Attribute Release:
uApprove and Related Approaches and Issues

The Problem Space

- The need to scale access control
  - Number of sites, number of users, etc…
- The need to provide security and protect privacy
  - Put the enterprise and the user in control
  - Inform the user
- New policy area
  - International legal confusion
  - Campus confusion and lack of process
- Tools, and so issues, are coming…

Context within the big picture

- Privacy management always part of the federated identity picture
  - An immediate consequence of federated identity is the need for scalable access control
  - The Ethiopean place mat…
- Always seen as the hardest part of what was already a really hard path (so maybe we’d never get there)
- And here we are…
- Good technology always challenges policy

A self-inflicted wound…

- I visit at least 30 federated access controlled web sites regularly
  - Most are wikis for wg, staff, international collabs
  - Some are management of lists, approvals and accounting, etc.
  - An increasing number are part of collaborations – shared calendaring, netmeetings, etc.
  - Getting the right attributes released has been a pain
- I manage several access controlled web sites
  - Keeping track of all those login names…
  - Getting those names (or attributes) released has been a pain

The panel

- Brad Myers, University Registrar, Ohio State University
- Sarah Morrow, Chief Privacy Officer, Penn State
- Matt Kolb, Assistant Director, Computing Services, Academic Technology Services, Michigan State University
- Moderator: Ken Klingenstein, middleware dude

The Panel Format

- A quick level set with the attendees on the basic concepts
- A round table set of discussions on the sets of issues generated by both the requirements and the technologies

Level Set

- Attributes and release policies
- uApprove and other technologies
- Some policy structures
  - Consent and informed consent
  - Contractual outsourced relationships
  - PII and the EU Privacy Directives

Attributes and attribute authorities

- Institutional
  - User who has an established, authenticated identity
  - Organizational
  - Reassertion of other official credentials (e.g. citizenship, age, etc.)
- Temporal – geolocation, etc.
- Community or collaboration asserted
  - Formal – Virtual organizations, groups
  - Informal – Reputation systems, FoF
- Self-asserted – Preferred language, accessability

Our basic attributes

- Name (e.g. Display Name)
- Email address
- High-level affiliation (eg, faculty, staff, student)
- A persistent and human-usable identifier (eg, kjk@internet2.edu).
- Opaque, persistent and non-correlating identifiers (ePTID)
- An open-ended set of entitlements assigned by the institution, including group membership

User attribute release management uApprove

- For scaling of number of sites, number of IdP’s, number of countries, number of laws, numbers of users
- Lots still to figure out
  - How to convey the minimum required set for the SP to the IdP/ user? The desirable set?
  - How to convey the default release set of the IdP? Where is that policy set?
- Getting the UI, and the defaults, right… the multiplier is in the billions…
- Several campuses bravely starting down the path

Privacy, consent, and attribute release policies

- Complex, sometimes contradictory requirements from governments around the world
  - EU Privacy Directives important, confusing, and under revision
  - FICAM Directives important, confusing, and under revision
  - State and local laws and lots of institutional folklore
- In federated identity, the key focus is around attribute release and consent
  - Some attributes required for transaction; some may be optional
  - Control points at service provider, at identity provider, and with the user

Consent

- Consent
  - Where and when
  - How the interface looks today
  - Where it needs to go
- Informed consent
  - Setting the bar
  - Engaging the SP’ s
  - Educating the User

