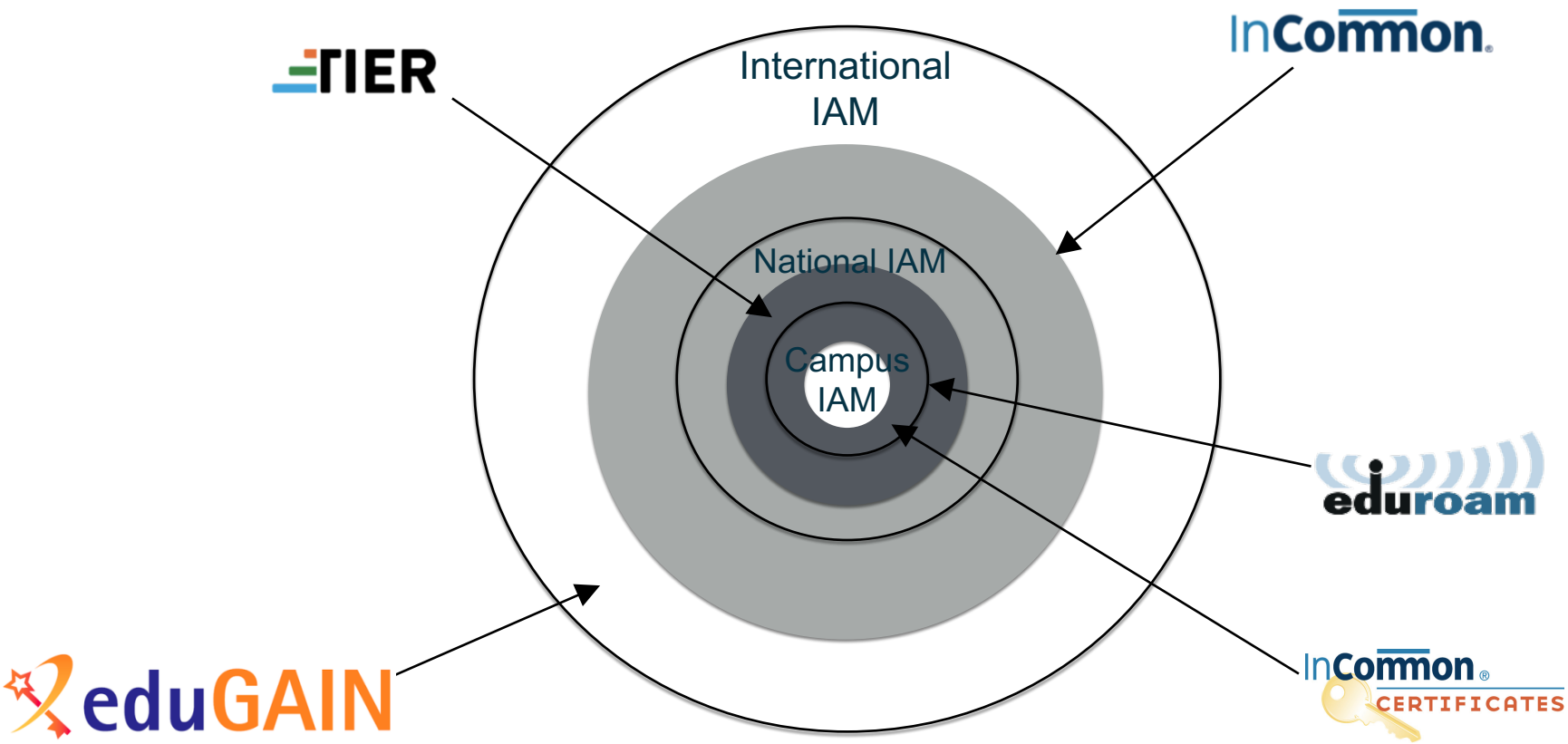
Trust and Identity Update – Westnet CIOs, January 2017

