TIER WOrkshops

Thematic Groupings

## The Core of Solution functionality:

The workshops explored some of the core functionality that the TIER program must address. While these are expressions of the solution in the highest functional aggregation, they do not fully describe the depth of the program’s scope. For example, ALL aspects of facilitating the operation of the federation itself must be taken into consideration during the construction of the solution and supporting components. Therefore we have also included groups which specifically address the **Campus Success** criteria either implied by or specifically called for within the user stories and workshop contexts.

Table of Contents

[The Core of Solution functionality: 1](#_Toc416963108)

[Solution Themes 2](#_Toc416963109)

[Community Documentation and Interaction 2](#_Toc416963110)

[De/Provisioning 2](#_Toc416963111)

[Federation and Inter-Federation 2](#_Toc416963112)

[Interoperability 2](#_Toc416963113)

[Levels of Assurance (LoA)/MFA (Quality of Identity and Identification) 3](#_Toc416963114)

[Person Registry/Personae/Individuals 3](#_Toc416963115)

[Standards and Enforcement 3](#_Toc416963116)

[Research Organization Support 3](#_Toc416963117)

[Service Providers and Third-Parties 4](#_Toc416963118)

[User Interface/User Experience (UI/UX) 4](#_Toc416963119)

[Engagement and Campus Success 5](#_Toc416963120)

[Contexts 5](#_Toc416963121)

[Campus Success Components 5](#_Toc416963122)

[Governance 5](#_Toc416963123)

[RFC 2119 Conventions 7](#_Toc416963124)

[Summary Document Authors/Contributors 10](#_Toc416963125)

## Solution Themes

* Auditing Monitoring and Management
* Logging and all other forms of application Instrumentation for Policy and Performance monitoring and management **must** be rigorously implemented within all components of the solution.

### Community Documentation and Interaction

* Solution **must** enable the sharing of a common documentation repository as well as a place for school practitioners and service providers to go to find useful instructions, standards, practices and guidelines for building end-to-end services based on TIER components and default configurations.
* Solution extensions **must** be available in the form of a Marketplace or some other suitable means of presenting a catalog of available functionality, contributed by the community, for utilization by others.

### De/Provisioning

* Events (such as admission, enrollment, new hire, etc.) **must** trigger lifecycle stage transitions, role changes, affiliation changes, etc. Those can then cause other events such as service eligibility. Lifecycle changes or affiliations all precipitate a need for provisioning wherein roles are mapped to services / entitlements.
* The solution **must** support high level workflows between states.
* The solution **must** anticipate the possibility of conflicting roles in the case of multiple personae
* The solutions **may** take into consideration the most COMMON decision making rules and the most RESTRICTIVE decision making should be at the institutional control. Default is DENY then rules-based addition of eligibility to access a service or an object.
* The solutions **must** enable individuals to have multiple roles/affiliations/relationships/whatever with the institution, each with its own lifecycle and overlapping set of access privileges needed to undertake each role. Statefulness (persistence and preservation of state) must permeate the design goals of all solution components in order to correctly and efficiently manage their access over the course of these multiple lifecycles.

### Federation and Inter-Federation

* Inter-Federation and Federation needs **must** be held high in considerations when building core solutions and artifacts related to TIER.

### Interoperability

* The Solution **should** provide “other technology” interfaces to facilitate operation with non-NET+ solutions (campus ERP, non-NET+ vendors, etc.). (e.g., OAuth, SCIM, etc.).
* Pre-built connectors for the most common of systems of record **should** be in the “core” TIER release.
* A mechanism to augment the catalog of Core Connectors **must** be provided to the community for inter-institutional sharing and implementation.
* An extensible Publish/Subscribe mechanism **must** be supported to enable near-real-time communication between dependent systems of record.
* CommonAPP like Integration process **should** be devised for identity creation, etc. IdP (CommIT) integration not specifically mentioned but is also a clear need.
* Non-Web-based authentication **must** be enabled as for Research/Collaborative computing.
* The solution must enable smooth runtime integration / mapping between SAML and OpenID/OAuth Protected services

### Levels of Assurance (LoA)/MFA (Quality of Identity and Identification)

* The ability to promote and demote the Levels of Assurance of an identity over time **should** be implemented in the component suite. For example, having a higher Levels of Assurance while student, then lower (social?) when alumni, and later yet higher again as grad student or employee.
* Flexible Multi-Factor Authentication in Single-Signon **should** be enabled by default, with the ability to require Multi-Factor Authentication per-Service Provider and/or per-Individual

