IAM Online

January 27, 2016 – 2 pm ET

Steve Carmody (Brown University), InCommon Technical Advisory Committee
Walter Hoehn (University of Memphis), Federation Interop WG
Chris Bongaarts (University of Minnesota), Certificate Service Review WG
C.W. Belcher (University of Texas - Austin), Workday WG
David Walker (Consultant), Multicontext Broker/MFA

Today's Agenda

1. InCommon Technical Advisory Committee (TAC) 2016 Priorities
2. Certificate Service Review Working Group Update
3. Federation Interoperability Working Group Draft Report
4. Workday Working Group Progress Report
5. Multi-Context Broker and Multifactor Authentication and Shib IdPv3

InCommon Technical Advisory Committee

InCommon Technical Advisory Committee (TAC)

The InCommon Technical Advisory Committee provides recommendations relating to the operation and management of InCommon with respect to technical issues.

TAC - Developing recommendations on strategies for the longer term.

InCommon Operations (Ops) - Delivers services and functionality.

TAC Minutes - https://spaces.internet2.edu/x/_QHkAg (InC-Collaborate wiki)

InCommon Working Groups Wiki: https://spaces.internet2.edu/x/poNRBQ

TAC 2015 Accomplishments

1. New TAC Charter

   http://www.incommon.org/docs/policies/TACcharter.html

2. New TAC membership process
3. Comments and involvement with REFEDS (international federation operators) consultations
   a. Metadata Registration Practice Statement
   b. Entity Category Consultation: Academia

TAC 2015 Accomplishments

3. Working Groups
    a. Metadata Distribution
    b. New Entities WG
    c. External Identities
    d. IdP of Last Resort
    e. Federation Interoperability
    f. Packaging for Ease of Deployment Working Group
    g. Standing OPS Group

TAC 2015 Accomplishments

4. Recommendations to Steering
    a. Attribute Release Recommendations
    b. 2015 Work Plan
5. New Categories
    a. Hide From Discovery Category
    b. Registered by InCommon Category

TAC 2015 Accomplishments

6. External Participation by TAC Members
    a. OTTO
    b. Federated Incident Response
    c. OIDC

TAC 2015 Accomplishments

7. Support for Ops
   a. Per-entity Metadata Pilot
   b. REFEDS R&S Migration Strategy
   c. Using Other Software
   d. MD-RPI Elements in Metadata
   e. Roadmap for Operationalizing eduGAIN
   f. Metadata for the InCommon Steward Model

Today's Important Issues and Priorities

What are today's important issues and priorities around which TAC could create new working groups?

Share your suggestions and thoughts in the chat.

At the end of the webinar, we'll do a quick poll to identify and prioritize.

Federation Interoperability

Working Group

Goals (Fed-Interop-WG)

- Provide creators of SAML products with a concrete set of requirements for interoperating within InCommon
- Provide direction for addressing the most common interoperability problems encountered by InCommon participants.
- Outline SP and IdP operational and deployment practices that are necessary for interoperability with minimal or no administrator involvement

Current Status (Fed-Interop-WG)

- Call for Participation - July 7, 2015
- Matrix - common interoperability problems
  - Categorized (Software vs. Deployment/Operational)
- SAML Software Implementation Specification
  - “SAML V2.0 Implementation Profile for Federation Interoperability”
  - Building on pre-existing, but informal, InCommon materials
  - Common Interoperability Issues Matrix
  - Kantara/eGov Profiles
  - Draft Completed: Under Public Review

Next Steps (Fed-Interop-WG)

- Solicit feedback within InCommon
- Engage other communities - REFEDS/Vendors/Shibboleth Developers/SimpleSAML.php Developers
- Review/Incorporate Feedback
- Submit Final Report to InCommon TAC
- Publish profile through Kantara Initiative
- Federation lab (GÉANT and Kantara) Test Suite
- Proposed follow-on work:
  - SAML2int
  - InCommon Deployment Profile

