Trust and Identity in Education and Research: Identity for Everyone

Ron Kraemer, Notre Dame • Kevin Morooney, Penn State • Ann West, Internet2 • Steve Zoppi, Internet2

Goals of Today's Meeting

- TIER Quick Overview
- Program Status
- Work In Progress
- International Implications
- Campus Readiness

What is Trust and Identity in Education and Research (TIER)?

What is TIER

T(rust)
- A secure and privacy-preserving trust fabric for research and higher education, and their partners.

I(dentity)
- Management of individual principals, their authentication, authorization, and privileges within or across system and enterprise boundaries.

E(ducation)
- Communities of students, teachers and scholars interacting on a global scale.

R(esearch)
- An increasingly virtual, mobile and global research community.

What is Trust and Identity and Education and Research?

Summary: What is TIER all About?

✓ Sustain components that we've developed together.

✓ Fill the gaps by providing a set of integrated components that addresses IAM as a whole.*

✓ Address community requirements across the components.

* Includes Corporate and Community Partnerships

TIER vision

- We believe that identity will be a service
- We believe that it will be a cloud service with campus localization
- We believe that if we do not develop it we will have to accept that someone else will (this means social identities)
- We believe that effective collaboration with partners will be key (and that includes federal agencies)
- We know we are at least 3-5 years from achieving this vision

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 — Apply policy

Manage Groups

Schools Departments | Projects | Programs

Manage Privileges

Teams | Users ...

TIER Goal: Unified (& Scalable) Model

Secure Directory, Identity and Metadata Services

Single Signon and Identity Components

Registry Services

Workflow Services

AuthN (Who)

AuthZ (What)

Federated Registry (Directory Search / Lookup)

Persistence and Replication

Automated Provisioning / Deprovisioning and Rules Enforcement

Multi Factor

Multi-Level (Groups)

Business Rules Engine / Grammar

Network Objects (Files, Datasets, etc.)

People

Files / Datasets

Nodes

TIER Moves from Investor to Sustainable Model (Financials and Governance)

TCI and TCIC

TIER Community Investor / Council

Limited in Charter
- Duration: 3 years
- Scope: Initial Investment Oversight

The Need for Permanence
- Funding (dues and fees)
- Governance (Internet2 PAG model)

More to Explore

- With 2.5 Years Remaining …
  - How should we think about new TCI members?
    - Replace as need arises?
    - More structured renewal?

    Note: loss of time in onboarding (2 year appointment minimum)

- How do we start up a permanent governance structure?

TIER Community Investor Council

- Klara Jelinkova   Rice University (Chair)
- Dennis Cromwell   Indiana University
- Eric Denna   University of Maryland
- Tracy Futhey   Duke University
- Chris Holmes   Baylor University
- Ron Kraemer   University of Notre Dame
- Kevin Morooney   Penn State University
- John O'Keefe   Lafayette College
- Kelli Trosvig   University of Washington
- Melissa Woo   University of Oregon
- Shel Waggener   Internet2