PRESENTED BY: Kevin M. Morooney, Vice President Trust and Identity Services

The Trust and Identity portfolio

- InCommon trust federation
- InCommon Certificate Service
- eduroam
- TIER

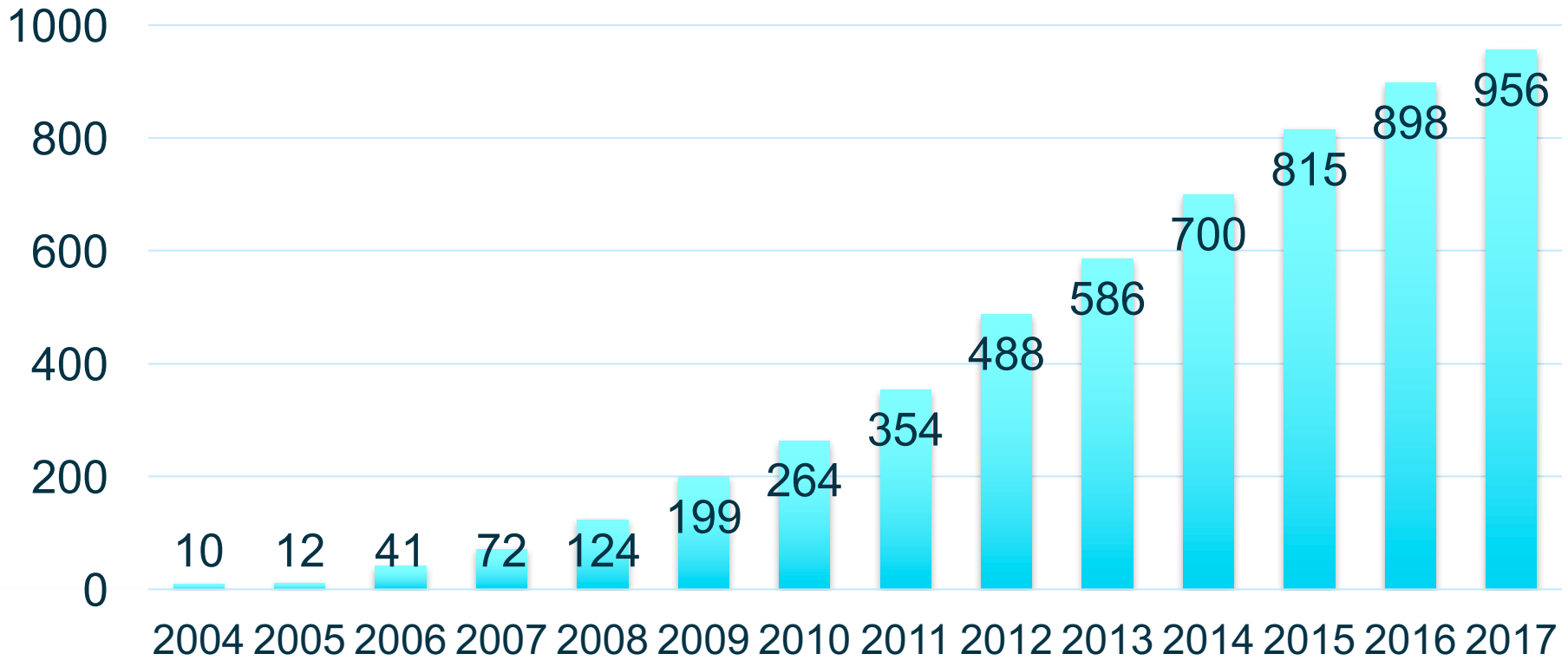
But first, an important framing…


TIER
InCommon
International IAM
National IAM
Campus IAM
eduroam
eduGAIN
InCommon CERTIFICATES

