Trust and Identity in Research and Education (TIER)
Community Collaboration for the Next Decade
Tuesday, May 17th, 2016 3:00PM CT
Indiana/Iowa Meeting Rooms (6th Floor)

Jim Jokl (University of Virginia), Chair of the TIER Packaging Working Group
Keith Hazelton (University of Wisconsin-Madison), Chair of the TIER API and Data Structures Working Group
Kevin Morooney (Internet2), Vice President Trust and Identity
Ann West (Internet2), Associate Vice President Trust and Identity
Steve Zoppi (Internet2), Associate Vice President, Services Integration and Architecture
Introduction

Ann West
Foundation Principles

- Sustain
- Integrate
- Enhance
- Extend
Release One: Overview

Ann West
Steve Zoppi
General Principles

• Leverage Existing Work Wherever Possible
• Narrow The Toolsets
• Utilize Virtual Machine Images and Containers
• Fortify the Federation’s Operation
General Principles

- Support Campus and Software Engineering “Best Practices”
  - Abstract Provided Components
  - Define Stable Interfaces for Campuses
- Provide Firm Foundation for Future Development
Groundwork

- Amazon Web Services (Deployment Target)
- Community Forum (Vanilla Forums)
- Contact Management Systems (SalesForce)
- Defect and Feature Tracking Systems (JIRA)
- Financial and Accounting Systems
- Mail List Managers (Sympa / 21 lists and community groups)
Groundwork

- Project Management  (Web Portal/Web2Project)
- Service Management  (ServiceNow)
- Source Management  (GitHub - Enterprise)
- Support Databases and Reporting Systems  (Various)
- Document Management  (Confluence)
- Packaging and Container Generation  (Packer and Docker)
Contents of Release One

• Single Sign-On and Federating Software
  Shibboleth (Identity Provider Version 3.2.1)
• Enterprise Access Management, Authorization and Provisioning System
  Grouper (Version 2.3)

• Entity Registry (Person and Thing)
  COmanage Registry (Version 1.0.3)
• APIs to enable extension and flexibility
• MACE-Dir eduPerson (Version 201602, released March 9, 2016)
Contents of Release One

• First Look Containers and Virtual Machine Images
  COmanage Registry 1.0.2 (VM/Container), Grouper 2.2 (Container), Shibboleth idP 3.2.1 (Coming)

• InCommon Federation
  - InCommon Multifactor Authentication Profile (Draft)
  - InCommon SAML V2.0 Implementation Profile for Federation Interoperability 20160303
  - InCommon Global Interfederation Integration (In production February 15, 2016)
Release Details – TIER Package Delivery

- Instructions and obtaining VMs
  - [https://spaces.internet2.edu/display/TPD](https://spaces.internet2.edu/display/TPD)

- Release Document
  - **PDF** (22 pages)
    - Introduction and background re: TIER
    - Arriving at Release One
    - Contents of the release
    - Next steps
Feedback

• Survey concerning Release One: https://goo.gl/t8VNVH

• TIER website
  ▪ https://www.internet2.edu/vision-initiatives/initiatives/trust-identity-education-research

• Questions and comments page
  ▪ https://www.internet2.edu/vision-initiatives/initiatives/trust-identity-education-research/tier-comments/
Packaging: Ease of Installation and Operation

Jim Jokl
TIER Packaging: Mission

- Develop packaging specifications and recommendations
- What should be done to make TIER components
  - Simple to deploy
  - Easy to operate
  - Less difficult to maintain
- Deliver to TIER staff for use in implementation and long-term maintenance of TIER software components.
TIER Packaging: Goals

• Identify common component needs and pain points
• Focus especially on sites impeded by current packaging
  ▪ Example: Shibboleth ease of use with InCommon

• Simplify, streamline per-site configuration
  ▪ Administrative tools, scripts, GUIs,
  ▪ Define appropriate out-of-the-box component configurations
TIER Packaging: Goals

• Component packaging solutions
  ▪ What can work well for the Shibboleth, Grouper, and COmanage
  ▪ Position TIER for the future
    • Additional components
    • Meet our ease of installation, configuration, operation, and upgrade goals
Process: Two Parallel Streams

