Agenda and Notes - 2016-07-27

Per-Entity Metadata Working Group - 2016-07-27
Agenda and Notes

[EtherPad used to create these notes: Agenda_and_Notes_-_2016-07-27.etherpad]

Dial in from a Phone:
Dial one of the following numbers:
+1.408.740.7256
+1.888.240.2560
+1.408.317.9253
331718470 #
Meeting URL (for VOIP and video): https://bluejeans.com/331718470
Wiki space: https://spaces.at.internet2.edu/x/T4PmBQ

Attendees

- Nick Roy
- David Walker, Internet2
- Michael Domingues, University of Iowa
- Tom Mitchell, GENI
- Walter Hoehn, Memphis
- Scott Koranda
- Tom Scavo, InCommon/Internet2
- Phil Pishioneri, Penn State
- John Kazmerzak, University of Iowa
- Ian Young
- Scott Cantor, tOSU
- Tommy Doan, Southern Methodist University
- Rhys Smith, Jisc
- Paul Caskey,
- Paul Engle

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 may be recorded.
3. Agenda bash
4. Rhys Smith will present on his MDQ work for UK fed
    a. Planning to deploy an instance of mdq-server starting in August
        i. The mdq-server instance will run behind the firewall
        ii. Signed per-entity metadata will then be pushed to a standalone apache server (possibly with a static cache)
        iii. Every time new aggregates are created, the per-entity static cache is recreated
    b. Introduce a new signing key with HSM (Thales) on mdq-server (old key is 10 years old)
        i. Want to use a key that's never been anywhere but the HSM.
        ii. No decision to migrate the aggregate's key at this time. Could be done in the future, although it would be a good amount of work.
        iii. HSMs can be expensive. Amazon's solution (buy one for you and rack it up) is "pretty eye watering" (Ian)
    c. Will implement a push model via github to distribute static signed per-entity metadata to cloud-based servers that are queried by IdPs and SP.
    d. A few months of pilot with selected customers
    e. Does it make sense to consider outsourcing of MDQ service?
        i. Yes, assuming the service is sufficiently secure, highly available, and not horrendously expensive.
        ii. Our group should think about describing requirements for InCommon's MDQ service in a way that could be put into an RFP or SLA without too much effort.
5. Begin in depth discussion: What are the risks for a per-entity metadata service and the possible mitigations
    a. Availability
        i. Need 100% availability, not even "5 9's"
        ii. Internet2 would need to develop such a capability.
        iii. This points to using a cloud infrastructure
        iv. The model of pushing static files to a highly-available web service should enhance this.
        v. A there are things clients could do to mitigate this?
            1. Failure mode is the same as if the entity were not in an aggregate, if the entity is not already in the cache.
            2. Shib will cache entities until they are no longer valid.
        vi. This is, by the way, how OIDC works
        vii. What's important here is availability of the query service for IdPs and SPs
        viii. Need to keep in mind not only failures of the actual service but locally inflicted problems that prevent consumers from getting to the service. How do they respond to a network outage that endures? What can a campus expect in that instance?
    b. Security
        i. Signing key
6. Next call is August 3, 2016 @ 10:00 AM (America/New York)
    a. Scott K. will be out for this call