IAM Online

What is TIER?
What Does It Mean for Me?

January 25, 2017

KEVIN MOROONEY
ANN WEST
STEVE ZOPPI

Two Topics for Today

- Trust and Identity Overview
- Dive into TIER (Trust and Identity for Education and Research)

The Story

Faculty Member

Collaborates With

Collaborative Science Project in UK

How it Works

InCommon

Campus A

Faculty Member

eduGAIN

The UK Access Management Federation FOR EDUCATION AND RESEARCH

Campus Z

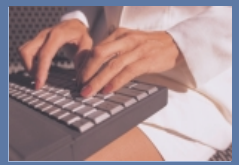
Science Project

How it Works

InCommon

Campus A

Faculty Member



eduGAIN

Focus of TIER

The UK Access Management Federation
FOR EDUCATION AND RESEARCH

Campus Z

Science Project

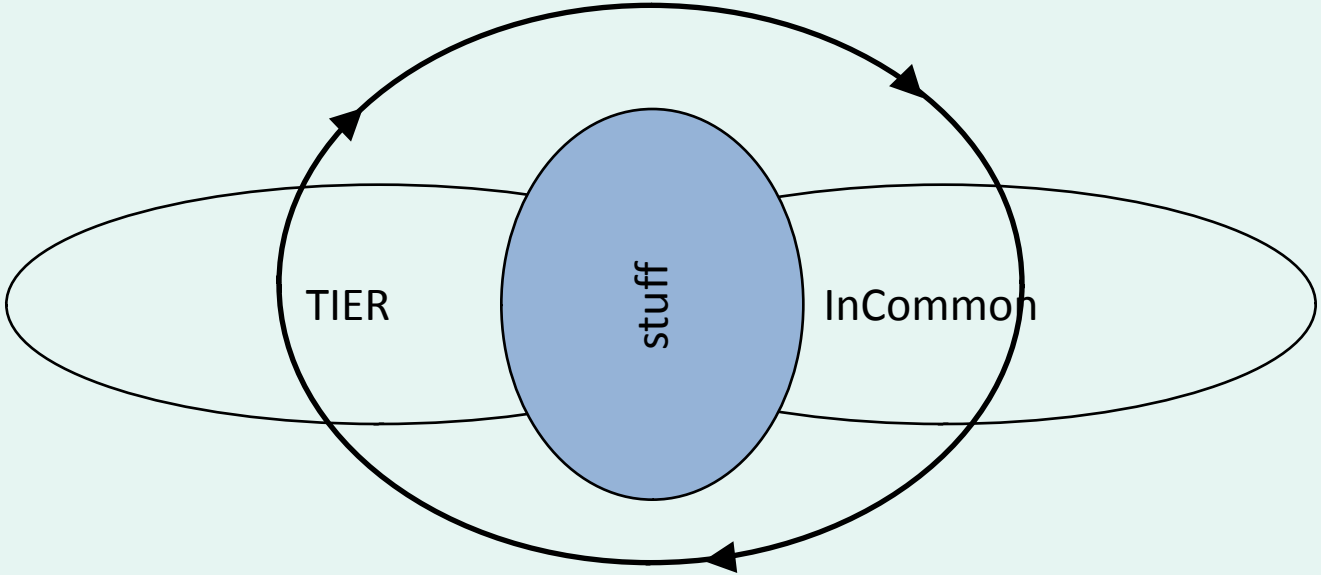
INTERNET

Trust and Identity at Internet2