Future Governance Structure

Internet 2 Board of Trustees
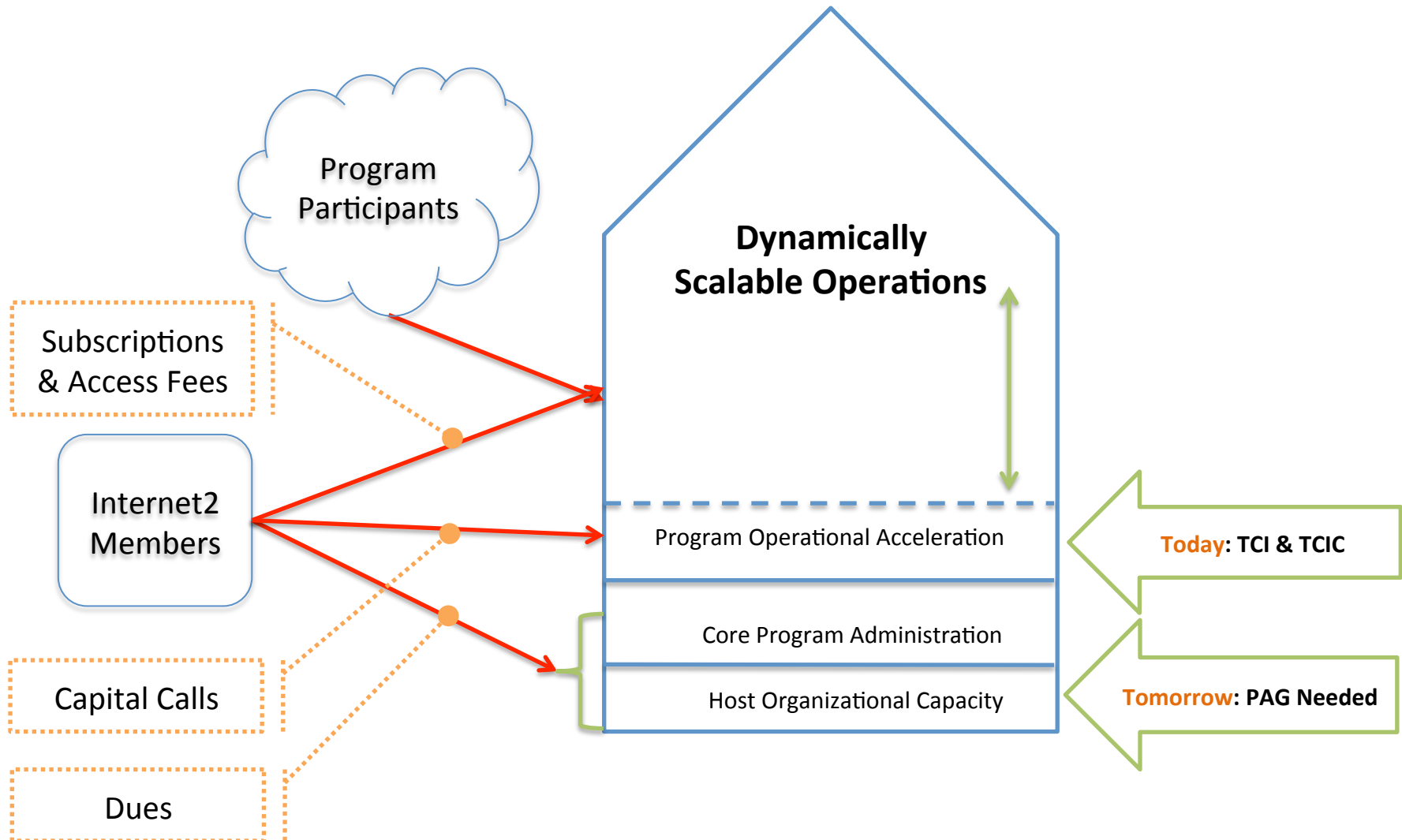
TIER Steering/Board

Service Development Steering Committee (SDSC)

InCommon Steering Committee (ICSC) *

External Relations Subcommittee (includes members from ICSD and SDSC)

* Rescoped InCommon Steering Focuses only on Federation

Membership and Early-Phase Funding Model

Program Participants

Subscriptions & Access Fees

Internet2 Members

Capital Calls

Dues

Dynamically Scalable Operations

Program Operational Acceleration

Core Program Administration

Host Organizational Capacity

Today: TCI & TCIC

Tomorrow: PAG Needed

Current Committed Participants

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

Program Status

Internet2 Program Support

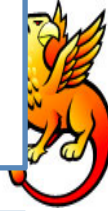| Community	Technology	Sustainability
Ann West (AVP Trust and Identity)	Steve Zoppi (AVP Services Integration and Architecture)	Community Engagement and Membership

Targeting …

2016 First Integrated Release

- Minimal Installation / Configuration User Interfaces
- Preliminary Requirements will be set for Scalable Consent
- Objective: Point In Time Consistency

Primary Focus for Release 1

- Container/Packaging
- APIs
- Initial Deployment
- Continuous Update Cycles
- Documentation

Shibboleth®

Grouper™

COmanage™

Under Consideration for R2

- Community Identity Provider?
- Scalable Consent?

