kantara INITIATIVE

Ruth Puente <ruth@kantarainitiative.org>

[WG-IDAssurance] 800-63-3 comments

Andrew Hughes <andrewhughes3000@gmail.com> Thu, Aug 6, 2020 at 12:42 PM
To: IAWG <wg-idassurance@kantarainitiative.org>

Hi - a couple comments that I don't think I see in the group response.- please consider:

* As described in the NIST SP 800-63-3 Implementation Guidelines and 800-63-3 Conformance Criteria publications, identification credentials such as REAL ID and Federal Agency authorized identification credential equivalents (REAL ID, Enhanced ID, US Military ID) have a "special" status somewhere above STRONG evidence and somewhere below SUPERIOR evidence. These supplemental publications have invented a "STRONG+" category. STRONG+ evidence issuers in effect, are deemed to employ sufficiently robust ID Proofing processes that can be relied on by CSPs without requiring that CSPs explicitly evaluate those issuer ID Proofing processes.
Consider explicitly stating the underlying conditions that shall indicate what issuers are deemed to employ sufficiently robust ID Proofing processes. For example, for REAL ID cards, each State DMV is authorized by DHS to issue REAL ID cards. That authorization is the indication that the specific DMV complies with the REAL ID rules as enforced/evaluated by DHS.
Alternatively, NIST could explicitly list 'known strong' issuer programs TWIC, PIV-I, CAC, US Passport, PRC etc. This approach would imply that NIST authorizes use of credentials issued by those programs as identification evidence at documented strengths used by applicants to claim an identity. The first option is preferred (reliance on authorization from a recognized authority).

* Consider a more explicit shift from document-based evidence towards electronic access to authoritative record evidence for identity proofing processes. For example, binding verification at IAL2 requires the CSP to physically compare the applicant to the strongest presented evidence. However, if the CSP is able to compare the applicant to the authoritative record on file at the issuing source, the current 800-63-3A does not indicate that this is acceptable. Which raises the question: if the goals of ID Proofing include confirmation that the applicant is the same individual as recorded in the authoritative source record, which is 'better': comparison to a physical document (or photo of a physical document if unattended) or comparison to a 'photo-on-file' of the applicant? We suggest the latter should be preferred.

* Guidelines for Credential Lifecycle Management and the role of Credentials in Digital Identity are missing in 800-63-3. However, throughout the volumes, credentials are frequently invoked and lifecycle management of credentials is strongly implied. After all, the *Credential* Service Provider is the entity to which 800-63-3 is directed!
Without explicit treatment of credentials, topics such as 'authenticator binding', derivation of credentials, use of multiple authenticators, and 'bring your own authenticator' are convoluted. The reality of CSP implementations is such that the CSP creates, issues and activates a credential for a subscriber and that credential serves as the binding object between the outcome of the Proofing process, the subscriber and any appropriate Authenticators. If there is no strong concept of 'credential' then the CSP has to try to figure out how to represent all the different bindings (device, app, person, authenticators, identity records, service records, etc) and also invent how to handle 'credentials' that contain data, cryptographic material (keys are not authenticators), etc. By explicitly recognizing 'credentials' and their lifecycles, 800-63-3 could enumerate threat categories for which controls are required.
Consider adding a new, substantial, section on Credentials and Credential LIfecycle Management.

* Kantara Initiative and ISO SC 27/WG 5 have, for the last several years, been developing standards and specifications related to notice, consent and 'consent receipts'. These publications should be used as inputs into future versions of 800-63 as they highlight and enhance the privacy-related requirements in the current 800-63-3 publication. In particular the concept of a 'consent receipt" (See Consent Receipt Specification 1.1.0. Kantara Initiative Consent & Information Sharing Work
32 Group. 2018-02-20. Kantara Initiative Technical Specification Recommendation.
33 https://kantarainitiative.org/file-downloads/consent-receipt-specification-v1-1-0/) is a personal record that memorializes events where a service provider has obtained consent of the individual for data processing. These receipts are powerful personal recordkeeping records that enable the individual to understand where their data has been shared and to initiate recourse processes if necessary.

And here's one that the Better Identity Coalition is planning to submit, that Kantara should consider amplifying:

- *Consider providing performance metrics for selfie-to-credential face matching.* The use of these tools has exploded in the market since NIST guidance was last updated in 2017. Groups including FIDO Alliance have launched new programs to develop

performance requirements and certification programs for these new remote ID verification tools. It may be helpful for NIST to provide guidance as to the acceptable FAR/FRR of biometric matching in these tools.

Andrew Hughes CISM CISSP
In Turn Information Management Consulting

o +1 650.209.7542
m +1 250.888.9474
5043 Del Monte Ave., Victoria, BC V8Y 1W9
AndrewHughes3000@gmail.com
https://www.linkedin.com/in/andrew-hughes-682058a
Digital Identity | International Standards | Information Security