800-63-3 KI Comments 2017

KANTARA IAWG comments on 800-63-3

Kantara Comments on GitHub - May 1 2017: **Consolidation_comments 800-63-3_rev1_May1_2017.docx**

Kantara Comments on GitHub - March 31 2017: KI Community comments on 800-63-3_20170331.pdf

Status of IAWG comments: Status of IAWG comments on 800-63-3_May 25th.docx

Process of gathering comments within IAWG

FIRST SESSION

Key discussion items Feb 9th 2017:

- Get comments in at least a week before March 31. Switching back to weekly meetings to accomplish that.
- Comments regarding cost and impact of the changes in the CSPs.
- Concern about implementation timeframe.

GENERAL COMMENTS of the document:

- Kolin Whitley, Experian - ID proofing strategies were put in place as part of multiyear contracts, how might that impact the component given that the new guidelines are significantly different.
- Russ Weiser, Zentry/Synchronoss - requirements for authoritative data sources, chasing identity documents to their source. The federal and state governments have failed to provide a verification service. TFS work on standard operating procedures, the implication was that there were changes underway to make things easier for agencies to understand. It's more unrealistic if agencies must grapple with new standard procedures from TFS at the same time that 800-63-3 hits.
- One problem with 800-63 has been lack of flexibility in the face of considerable CSP innovation in how services are provided, we shouldn't try to stand in the way.
- The simplification of the levels from 4 to 3 may have made it more difficult to obtain the levels. Removes the lower cost category and increased the cost to comply.
- The different numbers of levels in different countries may result in interoperability issues between the jurisdictions.

Reference: IAWG Meeting Minutes 2017-02-09

SECOND SESSION

Key discussion items February 16th

GENERAL COMMENTS

- Continued use of bulleted lists - if the lists convey requirements, the implementer or the reviewer or the assessor needs to be able to refer to the requirements. Richard has suggested numbers instead of bullets, so that requirements could be uniquely identified.
- Scott will include this among the recommended IAWG comments as well - uniqueness of requirements clauses is great assistance to implementers and assessors alike.

Reference: IAWG Meeting Minutes 2017-02-16

THIRD SESSION

Key discussion items February 23rd:

REVIEW OF 800-63-3

- Discussion of the need to uniquely identify clauses in the requirements.
- Ken Crowl shared his list of his organization's concerns: Level of Assurance vs Identity Assurance Levels; Document verification; "Issuing Source". Overview of Experian position on NIST 800-63-3.pdf
- Scott Shorter included a comment in support of the flow charts / decision trees included in 800-63-3.
- Discussion of requirement for document verification for all remote proofing. Call for a need for intermediate verification options that don't require the full rigor of IAL2 (remote + document verification). Technical challenges to document verification.

Reference: IAWG Meeting Minutes 2017-02-23

FOURTH SESSION

Key discussion items March 2nd:

REVIEW OF 800-63A

- Richard mentioned that NIST has effectively taken away AL2.
- Discussion of the fact that there are no mechanisms for validating drivers license, although AAMVA would like to be in that business.
- Right now the only viable implementations are PKI or self-assertion.
- Russ has had discussion with someone at GSA has looked into expanding passport service to support this, but they run into funding problems for this. Financial institutions will also have difficulty verifying those sources. Would not be surprised if there was an order of magnitude increase in costs - negotiating individual contracts with different states for drivers license validation would expand costs considerably, even if it was possible. Will probably result in stagnating the online credential business, unless GSA were to step in and provide those services on behalf of the government (along the lines of the ACES program).
- Ken mentions the concern from CSPs about the implementation roadmap for when the new changes will be required. Colin says discussions have not taken place, but NIST are aware of Kantara's view on that.
- Richard Wilsher points out that the enrollment processes of most CSPs would need to be changed to meet the new standard, that will not be rapid. Furthermore the question from Kantara's perspective - how soon would Kantara be able to perform assessments? Thirdly, what would Kantara do to set a deadline by which CSPs would be required to comply.
- Ken asks whether existing credentials would need to be re-proofed. Russ Weiser has mentioned that customers will be unhappy about that. Customers are already asking what to do about the standard. Something like that could result in a years of delay while credentials are updated.
- Richard inquires what will happen with the existing SAC aligned with 63-2 - would we continue it in parallel? Would there be an overlap? What about those who are not in the US who are approved against the current criteria

Reference: IAWG Meeting Minutes 2017-03-02

FIFTH SESSION

Key discussion items March 9th:

REVIEW OF 800-63-B

- Numerous references to "digital service" without being clear what they mean.
- Refer extensively to the "subscriber" whereas other schemes include "subscriber" and a "subject". The "subscriber" may be the organization who wants credentials issued to a number of subjects. Would make easier alignment with other sources.
- Model and state diagrams are inconsistently applied. When you become a subscriber because you have enrolled, the definition of enrollment doesn't include the definition of a service account. Since they are unclear on the enrollment process its not clear what the subscriber is.
- RGW suggests maybe this means that 800-63A should include the idea of enrollment and becoming a subscriber/subject. Overall, changing the term from subscriber to subject.
- Andrew is wrestling with the question of "are you still a subscriber when you are federating authentication?"
- Part of the model inconsistency is differences in how the verb "authenticate" is applied, does the subscriber authenticate or does the CSP do the authenticating.
- Andrew is reviewing and finding internal inconsistencies in the way terms are used, it's not clear what the state model is to get from non-authenticated to authenticate state, versus the authenticators and secrets and other things needed to assert the identifier. They do say that the purpose of authentication is to produce an identifier, versus the purpose is to get access to a service.
- Scott suggests whether it's possible to use the term identified access to a service.
- Andrew notes that they reference "classic kerberos" versus "modern kerberos"
- Denny notes that there's a section around usability, but how it looks on the screen and the user interface, is that something that is in the scope now? Andrew Hughes responds that they obtain usability from following the NSTIC guiding principles, which include usability. The idea being that authenticators that are difficult to use are not trusted.
- Ken notes that there are currently no normative usability requirements.
- RGW mentions the issue of uniqueness of credentials, and inconsistency in the use of the term "digital service" in the introduction to SP-800-63-B. Section 4 uses the term as if it refers to the Credential Service Provider, whereas the introductory text uses the term as if means the Relying Party.
- Section 4 is marked normative, so it should be clear about requirements, use shall statements for that.

- On guidance versus technical requirements. Richard observes that on the first page they should be referring to requirements rather than guidance. Calling it guidelines dilutes the force of the requirement. Andrew can observe that they are putting normative statements in the document but not using normative language. The documents are called "guidance" but it contains requirements. Are the contents mandatory or not?
- Andrew observes that a state model would be helpful to show how entities go from non-authenticated to authenticated state, verifiers in pre-authenticated to post-authenticated state. Scott concurs on the state model.
- Denny asks about if there's a model for them to reference. Andrew observes that 800-63-3 describes the model of the architecture for the discussion in the documents. There's a role diagram that infers some changes of state, it's indistinct but it illustrates that a claimant becomes a subscriber. Probably not complex, but not documented at this point. Denny wonders about disability acts in various parts of the world.

- Additional comments from RGW - section 4.1.2 - cryptographic authenticators at AAL1 shall use approved cryptography. Scott suggests that this is in line with NIST's mission to push approved cryptography for all uses of government cryptography.
- Additional comment RGW - 4.1.4, 4.2.4, 4.3.4 there are references to 800-53 "or equivalent standard" but what is the method of judging what an equivalent standard is.
- Andrew has a comment on section 4.5 - summary of requirements, they don't have rows for records retention or privacy requirements.

Reference: IAWG Meeting Minutes 2017-03-09

SIXTH SESSION

Key discussion items March 16th:

REVIEW OF 800-63C

- Credential generation and other lifecycle issues are missing from the discussion. Andrew points out 800-63B has a section called lifecycle management.
- Ken asks if anything changes if it happens in a federated context as opposed to the context B was written in.
- RGW suggests that it depends whether the federation includes requirements to be a member of the club. Only becoming more of a concern as reading 63B and 63C. Many SHOULD statements - as we know, if is says SHOULD then they probably won't.
- Globally we have a comment that SHALL and SHOULD need to be clear. Each distinct SHALL or SHOULD ought to be in a single paragraph.
- Andrew observes it's a similar comment to last week - the document is a mixture of explanatory material, guidance material and requirements material.
- Ken suggest we could comment them for adopting a normative style.
- General agreement that the document is not ready for prime time.
- Andrew notes that we appreciate the shift towards normative language in the requirements, but the phrasing of some requirements makes it difficult to have certainty that the implementation meets those requirements. As assessors there is also uncertainty about how to evaluate the conformity. Uncertainty then leads to inconsistency.
- RGW has one other broad topic - 4.2 of 63C - requirements on federal agencies slapped on the end of the section. Perhaps including it in an annex instead of including in the rest of the flow of the document. The agency guidance at the end of the privacy section is a non-sequitur with respect to the rest of the document
- Andrew notes that the audience section of 63-3 is blank.
- We could use clarity from the authors on when the agency specific text applies.

- Next steps: Thursday 243rd we will take the first cut at looking at the comments. We can package and submit them early if we're happy with them next week.

Reference: IAWG Meeting Minutes 2017-03-16

Archives:

- Previous KI comments - 2016: Previous submission to NIST