SG GSA 2017-12-05 Meeting notes

Attendees

Aakash Yakash, OKTA

Colin Wallis, KI ED

Ken Dagg, IAWG Chair

Scott Shorter, KUMA

Andrew Hughes, LC Chair

Richard Wilsher, Zygma

Ruth Puente, KI PM

Mark Hapner, Resillient

Meeting Notes

RGW overview comments – great costs and great expense to comply with certification requirements.

Andrew – their definition of trust framework is actually “federation operator”, very similar to the commonwealth of Virginia definition. Kantara doesn’t offer federation operator services, need to be cautious that we don’t change what Kantara’s program does.

Scott asks Andrew what would be removed from GSA’s definition to remove the federation operator aspect?

Colin agrees with Andrew’s perspective.   Federation operations are not necessarily part of trust framework. tScheme loads liability onto the framework (?)

Colin – would you agree that they are trying to merge PKI with non-PKI governance?

Colin will be reaching out to KI’s approved CSP’s to understand the market and the specifics. KI, for reasons that Andrew mentioned, has kept at arms length. Need to understand what the commercial viability of an offering that delivered authenticated identities at lower assurance levels.

Andrew did skim the documents – do we perceive that the document as written assume that connect.gov is in existence and viable? That could explain why a federated shared risk pool is the way to go?

RGW suggests that if Andrew is correct. Organizations he knows are dealing on a one-to-one basis, there’s no notion of federation going on. This appears to be a replacement for the FICAM program, with forced federation.

Andrew: As connect.gov was being retired, there was desire from FICAM to push certification responsibility towards the industry. This looks like an overcompensation because the federal agencies may not bear the costs of having a fully certified CSP relationship.

RGW – should we respond that we are confused by this and don’t understand what happens to the FICAM program. Need to understand the fundamentals before we comment on the details.

Colin points out that we are very constrained in what we can say since this is in the public domain.

RGW reminds that GSA has been invited to discuss with CSPs and TSFs but they don’t have much to say on the group meetings.

Scott asks if federation and certification are the only issues? What about 800-53?

Andrew quotes section 2 roles and responsibilities,

“A Trust Framework establishes the set of rules and policies that govern how their trusted identity federation members will operate and interact. These rules and policies include how to:

> Conduct identity management responsibilities;
>
> Protect and securing identity information;
>
> Perform operational and administrative roles within the federation; and
>
> Manage liability and legal issues.

Trust Frameworks establish multilateral agreements among all identity federation members enabling the trust and governance of a federation’s operations.”

Andrew points out that this model doesn't match Kantara Initiative. The closes existing model would be InCommon, since they have multilateral agreements among identity framework members.

Colin mentions that InCommon doesn't see itself in either of the GSA CONOPs scenarios.

Andrew points out that we know that the authors mean "Trust Framework" to mean Trust Framework Operator. Internet2 federation rules are not what the trust framework provider does.

RGW says it's as if they are trying to create a Federal federation, almost like connect.gov could have been.

Mark asks if this framework would apply to SAFE BioPharma as well? Andrew says probably closer to yes. RGW says if SBP has standardize terms that are included in the scope of an assessment, then all certified proved individuals have to agree to a set of common operating standards. That would be leading towards establishing a federation. Andrew points out that SBP operates a federation and is a federation operator, which resembles what in this document is called a trust framework.

Mark says he sees KI listed as a Partner of SBP.

Andrew references section 2.2, which says that "Agencies do not have to establish agreements with an independent Trust Framework. They are considered a member of the U.S. Government's trust governance framework." So, we're talking about inter-federation between trust framework providers and the US government's trust governance framework. Once again this is different than the model than KI is supporting.

RGW points out that comments may not be as useful to our understanding as conducting a joint whiteboard session to obtain complete understanding of GSA's perspective.

Ken points out that these gaps are so big that there's more to be said than we can say in two weeks. Do we put in a few conceptual issues?

Andrew points out that there was an email thread in which Colin mentions that KI has an MOA with GSA. The document talks about the memorandum of agreement, and Colin has a copy that was signed in 2010. Andrew asks if it is counter signed? Colin confirms. Andrew says we can point out that we have a contract, and modifying the contract is a separate issue than the trust framework solutions docs.

Colin agrees and separated out the issues that way.

Andrew points out that we could comment that signatories (garbled) on what they describe. There must be a renegotiation of the terms regardless.

Andrew suggest that we point out that roles and responsibilities do not match what we see in the document. Commenting on the procedures does not constitute renegotiation of our MOA.

RGW suggests that we can't afford not to make comments. We should make comments and keep them high level, explain our concerns, may require a letter. Request a public meeting to discuss the concepts and principles – face to face between CPS and trust framework providers together with GSA.

Colin suggests we start pulling together – RGW has taken a crack at it, CW has commented on the word doc. Is there value in a GDoc to collaborate on?

Ken suggests Scott document the three major issues he referenced earlier (federation, certification and security controls), that might satisfy concerns.

RGW will comment again and decide whether to remove comments, will filter and share with the group.

Ruth will put out a doodle poll to schedule the call for 12/11.