InCommon Technical Advisory Committee

Community Update - August 24, 2016

Steven Carmody, Brown University
Scott Koranda, LIGO
Keith Wessel, University of Illinois
Albert Wu, UCLA
Janemarie Duh, Lafayette College

Agenda

1. Welcome and introduction - Steven Carmody, Brown Univ., TAC Chair
2. Working Group Reports and Discussion
    a. Per-Entity Metadata Working Group - Scott Koranda, LIGO
    b. InCommon Deployment Profile WG - Keith Wessel, Univ. of Illinois
    c. OpenID Connect, OAuth2 - Albert Wu, UCLA
3. IdP Configuration Documentation for Popular SPs - Janemarie Duh, Lafayette College
4. TAC Membership - Steven Carmody
5. Quick Updates - Steven Carmody

InCommon Technical Advisory Committee (TAC)

The InCommon Technical Advisory Committee provides recommendations to InCommon Steering and InCommon Operations on technical issues relating to the operation and management of InCommon.

TAC - Developing recommendations on strategies for the longer term.

InCommon Operations (Ops) - Delivers services and functionality.

Minutes - biweekly TAC Conference Calls

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

TAC Process

- TAC does most of its work by convening Working Groups
  - TAC develops a charter, scopes the work, and sets a timeline
  - Interested community members join the group, and develop the recommendations
    - Work is done via email, regular conference calls, and document development
  - Reports and documents are forwarded to the TAC for review
  - Reports and documents are then forwarded to InCommon Steering for review
- Today three new Working Groups will describe what they are working on
- Use the chat to suggest other topics that the TAC should address

Per-Entity Metadata Working Group

Scott Koranda (LIGO), Chair

Per-Entity Metadata Working Group

- Mission: develop criteria and road map for per-entity metadata distribution
  - Triage the immediate issues caused by current metadata aggregate size
  - Identify milestones along a trajectory to a sustainable future state
  - Include interim solutions if necessary

Per-Entity Metadata Distribution

- Per-entity metadata distribution? What? Why?
  - All IdP and SP metadata currently distributed in a single, rapidly-growing file (the "aggregate")
  - Metadata consumers must process the ENTIRE file
    - Even if only a few relying parties ever exercised
    - Signature of entire file must be checked for security
    - Blacklisting does not happen until after signature check
  - Per-entity metadata distribution allows entity to consume metadata only for relying parties it exercises

Current Problems with Single Aggregate Approach

- Aggregates are inherently brittle
  - an error in single entity descriptor can invalidate the entire aggregate
- Increased bandwidth use to distribute the large file
- Inefficient use of client bandwidth to download on a regular basis
- Increased time to verify the aggregate signature
  - increasing time to start up IdPs and SPs
- Increased memory needed by IdPs and SPs
  - now on the order of gigabytes
  - waste of deployer resources

This will only get worse as federations grow

Is My IdP or SP Affected?

Do you operate an IdP or SP that is federated with InCommon?

Yes? Then you are affected.

What should you do?

Keep calm and read the emails from InCommon Ops

- Ops "has your back"
- They will keep you updated on aggregate growth and any necessary changes in resource requirements
- Subscribe to: https://lists.incommon.org/sympa/info/inc-ops-notifications

Meanwhile the working group is working...

Metadata Query (MDQ) Protocol

- IETF draft: https://tools.ietf.org/html/draft-young-md-query-05
- Simple protocol for retrieving metadata about single entities
- Protocol design goals
  - easy for clients to perform queries
  - efficient for both requesters and responders
  - allow the responder to scale in various ways
- Shibboleth IdP/SP and SimpleSAMLphp support MDQ protocol
  - more field testing is required
- For over two years InCommon running MDQ testbed to gain experience
- Working group charged with items necessary to allow InCommon Ops to move technology into a production-ready service

Per-Entity Metadata - Charter

- Develop a roadmap for per-entity metadata distribution using MDQ protocol
- Address issues of
  - High availability
  - Performance
  - Server redundancy
- Develop requirements, risks, and risk mitigation strategies
- Advise InCommon staff on implementation of a solution
- Identify campus requirements for adoption
- Draft report to TAC and Technology Exchange session in September, 2016
- Final report to TAC in November, 2016

Per-Entity Metadata - Participation

- Weekly calls
- Participants include
  - SAML deployers
  - SAML implementers
  - InCommon staff
  - InCommon Participants
  - Members of the international community
- Wiki Space: https://spaces.internet2.edu/x/T4PmBQ
- Sympa List: per-entity@incommon.org
- To join, email sympa@incommon.org with the subject line “subscribe per-entity” or visit https://lists.incommon.org/sympa/info/per-entity

Will I need to make changes to my IdP or SP?

Eventually, yes

- Shibboleth deployers will change configuration to leverage MDQ
- Same for SimpleSAMLphp
- Expect it will take longer for other SAML products

But...

- The single large aggregate file is not going away any time soon
- InCommon Ops will continue to keep you informed
- SAML metadata is InCommon "crown jewels"
  - Process is well in hand

Keep calm and federate

Deployment Profile Working Group

Keith Wessel, Identity and Access Service Manager
University of Illinois at Urbana-Champaign

Purpose

- Develop configuration best practices
- Extend SAML2int for research and higher-ed
- Build off of the work of the Fed Inter-Op Working Group
- Lower barriers for federating

Possible areas of work

- Challenges with unique identifiers
- Appropriate methods for metadata exchange
- Default attribute release
- Entity tagging
- Incorporation of the MFA inter-op profile

Who should participate?