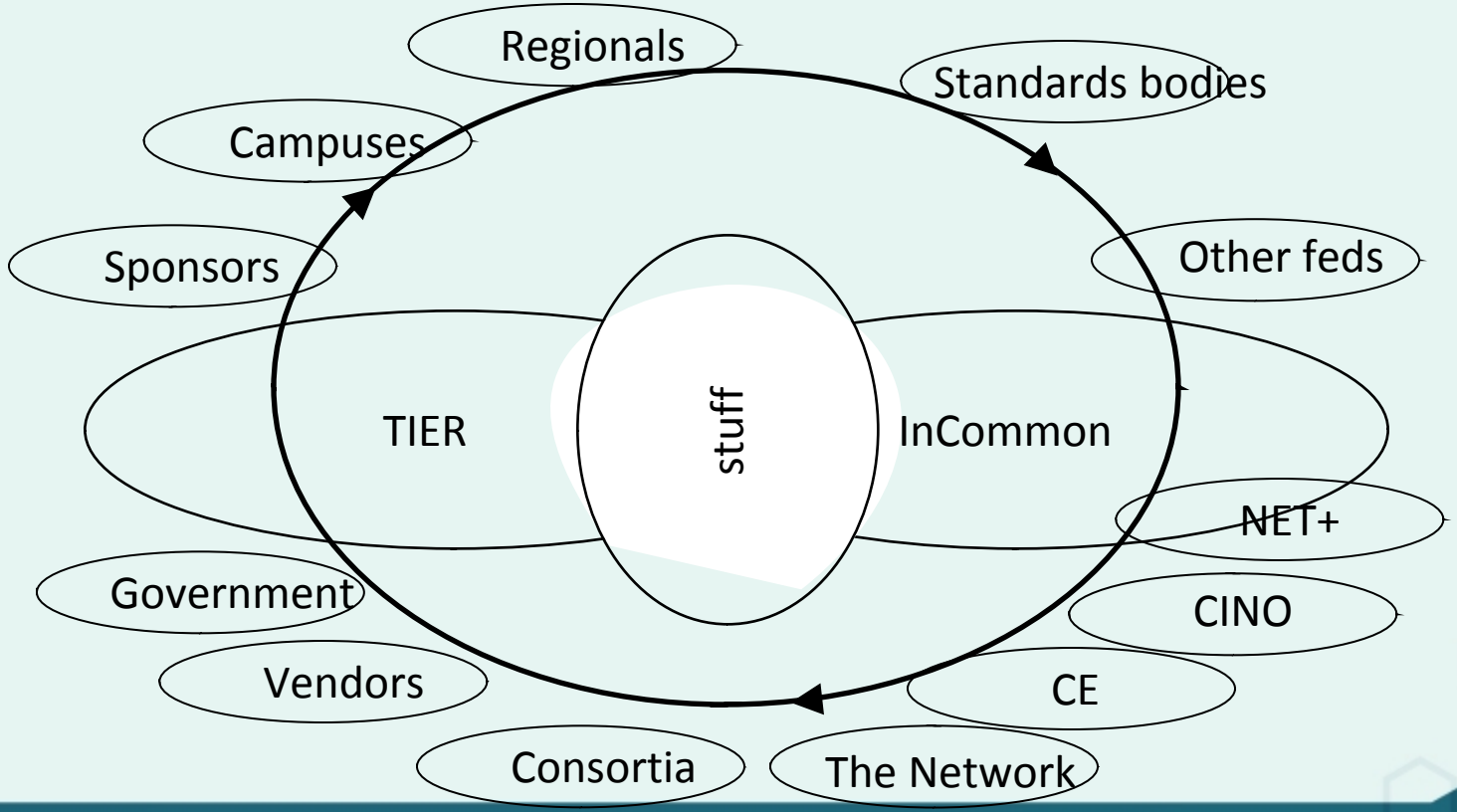
- In January 2016, Internet2 established a division of Trust and Identity Services
  - However, the work has been going on for a *long* time

- The core services/activities are InCommon Trust Federation, TIER, eduroam, and the InCommon Certificate Service

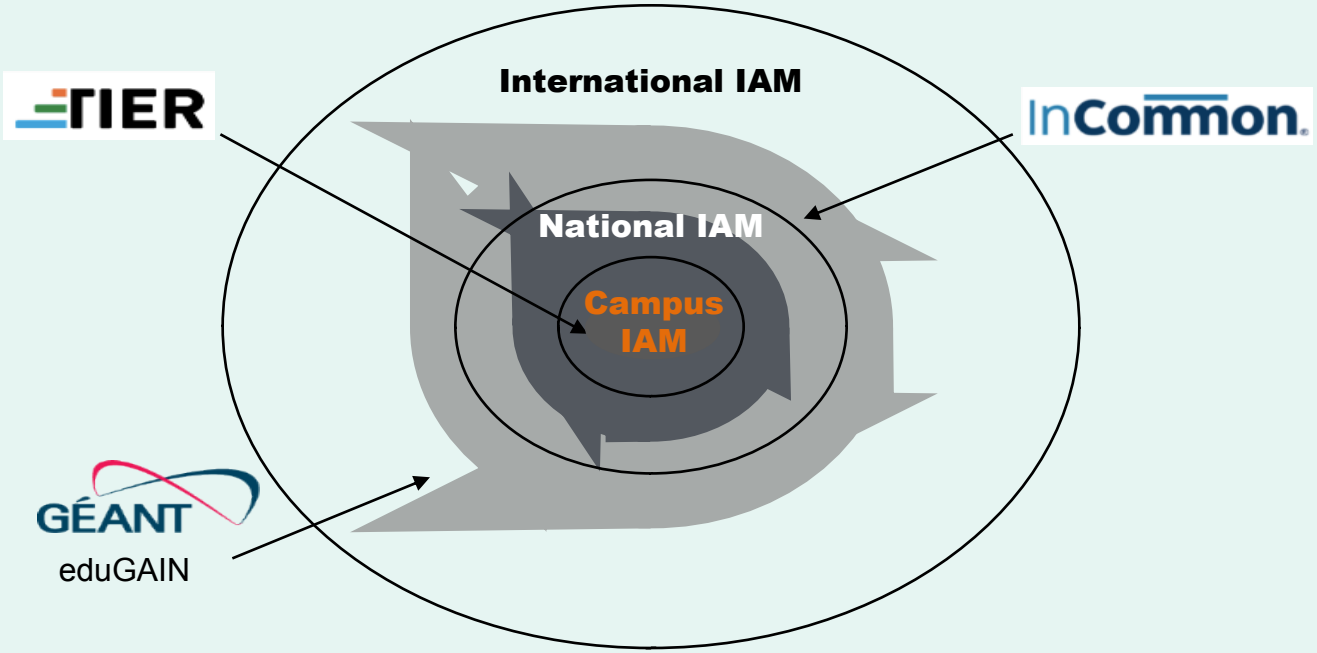
How TIER and InCommon Interact



Trust and Identity - The Vanity View



How TIER and InCommon Federation Interact



Important Guiding Principles

- Reductions in the variances of technologies leveraged and policies developed - among the membership/participants - increases the collective ability to trust, to collaborate.
- “Participants” need flexibility
- All moving parts have to become more trustworthy over time