Revised Program Timeline (Funding Driven)

Progress

Communities of Interest

Financial Tracking and Reporting

MOU Management

Community Forum (Online!)

Technical Requirements Revision

– Dependencies Identified

– Relationships Identified

Working Groups

Component Leadership In-Place and Roadmap Underway

First Two Corporate Partnerships

- Unicon (⚑)
    – Shibboleth
    – Grouper
- Spherical Cow Group (⚑)
    – COmanage

⚑ **Complete**
⚑ **Pending**

Meaningful Impacts

Milestone	Impact
Communities of Interest	Form working groups quickly
Financial Tracking and Reporting	Report out on cash flow and project spend to the community
MOU Management	Bring in seed funding to support early stages of the program
Community Forum	Enable community input, discussion and decision making
Technical Requirements Revision	Finalize for TIER developers. Enable best coherent first release.
Working Groups	Develop key specifications per community requirements.

Sponsors of the Work

Community responsible for Higher-Education standards

Internet2 responsible for industry approaches

Currently convened under Internet2 (rather than TCIC) …

… but with connections to both and InCommon

TIER Working Group Structure

Optimized Approach*:

- Several Key working groups will be composed of Appointed Community Participants (Rather than having an "Open Call")

- Rationale: Expeditious movement using smaller, focused Teams

- Open / Published
  - Charter / Chair / Participants
  - Forum
  - Summaries
  - Feedback and Vetting (Includes International Review)

* Note that Community Adoption Working Group WILL be conducted as an "Open Call"

Community Working Groups "*Group A*"

Data Structures and APIs (Keith Hazelton)	Participate in working groups related to exploration of Data Structures and APIs commonly supported, implemented and exchanged between ALL TIER and TIER-Related Components.
Packaging and Containerization (Jim Jokl)	Participate in working groups related to exploration of Packaging and Containerization practices and procedures commonly supported and implemented in ALL TIER Components.
Security & Audit	Participate in working groups related to exploration of Security practices and procedures commonly supported and implemented in ALL TIER Components. (INCLUDES "3M" INSTRUMENTATION AND REPORTING)
User Acceptance	Participate in working groups related to exploration of User Acceptance practices and procedures commonly supported and implemented in ALL TIER Components. (INCLUDES TEST AUTOMATION AND USABILITY)

Community Working Groups "*Group B*"

Accessibility	Participate in working groups related to exploration of Accessibility practices and procedures commonly supported and implemented in ALL TIER Components.
Defect & Vulnerability Management	Participate in working groups related to exploration of Defect Management practices and procedures commonly supported and implemented in ALL TIER Components.
Document Management	Participate in working groups related to exploration of Document Management technologies, practices and procedures commonly supported and implemented in ALL TIER Components. (SHOULD THIS BE BOARDING GROUP "A"?)
Internationalization (I18N)	Participate in working groups related to exploration of Internationalization practices and procedures commonly supported and implemented in ALL TIER Components.
Partnerships and Third-Party Engagement	Participate in working groups related to exploration of Partnerships and Third-Party Engagement practices and procedures commonly supported and implemented in ALL TIER Components.
User Interface / User Experience	Participate in working groups related to exploration of User Interface / User Experiences practices and procedures commonly supported and implemented in ALL TIER Components.

"3M" Working Group Needed?

Instrumentation: Monitoring, Measuring, Managing

- – Continuous, Meaningful feedback on how the community is utilizing the components - Everywhere

Tune-In: tier-discussion@internet2.edu

Community Adoption Working Group Needed?

