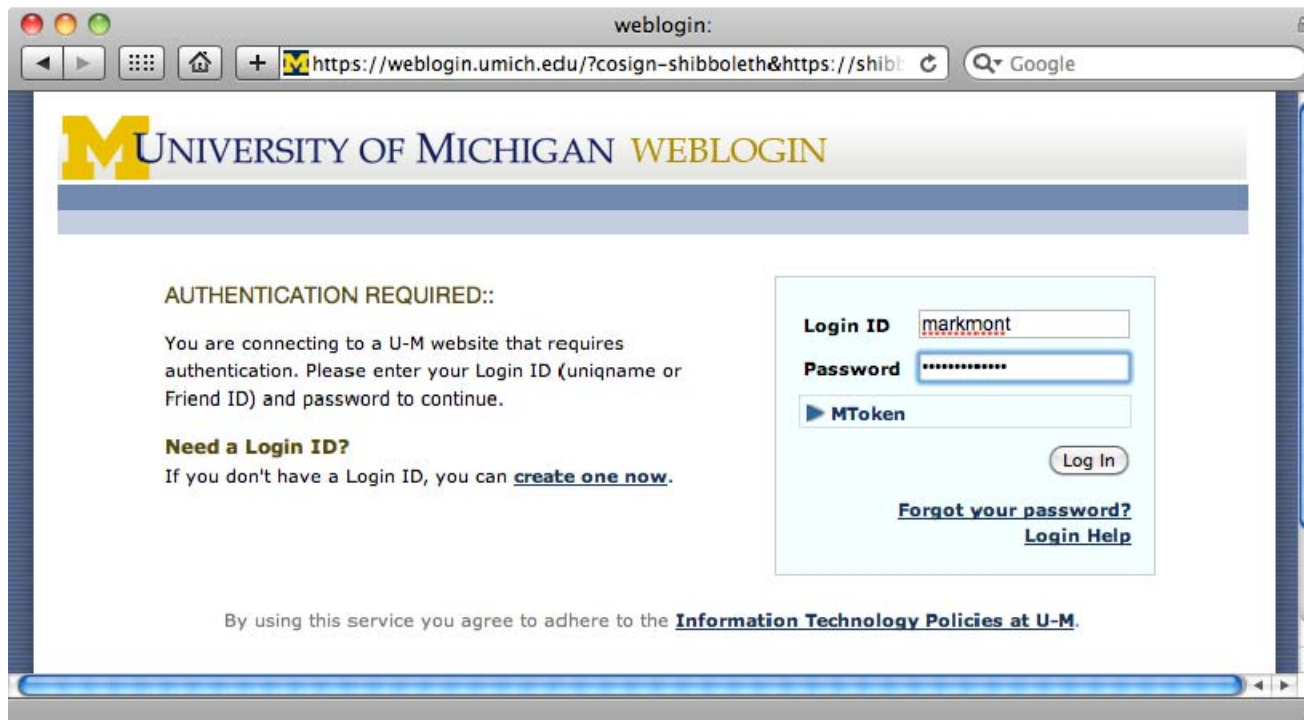
uApprove

- Determined best method was to prompt each time (until a more elegant solution was possible, maybe)
- Discussed with uApprove developers method for forcing prompt every time
 - Decided together that in short term, using database triggers was optimal

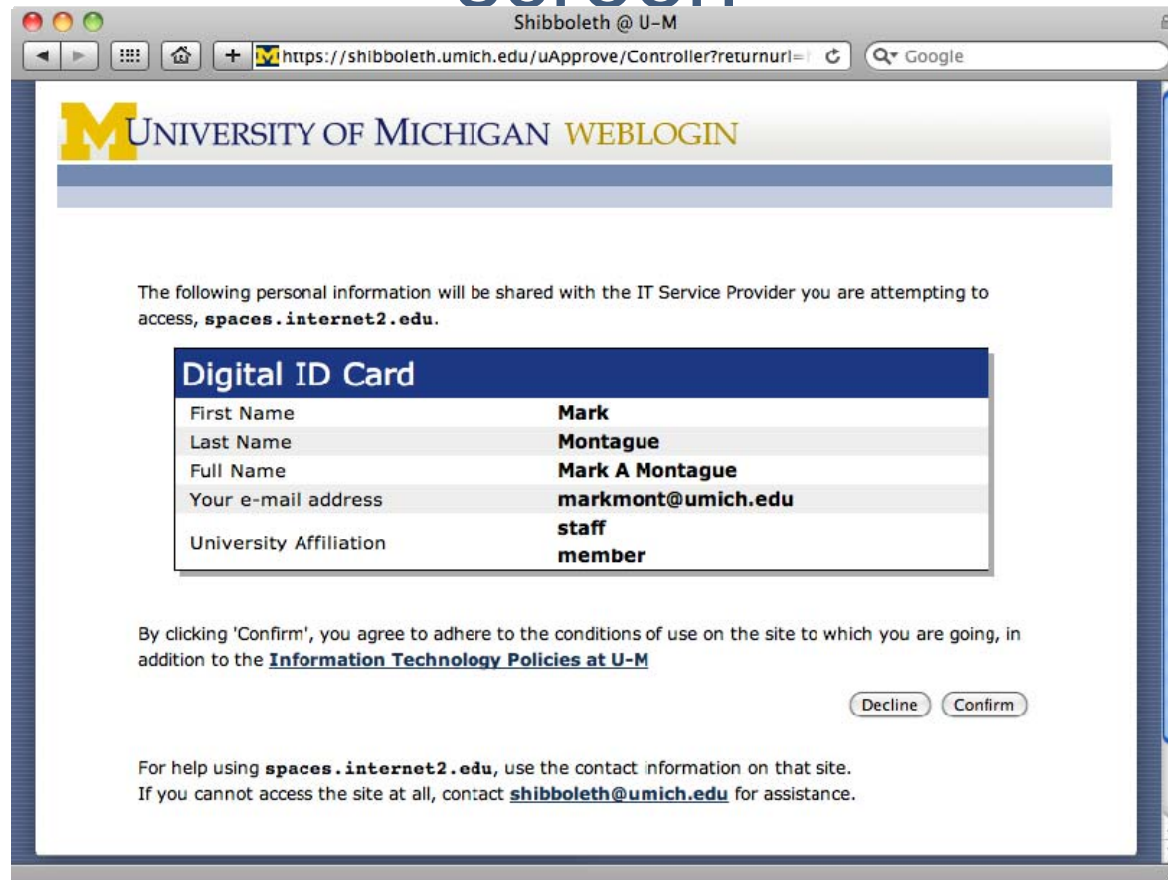
User Visits Site and Selects Home University