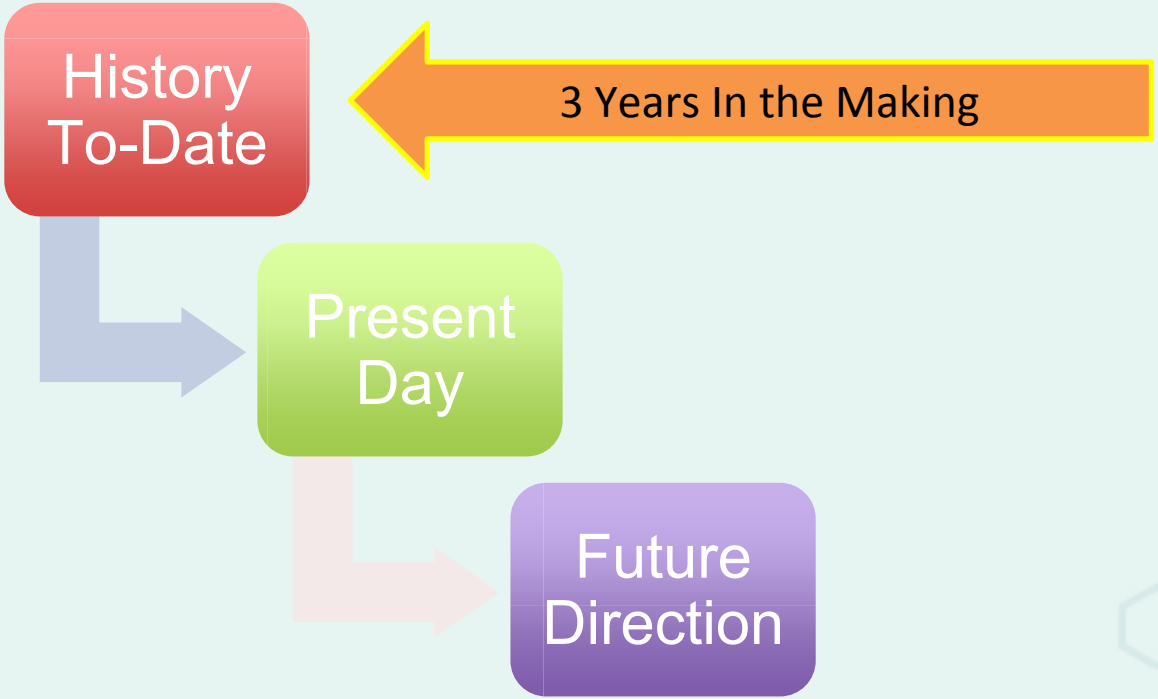

INTERNET 2
QUESTIONS SO FAR?


INTERNET 2
LET’S DIVE INTO TIER

What is TIER all about?

- Sustain components that we've developed together
- Fill the gaps by providing a set of integrated components that address IAM as a whole
- Address community requirements across the components
- Developing, maintaining community and corporate partnerships

Evolution of TIER



TIER Background

- Investors:
  - 49 CIO investors
  - All Internet2 members.
  - 25K/year for three years.
- 9 months of requirements gathering among the investors institutions, generating 200+ use cases and 70 requirements
- Final Year of 3-year Financial Enrichment

