IAM Online – September 11, 2013

Multi-Factor Authentication: All in This Together

Host:

Tom Barton, University of Chicago

Speakers:

Eric Goodman, University of California Office of the President

Mike Grady, Scalable Privacy Project, Senior IAM Consultant, Unicon

David Walker, Scalable Privacy Project, Independent Consultant

IAM Online is brought to you by Internet2's InCommon in cooperation with the EDUCAUSE Identity and Access Management Working Group

Passwords are bad and will get worse. We know!

- Use stronger credentials
- Improve password practices until you no longer need them
  - InCommon's Identity Assurance Profiles

Stronger credentials

Factors

- Something you know
- Something you have
- Something you are

Stronger authentication & multi-factor authentication

- One-Time Password (1 factor)
- Biometric (1 factor)
- Pass phrase (1 factor)
- PIN + token (2 factors)
- Password + another password (2 factors)
- Password + cellphone confirmation (2 factors)

Poll: How long do I have to wait?

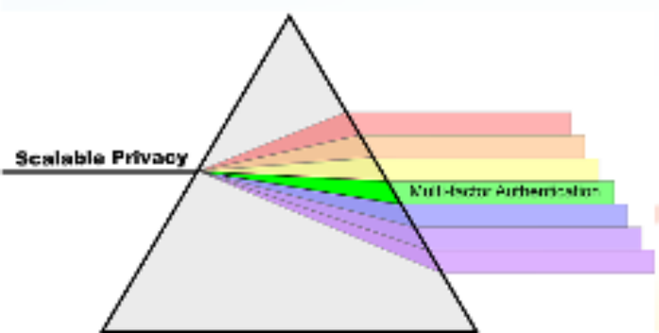
The MFA Cohortium

- Community jointly tackling questions of
  - Strong authentication strategy
  - Pros/cons of various multi-factor technologies
  - Implementation approaches, lessons learned
  - Making the business case
  - ...
- Eric Goodman (U California Office of the President)
- Mike Grady (Unicon)
- David Walker (consultant)

The Multi-Factor Authentication (MFA) Cohortium

All In This Together

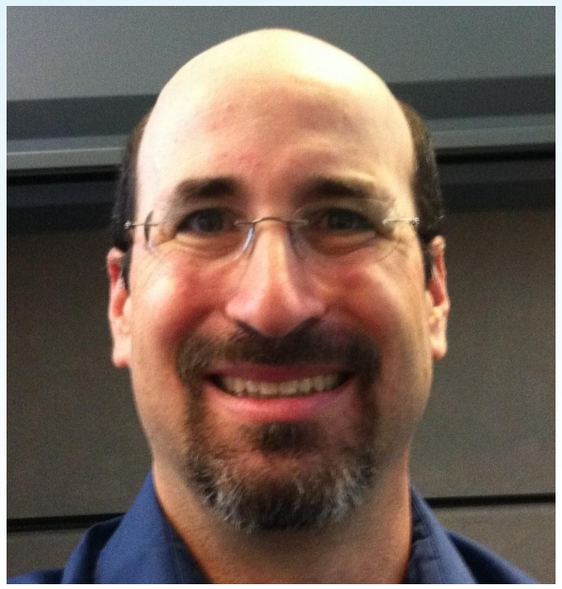
https://spaces.internet2.edu/display/mfacohortium



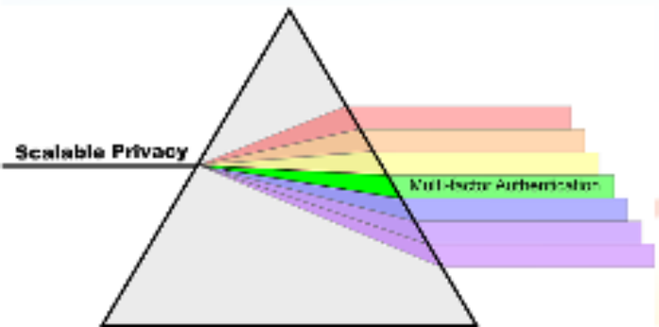
Today's Presenters

Mike Grady, Scalable Privacy Project
Senior IAM Consultant, Unicon

David Walker, Scalable Privacy Project
Independent Consultant



Eric Goodman, Identity and Access Management Architect, University of California Office of the President