Community Adopter Coordination:

- Process Management

- Early Adopter Management

- Case Studies (Success/Failure Criteria Measurement) {Continuous Improvement}

- Training Required

Tune-In: tier-discussion@internet2.edu

Emerging Community Contribution

Soon Calling For:

Subject Matter Experts

Topic Owners

- Community Forum
- Mailing Lists (1st Responders)

Tune-In: tier-discussion@internet2.edu

Emerging Community Contribution

- Documentation {Authoring}, {Tagging}, {Writing} …

- Automated Test Cases

- CI (Continuous Integration)

Tune-In: tier-discussion@internet2.edu

Tune-In: tier-architecture@internet2.edu

Emerging Community Contribution

Software Specialties

- Logging and Instrumentation: Error/ Messages/Stats

- Analytics: Making "server-exhaust" More Useful

Tune-In: tier-architecture@internet2.edu

International Community Contribution

Software Opportunities and Realities

- Federation Operations Management
  - Shared Features
  - Shared Architectures and Data Structures
- Federation Interoperation: eduGAIN

Tune-In: tier-architecture@internet2.edu

Work in Progress

Launching the Program: Ad Hoc Architecture Strategy Group

Pulled requirements for the TIER Community Investor Council to prioritize

Tightened up the requirements once prioritized so they could be given to working groups

Spinning up the first working groups

Helping to define the TIER process and who does what

Launching the Program: Ad Hoc Architecture Strategy Group

Tom Barton	University of Chicago
Paul Caskey	Internet2
Jacob Farmer	Indiana University
Keith Hazelton	University of Wisconsin-Madison
Jim Jokl	University of Virginia
Ken Klingenstein	Internet2
Nate Klingenstein	Internet2
Nick Roy	Internet2

TIER Prioritized Requirements
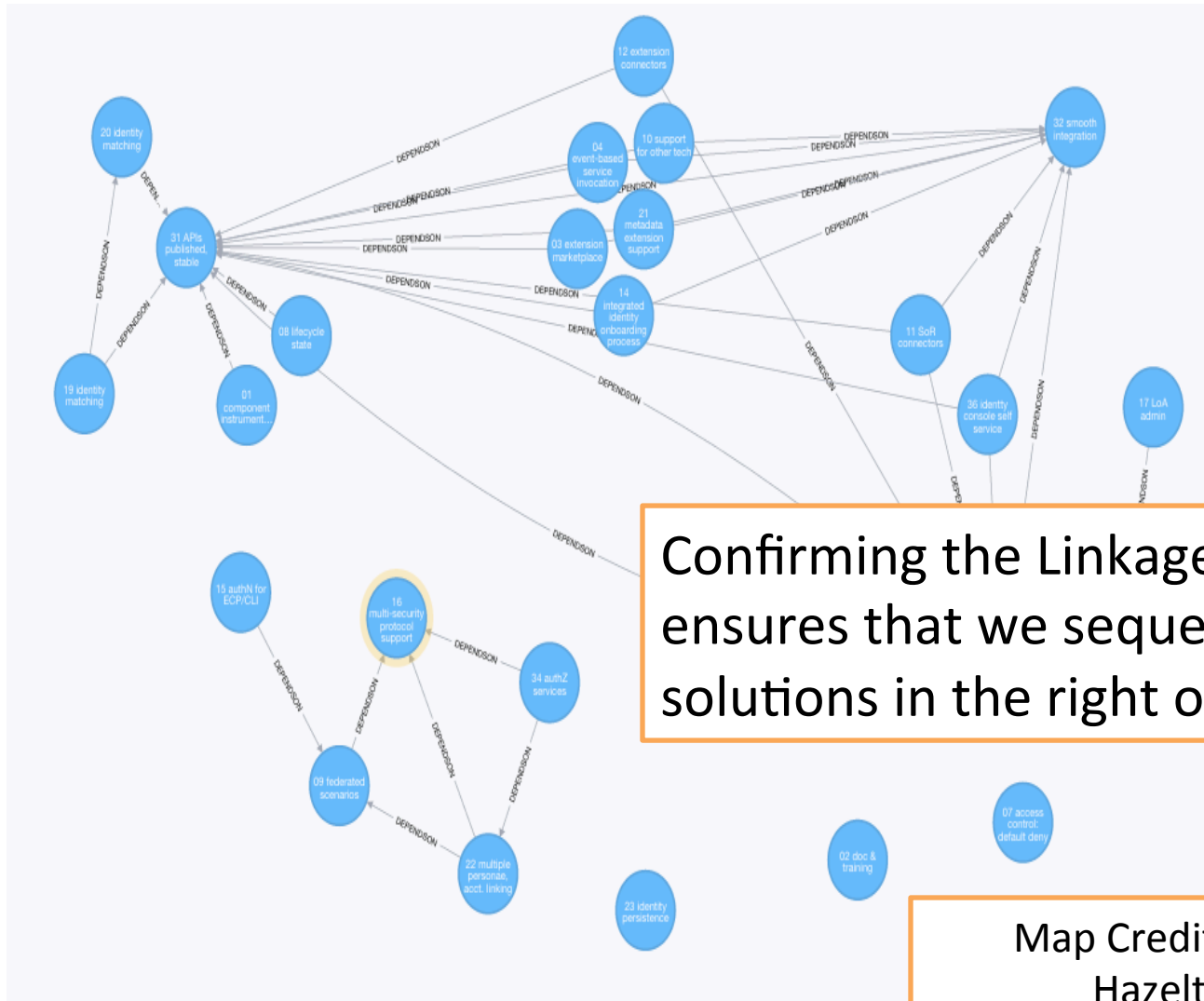
Requirements (Prioritized)
- https://internet2.box.com/ TIERInvestorReview
- Remember these?
- How do we bring these to a specification against which we can build?