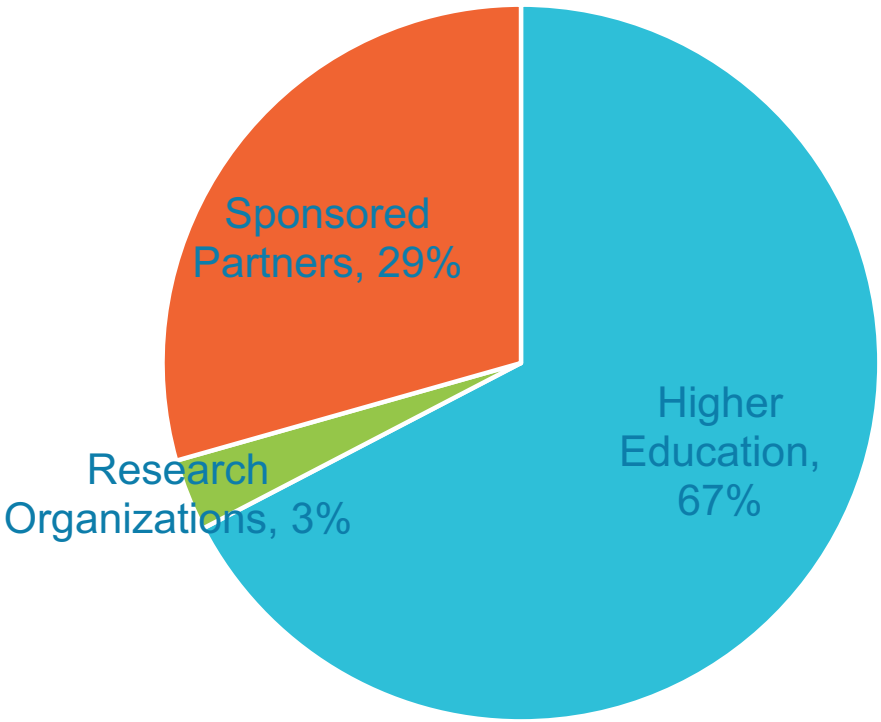
InCommon trust federation

- Demographics
- Hot topics

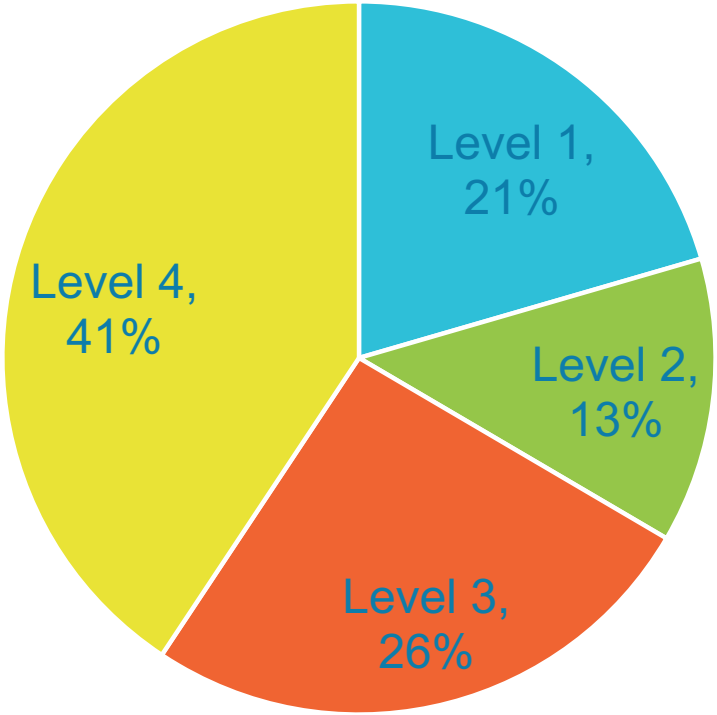
InCommon Participants Year-by-Year



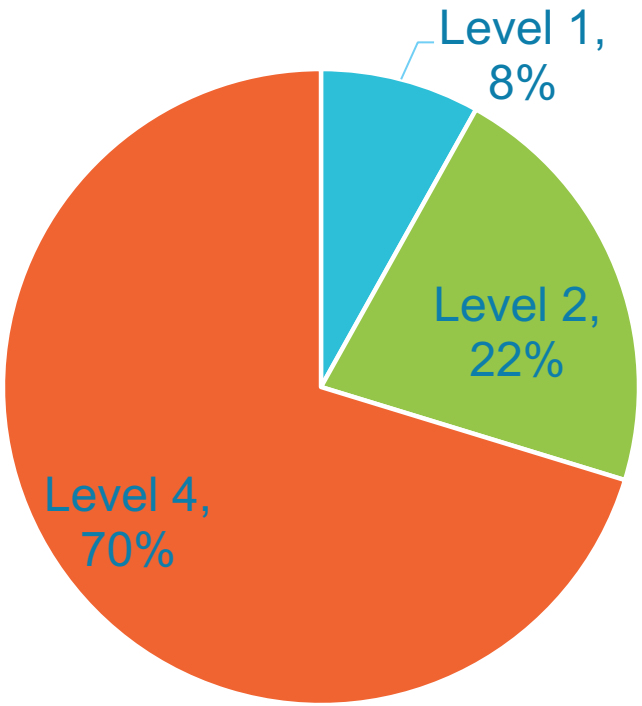
InCommon Participants by type



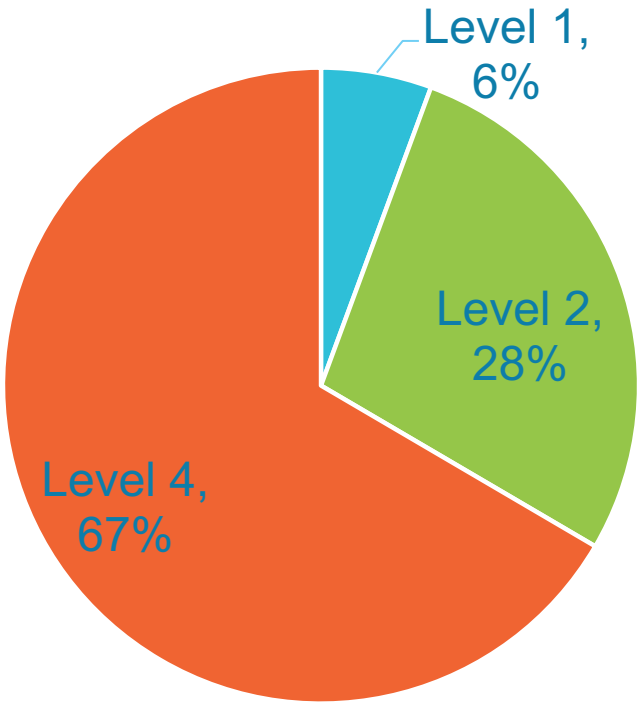
Higher Education Participants by Fee Level (Size of Institution)



Sponsored Partner Participants by Fee Level (Size of Organization)



Research Organization Participants by Fee Level (Size of Organization)



InCommon trust federation – hot topics

- Baseline Expectations
- Operational scaling and security
- Stewards Program
- Shibboleth IdPv3 vs IdPv2 upgrades
- NSF CC* Solicitation

InCommon trust federation – hot topics

- SIRTFI is in production – Security Incident Response Trust Framework for Federated Identity (https://refeds.org/sirtfi, https://spaces.internet2.edu/display/InCFederation/Asserting+SIRTFI)
- edugain, REFEDs
- Shibboleth Consortium
- Active InCommon working groups
    - OIDC-OAuth Deployment Working Group
    - Streamlining SP Onboarding Working Group
    - Attributes for Collaboration and Federation Working Group
    - Deployment Profile Working Group

InCommon Certificate Service

- There are currently 422 subscribers for the service
- Service portal now support federated access via InCommon **and MFA**
- The TIER version of the Shib IdP supports configuration for MFA support
- Backend provider is under new management and we've had meetings with new leadership and are positive about the future

eduroam

- There are 560 US subscribers to the service

eduroam

Eduroam – hot topics

- For the last 9 months, we have been moving the service from ad-hoc to fully managed
- Of the 560 subscribers, only 40 are left to go through the transition

TIER

- Background
  - 49 campuses and their CIOs funded a three year program called TIER