Jurisdictional Issues at the Start

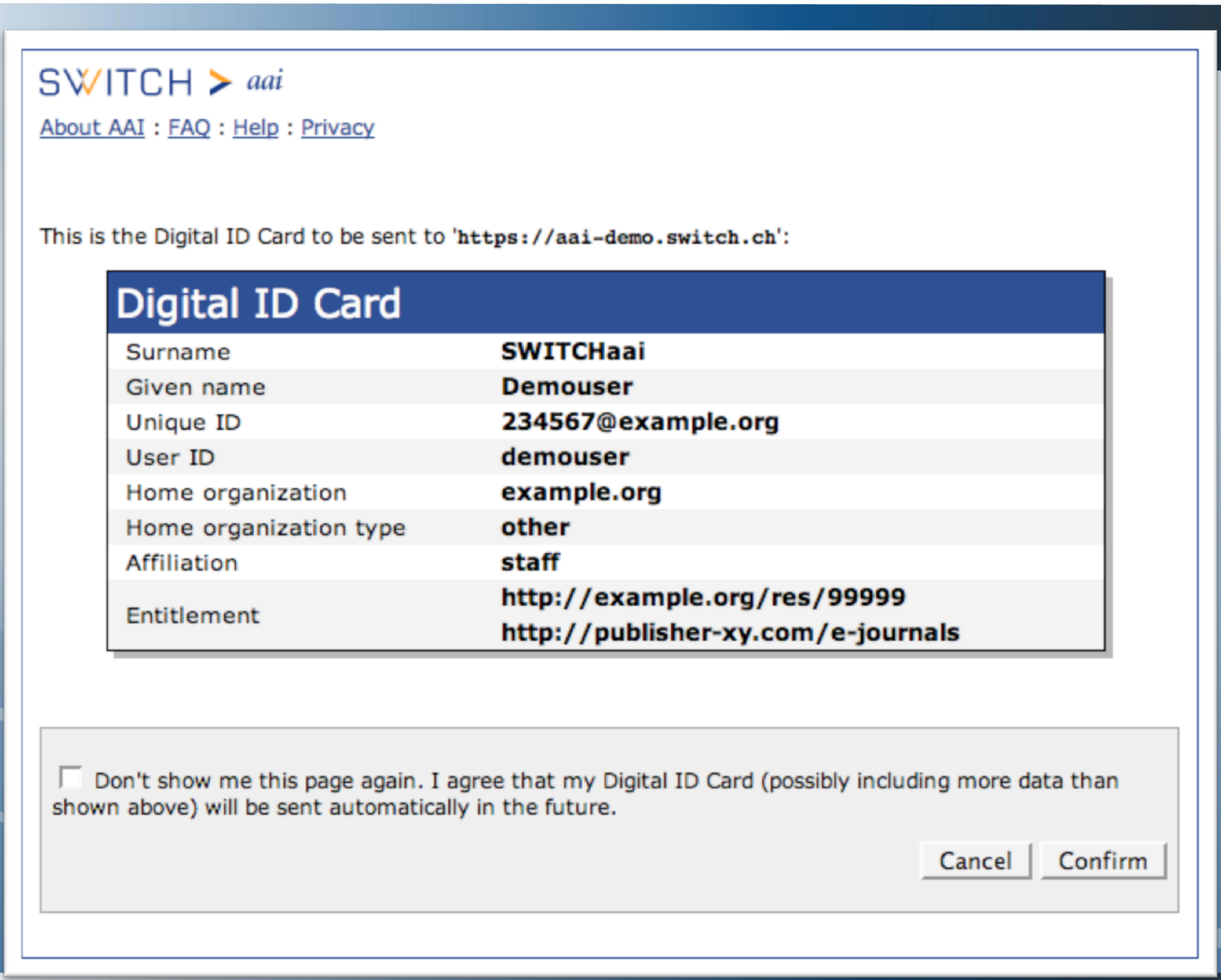
- At least three policy spaces at play
  - IdP location
  - SP location
  - User’s national and local laws
- Known exploits exist today…

When to do Consent

- At the point of collection of information
  - “We intend to use what you give us in the following ways”
- At the point of release of information
  - “I authorize the release of this data in order to get my rubber squeeze toy…”
  - Per transaction or persistent for some time

uApprove

- Provide users with control, and guidance, over the release of attributes
  - Includes consent, privacy management, etc.
- Basic controls (from the Swiss) now built into Shibboleth, but largely untapped in deployments.
- Additional technical developments would help scalability
- Human interface issues largely not yet understood – getting the defaults right, putting the informed into informed consent, etc.