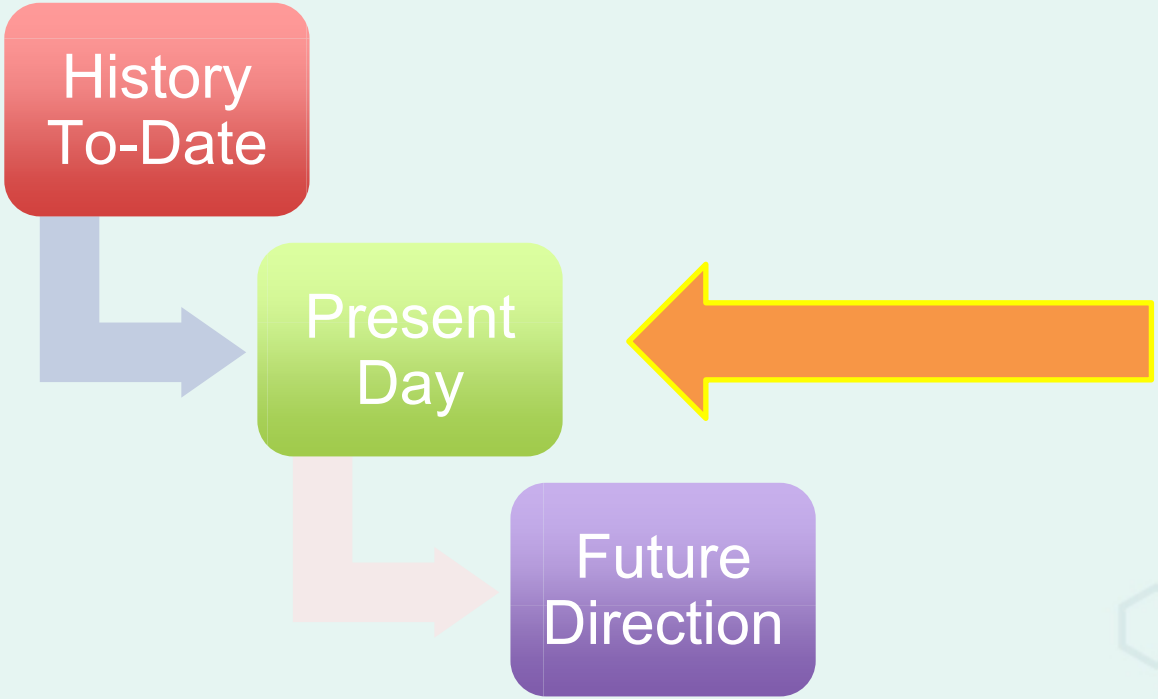
TIER Investors

Arizona State University	Old Dominion University	University of Maryland - College Park
Baylor University	Oregon State University	University of Michigan - Ann Arbor
Boston University	Penn State (Pennsylvania State University, The)	University of Missouri - Columbia
CALTECH (California Institute of Technology)	Purdue University - Main Campus	University of Nebraska - Lincoln
Carnegie Mellon University	Rice University	University of North Carolina - Chapel Hill
Case Western Reserve University	Stanford University	University of Notre Dame
Clemson University	Tulane University	University of Oregon
Cornell University	University of Arizona	University of Pittsburgh - Pittsburgh Campus
Duke University	University of California – Berkeley	University of Utah
Harvard University	University of California – Merced	University of Virginia
Indiana University	University of Chicago	University of Washington
Lafayette College	University of Florida	University of Wisconsin - Madison
Louisiana State University	University of Hawaii – Manoa	Virginia Polytechnic Institute and State University
MIT (Massachusetts Institute of Technology)	University of Illinois - Urbana-Champaign	Washington University in Saint Louis
New York University	University of Iowa	Yale University
Northwestern University	University of Maryland - Baltimore County	

TIER Community Investor Council

- Klara Jelinkova, Rice University (Chair)
- Dennis Cromwell, Indiana University
- Eric Denna, University of Maryland
- Tracy Futhey, Duke University
- Ron Kraemer, University of Notre Dame
- Tom Barton, University of Chicago
- John O'Keefe, Lafayette College
- Kelli Trosvig, University of Michigan

Evolution of TIER



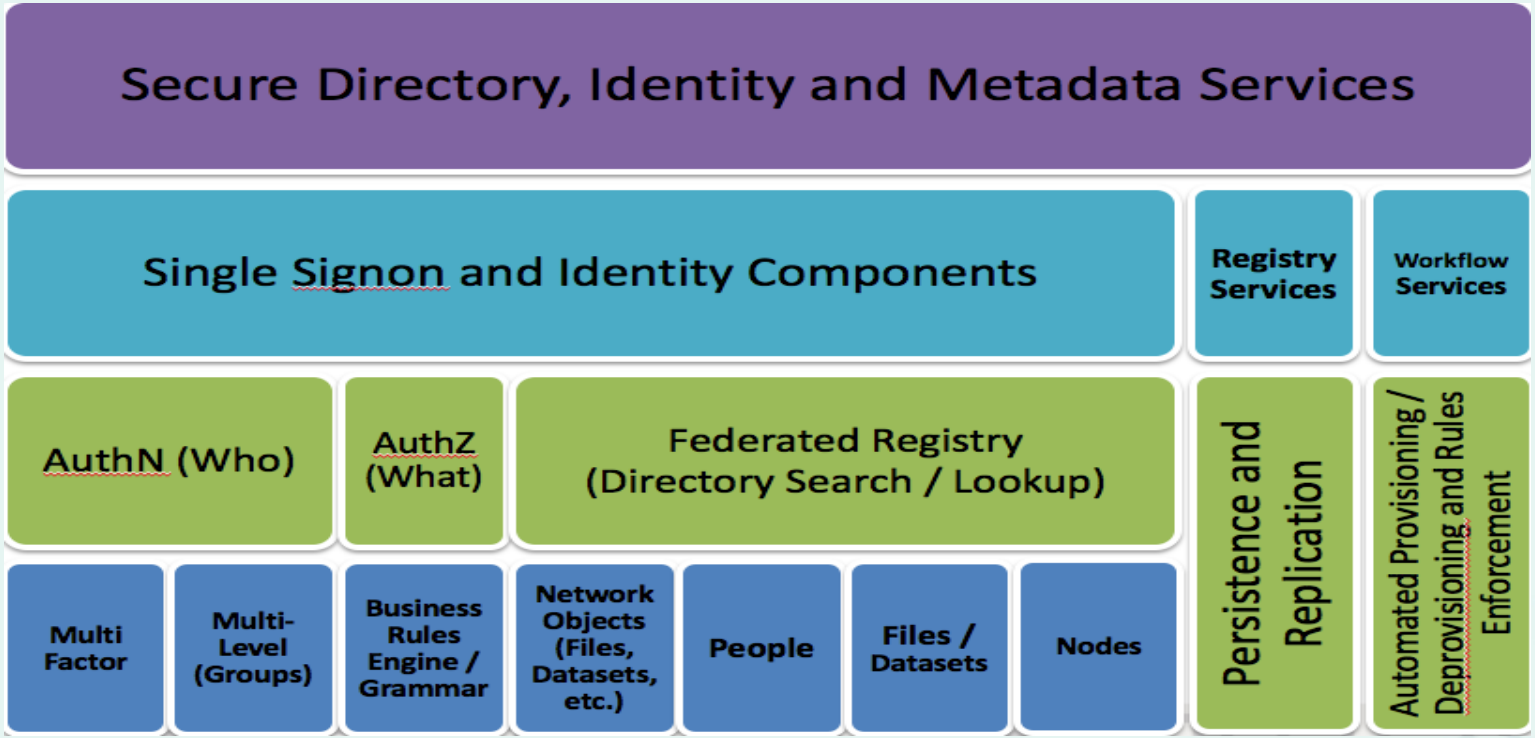
Trust and Identity Governance & Areas of Work

