FICAM Workshop – Thursday, January 14, 2016

Meeting Notes

Attendees
Andrew Hughes, IAWG Vice-Chair
Richard Wilsher, Zygma (Assessor)
Kolin Whitley, Experian (CSP)
Zachery Vallery, athenahealth (CSP)
Ray Kimble, Kimble & Associates (Assessor)
Scott Perry, Scott Perry (Assessor)
Peter Alterman, SAFE Biopharma (TFP)
Paul Caskey, Incommon (TFP)
Blake Hall, ID.me
Steve Smith, ID.me
Mike Garcia, NIST
Paul Grassi, NIST
Scott Shorter, Electrosoft
Stephen Skordinski, Electrosoft
Dennis Cronyn, FICAM (Protiviti)
Adam Madlin, Symantec
Chi Hickey, FICAM (GSA)
Russ Weizer, Verizon
Chris Louden, FICAM (Protiviti?)
David Dewy, TFS and connect.gov
Lee Aber, ID.me
LaChelle LeVan, FICAM
Allan Foster, KI BoT
Ruth Puente, KI

Focus:
US Federal (civilian) Government and suggestions to a) improve the processes for certification and b) improve the services provided to agency customers.

- **Comments during the "tour de table"**

  - FICAM commented that the aim of the meeting was to discuss how they could help change and improve the Program processes. They are open to change in a transparent manner.
  - It was encouraged the CSPs to participate in the IAWG.
  - More collaboration between vendors.
  - Have a clear track equivalent assessment between FICAM and KI.

- There are some gaps in name change or delegation capabilities when a person dies. It should be a policy on the Relying Parties on how to manage the data in this case.
- Create awareness in the agencies on how to integrate connect.gov
- FICAM documentation needs to be updated and make it more usable.

➢ **Group Dynamic: What is Trust Framework Solutions**?

Items identified by participants:

- Body that does accreditation
- Seal of approval
- Set of best practices.
- Equivalent of the PKI policy management
- Cost driver
- Vague
- Subject to interpretation to everyone
- It´s dangerous.
- The objectives behind the requirements are not well understood.
- Not clue
- Not trusted
- Secret passageway
- Unclear relationships with TFPs vs CSPs
- We don´t like.
- Authorizer/Authority for C2G auth´n services
- Over-engineered
- Perceived as irrelevant
- Unclear accountability
- Boxes to check
- LoA
- Not universally accepted
- Framework that RP don´t want to use
- Not trusted

➢ **The following 4 areas were identified during the morning discussion:**

1. Documentation and processes
2. Usability.
3. Demographics.
4. Actual technology profiles and processes being certified.

Processes:

- The TFS needs to have a charter.
- RPs need to be involved in the process, they are important stakeholders. They need to understand the requirements.
- Agencies need to drive the requirements.

- The Web application Program Managers of FICAM need to be involved in the discussion.
- There is a need of simplification in the language, definitions and processes.
- It was clarified that ICAM implies the systems; processes and services built within and across the agencies around Identity management procedures, credential procedures, authentication, and authorization. ICAM is the individual agency programs, and FICAM is the federal program. The Trust Framework is how ICAM works with third parties.
- Boundaries/relationships between governance of PKI credentials and non-PKI credentials (800-63, TFS, FPKIPA). Within ICAM, there is a PKI based federation and TFS Program, how they align with PKI and non-PKI federations? Also, there is a comparability between the 2, and 800-63 has language that relates the 2 together. We cannot modify a framework without modifying standards.
- The need for FICAM PMO to have a Charter was focused on their need to define the purpose and scope of FICAM and their office, including, importantly, operational procedures that partners could rely on the PMO to follow.