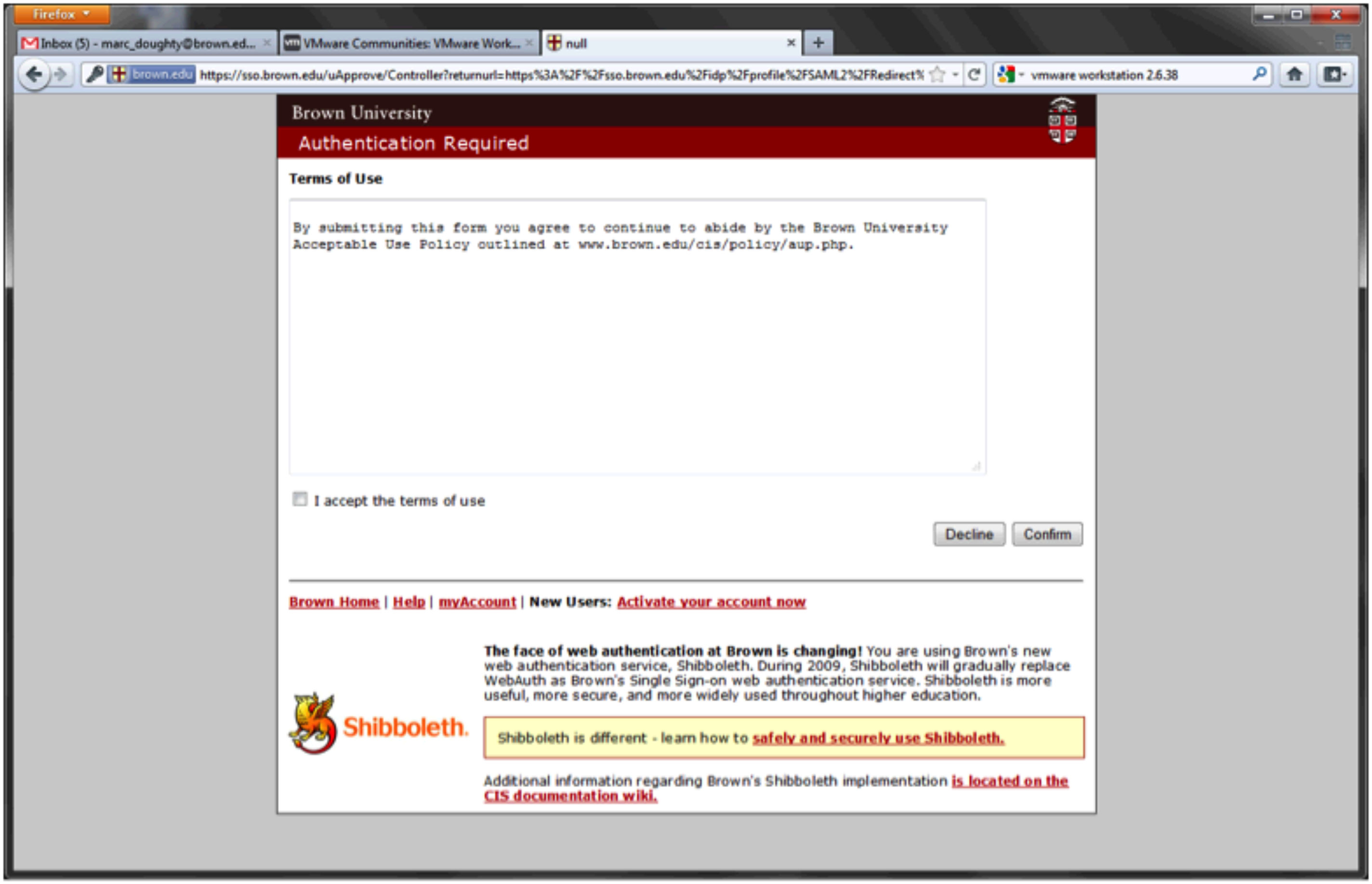


This is the Digital ID Card to be sent to '`https://aai-demo.switch.ch`':

Digital ID Card

Surname	**SWITCHaai**
Given name	**Demouser**
Unique ID	**234567@example.org**
User ID	**demouser**
Home organization	**example.org**
Home organization type	**other**
Affiliation	**staff**
Entitlement	**http://example.org/res/99999** **http://publisher-xy.com/e-journals**

□ Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future.



Firefox
Inbox (5) - marc_doughty@brown.ed...
VMware Communities: VMware Work...
null
brown.edu
https://sso.brown.edu/uApprove/Controller?returnurl=https%3A%2F%2Fsso.brown.edu%2Fidp%2Fprofile%2FSAML2%2FRedirect%
vmware workstation 2.6.38

Brown University

Authentication Required

Terms of Use

```
By submitting this form you agree to continue to abide by the Brown University
Acceptable Use Policy outlined at www.brown.edu/cis/policy/aup.php.
```