- CACTI – Ad-Hoc Architecture Council (Tom Barton / Trust and Identity / Internet2)
- Security and Audit (Helen Patton)
- Component Architecture (Steve Zoppi)
- APIs and Data Structures (Keith Hazelton)
- Entity Registry (Warren Curry / Benn Oshrin)
- Packaging and Deployment (Jim Jokl)
- Federation Operation (Nick Roy)
- Instrumentation and Monitoring [Preliminary] (Paul Caskey)
- TIER Community Investor Council (Klara Jelinkova)
- InCommon AAC (Brett Bieber)
- InCommon Steering (Sean Reynolds)
- InCommon TAC (Mark Scheible)
- InCommon TAC – OpenIDConnect Use Cases (Albert Wu)
- InCommon TAC – Federation Deployment Profile (Keith Wessel)

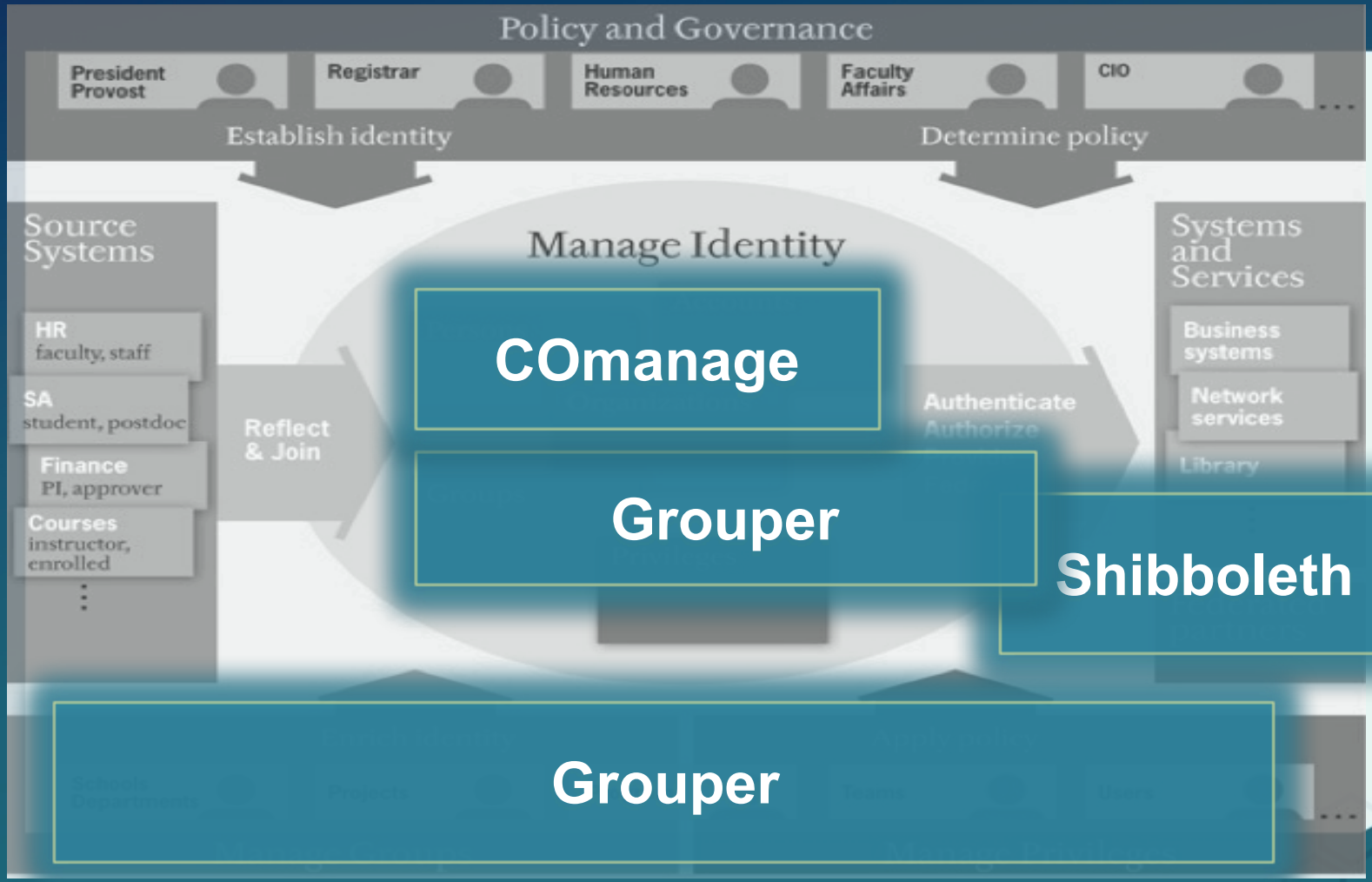
Over 400 People!