Demographics and Communities of interest (COI) e.g. NASA, IRS:

- There are certain number of users, transactions, services, solutions, interests and mission areas within these relationships: Government to Government (G2G); Business to Government (B2G); Government to Business (G2B); Citizen to Government (C2G); Business to Business (B2B); Citizen to Business (C2B).
    - What demographics cover?
    - There are 204 agencies.
    - Avoid losing boundaries as it causes confusion in the trust and what it is certified.
    - How TFS and the other areas, non-PKI and PKI federations, SAFE vs Kantara vs Incommon, can work together to build a nice ecosystem and services?
    - Industry: From the 204 agencies, which interacts with the federal government? The objective is enabling the parties to work with government, so CSPs need to know who does those interactions.
    - Analysis G2G transactions vs users, higher number of users, lower number of transactions versus lower number of users, higher number of transactions.
    - Work together to improve the services to the particular communities of interest.

Usability

- Big challenge: Establish a strong online identity.
- Improve the service and usability. How we protect metadata in the transactions (C2B, B2B, etc.)?

- Comparability is qualitative based on the assessors. There are assumptions around of what comparability is.
- Re-write the requirements based on the objective and outcome perspective, rather compliance to the process, e.g. what´s the outcome from this requirement?
- Assessors need to know the objectives of the comparability requirements.
- Authentication risk (low level of assurance), the challenge is the scalability in the implementation.
- Assessors perform an overview audit.
- FICAM is making a comparison between the US and UK model. It is important to consider the user, provide value to the customers.
- Stronger authentication (higher assurance credentials) in the C2G and B2G communities.
- Need to have standardized reliable trust validation policies and procedures and allow the low assurance level to operate. The low assurance levels are easy for citizen to use.
- Challenge for FICAM: scalability. Agencies do not want to be responsible for id proofing. The RPs do not want to spend the resources (capabilities) on this.
- Improve driving solutions that are usable.
- Form Vector. Social + login (additional factors) ubi key authentication.
- 2-factor authentication has no meaning without the appropriate policy.
- FICAM problem is the identity verification first (who are you online and get it proved).
- What happens during authentication?

➢ **Main topics of interest for the afternoon discussion:**

1. Process improvement
2. Information improvements
3. Documentation improvements
4. Comparability
5. Specific Programs + RPs (civil agencies) and C2G, B2G, G2G.
6. Usability

Other topics of interest:

- Future liability across the entire transaction.
- Alignment with the European framework and other frameworks.
- PKI vs non PKI
- Government metadata to prove identification verification.
- Registry of “names”
- Well-defined requirements for C, B, G.
- Terminology (unified terms and plan language).
- Simplify attributes bundles documentation (for a next round).

Highlights:

- FICAM needs a charter that defines the relationship PKI, TFS and other solutions. Operational procedures: Define the rules.
- Revise/update the requirements goal oriented rather than process oriented.
- Important to know which FRPs will be the first adopters, level of adoption. What the early adopters will need? So the CSPs can adapt the innovation to that.

➢ **Key discussion topics:**

- Equivalency in the framework with other frameworks and on assessments.
    - CSP need to certify against multiple frameworks- each scheme runs mostly independent of others and typically don't allow mutual recognition
    - Discussion about the role of NIST in standards setting - this might be a starting place to begin the equivalency work
- Connect.gov: challenges in adoption and usability by citizens.
    - Major issue dragging down adoption rate is usability - lots of friction in the system from handoffs between providers (because the handoffs are not anybody's direct responsibility)
    - CSPs would like to hear directly from RPs to be able to improve/enhance product faster
- Access to government.
    - FICAM thinks its a good idea to allow access to government datasets, but does not know what the path forward should be.
    - RPs are asking FICAM to make a mapping of the TFPs with differences and equivalences.
    - NIST/FICAM. FICAM should lead on discrepancies when NIST requirements are not align with the TFPs. Normalization for interoperability.
    - Standardize across the frameworks.
    - FICAM is reviewing the UK model. In the assessments they also include physical check.
    - OIDF started a working group to profile openid connect for government digital identity transactions. The wg name is iGov and we invite participants to join. The group is co-led by UK GDS, Ping Identity, and NIST.

➢ **Next steps:**

- Charters drafts via hub model.
- Matching services.
- Coordinate a meeting with the RPs to talk on particular areas.
- Meet quarterly – virtual and face-to-face.
- Work in demographics.