IMPACT
RESEARCH
INVESTMENT
DISCOVERY
OPPORTUNITIES
STRENGTHS
ACCESS
RESOURCES
EFFICIENCIES
COLLABORATION

University of Chicago
University of Illinois
Indiana University
University of Iowa
University of Maryland
University of Michigan
Michigan State University
University of Minnesota
University of Nebraska-Lincoln
Northwestern University
Ohio State University
Pennsylvania State University
Purdue University
Rutgers University
University of Wisconsin-Madison

C·I·C
COMMITTEE ON INSTITUTIONAL COOPERATION
Cloud Services Cookbook

Mark Nye, University of Illinois at Urbana-Champaign
Keith Wessel, University of Illinois at Urbana-Champaign
Keith Brautigam, University of Iowa
What is the CIC?

TOGETHER WE WORK.
TOGETHER IT WORKS.
Challenges of the Cloud

VS.

[Diagram of a mushroom cloud on the left and a smiling cloud on the right]
What is the Cloud Service Cookbook?

• Currently in **draft**

• Targeted at two audiences
  – Campus IT
  – Cloud Service Providers

• Simple format
  – **DO, DON’T, CONSIDER**
Creating the Cookbook

Process overview
1. We identified the problem
2. We did surveys amongst CIC
3. Technical writing
4. Technical editing
5. Pilot with a vended app
Why a Cloud Service Cookbook?

• Oranges and garlic
  – Vendors might not tell you everything you need to do; they might not even know. The cookbook will point out things that the vendor doesn’t.

• Frozen pizza
  – It's easy to cut corners when it means more cost to someone else.
How Can it Save You Time?
Past Presentations

InCommon
Identity Week 2013

- Keith Wessel, University of Illinois at Urbana-Champaign
- Mark Nye, University of Illinois at Urbana-Champaign
- Keith Brautigam, The University of Iowa

http://spaces.internet2.edu/download/attachments/37650846/1430+Wessel.pptx

- Keith Wessel, University of Illinois at Urbana-Champaign
- Oren Sreebny, The University of Chicago

http://meetings.internet2.edu/2014-global-summit/detail/10003128/
## Content

### Major Headings
- Authentication
- Identity Provider discovery
- Identifiers
- Authorization
- Provisioning & De-provisioning
- Technical Trust Framework
- Operational Agility
- User Experience
- Policy & Compliance

### Additional Content
- Higher Ed. IdM Landscape
- Case Studies
- Sample RFP Language
Challenges: Network IDs and Email Addresses

**CONSIDER** the relationship between ePPN and mail.

*Campus:* DO socialize the use of organizational email addresses.

*Campus:* DO make eduPersonPrincipalName useful.

*Vendor:* DO be cautious about using mail as a unique identifier.
Challenges: Scoped and Unscoped Identifiers

Campus: **DO** work with service providers to understand how data is being interpreted.

Vendor: **DON'T** assume that a simple username is unique across domains and subdomains.
Challenges: Overloading Attributes

**DON'T** call a Foo a Bar
Challenges: Out-of-Band Metadata

**DO** register SAML metadata with the InCommon federation.

*Campus:* **DO** define a process for maintaining SAML Service Provider metadata.

**DO** understand your partners' limitations.
Challenge: Just-in-Time Provisioning

*Campus:* **CONSIDER** whether a service is dependent on service-specific "local" user accounts.

*Campus:* **DON'T** require out-of-band acceptance of Terms of Use.

*Vendor:* **DO** manage your provisioning API in a way that respects the service subscriber interests.

*Vendor:* **DO** refresh user attributes upon login
Challenge: De-Provisioning

*Campus:* DON'T expect robust de-provisioning support.
**Challenge: Service-specific Passwords**

**DON’T** use separate service passwords, unless you must.

*Vendor: DO* let the identity provider handle authentication.

*Vendor: DO* provide an API for password setting if you must use a service-specific password.
Challenge: Where to do Authorization

**DO** just the right amount of authorization at the IDP.

**CONSIDER** where the allow/deny decision logic is evaluated.

*Vendor:* **DO** leverage eduPerson attributes for authorization.
Challenge: Usernames Change

“What's in a name?
...a rose by any other name would smell as sweet”
--Act II, Scene II. Romeo and Juliet

Vendor: DO be prepared for username changes.

Campus: DO standardize internally on a stable "serial number" for users.

Campus: DO support a varied set of identifiers.

DON'T be afraid of eduPersonTargetedID.
Challenge: Higher Education Environment

Cloud Cookbook Section:
*Overview of Higher Education IDM Landscape*
Conclusion

Cookbook draft: https://carmenwiki.osu.edu/x/nLdCAg

Please share with your technical staff and project managers.

  – Feedback welcome!

• Keith Wessel, kwessel@illinois.edu
• Mark Nye, marknye@illinois.edu
• Keith Brautigam, keith-brautigam@uiowa.edu