

TFTM Meeting Notes for Standards 12 September 2013

Ann Racuya-Robbins Note taker

Discussed

Terms of Reference Draft

Project Management Lite demonstrated at the link below

https://www.idecosystem.org/wiki/TFTM_Deliverables

Very interesting—we may be able to adopt the wiki structure for our projects going forward.

Some of these work items can be done by other committees.

For our discussion:

Which areas from https://www.idecosystem.org/wiki/TFTM_Deliverables

might Standards be interested working on? Frame out deliverables on wiki?

Impression: When TFTM and Standards, Taxonomy, Security meetings overlap people just hop from one call to the other and try to coprocess. I thought the main reason that TFTM had to overlap Standards, Taxonomy, Security was to accommodate the previous Chair. If possible we should review the overlap. I will mention this to Andrew Hughes.

Does SCC think it would be useful to review the Survey for possible additions/corrections from a Standards point of view? There is a doodle poll out calling for interested parties.

Current survey language

Section 1. Your Information

1. Organization Name
2. Contact name
3. Contact email
4. Are you now a member of the IDESG? Yes or No
5. How would you describe your organization
Choose 1
 - a. Trust Framework Provider
 - b. IDESG Relying Party for Services
 - c. Potential IDESG Identity Provider
 - d. Vendor or Consulting partner for IDESG

Section 2 A

A. TF Analysis Questionnaire

(these questions are from NPO and need to be edited or reduced).

- I. What is the role of your organization with respect to Trust Frameworks (TF)?
 - II. Is there a specific community that you provide services to? If more than one, which ones?
 - III. What operational structures does your TF (or organization) have in place? How do they operate and what are their roles and responsibilities?
 - IV. What participants in your TF do you require to undergo certification and do you require third party certification? If you provide certifications, what types of participants do you provide certifications to?
 - V. Does your organization issue a trustmark?
 - VI. How are your certification criteria developed and assessed within the organization?
 - VII. What legal agreements exist within your TF and who is bound by these legal agreements? Do these agreements address liability within the TF and does that liability cover all participants?
 - VIII. How do you address violations of certification criteria or TF agreements? Do you have revocation policies? If so, please describe them.
 - IX. Based on your knowledge of the NSTIC Guiding Principles, does your framework adequately address all of them for all participants? If not, which one would you consider least covered?
- Privacy:
- I. Do you currently have measures in place to protect the privacy of participants within your TF? If so, please describe these measures and how they operate.
 - II. Do you have specific guidelines, criteria, and/or policies that define how protected information (PII, PHI, etc.) will be managed by participants in your TF, or those certified by your organization? Are these defined by regulation within the communities you serve or by the TF participants?
 - III. Do you have guidelines, criteria, and/or policies that address the privacy roles, responsibilities, and requirements of **all** participants in the TF? Are these part of a certification process for your TF and/or are these included in certifications that you conduct?
 - IV. Do tools exist within your TF to assist participants in the identification and mitigation of potential privacy risks? If yes, what are they?
- Security:
- I. Do you follow an established set of security requirements that define the roles, responsibilities, and requirements of all participants in your TF or certified by your organization? If so, please describe.
 - II. Do you operate, or assess participants against an established security and risk-based assurance models? If so if so, please describe.
 - III. Do tools exist within your TF to assist participants in the identification and mitigation of potential security risks? If yes, what are they?
- Interoperability
- V. Are credentials issued within your TF, or by organizations you have certified, currently accepted by other TFs? If so, which credentials and which TFs?
 - VI. Do you hold cross certifications or similar agreements with other TFs that facilitate interoperability and credential re-use? Are they effective means for facilitating interoperability and credential re-use?
 - VII. Do you implement, incorporate, or certify against specific standards, technologies, or solutions (Oauth, OpenID, etc.)? If so, which ones and why?

VIII. Easy to Use/ Cost Effective

IX. Do you have any policies, procedures, or guidelines in place that define usability requirements, roles, and responsibilities for participants in your TF or that you certify? If so, please describe.

Scoping Questions: Why build a trust framework? Please describe your community of interest and the reasons why a trust framework makes sense for you. What are the benefits and drawbacks? Please describe your Trust Framework model in terms of Business, Legal, Technical, Privacy and Audit/Certification. Please describe your monetization model or expected benefits to your community of interest. What are the resources required to develop and implement a Trust Framework in terms of level of effort and time?

- **Motivation/Monetization Questions:** Please describe how your Trust Framework participants benefit or make money. What sources of income will perpetuate your Trust Framework? How does your community save money, derive significant business advantages, or realize efficiencies to justify the costs involved? Do you measure outcomes in terms of revenues, cost savings or efficiency gains?

- **Accreditation and Certification Questions:** How are new technologies introduced to your Trust Framework? How do you implement Certification and Accreditation? How much does this cost initially and over time? Do you expect this process and set of requirements to change over time – how and why?

- **Trust Framework Interoperability:** What is needed to drive interoperability between Trust Frameworks? What are the pros and cons of an interoperable identity ecosystem in terms of business, legal, privacy, audit/certification, community motivations, and user experience?