INTERNET 2

TIER Goal: Unified (and Scalable) Model




Policy and Governance
President Provost
Registrar
Human Resources
Faculty Affairs
CIO
Establish identity
Determine policy
Source Systems
HR
faculty, staff
SA
student, postdoc
Finance
PI, approver
Courses
instructor, enrolled
Reflect & Join
Manage Identity
Persons
Accounts
Organizations
Groups
Privileges
Authenticate
Authorize
Provide
Federate
Systems and Services
Business systems
Network services
Library
Federated partners
Enrich identity
Schools Departments
Projects
Programs
Manage Groups
Apply policy
Teams
Users
Manage Privileges


Policy and Governance
President Provost
Registrar
Human Resources
Faculty Affairs
CIO
Establish identity
Determine policy
Source Systems
HR
faculty, staff
SA
student, postdoc
Finance
PI, approver
Courses
instructor, enrolled
Reflect & Join
Manage Identity
COmanage
Grouper
Authenticate
Authorize
Shibboleth
Systems and Services
Business systems
Network services
Library
Grouper

What's Been Completed

- Held workshops for investor CIOs and Identity Architects
- Collected hundreds of use cases and requirements
- Priorities developed
- Two releases (April 2016, December 2016)

Proposed Milestones for April 2016

- Backbone usage scenario (BUS) proof of concept
- An open IAM testbed based on the proof of concept
- A containerized version of the IAM testbed for local experimentation
- Well-instrumented code that can reveal behavior and health of the IAM infrastructure components and their interactions
- First edition of a living guidebook: *architectural patterns for IAM integration*

Delivered April 2016

- Backbone usage scenario (BUS) proof of concept — In Progress
- An open IAM testbed based on the proof of concept — POC Ready
- A containerized version of the IAM testbed for local experimentation — Ready
- Well-instrumented code that can reveal behavior and health of the IAM infrastructure components and their interactions — Requirements Gathering
- First edition of a living guidebook: *architectural patterns for IAM integration* — Grouper Outline In Dev

Proposed Milestones for End of Year 2016

- Testing and enhancement of the container/vm distributions
- Exploring Instrumentation
- Prioritize usability enhancements
  - Setup automation and pre-configuration
  - Campus metadata
  - etc., etc.
- Build on the packaging foundation
  - Automate the container and VM builds
  - Operationalize the build process; produce regularly scheduled updates
  - Start the process of automating testing
  - Complete the work with the initial components

