2016-08-10 Draft Meeting Notes

TFS Monthly Sync – Draft Meeting Notes

Wednesday, August 10, 2016

Attendees

Andrew Hughes, KI LC Chair

Colin Wallis, KI

Ken Crowl, Experian

Kevin Morooney, Incommon

Richard Wilsher, Zygma

Andrew Hatter, AYIN

Vlad Umansky, Athenahealth

Ann West, Incommon

Paul Caskey, Incommon

Nandini Diamond, GSA/FICAM

Ruth Puente, KI

KI IAWG Update

- Since May there have been discussion calls on 800-63-3 update and compilation of comments from those ad-hoc meetings. A comment matrix with almost 40 items was circulated to the Working Group before the submission to NIST through the GitHub system. Comments submitted are available at the IAWG wiki: https://kantarainitiative.org/confluence/display/idassurance/800-63-3+Review
- IDESG has prepared a comparison tool to see if the KI Service Assessment Criteria (SAC) meets the baseline requirements of the IDESG Identity ecosystem and how. The mapping is under IAWG review. IDESG has a Registry of entities that claim some level of meeting the baseline requirements, the concept is to use existing federations and TFPs communities to claim credit for some of these requirements. IAWG question: If a CSP is an approved KI entity what requirements are fully satisfied and what are partially satisfied? The catalyst of this pilot was the IDESG liaison to KI. The mapping is a learning exercise and the benefits are being evaluated. After the review of the process there will be more clarity on the way forward, as will then apply to other Trust Frameworks.
- IAWG is interested in reviewing the schema for attribute metadata, NISTIR 8112, which is for public comment until end of September, and will schedule a community discussion in parallel to the GitHub system. IAWG discussion link: https://kantarainitiative.org/confluence/display/idassurance/NISTIR+8112+Attribute+Metadata+community+review?src=contextnavchildmode

Incommon Update

- Incommon is looking to raise the level of trust across their participants, which includes not only identity assurance but also interoperability work and security related practices to service providers to ensure that the identity data is not compromised. They have been working on the Baseline practices for Identity Providers, Service Providers Federation Operators.
- Ongoing work on the Multifactor Authentication Interoperability profile, the Service Provider can request it to ensure that the user has used multifactor. It is a way of requesting a self -asserting that you use multifactor, in the future there may be a tag in the metadata associated to the service provider and identity provider and there will be requirements for that in trustmark fashion.
- Incommon is participating in a EU research group, the Federated Identity Management for Research Collaborations (FIM4R), where researchers provided solutions to the gaps they have identified. GEANT has leaded the report and The European Commission has funded parts of it. The paper includes, a Federated Internet Response mechanism, a framework for IdPs, CSPs and RPs to support federated Internet response when needed, and a security context that is shared through a shared metadata service. There is a global metadata service called eduGAIN, which aggregates metadata from research and education federations. There is also a tag or entity attribute that is shared in metadata that indicates which IdPs, Services Providers and RPs support this. It is relevant as currently there are not requirements to notify the service providers of a compromised credential. Link to the FIM4R paper: https://cdsweb.cern.ch/record/1442597/files/CERN-OPEN-2012-006.pdf
- FIM4R will introduce their own baseline assurance profile, possibly two levels, international profile that will be shared among the research and education federation operators and their participants.

- Trust marks and interoperability tags: In international federation operations, every country has its own indicator, its own tag with its own meaning, sometimes they are practices driven by regulations. Trust marks and interoperability tags are specific practices or set of policies. There will be trust marks everywhere and we will have to consider how we manage those from our own community perspectives.
- Incommon joined eduGAIN in February, and they are facing some challenges having an international aggregate, constraints on the signature validation and management of signatures in memory in particular the service providers. Incommon is trying to change the approach from a host file to a DNS mentality. IAWG and Incommon will interchange information about the Working Groups, OTTO and Per Entity Metadata, in order to merge efforts as both are related to OpenID Connect and metadata services for that. Per Entity Metadata Working Group (DNS for trust metadata delivery) link: https://spaces.internet2.edu/display/perentity/Per-Entity+Metadata+Working+Group KI OTTO WG link: http://kantarainitiative.org/confluence/display/OTTO/Home

FICAM

In relation to FICAM, some attendees raised the following issues:

- Concern on how the TFP Program will change and the impacts of the 800-63 revision.
- As a follow up of the January Workshop some participants are looking forward to contribute on how FICAM processes can be defined and improved.
- In order to make contributions on the implementation of the technical guidance, the participants need to know its context, scope and objectives.
- It was commented that in 2014 the TFs sent to Anil a letter with recommendations on how to make the FICAM Program more transparent and efficient and it will be reviewed to see if it still valid to re-send it to FICAM team.

Nandini Diamond, FICAM/GSA, provided her email (nandini.diamond@gsa.gov) for those who want to reach out FICAM team with recommendations or questions, and she will inform LaChelle LeVan and Chi Hickey accordingly.