Comments on NIST 800-63-3

Submitted by Tom Jones

The current version 3 is hard to apply with precision because the terminology does not match current or future scope of identity functionality. In particular, the range of use cases has grown into areas like finance and health care where the old models are inadequate. Also new technologies are in development for zero-knowledge proofs and self-issued identifiers with intelligent user agents that need even more drastic changes to the old models. This comment addresses the highest levels of a taxonomy for identifier management. It is to be expected that clarifications at this top level should be expected to ripple down throughout the specifications. This taxonomy is specifically designed to be human-centric, which is really the only purpose of an identity system as defined in 800-63. Specifically, it is a requirement that any digital entity (such as a web site) fully identify itself to a human before it is permitted to ask for any human identity information. This requires rethinking identity to being a bilateral transaction where the identity of the web site has similar requirements to prove its identity and what assurances it gives the user in pretty much the same terms that the user has to prove their identity. A major component of that assurance to the user is the level of privacy that the promise to deliver.

Another object of version 4 should be a move away from the simple presentation of user attributes for IAL and AAL level determination to a distributed model where a variety of trusted sources provide a variety of strong assertions about the identity, assurance and presence of the user to the Relying Party based on the stated needs of that Relying party. This will enable many of the user attributes to be hidden behind walls that block user data from passing to the Relying Party, while giving the Relying Party the assurances that they need. We already have examples of this technology in place with the remote attestation of computer systems that are protected by a TPM. Since all modern smart phones come with a Trusted Execution Environment, that capability can be utilized to help protect user privacy by providing assurance with little or not user attributes.

Here is a start of one way to clarify the meanings of real world and digital entities that are involved.

1. Real-World entities:
    1.1. Human users
    1.2. Legal enterprise (corporations, government entities, AIs in Saudi Arabia, etc.)
    1.3. Legal names: brand or dba (particularly those that are known to human users)
    1.4. Pseudonymous users
2. Digital representations of Real-World entities
    2.1. Subjects of discourse (human or other, may be the end user of the interchange)
    2.2. End-users of computers systems (often assumed to be human)
    2.3. Delegates which are end-users that have been give rights of access by others.
    2.4. Addressable digital endpoints (typically refers to api endpoints)
    2.5. Web Sites without identity roles accessible by browsers (at least https going forward)
        2.5.1.URL (just a unique address)
        2.5.2.Legal owner (either 1.1, 1.2 or 1.3 – 1.4 is disallowed in identity systems.)
        2.5.3.Web Identifiers, Manifests, etc. (already in development)
    2.6. Identity Provider – a bucket of identity roles to be determined from the list below.
    2.7. Credential Service Provider – a bucket of identity roles to be determined.

2.8. Credential Provider – seems to be an amalgam of the two above.
2.9. Certification Authority – usually an RA and a verification function.
2.10. Federation Authority – a registry and other identity roles as determined by the federation.

3. Roles
   3.1. Registration Authority
   3.2. Identity issuing function (may be the same as an RA)
   3.3. Registry – an official list of semantics and perhaps of certificates.
   3.4. Identity Proofing function
   3.5. Authentication proofing function
   3.6. Federation that controls the terms of membership of users and sites.
   3.7. Proof of presence function
   3.8. Proof of financial responsibility functions (some financial enterprise.)
   3.9. Authorization or grant function
   3.10. Certificate of membership or achievement (may be just a grant)
   3.11. Verification or attestation function – can both issue and validate assertions
   3.12. Trust registry – a searchable attestation function
   3.13. Web site storing user information (PII)
      3.13.1. Requestor of PII (aka client)
      3.13.2. Source of PII or other resources (aka. resource server)

The Authenticator

It is likely that user smart phones will become the source of identity for most users. It is therefor important to expand 63B to specially target that source of identity information. Kantara was been focused on how the behavior of the patient would interact with a hospital's electric health records as an example of this in these two areas:

Patient choice

Phone as Health Care Credential

Kantara and the author would be please to work with NIST in expanding the scope of 800-63-4