- Discover enhancement opportunities
  - Survey to find
    - Pain points and needs
    - Computing environment: current & future
  - Results
    - ~80 questions
    - Responses from ~60 institutions

- Packaging technical opportunities
  - Preconfiguration / enhancement of existing installers
  - Virtual machines
  - Containers
Highlighted Survey Results

Impediments to Software Adoption

https://spaces.internet2.edu/display/TPWG/Survey+Results
Highlighted Survey Results

Packaging Preferences

1. Local installation using existing packaging solution
2. Local installation from pre-configured containers (Docker, etc)
3. A preconfigured VM/appliance that you run and maintain locally (“local” virtual appliance)
4. A virtual appliance managed remotely
5. A cloud-based virtual infrastructure (IaaS)
6. A managed cloud-based service (SaaS)
7. Other

https://spaces.internet2.edu/display/TPWG/Survey+Results
Highlighted Survey Results

Campus use of Docker containers

https://spaces.internet2.edu/display/TPWG/Survey+Results
Highlighted Survey Results

1. Load and use InCommon metadata,
2. Include support for a default set of attribute definitions (LDAP - name, email; eduPerson - EPPN, ...)
3. Release EPPN, name, email, affiliation, eduPersonTargetedId to all InCommon SPs? (TIER to provide ...)
4. Release EPPN, name, email, affiliation, eduPersonTargetedId to SPs with the Research and Scholars ...
5. Respect a FERPA opt-out attribute to restrict attribute release for some users.
6. Avoid spurious errors in the logs from external scanners via a properly configured robots.txt
7. Support Enhanced Client or Proxy (ECP) by default? 8. Support multi-factor authentication by default?
9. Automatically reload config files when they are changed (relying-party.xml, attribute-filter.xml, ...)
10. Support CAS by default? 11. Support OpenID Connect by default (when available)?
15. Update itself automatically - security updates only? 16. Prompt users to consent to attribute release?

https://spaces.internet2.edu/display/TPWG/Survey+Results
Packaging Strategy

• Component teams retain traditional installers
  ▪ These will continue to be needed well into the future

• Provide additional release types for the components
  ▪ Docker containers
  ▪ Virtual machine images to run the containers

• Focus on automation tools
  ▪ Build containers and VMs
  ▪ Automate testing
  ▪ Over time, goal of weekly builds
  ▪ Identify and deploy tooling that is able to deliver multiple formats
  ▪ Keep pace as technology changes
Release One: New Packaging Status

- First Look Components
  - Initial analysis by workgroup
  - Ability to focus on usability goals once group has something real to touch
  - Open to community to test and watch progress
  - Access: https://spaces.internet2.edu/display/TPD

- Container and Virtual Machine Image First Look Status
  - COmanage Registry 1.0.2 (VM and Container)
  - Grouper 2.2 (Container)
  - Shibboleth IdP 3.2.1 (VM)

- Testbed environment
  - Available for use with testing/evaluation
  - Use likely to expand over time
Lessons Learned

• The community can accomplish a lot
  ▪ 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
Next Phase Objectives

• 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
Data Structures, APIs and Campus Autonomy

Keith Hazelton
API Shorthand

• In TIER-speak, ‘API’ is firstly shorthand for REST-ful APIs, but also for other protocols and language-specific SDKs

• A partial list of existing interface and integration approaches that TIER already leverages or will have to support going forward

<table>
<thead>
<tr>
<th>Shorthand</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>SAML 2</td>
</tr>
<tr>
<td>Oauth 2</td>
<td>UMA</td>
</tr>
<tr>
<td>ID Match</td>
<td>OpenID Connect</td>
</tr>
<tr>
<td>SCIM 2</td>
<td>VOOT 2</td>
</tr>
<tr>
<td>AMQP</td>
<td>ORCID</td>
</tr>
<tr>
<td>SQL</td>
<td>SNMP</td>
</tr>
</tbody>
</table>
Data Structures  (aka Resource Representations, aka Schema)