  - Each campus contributed $25K/year for three years
  - The TIER contributions will be exhausted by approximately the end of 2018. Internet2's on going commitment for software engineering/middleware development will continue, as will the Shibboleth Consortium
  - The 49 investor schools convened their CIOs and their lead IAM architects to develop hundreds of use cases that were distilled into a handful of priorities
  - The core components are Shibboleth, Grouper, CoManage, and now Midpoint (entity registry)
  - TIER is of, for and by the community – driven by working groups

TIER Working Groups

TIER Working Group	Chair/Contact	Chartered by	Status	Meeting Date/Time
TIER Data Structures and APIs Working Group	Keith Hazelton, University of Wisconsin-Madison	TIER Ad Hoc Advisory Group. (Accountable to CACTI, as of July 2017)	Active	Weds. 3 pm ET Fri, 10 am ET
TIER Packaging Working Group	Jim Jokl, University of Virginia	TIER Ad Hoc Advisory Group. (Accountable to CACTI, as of July 2017)	Active	Mon., 4 pm ET
TIER Security and Audit Working Group	*Group is currently inactive, with security for TIER components being handled by individual working groups*	TIER Ad Hoc Advisory Group. (Accountable to CACTI, as of July 2017)	Inactive. Wiki has restricted access. • Charter • Work Priorities	*N/A*
TIER Entity Registry Working Group	Warren Curry, University of Florida and Benn Oshrin, Spherical Cow Group	TIER Ad Hoc Advisory Group. (Accountable to CACTI, as of July 2017)	Active	Weds. 3 pm ET Fri, 10 am ET
Big Ten Academic Alliance (BTAA) and TIER Collaboration on Provisioning and De-Provisioning	Keith Wessel, University of Illinois	Big Ten Academic Alliance CIOs	Active	
Grouper Deployment Guide Working Group (this group met as part of the TIER Data Structures and APIs Working Group)	Bill Thompson, Lafayette College	TIER Ad Hoc Advisory Group	Complete see TIER Grouper Deployment Guide	