Overview

- What is the MFA Cohortium?
- Why are Institutions Participating?
- Cohortium Goals and Deliverables
  - Help for campuses trying to understand their need for multi-factor authentication
  - Help for campuses deploying multi-factor authentication
  - Sponsorship for development of MFA software infrastructure

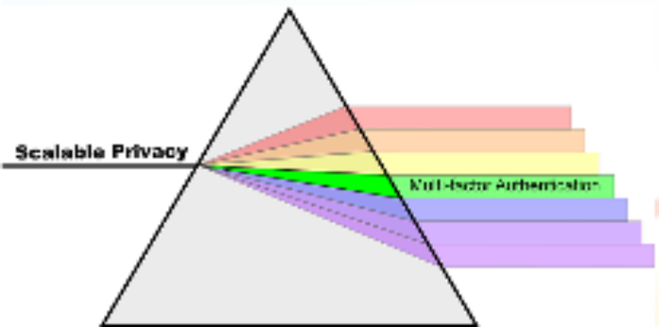
What is the MFA Cohortium?

- Objective: Advance the deployment of Multi-factor Authentication (MFA) in Higher Education
- Roughly 40 institutions participating
- Started end of May 2013, ending in August 2014
- Collaborative effort to help each other understand the business case, technologies, deployment models, issues, costs, requirements, ROI, etc. around deploying MFA.

What is it, continued ….

- Ultimately, collect and create extensive set of resources/artifacts on “all things MFA planning and deployment” for Higher Ed, establishing a public web site to serve as lasting resource site.

- One of a number of efforts that are all part of the Internet2 Scalable Privacy project.

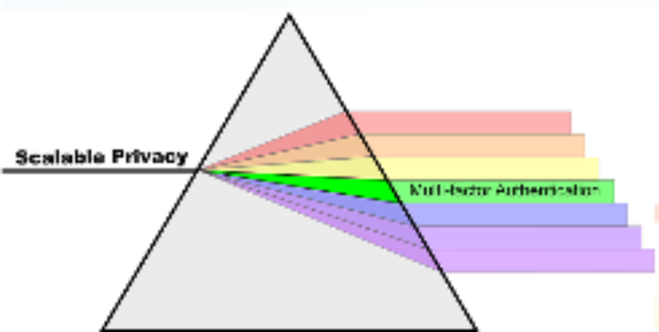


Scalable Privacy

- 2+ year grant to Internet2/InCommon, funded as part of the National Strategy for Trusted Identities in Cyberspace (NSTIC)
- Development partners are CMU, Brown, with expertise from Wisconsin, Ohio State and others
- Several focal points
  - Promotion of multi-factor authentication (MFA)
  - Citizen-centric attributes and schema
  - Development and deployment of privacy managers
  - Introduction of anonymous credentials
- https://spaces.internet2.edu/display/scalepriv

Scalable Privacy - MFA activities

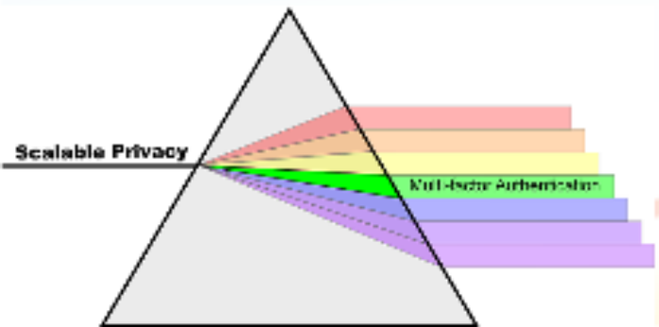
- MFA Cohortium (today's talk)
- Three funded pilot deployments of MFA at MIT, University of Texas System, and University of Utah
- Sponsorship of software development activities related to ease of integration and support of MFA:
  - Shibboleth Assurance and MFA Enhancements for the Shib Identity Provider
  - InCert: Installation and lifecycle management of certificates on client device(s)
  - CAS: Provide similar assurance & MFA support as per Shibboleth effort above



Why Are Institutions Participating?