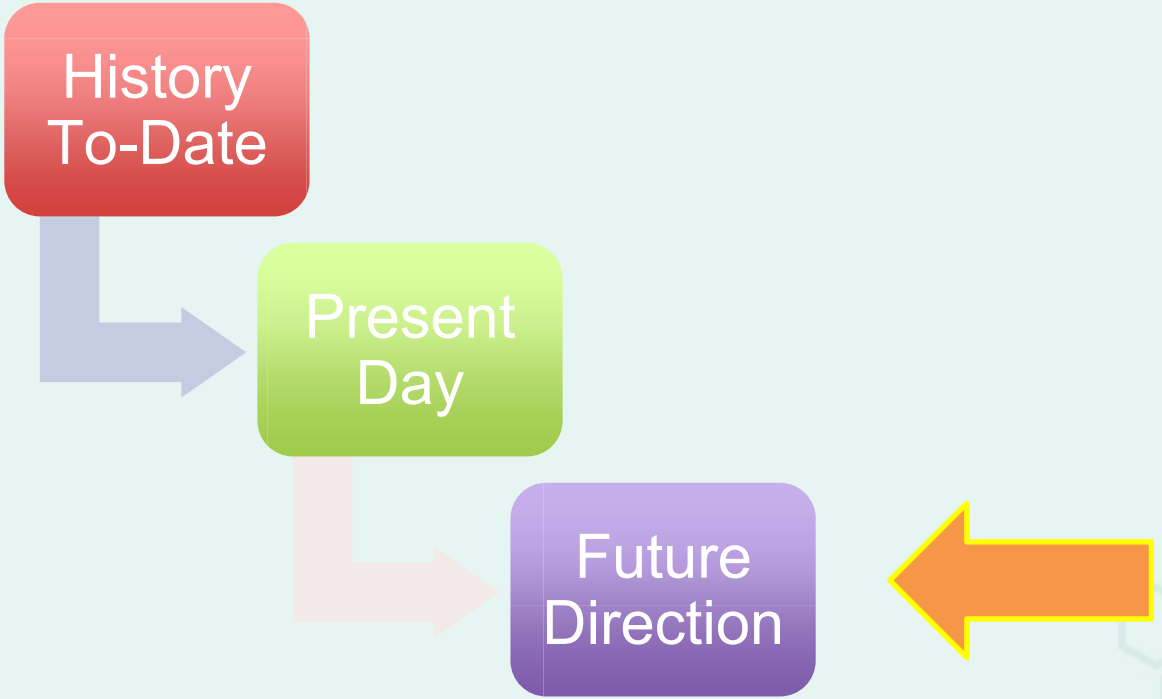
Delivered December 2016

- Testing and enhancement of the container/vm distributions — In Progress
- Exploring Instrumentation — POC Ready
- Prioritize usability enhancements — PENDING
  - Setup automation and pre-configuration — CAMPUS ADOPTION
  - Campus metadata
  - etc., etc.

Build on the packaging foundation

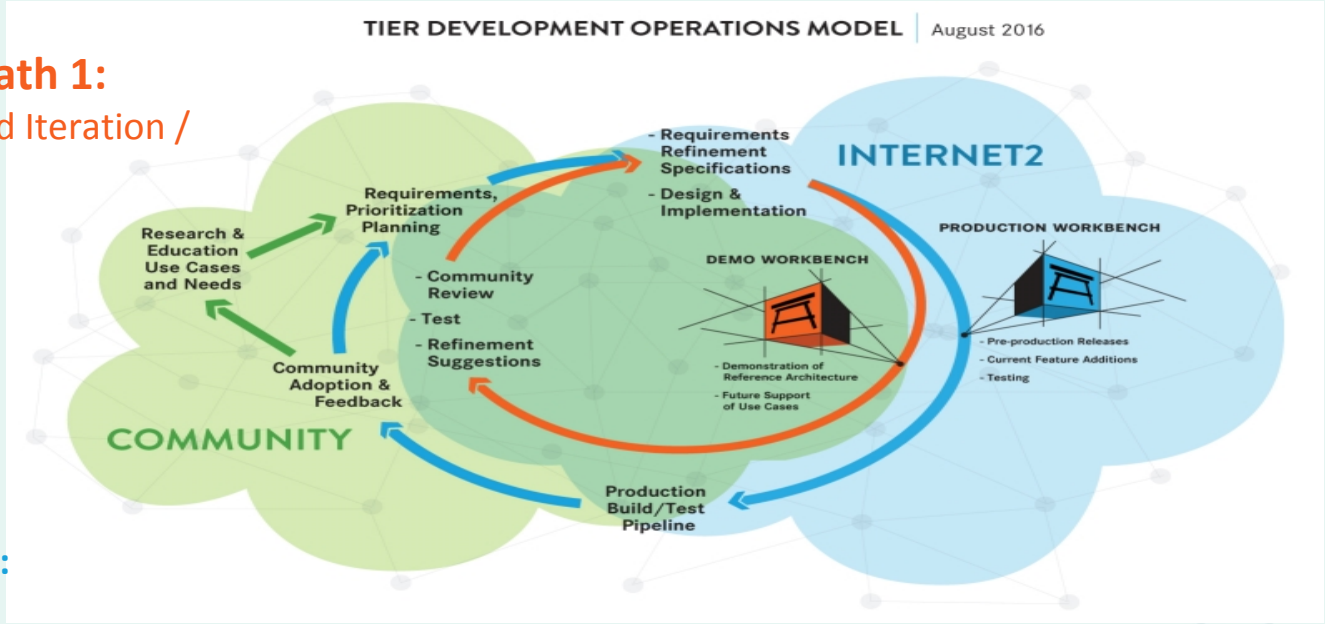
- Automate the container and VM builds — THIS RELEASE
- Operationalize the build process; produce regularly scheduled updates — NEXT
- Start the process of automating testing — NEXT
- Complete the work with the initial components — THIS RELEASE

Evolution of TIER



DevOps Model: Enabling Autonomy

Workbench Path 1:
Development and Iteration / Ideation



Workbench Path 2:
UAT/QA/Security Audit/Performance Assessment/Release

Lessons Learned

- Data Structures and APIs Working Group (WG) and Entity Registry Working Group
  - attracted talented people from higher education institutions across the land (well over 120 on the mailing lists)
  - work hard and deliver what the WG charters required
- Institutions share their experience, documents and code
  - Penn State contributed Apache 2-licensed SCIM server and client libraries, significantly accelerating the API work.

