THE CASE FOR TIER

Federated Identity is an essential asset and infrastructure for higher education. Relative maturity of Identity and Access Management (IAM) on campuses can roughly be categorized as: Emerging; Established and Advanced (as outlined herein). The fundamental objectives of TIER are to provide a common framework for campus IAM components whose adoption enables campuses to increase their IAM maturity while also supporting the means by which higher-order goals can be achieved, including: (1) a consistent approach to IAM that advances inter-institutional research; (2) a shift to managing *attributes* rather than *identities*, in recognition that future students will have well-established identities that they wish to maintain; and (3) interoperable IT service models that integrate distributed IT services both in terms of delivery method—on premises and in the cloud—and location—campus-based and globally users.

Today, there is extensive use of the ten-year-old InCommon federation across colleges and universities, cross institutional research collaborations and sponsored service providers. Institutions of all sizes rely heavily upon community developed on-premise IAM software components such as single-sign-on authentication (AuthN) software – Shibboleth – and authorization (AuthZ) framework - Grouper. These open source software components are principally the result of one-time grants combined with matching community-contributed staff. Though effective the community-contributed development model lacks a routine, ongoing financial commitment and a sustained development plan. Incremental development has also complicated deployment and administration. Although commercial enterprise identity solutions are emerging, to-date most continue to be designed for centrally-controlled, inward-facing enterprises and lack the support for our diverse, individually-focused open community.

The rapid adoption of cloud services, combined with the significant increase in multi-campus research and pedagogical initiatives, requires both the scale and sustainability of our community efforts and identity environments be re-engineered. We need a coordinated approach to enable *Trust and Identity in Education and Research* at scale for thousands of institutions and service providers while also satisfying diverse local use cases.

To achieve the objectives detailed below, a coordinated effort needs to build on and extend current investments, enhance them to simplify their deployment, and package the solution to achieve the goals of broader adoption and increasing IAM maturity. Wherever possible the effort will follow the principle of integrating existing best of breed solutions together into a more comprehensive set of component solutions that will satisfy a range of needs; from those with limited technical resources to institutions of significant complexity.

The result will be a properly integrated set of components in a solution designed to be deployed both on premise (at a campus site) in concert with enriched services delivered from a community cloud. This will enable all participants to be better prepared to provide and access services both on and off-campus.

Risks of the community not undertaking this effort far outweigh those of the project itself. The complexity of integrating cloud-based and on-premises services will not be reduced by inaction. Additionally, the use of commercial identities are being actively promoted by their owners (e.g. Facebook, Google, Baidu). As they become more prevalent within degree granting programs, it is likely to result in considerable (perhaps permanent) erosion of privacy for those individuals while presenting an overall degradation in the Academy relationships with their constituents.

CAMPUS AND RESEARCH FOCUSED OBJECTIVES

The following objectives were considered in developing the straw man road map:

1. Simplify/Enable broader adoption and deployment of campus IAM solutions, including ongoing upgrade and maintenance
2. Provide cloud-based options which extend the features of the campus set of IAM solutions beyond what can be accomplished on-premises alone
3. Establish IAM solution and campus IAM extensions for researchers as a new, Hybrid IAM service between the on-premises and cloud offerings
4. Expand IAM capabilities by blending commercial offerings (services and tools), community solutions and partnerships wherever practical
5. Synchronize software and feature release cycles across the IAM components
6. Continue research & development of novel IAM solutions to unmet use cases

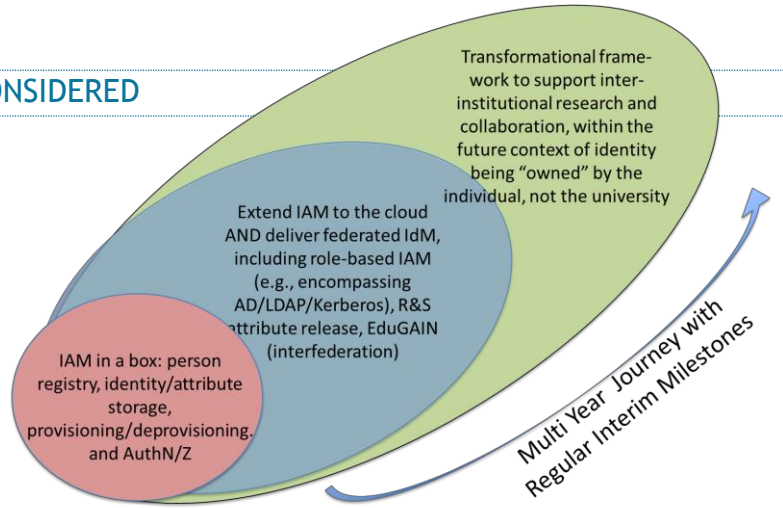
Based on the straw man road map the following specific deliverables were articulated by the TIER charter group:

1. Develop an "IAM-in-a-box" solution for colleges and universities comprised of core identity components including person registry, identity and attribute storage, and account lifecycle procedures, and AuthN/Z capabilities
2. Extend IAM to the cloud, delivering federated IdM and role-based IAM for services such as AD/LDAP/Kerberos
3. Improve R&S attribute release and EduGain interfederation
4. Begin transformational effort to support inter-institutional research and collaboration, understanding that future identities are "owned" by individuals, not institutions.

