

# Agenda and Notes - 2016-10-05

## Per-Entity Metadata Working Group - 2016-10-05 Agenda and Notes

[Etherpad used to create these notes: [Agenda\\_and\\_Notes\\_-\\_2016-10-05.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
- IJ, Internet2
- Nick Roy, InCommon
- Tom Scavo, Internet2/InCommon
- Tommy Doan, Southern Methodist University
- Ian Young
- Tom Mitchell, GENI
- Phil Pishioneri, Penn State
- Scott Cantor, tOSU
- Rhys Smith, Jisc

### 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. Highlights of our TechEx session
  - a. We'll recommend TLS, leaving final decision of how to manage keys based on some more research of CDNs. (It won't be the same as the metadata signing cert.)
  - b. For the validUntil setting, Tom Scavo suggested recommended as short a period as operationally feasible.
  - c. A couple of people mentioned that they plan to implement their own MDQ service.
    - i. This was either for increased availability and performance, or because they will be distributing a different set of entity metadata.
  - d. From the Sharepoint session, MDQ helps with clients (like ADFS) that requires TLS.
    - i. ADFS still has challenges with the volume of entities we have.
  - e. Use of a non-commercial cert for this is a good idea, as suggested by ScottC
5. Finalizing our report - <https://docs.google.com/document/d/1MSRAO6FkEltsIM0E9X5y7dnfalephialvS1ZE2WTeFM/edit?usp=sharing>
  - a. Please add comments and suggested edits for discussion during the call. Please use "suggesting" mode, unless you are correcting grammar, punctuation, etc.
  - b. We'll add section numbers (or some other section identification that Google Docs supports)
  - c. Somewhere, mention impacts on implementation and deployment profiles
  - d. Most notes were made in the document itself. Here are highlights.
    - i. David will draft the executive summary for discussion next week. Any calls to action by InCommon will need to be here, with details in the body of the report.
    - ii. Make sure discovery is appropriately highlighted as critical for a significant population of SPs.
    - iii. The issue of client bandwidth consumption will be rolled into other client issues.
    - iv. In the "Risks of Per-Entity Metadata Distribution" section, we'll note that the risks are not presented in any particular order.
    - v. Regarding "bad" vs. "malicious" actors, we'll look for wording that also includes poor implementations that cause unintended "attacks" on the infrastructure.
    - vi. Need better language to describe IdP and SP transactions that require metadata. "SSO web flows" is not right.