All background materials:
- https://internet2.box.com/ TIERInvestorBackgroundDocs

Requirements Dependency Analysis

Confirming the Linkages ensures that we sequence solutions in the right order....

Map Credit: Keith Hazelton

TIER Component Architects

Scott Cantor	Shibboleth
Chris Hyzer	Grouper
Benn Oshrin*	COmanage
Ken Klingenstein	Scalable Consent
Nate Klingenstein	Community Identity Provider and Person Registry
Keith Hazelton	APIs and Data Structures
Jim Jokl	Packaging and Containerization
Nick Roy	Federation Manager

* Commercial partner

Staffing Progress and Priorities (First Wave)

1. Existing Contracts / Assignments (Renewed)
2. Grouper Dev Replacement (Done)
3. Sr. Technical Project Manager (Under Contract)
4. UI/UX Technology Lead (Recruiting)
5. UI/Front End Developer (Recruiting)
6. DEV/QA and Packaging Engineer (Recruiting)
7. Campus "Enablement" (Defining)
8. Information Architect (Next)

Campus Preparation

Release 1 is Important

It establishes…

- New and current baseline for all products
- Foundation for future (incremental) updates and enhancements
  - 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)
  - API: forward compatibility; abstracted plug-in point for commercial partner integration; framework for further inter-campus collaboration by establishing common points for provisioning and deprovisioning
  - Participate in shared-adoption cohorts

More Ways to Prepare:

- Upgrade to the current version of Grouper

- Upgrade to Shibboleth Identity Provider 3.x

- Familiarize yourself with ~~CIFER~~ ≥ TIER-API Framework
  – TIER Components will have public interfaces on these APIs and their successors

- Track the InCommon Federation Interoperability Group
  – Will impact your local systems

Help Us Improve and Grow

Thank you for participating in today's session.

We're very interested in your feedback. Please take a minute to fill out the session evaluation found within the conference mobile app, or the online agenda.

Thank You!

EDUCAUSE
ANNUAL CONFERENCE 2015

Trust and Identity in Education and Research: Identity for Everyone

Ron Kraemer, Notre Dame • Kevin Morooney, Penn State • Ann West, Internet2 • Steve Zoppi, Internet2