TIER – working groups, continued

TIER Community Investor Council	Chair	Status
TIER Community Investor Council Charter (TCIC)	Klara Jelinkova, Rice University	Active through end of 2018 or decommissioned

TIER Advisory Group (retired)	Chair	Status
TIER Ad Hoc Advisory Group (charter)	Tom Barton, University of Chicago	Complete, replaced by CACTI in June 2017

TIER Technology Leadership	Chair/Contact	Chartered by	Status
TIER Component Architects Group	Steve Zoppi, Internet2	Charter under development as of June 2017, to be chartered by CACTI	Active

TIER – hot topics

- The attention of the working groups is to finalize packages for the *four* components (Shibboleth, Grouper, CoManage, Midpoint)
- Moving from Architecture to Reference Implementations to match the most common use cases
- Soon to offer a TIER-powered CoManage capability from Internet2
- Implementation of the TIER Campus Success Program
- With the emerging importance of Consent – should it become part of the sustainable activities in Internet2? (You're going to love Ken's material)

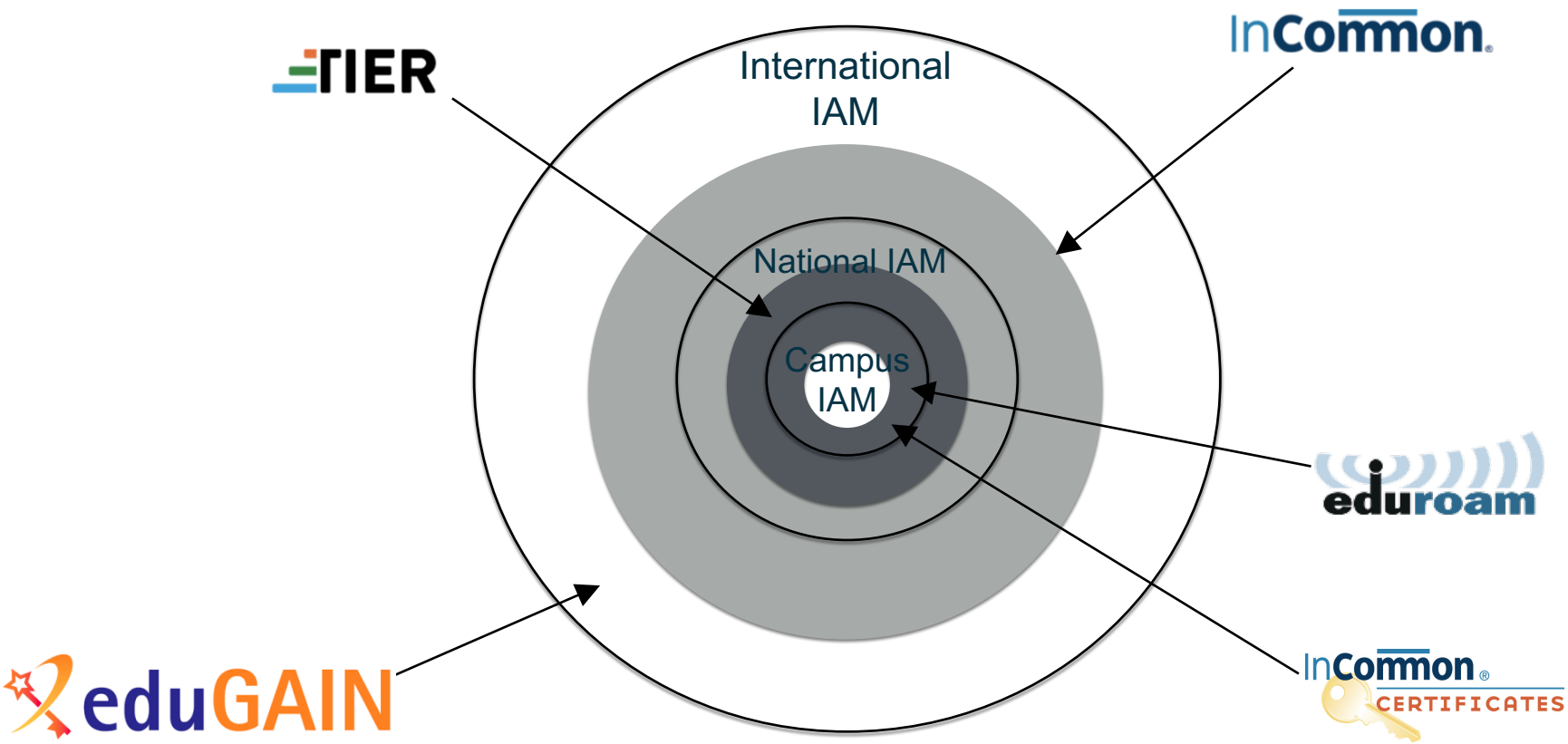
TIER Campus Success Program

- The TIER Community Investor Council approved the allocation of funds to develop a kick-start program for adoption – The TIER Campus Success Program
- Participating institutions

  Colorado School of Mines
  Colorado State University
  Georgia Tech
  Lafayette College
  Oregon State University
  Rice University
  University of California, Merced
  University of Illinois Urbana-Champaign
  University of Maryland Baltimore County
  University of Michigan

TIER Campus Success Program, continued

- Bi-weekly calls are held for all participants and with Internet2 staff. Subject matter experts from the working groups and community are brought in to do tutorials.
- Participants are required to do regular blogging about their TIER adoption experiences
- Participants will become knowledgeable evangelists for how to best migrate to TIER packaged components
- Expect to see status updates at the Internet2 Global Summit meeting May 6-9 in San Diego