MFA at University of California

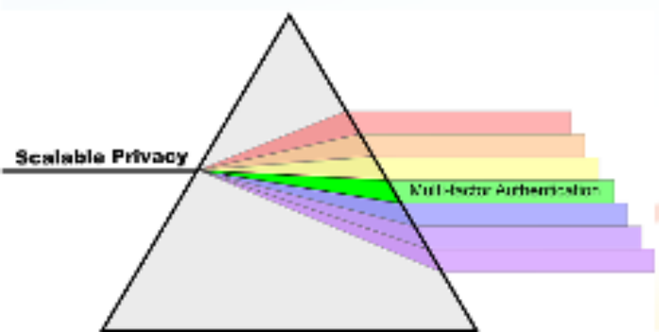
- As a system, UC falls into multiple MFA scenarios
  - Developing business cases
  - Pilots in progress
  - Deploying (and releasing) solutions
- Currently beginning development of system-wide MFA strategy
- This is typical of all universities



What Questions are Universities Asking About MFA

Campuses considering MFA solutions

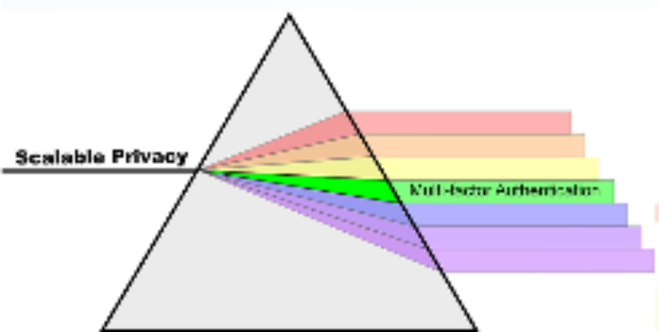
- Strategies for gaining funding
- Convincing execs to support efforts
  - Developing Business Case
  - Risk Management Focus
- Developing project plans
- MFA technology options
- Resource expectations/funding models



What Questions are Universities Asking About MFA

Campuses deploying MFA solutions

- Deployment strategies
- MFA product selection
- Integration options
  - ❖ Many specific platform questions
- Operational requirements and concerns
- User support models
- User communications (supporting roll out)



What Questions are Universities Asking About MFA

Campuses that have deployed MFA solutions

- Share technology solutions
- Support experience
- Areas of user satisfaction/dissatisfaction
- Other “lessons learned”

Poll: Current Deployment Status

Poll: Areas of Greatest Interest

Cohortium Goals

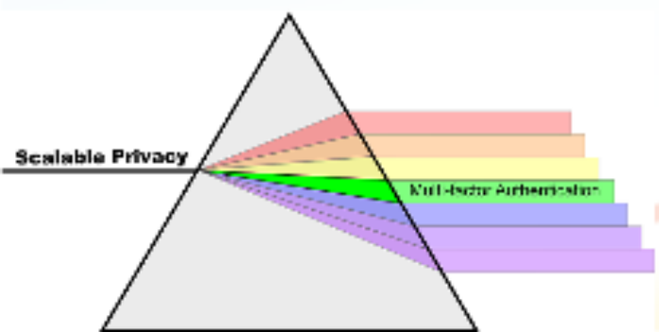
- Advance the use of Multi-factor Authentication in Higher Education.
- “Move the needle”
  - Help campuses without MFA understand the need for it, the risks it addresses, its costs, *etc*.
  - Help campuses that are implementing MFA with deployment, policy, technology, usability and accessibility.
  - Help sponsor development of core infrastructure software modules to facilitate technology integration.

Cohortium Deliverables

Subject to Concurrence of Cohortium

Cohortium Activities and Products

- A forum for discussion of common issues
  - Business Cases
  - Deployment
  - Technology
  - Product / Vendor Issues
- A source of white papers addressing best practices for business, technical, and operational issues
- Lots of example artifacts from institutions



Business Case Elements for Multi-Factor Authentication

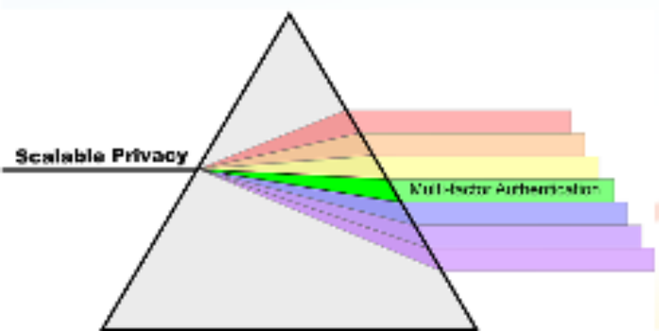
- Strategic Context
  - Alignment with Research and Education Community
- Benefits and Risk Mitigation
  - End-user security
  - Service provider based risk assessment
- Compliance
  - Policy and law
  - Assurance Profiles
- Costs
  - Initial and Ongoing
  - Technology refresh

