InCommon TAC Meeting 2014-01-23

InCommon Technical Advisory Committee Meeting Minutes

Thursday, January 23, 2014

Attending: Steve Carmody, Ian Young, Michael Gettes, Chris Misra, Jim Jokl, Jim Basney, David Walker, Tom Barton, Scott Cantor

With: Tom Scavo, IJ Kim, Ann West, Joe St Sauver, Nate Klingenstein, John Krienke

Action Items

(AI) John and Steven will review the Phase 2 Recommendations and propose to TAC a list of items that need to be addressed as a result of accepting the Recommendations

(AI) Ann will propose a Community Review process to TAC on the next call

(AI) TomS will add "Certificate Service Next Steps" to the next TAC agenda

(AI) Steven will send an email with a few suggested meeting times for the regularly scheduled TAC meeting

Ops Update

TAC comments re metadata server:

1. The FOG survey showed 10 of 13 federations enable TLS on their metadata server.
2. Multiple TAC members agree that enabling TLS on the metadata server will circumvent questions from customers in the future.
3. Multiple TAC members disagree that the absence of TLS on the metadata server will cause deployers to do the Right Thing (in particular, verify the signature on the metadata).
4. Multiple TAC members agree we should clearly document that deployers should do the Right Thing (in particular, verify the signature on the metadata).
5. Make it as easy as possible for deployers to do the Right Thing. For example, provide clear and explicit documentation for configuring metadata refresh in the Shibboleth software.
6. Enabling TLS on the metadata server is a perception issue more than anything else.
7. If we haven't received any questions about HTTPS yet, why would we start receiving questions now?
8. If we did start receiving questions from deployers, it's likely those same people won't understand TLS at all.
9. Regardless of what we decide to do with respect to TLS on the metadata server, this should have no effect on a deployer's decision to migrate to the new server by March 29. [NOTE: Actually, it does. If you have an outbound firewall, and we enable TLS on the metadata server, you must migrate or your deployment will break.]

Ops comments re metadata server:

1. Ops recommends to NOT deploy TLS on md.incommon.org
2. Metadata signed with a secure, offline signing key can not be replaced by HTTPS.
3. Metadata refresh via HTTPS assumes the metadata server is secure. Recall, however, that we run multiple physical servers, only one of which is under our direct control in Ann Arbor.
4. Signed metadata can be served from any server, regardless of whether it is TLS-enabled or not.
5. A TLS-enabled metadata server provides no real value.
6. InCommon has never advertised an HTTPS endpoint for metadata.
7. Even though we've never advertised an HTTPS endpoint for metadata, 2% of GET requests for metadata are HTTPS requests. [NOTE: This was erroneously reported as 20% on the call.]
8. Is TAC suggesting we publish an HTTPS endpoint for metadata? [inctac:that's not what we heard but we just want to be sure]
9. We do not want have the HTTP vs HTTPS conversation with deployers. We would rather avoid this conversation altogether.

TAC comments re metadata signing certificate:

1. https://lists.incommon.org/sympa/arc/tac/2014-01/msg00130.html
2. At least two TAC members strongly agree that the metadata signing certificate should be served from a secure server protected with an EV cert.
3. The trust anchor (and its fingerprint) need to be served from the strongest location possible, and moreover, we should do this independently of any decision made about metadata distribution.

Other TAC comments:

1. The documentation should make it clear to deployers what happens if they don't migrate. If things are gonna break, we should make that clear.
2. Is the March 29 milestone date negotiable?
3. There is concern about the redirect failing (or not being supported) at some point in the future.
4. Except for RHEL4, it is best to assume nothing will break. This isn't entirely true (a few deployments will break) but we don't expect significant numbers of deployments to break (otherwise we wouldn't be doing this).

Metadata Distribution WG

- John reports the work of the MD-Distro WG is complete and thanks the group's members for their efforts
- The MD-Distro WG has submitted its Phase 2 Recommendations to TAC (see John's note to the mailing list sent on 2014-01-16)
- For reference, the Phase 2 Recommendations are:
    1. Expand the usage of multiple metadata aggregates
    2. Conduct a pilot study that explores the feasibility and utility of per-entity metadata