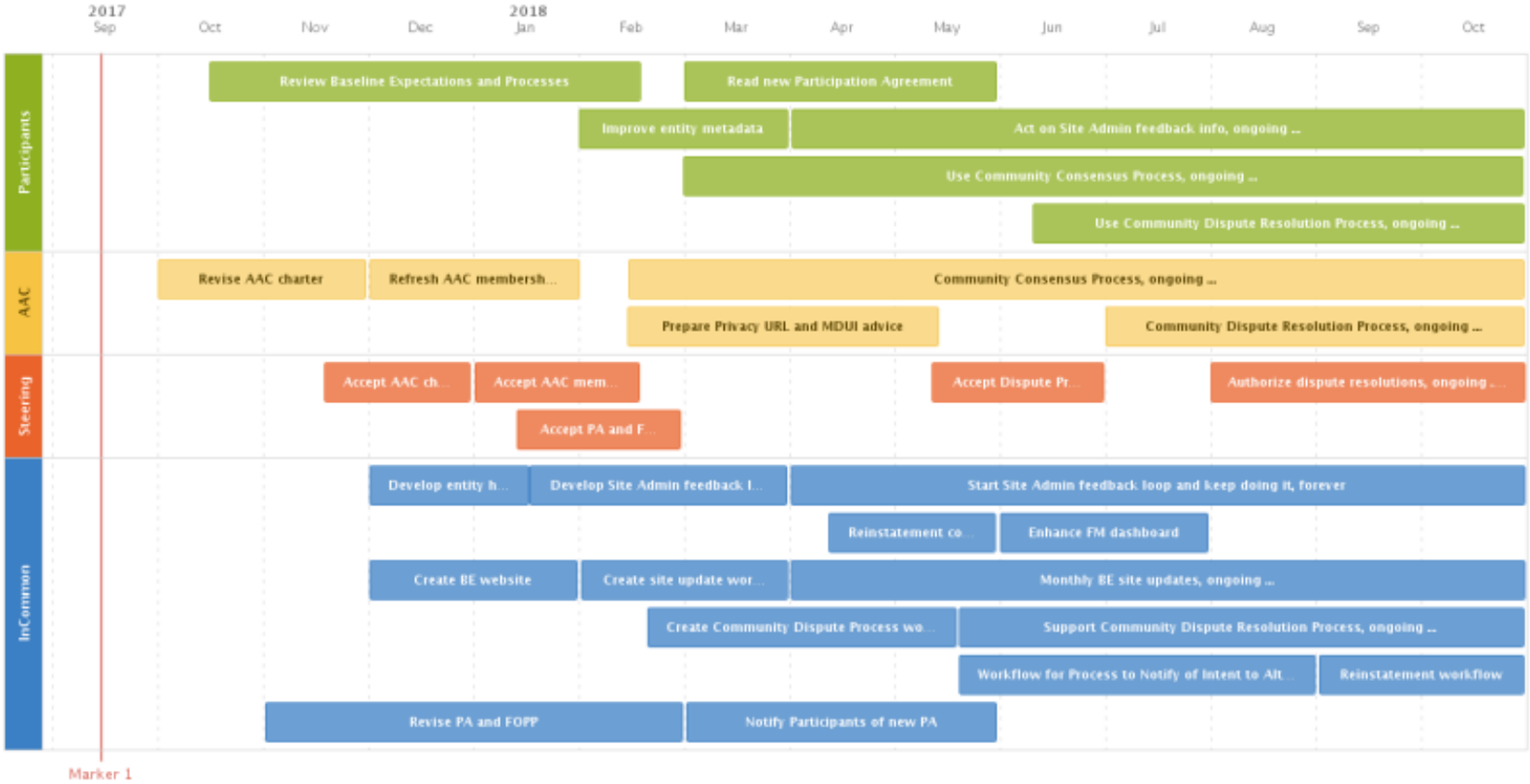

TIER
InCommon
International IAM
National IAM
Campus IAM
eduroam
eduGAIN
InCommon CERTIFICATES

Trust and Identity – a takeaway list

- Follow and adopt the changes arising from the InCommon Baseline Expectations Program
- Implement SIRTFI for your campus
- Follow the learning from the TIER Campus Success Program and make plans to move to TIER-enabled core components

Questions?

Appendix


2017
Sep
Oct
Nov
Dec
2018
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Participants
Review Baseline Expectations and Processes
Read new Participation Agreement
Improve entity metadata
Act on Site Admin feedback info, ongoing ...
Use Community Consensus Process, ongoing ...
Use Community Dispute Resolution Process, ongoing ...
AAC
Revise AAC charter
Refresh AAC membersh...
Community Consensus Process, ongoing ...
Prepare Privacy URL and MDUI advice
Community Dispute Resolution Process, ongoing ...
Steering
Accept AAC ch...
Accept AAC mem...
Accept Dispute Pr...
Authorize dispute resolutions, ongoing ...
Accept PA and F...
InCommon
Develop entity h...
Develop Site Admin feedback l...
Start Site Admin feedback loop and keep doing it, forever
Reinstatement co...
Enhance FM dashboard
Create BE website
Create site update wor...
Monthly BE site updates, ongoing ...
Create Community Dispute Process wo...
Support Community Dispute Resolution Process, ongoing ...
Workflow for Process to Notify of Intent to Alt...
Reinstatement workflow
Revise PA and FOPP
Notify Participants of new PA
Marker 1

Asserting SIRTFI

Created by Shannon Roddy, last modified by Dean Woodbeck on Jan 05, 2018

Self-Asserting of SIRTFI now available
As of the 3.2 release of the Federation Manager, sites can now self-assert SIRTFI compliance. Go to the REFEDS website for more information, including the complete SIRTFI spec.