A Little More about Assurance

- Multi-factor authentication often required to address risk for services related to health care and public safety
- NIH is likely to release services that require MFA
- InCommon Silver does not require MFA, but multiple institutions are finding it more effective than cleaning up their passwords
  - Virginia Tech

Gaining Acceptance in the User Community

- Require MFA only when necessary
- Make business rationale clear
- Build community of enthusiasts by implementing opt-in first
- Select tokens that fit well with users' work styles
- Extend session timeouts when MFA used
- Require based on location (e.g., only for remote access)



Initial Deployment Strategies

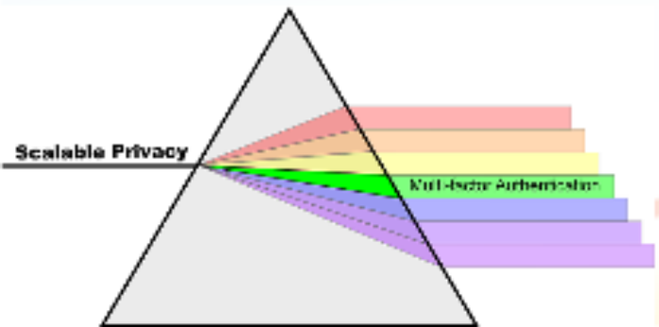
- Deploy for one or a small number of services
  - Minimize startup risks
  - May require re-implementation to add services
  - This is the most common scenario

- Deploy as part of SSO but use for one or a small number of services
  - Minimize startup risks
  - Addition of services is straightforward
  - Allows technology refresh without affecting services

Initial Deployment Strategies

- Deploy as part of SSO with focus on user “opt-in” for MFA
  - Gives users control, time for acceptance to build
  - Can then drive Service Provider adoption as a requirement

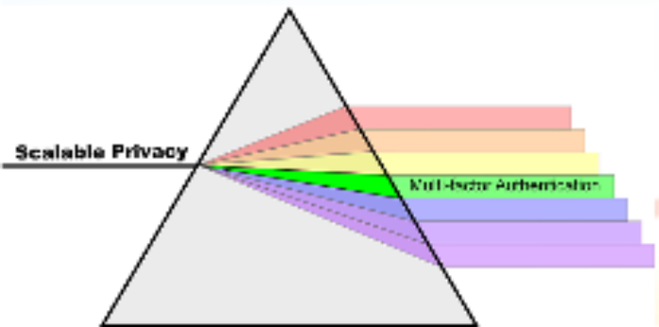
- Not aware of “whole hog” initial deployments, requiring, or just enabling, MFA for everything