Certificate Service Review

Working Group

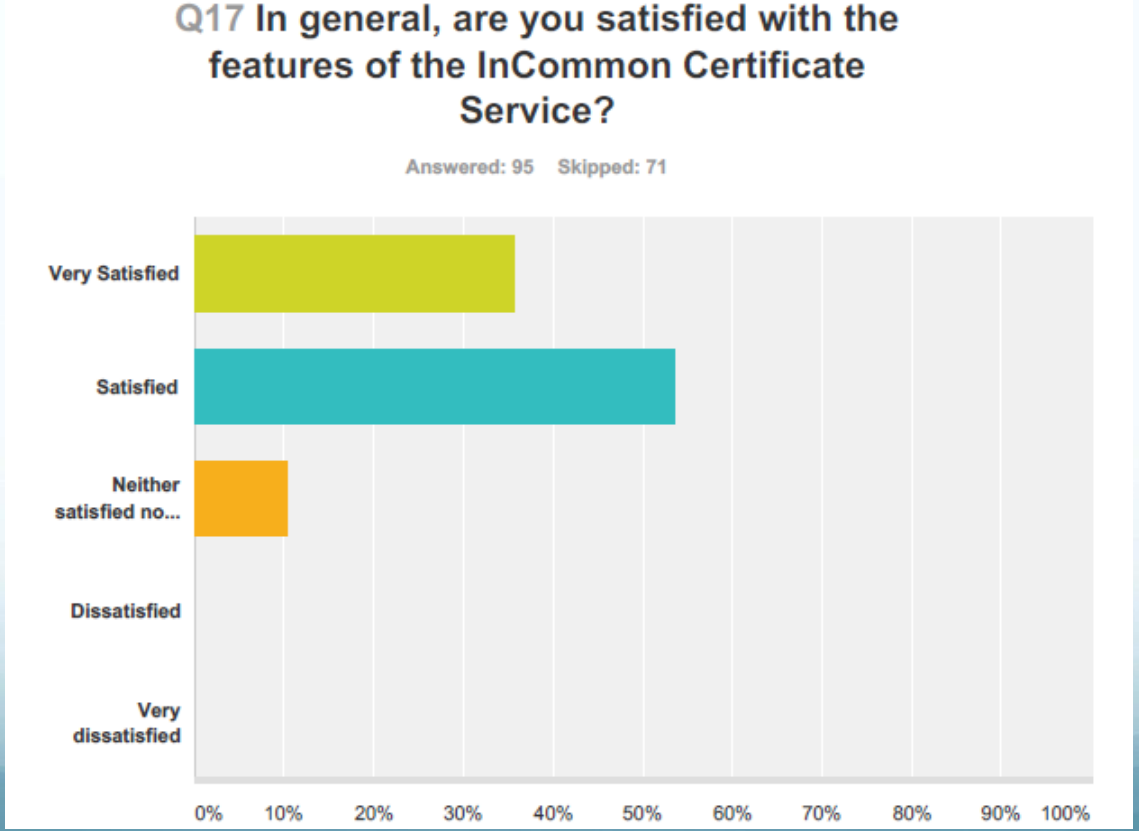
Goals (Certificate Service Review WG)

- Review & provide input for next gen Cert Service
  - Current contract with Comodo up for renewal this summer
  - Input will support negotiations or RFPs
- Address immediate change proposals
- Represent the voice of the community in directing the evolution of the Cert Service

Current Status (Certificate Service Review WG)

- New domain activation process reviewed (effective Feb. 1)
- Community Survey
  - Just closed; now reviewing, synthesizing, distilling
  - Good response rate - more than 160, mostly subscribers

Current Status (Certificate Service Review WG)



Next Steps (Certificate Service Review WG)

- Community survey analysis
  - Prioritize desired features
  - Gap analysis for existing service
- Review other short-term improvements
  - Private CA options
  - Federated access to Cert Manager

Workday

Working Group

Workday WG - Summer 2015

- Initial focus topic is multi-factor authentication
  - Specifically the need for step-up or “just-in-time” MFA for sensitive functions/groups
- Provided input on requirements to Workday:
  - Via brainstorm https://community.workday.com/idea/90665
  - Authentication design partner calls
  - Communication from individual campuses (at least UT Austin & NYU…)

Workday WG - Fall 2015

- Workday developed a design concept for authentication policy enhancement:
  - Enable configuration of specific functions / security groups to require step-up authentication
  - Step-up authentication provided provided within Workday (OTP via SMS or email)
- We requested that step-up authentication be handled via SAML (using a different authentication context) instead of within Workday
- With the help of a detailed SAML MFA for Workday proposal provided by NYU (thanks Gary Chapman and Scott Koranda!) Workday understands this need

Workday WG - Current State

- Workday is currently analyzing work required to support SAML-based step-up authentication
- They have asked UT Austin to help with a proof-of-concept over the next two weeks
- The next Workday authentication design partner call is February 11. Workday is supposed to indicate then whether SAML-based step-up authentication will make it into WD27

Federating Multifactor Authentication

The Multi-Context Broker and the MFA Interoperability Profile Working Group

Multi-Context Broker - History

- Multi-Context Broker (MCB)
  - Orchestrates among multiple authentication contexts to support MFA and assurance
  - Authentication methods and contexts are selected on the basis of SP requests, user certifications, and IdP configuration
  - Software plugin for IdPv2 released in February, 2014, based on requirements developed by CILogon, National Institutions of Health and the Department of Education, as well as input from the MFA Cohortium
  - IdPv3 released in late 2014

Multi-Context Broker - Current Status

- Educated by the MCB effort, IdPv3 has a native implementation of basic MCB functionality
- The MCB team has documented the MCB Model and provided recipes for configuring IdPv3 for MCB functionality in the context of that model
  - See Orchestrating Multiple Authentication Methods and Contexts - The Multi-Context Broker (MCB) on the Shibboleth wiki

The MFA Interoperability Profile Working Group

- The MCB coordinates among multiple authentication contexts, but the name and definition of each context must be known to both the IdP and the SP
  - The SAML-defined contexts tend not to address current use cases (*e.g.*, allow MFA to satisfy an SP's request for password)
- The MFA Interoperability Profile Working Group is addressing this issue
  - Creating a federation-wide name and definition for MFA
  - Chaired by Karen Herrington with support from David Walker
  - Currently rebooting the meeting schedule
  - https://spaces.internet2.edu/x/CY5HBQ

Poll – Issues and Priorities

IAM Online Evaluation

Please complete a short evaluation of today's presentation

https://www.surveymonkey.com/r/IAM_Online_Jan_2016

InCommon Shibboleth Installation Workshops

May 19 - 20, 2016 – University of Chicago

Details and registration at incommon.org/shibtraining

www.incommon.org/shibtraining