Lessons Learned

- The community is productive:
  - Dedicated set of volunteers
  - Weekly calls
  - Problem space evaluation
  - Survey development and analysis
  - Technical packaging strategy and prototyping
  - Initial testbed
  - If you have interest in this space, please join us
- Significant software development requires dedicated resources
  - The foundational work done by volunteers
  - Engaged commercial firm to build packaging

Lessons Learned

- Institutions with significant IAM projects underway have skin in the game and will make sure the Working Groups stay focused on essentials
- Measurement helps enable management

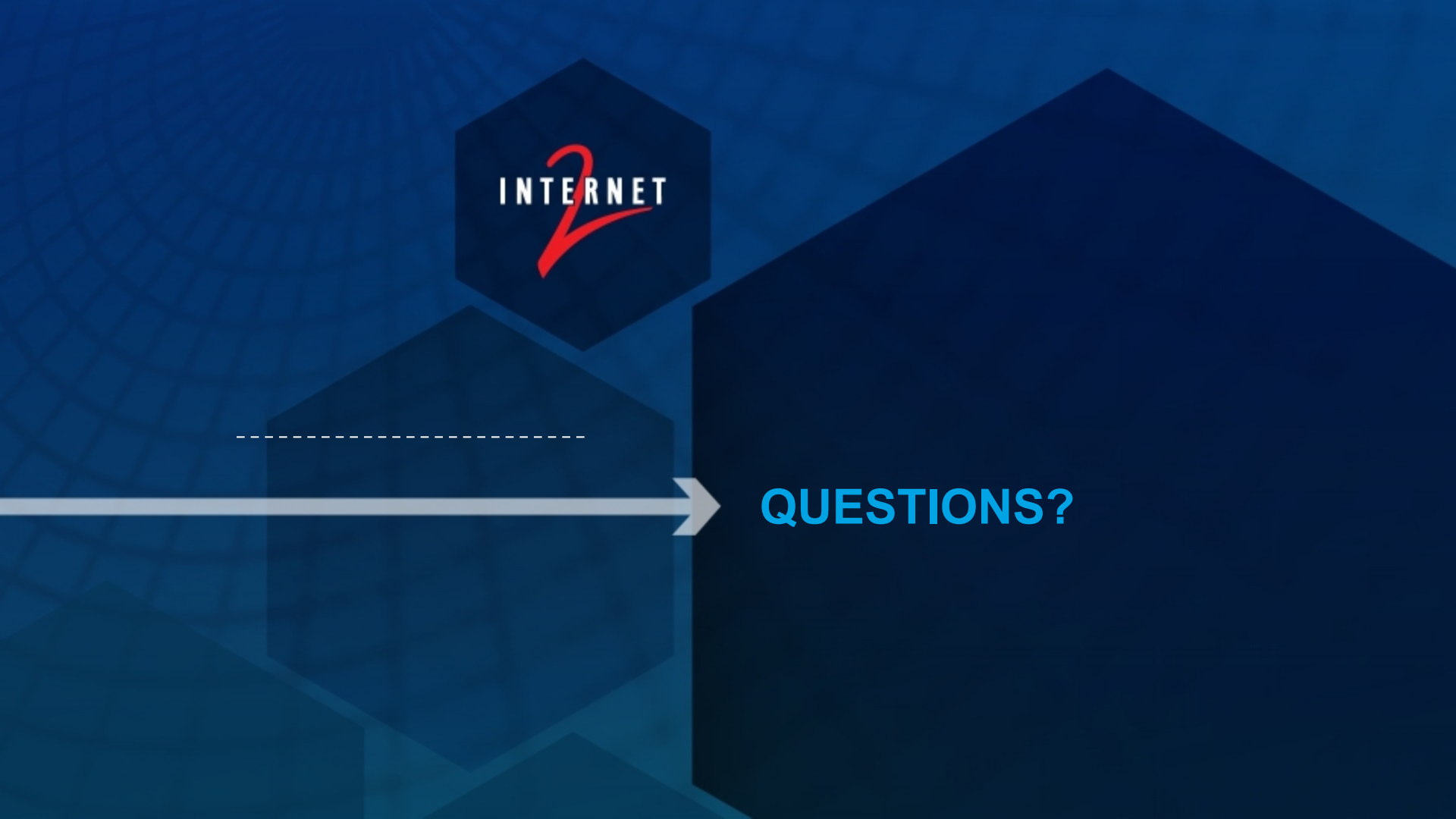

INTERNET 2
NEXT STEPS

Adoption Is Imperative Because …

- It establishes the new and current baseline for all products
- It establishes the foundation for future (incremental) updates and enhancements. Goals …
  - Simple upgrades using latest integration techniques
  - Simple deployment into a scalable environment
  - Releases are instrumented for continual feedback and improvement of the product (Anonymized data / Opt-In Data)

How can you stay engaged?

- Join a working group list
  - http://www.internet2.edu/vision-initiatives/initiatives/trust-identity-education-research/
- Download TIER Production Candidate Containers and ’Kick the Tires’


INTERNET 2
QUESTIONS?

February IAM Online

User Consent: Implementations and Advantages

Wednesday, February 8, 2017 – 2 pm ET

www.incommon.org/iamonline

IAM Online Evaluation

Please complete a short evaluation of today's presentation:

https://www.surveymonkey.com/r/IAM_Online_Jan_2017Jan_2017