Agenda and Notes - 2016-09-14

Per-Entity Metadata Working Group - 2016-09-14
Agenda and Notes

[Etherpad used to create these notes: Agenda_and_Notes_-_2016-09-14.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

- Nick Roy, InCommon/Internet2
- David Walker, InCommon / Internet2
- Tom Scavo, InCommon/Internet2
- Tommy Doan, Southern Methodist University
- Scott Koranda, LIGO
- Scott Cantor, tOSU
- John Kazmerzak, University of Iowa
- IJ Kim, Internet2
- Tom Mitchell, GENI
- Ian Young

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. MDQ service with HTTPS transport
    a. Proposal is that the InCommon MDQ service should use HTTPS as transport
        i. X.509 cert for TLS is NOT the metadata signing cert
        ii. X.509 cert for TLS chain of trust is rooted in standard commercial CA
        iii. Documentation will continue to state that clients must verify the XML signature of the metadata
        iv. Any negative change in risk posture due to clients (eg. ADFS) leveraging TLS only for metadata trust is outweighed by advantages for all other clients to help reduce risk posture increases due primarily to per-entity metadata being downloaded on demand and more often
    b. Do we have consensus?
        i. ScottC: Using a self-signed cert enables metadata consumers to make an explicit decision about trusting the server. Unfortunately, it also requires that decision.
        ii. TomS: Perhaps it's too soon to know what cert should be used. Perhaps this decision should be left to Ops during implementation.
        iii. David: There's a middle ground of using a commercial cert but telling everyone what cert is used.
        iv. The fact that we have to distribute the private key for the cert into the CDNs eliminates a lot of the benefits of using a specific (self-signed) cert.
            1. So, using a commercial cert may be the best way to go, because they'll be easier to deploy/use.
        v. Consensus is to leave the decision of what cert to use with Ops.
5. Should we use a new signing key for per-entity metadata distribution?
    a. Reasons to introduce a new signing key for MDQ service
        i. Path of least resistance is to use existing signing key.
        ii. This is a golden opportunity to deploy a new key, if that's something we want to do.
        iii. Current signing process is manual; it should be automated, removing the private key from people's hands.
            1. Timing, unfortunately, is that automated signing will come after MDQ.
        iv. UK's current pilot is using the same signing key. The decision for the production service is yet to be met.
        v. This may be an opportunity to educate the community as to the importance of verifying signing keys.
        vi. Consensus is to leave this decision to Ops(?)
    b. Reasons to NOT introduce a new signing key for MDQ service
    c. Any reasons to conflate new signing key for MDQ service with change of signing key for aggregates?
6. What should be the validity for the signed per-entity metadata?
    a. Longer validity in general increases risk since clients keep bad metadata longer as long as they have no access to updated metadata
    b. Cannot go below the maximum expected outage for MDQ service (99.9% equals 43.2 minutes per month)
    c. Is there any reason to conflate per-entity validity and the aggregate validity?
    d. There are two parameters, valid-until and cache-duration
        i. The current metadata aggregate calls out valid-until of two weeks. It doesn't have a cache-duration.
        ii. Valid-until limits the risk of having old metadata injected (e.g., with a compromised key)
        iii. Lower bound for validity is the rate at which new metadata is published.
        iv. Valid-until balances the risk of old metadata vs. business continuity
    e. ScottC: It seems like a shorter validity period makes sense for per-entity distribution, as there's greater opportunity for injecting old metadata.
        i. TomS: This could cause operational issues (e.g., for long holidays), but that doesn't mean we shouldn't do this.
        ii. David: Introduction of automated signing could provide the opportunity to shorten this.

    f. Consensus is to leave decision to Ops, recommending a week for validity
        i. Ian: This can be changed fairly easily. UK keeps it short, but lengthens it during holidays.
7. Report draft: https://goo.gl/hLYwsQ
    a. Everyone please look this over, fix errors, add comments and questions
8. TechX presentation
    a. Tuesday 09/27/16 02:30PM-03:20PM (local time)
    b. Slides shared via email (probably Monday)
9. Recommendation for follow up working groups
    a. Metadata signing key(s): future
    b. What comes after per-entity metadata
    c. Discovery