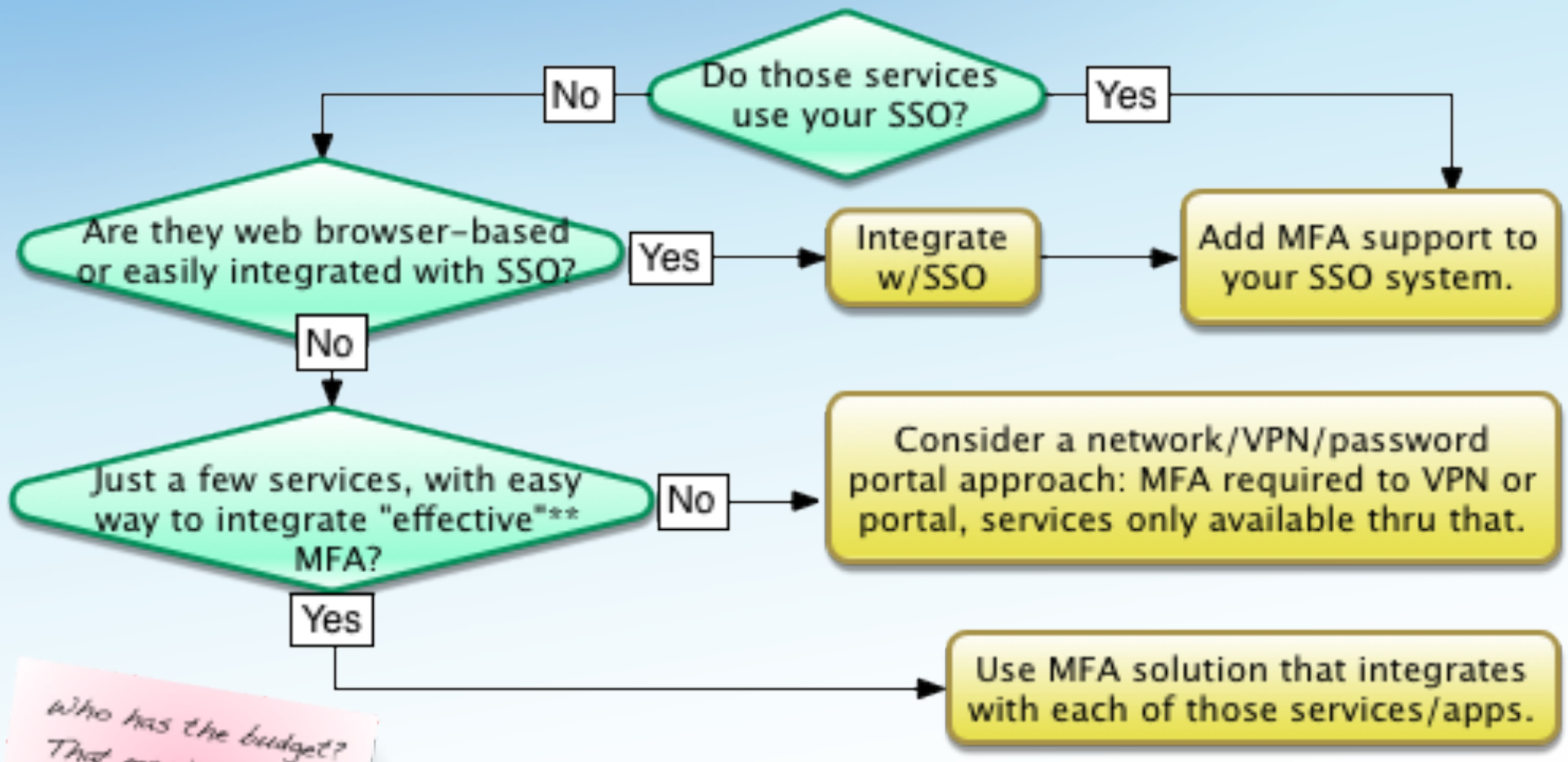
Initial Deployment Strategies

We will produce documents/ artifacts summarizing deployment strategy options. This is a sample (not yet vetted with the Cohortium) of a possible “Decision Tree” artifact.

This is from “institutional perspective”. Decision trees could also be produced from the end user perspective (opt-in), the Assurance use case perspective, etc.



Sample Partial Decision Tree



Architectural patterns of integration

- Individual Services
  - Mainframe
  - VPN
  - Unix login
  - Web application
- Access Control Systems
  - Portals
  - “VPN as a portal”
- Enterprise Single Sign-On and Federation
  - CAS
  - Shibboleth
  - User Option (“Opt-in”)

Technology-focused documents

- Comparative analysis/review of the various security properties of MFA technologies
  - Look at a class of solutions and highlight strengths and weaknesses
  - May start with review of security & privacy properties of telephony approach vs non-telephony approach
- Technologies Assessment Matrix
  - Assess on multiple factors, with broad categories such as Security, Usability, and Deployability
  - Accessibility as a specific criteria

Technology-focused documents

- Great example of analysis is the paper: “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes”
- http://t.co/VUdI7VNb
- Evaluate based on “broad set of twenty-five usability, deployability and security benefits that an ideal scheme might provide.”