    3. Conduct a community-driven review of InCommon key management practices
    4. Conduct a landscape study of the potential needs and uses of hardware security modules
    5. Participate in the samlbits.org project
- Comments, questions, and discussion:
    1. Most of the discussion centered around the proposed pilot study of per-entity metadata.
    2. The goal of the pilot is to bring relevant stakeholders to the table, explore the issues, and identify requirements. In particular, per-entity metadata has poorly understood consequences with respect to IdP discovery
    3. There's a relationship between per-entity metadata and HSMs that needs to be explored
    4. The per-entity metadata pilot will explore both infrastructure requirements and software requirements
    5. What is the overlap with the samlbits.org project? Well, we might decide to distribute per-entity metadata via the samlbits.org content delivery network as part of the pilot. (As mentioned in the Recommendations, this is a desired outcome, not a requirement.)
    6. Do we have any reason to believe that any software vendor or project (besides Shibboleth) is concerned about per-entity metadata? The answer is most likely no, and so one of the goals of the pilot is to raise awareness of this issue.
    7. We need to make a Call for Participation in the pilot study, and we probably need to do this sooner, rather than later, since potential participants will need to prepare by developing software, deploying infrastructure, or whatever needs to be done in advance to participate in the pilot.
    8. The appropriate scope of the pilot is probably at the level of REFEDS, but the 2014 Work Plan is already determined, so one possible path forward is for InCommon to do an initial pilot in 2014 and then continue the second phase of the pilot in 2015 in conjunction with REFEDS.
    9. In terms of software, we want to include simpleSAMLphp in the pilot, which is why working with REFEDS is important, so that the simpleSAMLphp federations are invited to the table.
    10. As an aside, it's probably unlikely Microsoft AD FS will ever support such a metadata distribution model.
    11. How does the pilot align with eduGAIN? Probably not at all since eduGAIN metadata is targeted at federations, not end entities.
    12. How do the Recommendations relate to the Priorities document recently submitted to Steering?
- See the full report for more detail
- John asked TAC to accept the Recommendations of the WG, and in the case of the key management recommendation at least, the ball is TAC's court to take next steps
- AI: John and Steven will review the Phase 2 Recommendations and propose to TAC a list of items that need to be addressed as a result of accepting the Recommendations

Approval of the IGTF SSL CPS

- Jim Jokl reports on the IGTF SSL CPS
- Previous issues have been worked out and so the CPS is ready wider dissemination
- The IGTF SSL CPS was approved yesterday by PKI Subcommittee, which now seeks TAC approval of the CPS so that it can be forwarded to Steering for further consideration
- Jim Basney summarizes the changes and edits to the previous version of the CPS:
    1. Added a clarification that the IGTF CPS falls under the Comodo CPS
    2. Comodo required InCommon to change the CRL distribution URL and OCSP endpoint location so that both are based on Comodo-controlled domains, not InCommon-controlled domains
    3. In the end, a compromise was agreed to such that *InCommon would own the domains but Comodo would control the domains* (it is anticipated that all InCommon CAs will have this property in the future)
- In summary, the totality of changes to the previous version of the CPS were very minor
- TAC approves this version of the CPS

Certificate Service Next Steps

- Jim Jokl gives a very brief overview and then asks that we tee it up next time
- Jim and MRG were approached by a couple of people at CSG wondering if other certificate vendors might be interested in sitting at the table (in the same way that multiple NET+ vendors compete for campus interest in a particular focus area)
- The PKI Subcommittee considered this question and decided that adding a second vendor in this area would be counterproductive
- Instead we should demonstrate to the community that Comodo is the best solution and that we've done (and continue to do) due diligence with respect to security, reliability, and affordability
- When time comes to renew the Comodo contract, should we do a simple renewal or actually put out an RFP
- So the PKI Subcommittee is asking for TAC reactions to any of the previous strategies
- Question: Are folks asking these questions because of concerns about Comodo or are they simply exercising due diligence?

Software Guidelines

- TomS reports that the Software Guidelines page has been revised as requested
- In fact, there are now two pages, a modified Software Guidelines page and a child page entitled Using Other Software
- InCommon Staff discussed the Software Guidelines internally and made two additional suggestions:
    1. Contact Roland Hedberg and make sure he's okay with the content (since one of his software projects is implicated)
    2. A Community Review process is recommended
- Ann suggests that since the Software Guidelines border on being a set of requirements, and since they are referred to in the Participation Agreement, we should probably conduct a Community Review with an eye towards gathering the input of community stakeholders before we finalize it
- TAC members agree with the staff proposal to conduct a Community Review
  Editorial suggestion: globally replace "AD FS" with "ADFSv2" (see this relevant factual report on the TAC mailing list)
- AI: Ann will propose a Community Review process to TAC on the next call
- A goal is to determine a concrete Community Review process, as a checklist if possible

New TAC meeting time

As mentioned at the beginning of this call, Steven wants to suggest that a new call time may be necessary since there is a conflicting NET+ call that is drawing folks away from the regularly scheduled TAC call. It is somewhat painful to even bring this up since this group has probably met at this time slot for close to 10 years now.

AI: Steven will send an email with a few suggested meeting times for the regularly scheduled TAC meeting