TIER Timeline and Deliverables for TechEx 2017

Items labeled (A) must be delivered by TechEx 2017

Items labeled (B) are intended to be done by TechEx 2017, but the schedule may slip on some of them

S,M,L: Small, Medium, Large in terms of relative effort to complete

1) Shortcut to Planning Pages for the TechEx Demos

- Grouper Messaging Demo for TechEx 2017: Overview; Detailed planning doc (coordinators: EthanK, Chris Hyzer)
- Registry Messaging Demo for TechEx (coordinators: EthanK, KeithH)
- Provisioning (coordinator KeithH)
- Client/Service Registry (coordinator: JimF)
- Person data APIs (coordinators: GaborE, WarrenC, BennO)

See the Demo Planning pages for further details on specific TechEx demonstrations

2) Deliver APIs

1. (A, m) Definitive TIER API Guideline document; The excavation, sifting and winnowing are likely to be the labor intensive bits.
2. (B, s) Evaluate need for Grouper permission and policy management
3. (A, m) SoR/Registry/ODS/Groups (for TechEx needs; Ultimately it will end up being Large)
4. (A, s) Registry to Grouper: Registry is authoritative source of subjects (LDAP, JDBC, API later?)
5. (A, s) Provisioning (for demo purposes, based on UW-Madison Global Summit demo)
6. (A, s) Consent-informed Attribute Release (CAR)
    a. External API authored by Marlena
    b. Presentation to TIER-API prior to their review of the API
7. (B, m) Certificate API
    a. An API for server certificate management for use by InCommon (check with ChrisHubing and JimJ)
    b. JimJ would help with a facade for Comodo APIs

3) Define and implement an event-driven messaging approach

1. (A, l) Asynch architecture, to complement the more synchronous API-based approach
    a. Messaging model where we only send identifiers of changed objects (probably modest effort)
    Demo: Grouper changelog publishes events onto an AMQP message transport. What"s available now or soon (RabbitMQ, ActiveMQ); This can be demonstrated with 3.1.b
    b. [EthanK] A provisioning/de-provisioning message consumer (perhaps via midPoint) adds/removes people to an external system based on changes in group membership.
    c. [EthanK] **Demo**: “Human Resource” system puts HR events on a subscribable message queue; Message subscriber reflecting changes into Person Registry

4) Publish Guidelines and Recommendations on Security Models for API Authentication and Authorization

1. (A, m) Develop guidelines and recommendation in cooperation with InCommon TAC OIDC WG and REFEDs WG
2. (A, m) First version of Jim Fox's Client-Service Registry (as an advanced CAMP un-conference session)

5) Design, implement an Entity Registry

1. (A, s) Refine data model for minimal Registry (AI - Warren)
    a. Map minimal entity registry to midPoint schema (EthanK, WarrenC)
2. (A, s) SCIM - user
3. (A, m) Midpoint Install
    a. JimJ has packaged MidPoint and an integrated OpenLDAP into a container so we can implement Warren and Ben's work on the Thin Registry as a start
    b. Provisioning is a strength of Midpoint that we want to test out
    c. Perhaps use a Canvas connector for this.
    d. Implementation to support requirements for Provisioning in the WG
4. (A, m?) COmanage Install - support for 3; Minimal Registry implemented in COmanage
5. (Post TechEx) add support for non-person entities

6) Implement simple identity matching and related features

1. (B, s) Single package used by both midPoint and COmanage; testbed instance was running last fall; Implemented the draft API; Miami demo: COmanage worked with an agent that actually invoked the ID Match API;

7) Define Person Registry and ODS connection

1. (B, l) TIER HAS to do the API for identity data a la ODS. Longer run we'll need an implementation package for those APIs.
    1. when APIs are largely defined, consider polling/surveying community for viability with existing systems as input to determining whether or not TIER needs to go build something.
2. (B, s) **Demonstrate** Person data APIs (using the registry, ODS, group repository to populate the user SCIM schema. WarrenC has a master data project that we could use as a model ODS for demo;

8) Advance Grouper training and adoption

1. (A, m) Building a training course for Grouper, leveraging both the Grouper Deployment Guide and Bill Thompson and Chris Hyzer,
2. (B, m) Demonstrations of more advanced features at Tech Ex (adv camp unconference session proposal)

9) Implement Provisioning tools

1. demos
    a. (A, s) Provisioning from midPoint to Slack and/or LucidChart via their SCIM APIs
    b. (A, m) Canvas API connector(s) for midPoint and/or COmanage ; See 2.5
2. (B) See above 5.3 and 5.4

10) Take next steps in Documenting TIER Components

1. (B, m?) BennO - Consideration for COmanage Deployment Guide
    1. Not sure that the GDG approach is possible
    2. More likely to take form of screen shares and web cases
2. (B, m) Would like to offer either Grouper or COmanage as general tools for SP integration
    1. Enrich SAML-delivered attributes with COmanage identity information to make sure SP gets everything it needs(?)
    2. Related to provisioning, see 5.3, 5.4, JITime and JICase provisioning; IdP Proxy
3. (B, m) Drill down on the integration pipe in Tom's reference architecture diagram. Add detail, substructures; will provide a basis for the overall demo narrative flow we want to include. Keith will draft a "TIER Integration Architecture" document for WG review.