### Person Registry/Personae/Individuals

* De-Duplication **must** be a part of the Person Registry Service (Directory)
* Identity Matching Logic **must** be a part of the Person Registry Service (Directory)
* Institutionally Defined Metadata must be enabled in the Cloud-Based solution as well as the on-Premise solution.
* Individuals **must** be able to support the association of various personae with their own identity. (Account Linking must also be a part of this functionality.)
* Once instantiated, the persistence of an identity **must** extend beyond a lifetime (forever).
* The person registry service **must** have a minimum threshold of assurance when linking an account.
* The person registry service **must** provide the ability to present a selected set or subset of attributes to a selected set of systems.
* The solution **may** enable user to be in control of their personal data stores such that when relying parties are requesting access to those data, users should have fine-grained controls over what pieces of personal data are shared with such parties.

### Standards and Enforcement

* The program **must** assert and enforce:
  + Datagram Standards
  + Policy Standards
  + Terminology Standards
  + Persistence (storage of data) standards
  + Published / Stable APIs for ALL core components.
* Implementation, Integration with and Adoption of Community or Commercial Services which have adopted TIER program standards **should** be “trivial” to implement from a school’s perspective as long as the school has implemented TIER and used the TIER default settings.

### Research Organization Support

* COManage **must** be included in the solution as a proper starting administration point for Research Organizations (Virtual Organizations)
* Authorization infrastructure **must** be constructed (or made available) that can be consumed by applications across both internal and external identities and services.

### Service Providers and Third-Parties

* The program and related solutions **must** enable the service owners of federation-facing campus services to directly manage the controls and access by external identities such that service owners won't need campus federation gurus to manage their services.

### User Interface/User Experience (UI/UX)

* An end user Identity Console **must** be instantiated with the ability to update centrally owned attributes (e.g., names, numbers, some addresses, preferences, etc.) and be confident that the data will be reliably propagated to relying party systems (e.g., ERPs, directories, etc.).
* User Interfaces **must** be created to ease the installation, implementation, administration and use of the most common tasks for all components. (e.g. the Lack of a User Interface should be a “fail” criterion for any critical feature or function.)
* Password Reset capabilities **must** be standardized upon and deployed in the out of the box solutions, with sufficient flexibility to meet institutional business practices.
* A Person **may** have multiple personas that an organization may require them to “act in the role of”, An easy way of switching personas should be constructed as a part of the final solution.
* “Constituent focused,” self-service Interfaces **must** be included in the final solutions that dynamically and simply expresses what each constituent is authorized to manage about their own or others’ attributes and access privileges. Key such constituencies: administrators supporting on-boarding processes, unit and group managers/leads, managing access to their groups’ resources, service owners managing characteristics of federation access to their services, and individuals managing their credentials and privacy of their attributes.

## Engagement and Campus Success

### Contexts

* Audiences for Engagement inside campuses
  + Campus leadership
  + Registrars
  + Research
  + Other business partners internal to the institutions
  + Academic Medical Centers
  + VPs of Research
* Audiences for Program Stakeholders
  + Smaller schools
  + Corporate Support Vendors
  + Corporate Service Provider
  + XSEDE, NSF, DoEd, Federal Agencies
  + Broad education including K12
  + State Department of Instruction
  + Campus Stakeholder national organizations (AACRAO, NACUBO, etc)

### Campus Success Components

#### Basic Communications

* One-pager for general stakeholders (elevator speech)
* One-pager targeted for identified stakeholders
* Glossary

#### Community Engagement

* Enable community to work together on items of mutual interest (cohorts)
* Require CIO/IAM architects to work together to more fully understand the landscape of implementation
* Enable the sharing of current practices and success among participating campuses
* Publish timeline of events, opportunities and major milestones

### program Governance

* Provide mechanisms for gathering ideas and suggestions from the broader community
* Provide mechanisms for gathering ideas and suggestions from the Investors
* Publish open source policy statement
* Publish governance model and method for participating in decision process

#### Adoption Assistance

* Develop IAM Assessment Model
  + Develop a complete IAM assessment tool, one comprehensive model that covers broad IAM topics.
  + Develop lightweight Assessment tool for each release, targeting the features supported for that functional set
  + Assessment Delivery Method
    - PDF document
    - Online form with automatic tally
    - Consultant service for on-site assessment
* Develop guidance for addressing gaps identified in IAM Assessment Model
  + Develop overall guidance for broad IAM
  + Develop specific guidance for each release
* Readiness Education
  + Workshop
  + Webinar
* Deployment practice recommendations
* Support models
  + Provide corporate consulting model
  + Provide peer/cohort model

## RFC 2119 Conventions

Network Working Group S. Bradner

Request for Comments: 2119 Harvard University

BCP: 14 March 1997

Category: Best Current Practice

Key words for use in RFCs to Indicate Requirement Levels

Status of this Memo

This document specifies an Internet Best Current Practices for the

Internet Community, and requests discussion and suggestions for

improvements. Distribution of this memo is unlimited.