MATURITY MODEL CONSIDERED

The TIER charter team developed the following maturity model as a straightforward way of thinking about the broad continuum of institutional IAM capabilities, and consequently of the range of needs that remain to be met across higher education. It strongly informs the straw man roadmap of deliverables below.

Please refer to *Appendix A* below for a deeper dive into this model. **Emerging ➲ Established ➲ Advanced** Continuum.



GENERAL ASSUMPTIONS

Subject to Further Refinement: The roadmap of deliverables below is a straw man outline of a realistic sequence of releases that achieve the objective set forth above. When funded, detailed design and analysis phases will result in the final determination of components, partners and participants. In planning, the following assumptions have been made:

- **Funding Levels** will ultimately drive scope and timing
- **Current Contributions** of talent (and future volunteer efforts) will continue as they have in previous years, including existing Internet2 investment of approximately $900K/year

STRAW MAN ROADMAP

	Campus IAM	Cloud-Enhanced Campus IAM	Research Connector	Professional Services
Ultimate Goals	Provide integrated and installable IAM solution that meets the common needs of higher education (aka "IAM in a box")	Provide cloud-deployed options that enhance Campus IAM capabilities to accelerate adoption and interaction of IAM capabilities for campuses	Partner with the national and international research programs and connectors to ensure appropriate integration and support for their distinctive solutions	Ensure availability of professional services, support, and training, and facilitate sharing of community contributed solutions
Release Target	**Campus IAM**	**Cloud-Enhanced Campus IAM**	**Research Connector**	**Professional Services**
Year 1 / Month 8 +Minimum Product	Basic "IAM in a box" components to establish or extend a fundamental implementation • Extend existing AuthN service with federated Single Sign-On (SSO) • R&S Category support • Non-browser SAML support for command line interface (CLI) and grids • Group Management and Group Based Access Controls • Two Factor AuthN	Foundational Design Work	Promote consistent release of R&S attributes. Further deliverables TBD. For example, may include developing partnerships for Research Connector through Globus Nexus (See Appendix for "Globus Nexus In Brief") or others if needs/interests align *(E.g., constructing agreements with potential partners such as LIGO, iPlant, CTSI, Argonne & UChicago Computation Institute, etc. about potential solution and developer support)*	Create training and self-study materials for deliverables in this release Develop community contributions framework. Business development with commercial affiliates

Release Target	Campus IAM	Cloud-Enhanced Campus IAM	Research Connector	Professional Services
Year 2 / Month 16 +Bug Fixes +New Features	Installable IAM components that promote expansion of campus SSO, extending reach of access management, and increasing IAM maturity • Links to user self-service credential management from SSO Login Page • Self-service integration of campus services and applications to SSO Introduction of a Person Registry designed specifically for Higher Ed, Version 1 • Optional integrated LDAP directory • Integrated message bus technology for provisioning • Integrated with previously delivered IAM components	Federated Single Sign-On (SSO) with pass-thru to campus authentication service Services provided in this initial release include • R&S Category support • Non-browser SAML support for CLI and grids • Two Factor Authentication Campus Management UI Version 1 • Define campus interface • Select desired functionality	Based on receptivity of and guidance from research partners, add Cloud Enhanced Campus IAM platform as credential provider to Research Connector	Preliminary "Community Contributions" Library: • Provide essential, most popular connectors for provisioning targets and System of Record integrations Likely Milestones: • First contributed System of Record connectors released • First contributed provisioning connectors for popular cloud services Continue to enrich and enhance training and self-study materials for deliverables in this release
Year 2 / Month 24 +Bug Fixes +New Features	Person Registry Version 2 • Initial System of Record connectors • Identity Matching • User Self-Service UI • Identity Proofing support User Managed Attribute Release • Extension to shibboleth	Services provided in this release include • Access management • Social and Scholarly IDs • Invitation-based access to campus resources Campus Management UI enhancements	Integrate Grouper-based access management with Research Connector *(Expectation of funding by NSF grant)*	Promote and maintain library of community contributions. Additional Two-Factor Authentication provider connectors for services. *(Continue to Enrich and Enhance Training and Self-Study materials for deliverables in this release.)*

Release Target	Campus IAM	Cloud-Enhanced Campus IAM	Research Connector	Professional Services
Year 3 / Month 30 +Bug Fixes +New Features	Person Registry Version 3 • Invitation Service • Enhanced and/or additional connectors	User Managed Attribute Release Campus Management UI enhancements	*(**Research** Connector continues to benefit from continued integration of Globus Nexus with research computing infrastructure)*	Professional Services and support expanded in line with offerings
Year 3 / Month 36 +Bug Fixes +New Feature	Enhancements and Maintenance • Groundwork for Identity Lifecycle Management	Enhancements and Maintenance		Professional Services and support expanded in line with offerings