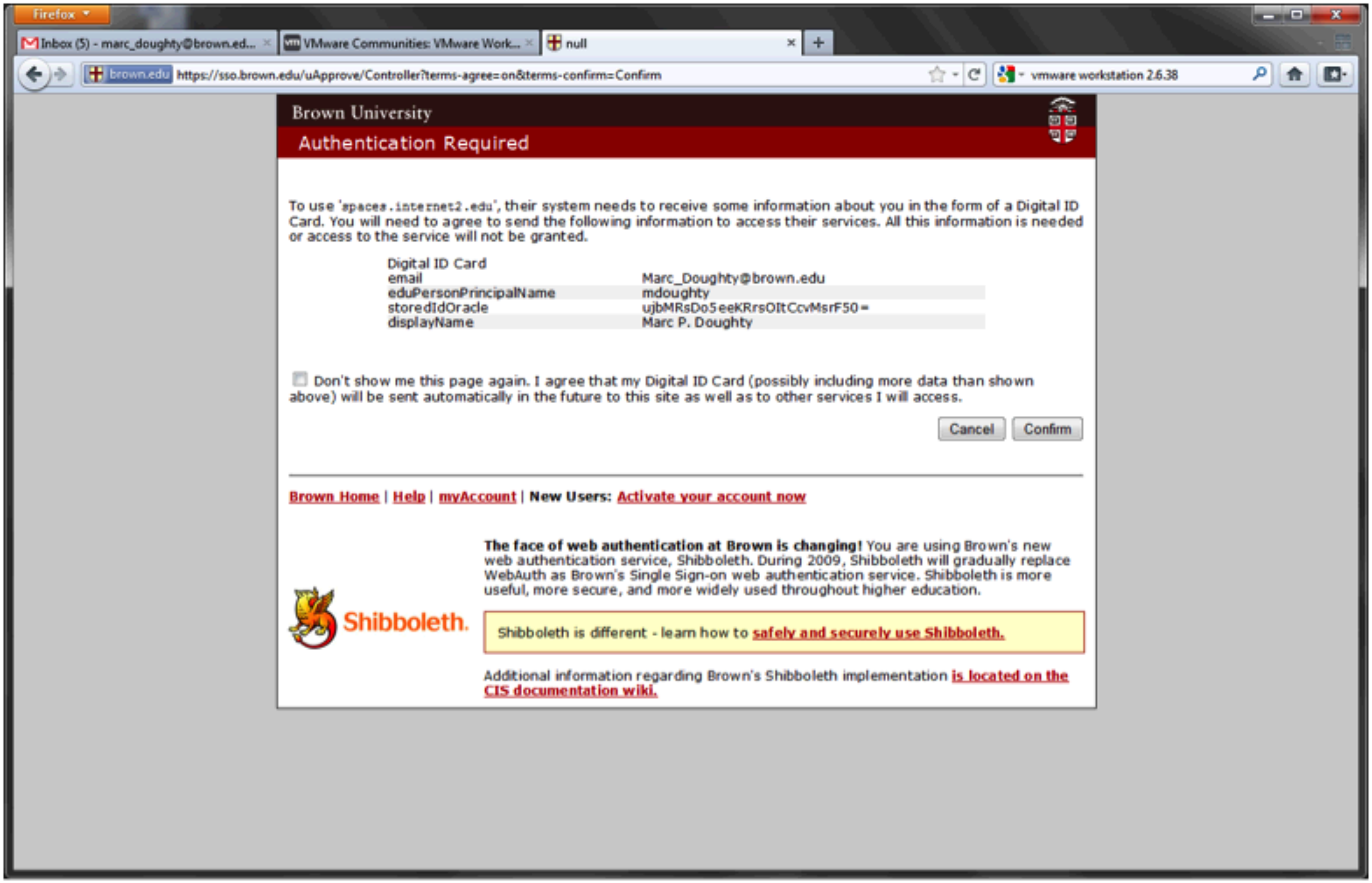
□ I accept the terms of use

Brown Home | Help | myAccount | **New Users:** Activate your account now

The face of web authentication at Brown is changing! You are using Brown's new web authentication service, Shibboleth. During 2009, Shibboleth will gradually replace WebAuth as Brown's Single Sign-on web authentication service. Shibboleth is more useful, more secure, and more widely used throughout higher education.

Shibboleth is different - learn how to safely and securely use Shibboleth.

Additional information regarding Brown's Shibboleth implementation is located on the CIS documentation wiki.



Firefox
Inbox (5) - marc_doughty@brown.ed...
VMware Communities: VMware Work...
null
brown.edu
https://sso.brown.edu/uApprove/Controller?terms-agree=on&terms-confirm=Confirm
vmware workstation 2.6.38

Brown University

Authentication Required

To use 'spaces.internet2.edu', their system needs to receive some information about you in the form of a Digital ID Card. You will need to agree to send the following information to access their services. All this information is needed or access to the service will not be granted.

Digital ID Card	
email	Marc_Doughty@brown.edu
eduPersonPrincipalName	mdoughty
storedIdOracle	ujbMRsDo5eeKRrsOItCcvMsrF50=
displayName	Marc P. Doughty

□ Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future to this site as well as to other services I will access.

Brown Home | Help | myAccount | **New Users:** Activate your account now

The face of web authentication at Brown is changing! You are using Brown's new web authentication service, Shibboleth. During 2009, Shibboleth will gradually replace WebAuth as Brown's Single Sign-on web authentication service. Shibboleth is more useful, more secure, and more widely used throughout higher education.

Shibboleth is different - learn how to safely and securely use Shibboleth.

Additional information regarding Brown's Shibboleth implementation is located on the CIS documentation wiki.

Discussion Topics – 1

- What are the issues that affect attribute release policies for students? Issues for faculty/staff? Can you tell them apart? Who makes the policy decisions?
- When and where to what type of consent?
- Helping users to understand privacy management. How, Whose responsibility?
- Are there opportunities for side benefits/cost saving?

Discussion topics -2

- What constraints would the IdP like to see on the SP use of attributes? How to enforce it as an SP? What about portals, CMP’s and other “reasserters”?
- Does the type of attribute determine the policy (e.g. self-asserted – preferred language)
- International issues
  - Students on campuses in other countries
- Attribute bundles and other hopes
- Operational issues – User education, log files, etc.