- Research SPs who have had trouble getting attributes
- IDP operators with a list of pain points
- International participation requested
- Info and participation details at https://spaces.internet2.edu/display/DPWG

Open ID Connect Landscape

Albert Wu (UCLA), Chair

What is OpenID Connect?

"OpenID Connect (OIDC) 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

OpenID Connect allows clients of all types, including Web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users…"

source: http://openid.net/connect/

Why do we care about OpenID Connect?

- OAuth-enabled web resources wants to integrate with campus SSO - e.g., LTI
- REST-ful API called by SSO-enabled applications wants to validate the identity of the SSO signed-in user
- Better SSO for “Response” Javascript applications (Node JS, Angular JS apps)
- SSO support for native mobile apps

The OIDC Survey Workgroup

There appears to be growing campus-level activity exploring the use of the OIDC-related protocols. We want to:

- Survey the campus community to understand:
  a. Who is using OIDC/OAuth2 today?
  b. How is OIDC/OAuth2 used at the campus level?
  c. What other possible use cases might OIDC/OAuth2 address?
  d. How immediate/urgent is the need?
- Organize the collected use cases; identify generalizable patterns and trends.
- Report the findings, include applicable next-step recommendations by February 2017:
  a. TIER, and developing IDP/SP federating software
  b. InCommon, and Federation level support, if appropriate, for these use cases
  c. and thoughts on the urgency, if any, of the recommended actions.

How can you help?

- Join the workgroup
- Submit your ideas, use cases, description of how OIDC/OAuth2 might help address your issue
- Help design the survey
- Help spread the word. Pass along the survey - the more interesting use cases likely come from outside the IDM community
- Wiki: https://spaces.internet2.edu/display/OIDCSurvey
- Mailing list: oidc-survey@incommon.org
- Contact: albertwu@ucla.edu

IdP Configurations for Popular SPs

Janemarie Duh (Lafayette College)

Curating integration guides for popular commercial SPs

- Increasing adoption of SaaS
- Collect, collate, and publish configurations from institutions that have successfully integrated their IDPs
- Help resource-constrained campuses
- Add to InCommon value statement
- Community based
- High value, low overhead

Which commercial SPs?

- Services could be InCommon members or not
- Sponsored Partners (256)
  - https://www.incommon.org/participants/
- Seed list
- Examples
  - Office 365
  - Workday

Configuration guide location and content

- Shibboleth wiki
  - https://wiki.shibboleth.net/confluence/display/IDP30/IntegrationGuides
- Content organization via template
  - Add an Integration Guide button

Configuration guide content

- Things to know
  - Create guides only for services for which you have reasonably current documentation
  - Template contains example code blocks
  - Describe things in a uniform way (e.g., metadata)
  - Note any “unique” requirements

- Once you do one, doing others may be mostly a matter of duplication with the addition of metadata and NameID

Technical Advisory Committee Membership

Steven Carmody

TAC Membership

- TAC is an InCommon Advisory Group
  - http://www.incommon.org/docs/policies/TACcharter.html
- It draws its membership from the community
- It seeks membership representative of the broader InCommon community
- Members serve three years terms; one third of the membership can change each year
- Over the next 50 days we will be seeking nominations
  - Send an email to nominations@incommon.org
  - Include information describing the strengths and experience the individual would bring to the TAC, and the constituencies they are familiar with
- For more information, ask any TAC member (e.g., at TechEx) :
  - https://www.incommon.org/about.html

Quick Updates

Steven Carmody

Quick Updates

- Upgrade to Shibboleth IDP v3 if you haven't yet done so !
  - Shibboleth IDP v2 no longer gets even security fixes !
- The Assurance Advisory Committee is currently reviewing all of the feedback the community provided on the **Baseline Expectations for Trust in Federation Profile**
- Two "IDP of Last Resort" (IOLR) are now available in InCommon
  - Individuals lacking a suitable IdP could be invited to register with a participating IdP that offered no-cost, easy self-registration processes.
  - http://unitedid.org/
  - National Center for Supercomputing Applications IDP
    - https://wiki.ncsa.illinois.edu/display/cybersec/IAM

Quick Updates

- eduGain membership continues to grow
  - https://technical.edugain.org/status.php
- Sirtfi (the Security Incident Response Trust Framework for Federated Identity)
  - Designed to facilitate incident response collaboration
  - An InCommon pilot is underway
  - Is coming .. watch for announcements
- The SAML Implementation Profile developed last year by a TAC Working group is currently being reviewed for broader adoption by a Kantara WG

2016 Internet2 Technology Exchange

September 25-29, 2016
Miami, Florida

https://meetings.internet2.edu/2016-technology-exchange/

Sunday – Base CAMP – for those new to the field

Monday/Tuesday – CAMP – Two tracks of case studies and solutions

Wednesday/Thursday – Advance CAMP (ACAMP) – Unconference tackling community issues

Upcoming Webinars

September 14, 2016 – September IAM Online – 2 pm ET

September 21, 2016 – Unicon webinar – 2 pm ET (Trust & Identity Industry Partner presentation)

InCommon Shibboleth Installation Workshop

October 27-28, 2016

California State University Office of the Chancellor

Long Beach, California

www.incommon.org/shibtraining