RESOURCING

Resources	Campus IAM	Cloud-Enhanced Campus IAM	Research Connector	Professional Services
	Internet2 Existing Resource Commitment $900K / year			
	Community Contributed Resource Need (Minimum) $1,440K / year			
Shared	6 Software Engineers		1 Coordinator / Program Manager	
Aligned	+½ Tech Writer +1 Lead +1 QA	+½ Tech Writer +1 Lead +1 QA	N/A	N/A
	Total Minimum Project Investment Internet2 + Community Contribution: **$2,340K / year * 3 years = $7,020K**			

APPENDIX A: IAM MATURITY MODEL CHARACTERISTICS / OTHER NOTES

The TIER charter team developed the following maturity model as a straightforward way of thinking about the broad spectrum of institutional IAM capabilities, and consequently of the range of needs that remain to be met across higher education.

EMERGING

Campus with emerging or less mature "IDM Program"

Characteristics

Recognizes value of I2 and InCommon services and participation

Lacks resources or ability to implement independently

Campus IdM not able or minimally able, to be leveraged for research

Solution Must Address (Descending Priority Order)

Simplified Deployment of current technology components

- Includes Authentication
- Includes Authorization
- Includes Group Management
- Includes Central Person Registry
- Includes identity/attribute storage

ESTABLISHED

Campus with IDM Team that has delivered Shibboleth/Grouper Functionality

Characteristics

Mature campus IDM operations are sustainable

IdM Infrastructure would benefit from systematic non-Web-Only SSO (or "command-line SSO") group-based|role-based IAM

Campus IdM in support of research via federation services

Campus IAM may benefit by leveraging standard components over locally developed systems

Solution Must Address

Enables IAM Components to be Cloud-Deployed in support of Federated IdM

- Standard pluggable components
- Support for other AuthN components such as AD/LDAP/Kerberos
- Inclusion of group-based|role-based AuthZ frameworks that extend to AD, LDAP and other components
- Supports R&S mandatory attribute release
- Supports EduGAIN

ADVANCED

Research Institution with advanced IDM team and inter-institutional collaboration needs

Characteristics

Researchers have urgent need to conduct research across two or more institutions (whether an I2 member or not)

Researchers have a need to identify using a consistent, single set of credentials

Researchers, Students, Faculty and Staff have a need to engage commercial service providers using a consistent, single set of credentials in multiple roles

Researchers have a need to work across collaborative units (Groups) within a variety of projects (Virtual Organization) and serve in different capacities (Roles = Groups) within those projects

Solution Must Address

Transformational framework to support pan-institutional research and collaboration

The need for Individuals to, within the future context of identity and an appropriate trust framework, have control of their own personas and credentials (AuthN). The individual, in this new context would own his/her credentials, not the University or Institution

The University or Institution would always retain control of Institution-Owned Resources (AuthZ)

GLOBUS NEXUS "IN BRIEF"

Globus Nexus is a flexible and powerful Platform-as-a-Service to which developers can outsource identity, group, and profile management needs. By providing these frequently important but always challenging capabilities as a service, accessible over the network, Globus Nexus streamlines web application development and makes it easy for individuals, teams, and institutions to create collaborative web applications such as science gateways for the science community.

Globus Nexus allows developers of science gateways to outsource identity, profile, and group management functions to a third party platform, Globus Nexus, which the University of Chicago operates for the research community. This platform addresses four major obstacles to the creation and operation of high-quality collaborative applications:

1. **Identity provisioning**: Create and manage identities for gateway users.
2. **Identity hub**: Link different user identities, so that for example a user can authenticate to a gateway with a campus (InCommon) credential.
3. **Group hub**: User-managed group creation and management functions. Groups can then be used in authorization decisions.
4. **Profile management**: User-managed profile attributes and visibility for those attributes. Profile attributes can be used in authorization decisions, for example to determine who is allowed to join a group.

SUMMARY RESOURCE ASSUMPTIONS

1. No assertions/assumptions were made regarding:
    a. the location or sourcing of these engineers and contributors
    b. the location or levels of resource investment
2. Existing investment and development plans are anticipated to continue on current trajectory by the current teams of part-time resources until augmented by and redefined under TIER charter. Internet2 will continue to maintain its existing $900K/yr investment throughout
3. Industry Standard Productivity ratio 60% (60% productive coding / 40% administrative support work)
4. External Resource Loaded average Rate $105,000-$120,000 per engineer (the latter is used for calculations)
5. Minimum Staffing As Defined: 12 Full-Time Equivalents in addition to current contribution levels
    a. Expected minimum investment based on 12 FTE per year at $120K = $1.4M per year (Three-year proposal)
    b. Greater precision in labor estimates can only be defined upon detailed design and creation of work breakdown structures
6. Needed community investment of $4.2M over the three year effort will be provided by direct campus funding and where possible, augmented by Grant funding. Once deployed, sustainability will be achieved by subscription to cloud components of TIER (beyond InCommon participation) which will be both a component of TIER and continue as a separate service.