Alternative Strategies When Multi-Factor Tokens Are Not Available

- What about failure cases?
  - Token left at home, so can't read mail
  - Battery failed in token, so can't submit $10M grant proposal

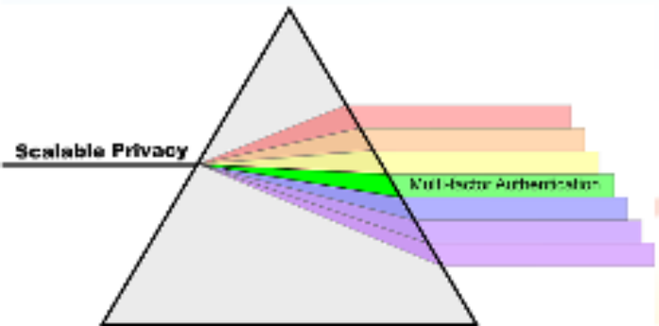
- Must balance risk of impersonation against risk to business continuity

Alternative Strategies When Multi-Factor Tokens Are Not Available - Strategies

- Strategies for opt-in MFA
  - Pre-registered proxies
  - Single-use passwords
- Strategies for service provider required MFA
  - Restricted but not denied access
  - Emergency access for limited time
  - Authorized third parties for authentication
- Strategies for federation required MFA
  - Re-registration
  - Authorized third parties for re-registration
- https://spaces.internet2.edu/x/RABtAg

MFA Enhancements for Shibboleth and CAS

- Enhancements to facilitate integration of MFA technologies into the enterprise SSO
- Issue is really handling *multiple* authentication contexts (*e.g.*, assurance profiles)
  - Integrating a single MFA approach as *only* method is straightforward
  - This work will provide a better framework for integrating a variety/multiple MFA technology options through a standard interface

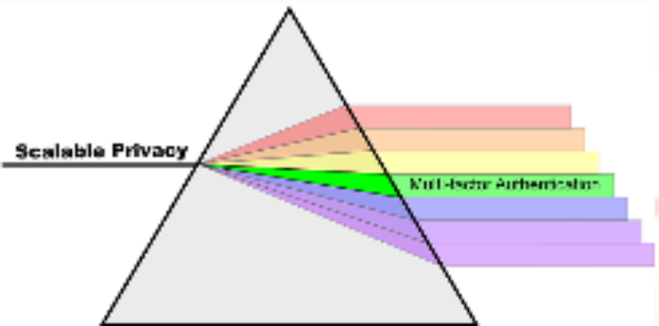


MFA Enhancements for Shibboleth and CAS

- Need to offer options to the user that meet SP needs and that the user is certified to use
- The IdP may be aware of other options that satisfy the SP's requirements
  - SP requests password; IdP satisfies with PKI token
- Initial Shibboleth testing next week; completion by end of year
- Still determining exactly what/how similar work will be done for CAS

Some Other Deliverables that are planned …

- Considerations around outsourced authentication
- Accessibility evaluation of MFA technologies
- FERPA and MFA contract language
- Funding Models
- Sample project & deployment plans
- Sample support documentation & processes, FAQs, etc.
- Sample user communication campaigns



Poll: What Deliverables are of most interest?

More Information about the Cohortium

- Cohortium Wiki Space
  - https://spaces.internet2.edu/x/4AwwAg
- Join the Cohortium
  - Share your questions
  - Share your expertise
  - Help set priorities for deliverables
  - Contribute example documents and artifacts from your institution
  - https://spaces.internet2.edu/x/4wwwAg
- Contact us: cohortium-reg@internet2.edu

Questions & discussion

Evaluation

Please complete the evaluation of today's IAM Online:

http://www.surveymonkey.com/s/IAMOnline_September_2013

InCommon Identity Week - November 11-15, 2013

www.incommon.org/idweek

San Francisco Airport Marriott Waterfront, Burlingame, CA

Monday Nov. 11	Tuesday Nov. 12	Wednesday Nov. 13	Thursday Nov. 14	Friday Nov. 15
REFEDS – Global R&E Federation Operators	Advance CAMP Identity Services Summit	Advance CAMP Identity Services Summit (through noon)	CAMP: Managing Identity and Access in an Era of Distributed Services	CAMP: Managing Identity and Access in an Era of Distributed Services (through noon)
		------ CAMP Pre-Conference: Getting Started with Federated Identity Management (afternoon)		

InCommon Shibboleth Workshop Series

Installation Training for Shibboleth

Single Sign-on and Federating Software

October 21-22 – University of Nebraska Omaha – Omaha, NE

Details and registration at www.incommon.org/shibtraining

IAM Online is brought to you by Internet2's InCommon in cooperation with the EDUCAUSE Identity and Access Management Working Group

Thank you to InCommon Affiliates for helping to make IAM Online possible.

Brought to you by Internet2's InCommon, in cooperation with the EDUCAUSE Identity and Access Management Working Group