General Comments

Recommendation: Tighten requirements language

Consider the guidance in ISO/IEC Directives Part 2, which provides requirements for the structure and drafting of international standards. This document is a valuable reference for authors of standards who wish to convey information in a clear and consistent manner. The document categorizes the expressions that can be found in a standards document into three types: statements, recommendations, and requirements. The definitions of these terms is useful to consider - a statement merely conveys information, while a recommendation indicates that one among various options may be preferred or more suitable under certain circumstances. A requirement is an expression containing criteria that must be fulfilled if compliance with the document is to be claimed.

The document stipulates that requirements are expressed using the verbs *shall* and *shall not*. We recommend that NIST adopt a similar syntax for expressing requirements. NIST SP 800-63-2 uses inconsistent language to describe its content with the result for potential ambiguity and misunderstanding by the reader. For example, Table 3 contains identity proofing requirements, but the syntax is a mixture of sentence fragments, narrative descriptions of procedures, and a few properly expressed “shall” type requirements. This table is the foundation for evaluating identity proofing implementations, and the current lack of clarity results in inconsistent implementations. Consider the rows labeled “basis for issuing credential.” It seems clear from context, but nowhere is it stated, that the contents of that row express criteria that must be met prior to issuance of the credential. Stating the contents of this row clearly as requirements, e.g. “applicant shall provide a valid, current government identity document,” allows the reader to understand what behavior is required and by whom.

Recommendation: Increase flexibility

Consider following the model of Common Criteria, in which a general requirements syntax supports the creation of Security Target and Protection Profile documents which are used specify the requirements that implementations must follow. Apply this conceptual approach to NIST SP 800-63-2 by restructuring the document to first define the syntax and terminology of identity assurance requirements in the areas of identity proofing, token management, credential management, etc.; and then to use that terminology to define Assurance Profiles that contain logically grouped sets of requirements. This permits the expression of OMB M-04-04 assurance levels as well as other sets of requirements developed for other purposes

NIST’s Questions

- What schemas for establishing identity assurance have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction? How do they differentiate trust based on risk? How is interoperability of divergent identity solutions facilitated?

- Could identity assurance processes and technologies be separated into distinct components? If so, what should the components be and how would this provide appropriate level of identity assurance?

  Token Manager, Identity Proofer, Credential Manager, Identity Register

- What innovative approaches are available to increase confidence in remote identity proofing? If possible, please share any performance metrics to corroborate increased confidence levels.

Recommendation: Add resilience to remote identity proofing

Incorporate NIST IR 7817 concepts of reliability and resilience to the model. Define requirements for identity proofers to notify credential issuers when information has discovered to have been breached, and processes for resolving and adjudicating remote identity theft.

Recommendation: Identify remote identity proofing for risk tailoring by RPs

Consider using the aforementioned profile approach to support scenarios in which remote identity proofing is not permitted. For example, relying parties that are government services pertaining to spousal conflict should be able to avoid the risk that a spouse's close relationships enables remote identity theft.

- What privacy considerations arising from identity assurance should be included in the revision? Are there specific privacy-enhancing technologies, requirements or architectures that should be considered?

Recommendation: Address privacy risks through user-centric risk assessment

As a consequence of being driven by a system-centric risk assessment, NIST 800-63-2 does not sufficiently address the privacy concerns of users. For the most part the document does not address core privacy principals identified by NSTIC (the TFPAP added some to the FICAM mix), but also fail to address privacy as it relates to selection of attributes to present to the world, e.g. a persona. For example, Steve operating as a private citizen (G2C) and accessing a government service has different privacy expectations than Steve, acting as an employee of Electrosoft and accessing a government system as part of a job assignment. One size does not fit all. Definition of privacy requirements and inclusion in certain profiles will enable identity services that meet a broader range of privacy needs.

Recommendation: Privacy Terms

Suggest incorporating the following privacy terms in the updated model:

- **anonymity**: the property of a service of not disclosing identifying information about users.
- **pseudonymity**: the property of a service that permits users to identify themselves by aliases and other unverified names.
- **reversible pseudonymity**: the property of a service that performs identity proofing during registration but permits users to identify themselves by aliases and other unverified names. Identified authorities are permitted to obtain the verified name of the user under controlled circumstances.
- **unlinkability**: the property of a service that prevents disclosure of multiple accesses of a service or resource by the same user.

- What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?

Recommendation: Electronic Authentication and Identification

Expand the scope to Electronic Authentication and Identification, reflecting the functional linkage of those two security mechanisms.

Recommendation: Note that “subject” and “subscriber” are synonyms in related specifications (e.g. X.509 vs 800-63)

Recommendation: “Subject” is often used with the same definition as “subscriber”, e.g. X.509 and related protocols. Suggest adding a remark that the term can be synonymous with subscriber.

Recommendation: “Identity” –> “Identifier”

The term “Identity” is a stubbornly difficult word to define, we recommend using the term “identifier” to mean “a set of attributes that uniquely describe a person within a given context” and do not define “identity”. To support the case when such an identifier is also a single attribute (e.g. a UID, national ID number, etc), add the term “unique identifier” with the definition “a single attribute that uniquely describes a person within a given context”.

Recommendation: Define “Context”

Context is used in the definition of identity/identifier, please define or remove from the definition. Section 5.3.1 states “all privacy requirements shall be satisfied”, recommend being clearer about which privacy requirements are intended.

Recommendation: Identity Register

Add to the model the concept of the Identity Register, which is the repository that maintains the binding between tokens and identifiers. This entity has certain privacy and security obligations that come with this role, including the protection of registration data for future dispute resolution balanced with user risk-mitigation goal of minimizing instances of PII. The Identity Register may provide support for federated authentication and identification and credential reliability and recovery services.

Recommendation: Elevate Biometrics

Biometrics should be a section in the document alongside Identity Proofing and Tokens. At high levels of identity assurance there is certainly a role for each of these different aspect of A&I. They answer the standard A&I questions (what you are, who you are, what you have, etc).

Recommendation: Address Liability

For the most part, Trust Framework Providers have not yet addressing the liability model for federated credentials, and NIST 800-63 does not address the topic at all. Technology does not stand in the way of expanding credential re-use, so much as concerns with permissible use and liability. Is the Credential Service Provider liable for damage done with a compromised credential? Under which circumstances? PKI and the CP is the only largely deployed trust framework that addresses the risks and limitations. Recommend that the document address the rights of the RP to recover damages and the limitations of risk for the CSP.

Recommendation: Decouple Identity Binding

Permit identity proofing to occur after token issuance.

- Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?

Recommendation: Risk Confidence Factors (?)

Instead of grouping assurance profiles solely as 1,2,3,4 per OMB M-04-04 requirements, permit the expression of risk confidence score with multiple factors including identity proofing, token strength, multiple factors, biometric verification, etc.

- What methods can be used to increase the trust or assurance level (sometimes referred to as “trust elevation”) of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.