- Canonical representations of entities (People, Groups, Course Rosters,...)
- Should be meaningful across IT systems and vertical domains
- In REST terminology these are Resource Representations
- Same resources are referenced in APIs and event-driven messaging patterns
- TIER guideline: APIs and messages should share common resource representations
The Foundations of TIER Infrastructure

- RESTful APIs are the primary interfaces between TIER IAM Components and between TIER Components and External Systems
- TIER-defined Resources are shared and manipulated by RESTful APIs
- The API first approach is a key element supporting campus autonomy
  - If you want to keep your identity registry, just expose its functionality as implementations of TIER APIs, it will then plug and play with other TIER components
  - Supports selective adoption of TIER components and hybrid infrastructure models
Consequential Early Choices

- Swagger 2 as the Primary TIER API Tool
  - Used for both Design and documentation of APIs
  - The language in which TIER APIs will be formally specified
- SCIM 2 as the anchor point for TIER API Style
  - New IETF standard (RFCs 7642, 7643 and 7644)
  - Provisioning and de-provisioning are the design center for SCIM, and a high priority for potential TIER adopters
  - It doesn’t cover all IAM functional needs, so TIER will end up defining new APIs: IdMatch is a good example
  - A potential common language for higher education and commercial SaaS
swagger: '2.0'
schemes:
  - http
  - https
host: tierapi.getsandbox.com
basePath: /tier/v2
info:
  contact:
    email: tier-api@internet2.edu
    name: TIER API Working Group
    url: 'https://spaces.internet2.edu/display/DSAWG'
description: "Courtesy of Brian Savage of Boston College. The TIER APIs helps education and research organizations with Identity and Access Management (IAM) challenges. This API definition represents the first few group-related operations using SCIM-compliant responses including eduPerson extension (as provided by PennState at https://github.com/PennState/tier). (* Note that only the first operation or two can be interactively tested at this time. *)
title: Basic TIER User and Group API Operations in Swagger 2.0
version: 1.0.0
externalDocs:
  url: 'https://spaces.internet2.edu/display/DSAWG/
consumes:
  - application/json
produces:
  - application/json
tags:
  - description: Users representation operations
    name: Users
  - description: Groups representation operations
    name: Groups
paths:
  '/Users/[userId]':
    get:
      summary: Get full SCIM eduPerson extension User representation with all groups (form 1)
      description: Get full SCIM eduPerson extension User representation with all groups (form 1)
Basic TIER User and Group API Operations in Swagger 2.0

 Courtesy of Brian Savage of Boston College. The TIER APIs helps education and research organizations with Identity and Access Management (IAM) challenges. This API definition represents the first few group-related operations using SCIM-compliant responses including eduPerson extension (as provided by PennState at https://github.com/PennState/tier). (Note that only the first operation or two can be interactively tested at this time.)

Version 1.0.0

Contact information
TIER API Working Group

tier-api@Internet2.edu

https://spaces.internet2.edu/display/DSAWG

Terms of service
http://www.internet2.edu/policies/intellectual-property-framework/

Filter operations by a tag:

- Users
  - Users representation operations

- Groups
  - Groups representation operations

Paths

/Users/{userId}

GET /Users/{userId}
swagger: '2.0'
schemes:
  - http
  - https
host: tierapi.gets.com
basePath: /tier/v2
info:
  contact:
    email: tier-api
    name: TIER API
    url: 'https://site.tierapi.gets.com'
description: "Counts mapping helps education and Identity Management (IAM) challenges. This API definition represents..."
Lessons Learned

• The Data Structures and APIs WG, along with the Entity Registry WG, attracted talented people from higher education institutions across the land (well over 120 on the mailing lists)
• The WG members will show up, work hard together and deliver what the WG charters asked for (our meeting notes alone amount to nearly 200 pages)
Lessons Learned

• Institutions will share their experience, their documents and their code: Penn State just released their Apache 2-licensed SCIM server and client libraries, significantly accelerating the API work.
Lessons Learned

• Institutions with significant IAM projects underway have skin in the game and will make sure the Working Groups stay focused on essentials
Next Round of Milestones

- Backbone usage scenario 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
Questions and Answers

TIER Release One Team