Abstract

In many standards track documents several words are used to signify

the requirements in the specification. These words are often

capitalized. This document defines these words as they should be

interpreted in IETF documents. Authors who follow these guidelines

should incorporate this phrase near the beginning of their document:

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL

NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and

"OPTIONAL" in this document are to be interpreted as described in

RFC 2119.

Note that the force of these words is modified by the requirement

level of the document in which they are used.

1. MUST This word, or the terms "REQUIRED" or "SHALL", mean that the

definition is an absolute requirement of the specification.

2. MUST NOT This phrase, or the phrase "SHALL NOT", mean that the

definition is an absolute prohibition of the specification.

3. SHOULD This word, or the adjective "RECOMMENDED", mean that there

may exist valid reasons in particular circumstances to ignore a

particular item, but the full implications must be understood and

carefully weighed before choosing a different course.

4. SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that

there may exist valid reasons in particular circumstances when the

particular behavior is acceptable or even useful, but the full

implications should be understood and the case carefully weighed

before implementing any behavior described with this label.

Bradner Best Current Practice [Page 1]

RFC 2119 RFC Key Words March 1997

5. MAY This word, or the adjective "OPTIONAL", mean that an item is

truly optional. One vendor may choose to include the item because a

particular marketplace requires it or because the vendor feels that

it enhances the product while another vendor may omit the same item.

An implementation which does not include a particular option MUST be

prepared to interoperate with another implementation which does

include the option, though perhaps with reduced functionality. In the

same vein an implementation which does include a particular option

MUST be prepared to interoperate with another implementation which

does not include the option (except, of course, for the feature the

option provides.)

6. Guidance in the use of these Imperatives

Imperatives of the type defined in this memo must be used with care

and sparingly. In particular, they MUST only be used where it is

actually required for interoperation or to limit behavior which has

potential for causing harm (e.g., limiting retransmisssions) For

example, they must not be used to try to impose a particular method

on implementors where the method is not required for

interoperability.

7. Security Considerations

These terms are frequently used to specify behavior with security

implications. The effects on security of not implementing a MUST or

SHOULD, or doing something the specification says MUST NOT or SHOULD

NOT be done may be very subtle. Document authors should take the time

to elaborate the security implications of not following

recommendations or requirements as most implementors will not have

had the benefit of the experience and discussion that produced the

specification.

8. Acknowledgments

The definitions of these terms are an amalgam of definitions taken

from a number of RFCs. In addition, suggestions have been

incorporated from a number of people including Robert Ullmann, Thomas

Narten, Neal McBurnett, and Robert Elz.

Bradner Best Current Practice [Page 2]

RFC 2119 RFC Key Words March 1997

9. Author's Address

Scott Bradner

Harvard University

1350 Mass. Ave.

Cambridge, MA 02138

phone - +1 617 495 3864

email - [sob@harvard.edu](mailto:sob@harvard.edu)

## Summary Document Authors/Contributors

Tom Barton [tbarton@uchicago.edu](mailto:tbarton@uchicago.edu)

Keith Hazelton [keith.hazelton@wisc.edu](mailto:keith.hazelton@wisc.edu)

Farmer, Jacob [jpfarmer@iu.edu](mailto:jpfarmer@iu.edu)

James A. Jokl [jaj@virginia.edu](mailto:jaj@virginia.edu)

Nate Klingenstein [ndk@internet2.edu](mailto:ndk@internet2.edu)

Ken Klingenstein [kjk@internet2.edu](mailto:kjk@internet2.edu)

Ann West [awest@internet2.edu](mailto:awest@internet2.edu)

Shelton Waggener [swaggener@internet2.edu](mailto:swaggener@internet2.edu)

Steven Zoppi [szoppi@internet2.edu](mailto:szoppi@internet2.edu)