What is SIRTFI?

The Security Incident Response Trust Framework for Federated Identity (SIRTFI) is an international standard to enable the coordination of incident response across federated organizations. The standard was developed by the international federation operators organization REFEDS and is documented at https://refeds.org/sirtfi.

SIRTFI provides a framework for effective incident response collaboration among federation and interfederation participants. One compromised account can create a security problem for a multitude of services across the interfederation community. When an organization complies with the SIRTFI framework, it agrees to participate in a federated incident response process. SIRTFI stipulates high-level practices and procedures, and identifies organizations that are capable of participating in a federated incident handling process. Federation participants that comply with SIRTFI are marked in the federation's metadata, raising the bar for operational security across federations.

What does it mean to be compliant with SIRTFI?

REFEDS, an organization of federation operators and participants from around the world, has published the SIRTFI framework, which specifies a set of assertions that comprises SIRTFI compliance. The assertions are divided into four areas: operational security, incident response, traceability, and participant responsibilities. Details are available on the REFEDS website (PDF). An organization agrees to abide by these assertions, which is demonstrated by the relevant Identity Provider or Service Provider metadata carrying the SIRTFI assurance entity attribute, and updating its security contact with the new REFEDS security contact type.

To self-assert compliance for an existing IdP or SP:

Log into the Federation Manager as a site admin.