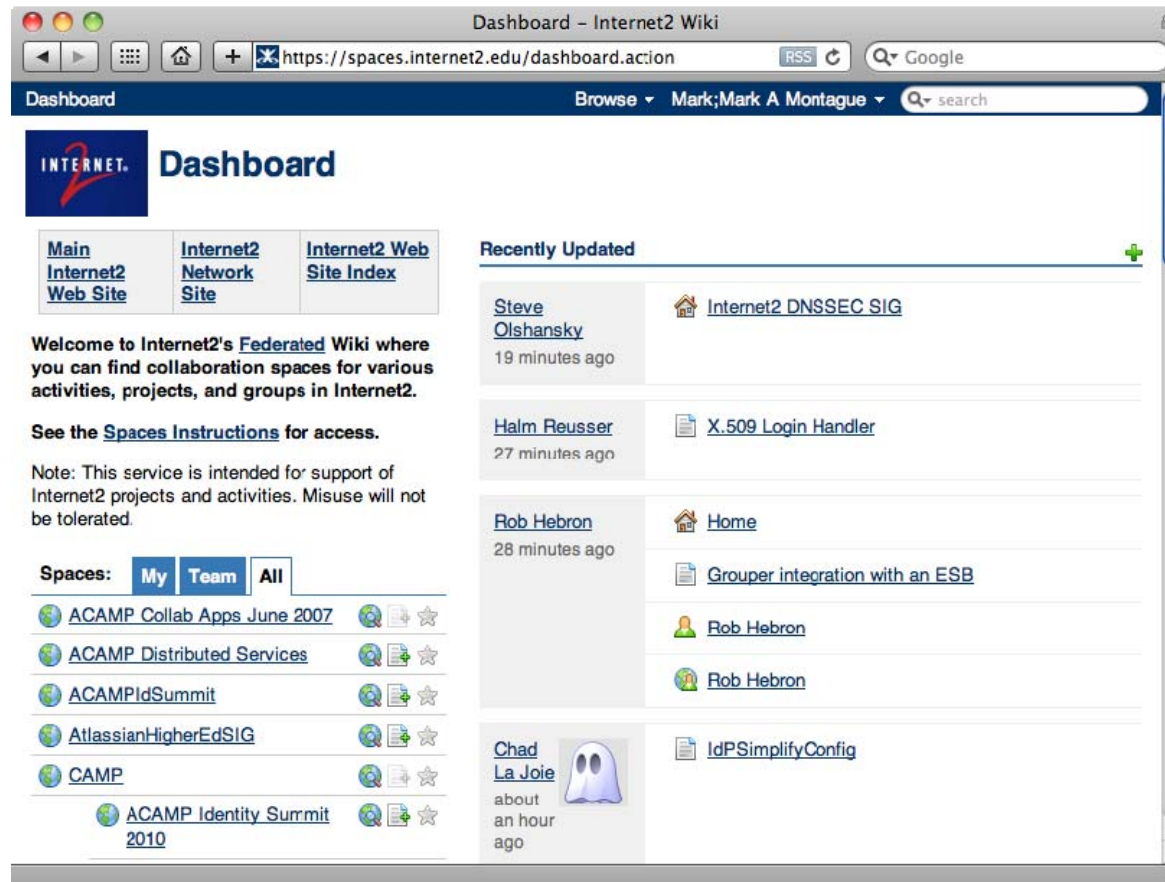
User Logs In Using Our Single Sign On Tool



User is presented with the uApprove screen



The user is sent to the site



If the user declines



MUNIVERSITY OF MICHIGAN WEBLOGIN

You did not agree to send your Digital ID Card to "spaces.internet2.edu".

Therefore, you will not be able to access "spaces.internet2.edu".

In order to cancel the login process, please close your web browser.

[Back](#)

U-M Gateway | Copyright © 2010 The Regents of the University of Michigan

Technical Priorities

<https://spaces.internet2.edu/x/8RSp>

Other Topics

Please fill out the evaluation for this session:

<http://www.surveymonkey.com/s/7JZNRKS>

Upcoming IAM Online (www.incommon.org/iamonline.html)

March 11, 2010, 1 p.m. (EST) “Provisioning of Remote Users,” by Mark Scheible, North Carolina State University, and Lori McNabb, incoming chair of the WCET Study Group on Academic Integrity and Student Authentication

April 8, 2010, 1 p.m. (EDT) “Making Federation Happen,” by Joel Cooper, Carleton College

Upcoming CAMPs (www.incommon.org/camp)

June 21-23, 2010 – InCommon CAMP – Raleigh, North Carolina
“Exploring and Supporting Federated Access” www.incommon.org/camp

June 23-25, 2010 – Advance CAMP: The Second Identity Services Summit –
Raleigh, North Carolina – www.incommon.org/camp