Agenda and Notes - 2016-09-21

Per-Entity Metadata Working Group - 2016-09-21
Agenda and Notes

[Etherpad used to create these notes: Agenda_and_Notes_-_2016-09-21.etherpad]

Dial in from a Phone:
Dial one of the following numbers:
+1.408.740.7256
+1.888.240.2560
+1.408.317.9253
195646158 #
Meeting URL (for VOIP and video): https://bluejeans.com/195646158
Wiki space: https://spaces.at.internet2.edu/x/T4PmBQ

Attendees

- David Walker InCommon / Internet2
- Phil Pishioneri, Penn State
- Nick Roy, InCommon/Internet2
- Ian Young
- Tom Scavo, InCommon/Internet2
- Scott Koranda (LIGO)
- Michael Domingues, University of Iowa
- John Kazmerzak, University of Iowa
- Scott Cantor, tOSU
- IJ Kim, Internet2
- Rhys Smith, Jisc
- Chris Phillips, CANARIE
- Tommy Doan, Southern Methodist University
- Tom Mitchell, GENI

Agenda and Notes

1. NOTE WELL: All Internet2 Activities are governed by the Internet2 Intellectual Property Framework. - http://www.internet2.edu/policies/intellectual-property-framework/
2. NOTE WELL: The call is being recorded.
3. Agenda bash
4. No call next week (9/28/2016)
    a. Please come to our TechEx session, Tuesday 2:30-3:20, Bayfront A - https://meetings.internet2.edu/2016-technology-exchange/detail/10004447/
5. IdP-only aggregate for SP consumption
    a. Status? (Tom Scavo)
    b. http://md.incommon.org/InCommon/InCommon-metadata-idp-only.xml
    c. What should we say about this at TechX session?
        i. This is in production as of yesterday. Not announced yet, but it's not a secret. We can mention it at TechEx
6. First draft of *Final Report of the Per-Entity Metadata Working Group*
    a. https://docs.google.com/document/d/1MSRAO6FkEltsIM0E9X5y7dnfalephiaIvS1ZE2WTeFM/edit?usp=sharing
        i. Chris: We should comment on adoption by commercial SAML implementations.
        ii. Nick mentioned that Workday recently asked for per-entity metadata. They also said their security people would require TLS.
        iii. It looks like we may get more uptake of metadata with MDQ than what we've seen with the aggregate.
            1. We can't really expect a lot of uptake of the signatures, though, and MDQ (being synchronous with SSO flows) is arguably weaker than the aggregates.
        iv. A reminder: our consensus last week was that we will require TLS but leave selection of the certificate to Ops
            1. Messaging to the community will be critical to describe what is provided by TLS *and* what is not.
            2. This would just be to mitigate (to some extent) injection of bad metadata. *Trust* comes from the signing key.
            3. Should we recommend that InCommon add verification of metadata signatures to its baseline practices?
                a. We can do that, but it may not be acceptable to the community, at least at this time.
            4. Consensus this week was not to offer http. TLS must be used. <-- CP: sure, like Scott C said though, doesn't exclude http delivery (in the spirit of additive confidence in data)
                a. We can continue this discussion next week.
        v. We should target some vendors: Workday, Ping, Microsoft.
            1. Nick will do this when we have a near-final version of the report.
    b. Goal of first draft is to get feedback from attendees of our TechEx session.
    c. Please review and comment prior to the call.
    d. Monitoring the InCommon MDQ Service - Requirements for Ops
        i. Need continuous monitoring by Ops from perspective of consumers
        ii. Monitoring information should be made transparent to federation participants - the manner of which (and details) should be left up to Ops
        iii. Interesting example: https://status.aaf.edu.au/
        iv. Another one: http://weathermap.canarie.ca/caf/eduroam/ (<-- not SAML but 802.1x which does live sign on/reachability tests)
        v. SWITCH also has internal monitoring -- ping Lukas Hammerle for a glimpse of it.
    e. Tom's BIG issues
        i. Do we need preview-main-fallback servers or is a single production server adequate?
            1. Preview yes, but not meet same HA and performance requirements.
        ii. Does the server need to support HTTP Conditional GET?

        1. It's desirable/recommended. Leave decision to Ops.
    iii. What is the range of permissible validUntil dates on each entity descriptor? (we discussed this briefly on today's call)
        1. We should continue this in email and at TechEx.
    iv. Is there a cacheDuration on each entity descriptor, and if so, what is its value?
    v. What is our failover strategy?
7. Post TechX plans for the working group
    a. Submit report to TAC
    b. Scott will probably not be available for calls until 11/19. David will lead 11/5 and 11/12 calls.
    c. Hopefully 11/19 could be our last call, but we'll want to start a couple-week community consultation at that time, so we may need to schedule another call after that.