Consolidation Comments on 800-63-3

General comments

CSPs main concerns regarding cost and impacts of the changes.

GitHub Comment #1067 – March 31, 2017

Substantial impact

a) Reducing the number of assurance levels from 4 to 3 will increase the cost as well as user friction. It will also reduce the performance of existing solutions.

b) Existing credentials will need to be re-proofed because of both the changes of applicable assurance levels and the changes in the proofing requirements. This will have high economic and time investment.

c) There are technical challenges of document verification requirement for every remote identity proofing transaction (lower success rate of Identity Proofing and user friction).

d) Because of a, b and c getting service implementations to be compliant with the revised standards will take time. As such, there needs to be consideration of the timeframe and roadmap for implementation.

e) There are technical challenges with requiring validation using the “issuing source”.

f) Due to the high level of significant comments that Kantara has submitted, we believe that this document should not go to publication without additional industry review.

SP 800-63A

Document Verification for all remote proofing (validation of driver´s license and passport).

GitHub comment #1068 – March 31, 2017

- Kantara is currently unaware of any real time automated mechanisms for validating driver's license. As such, the only viable implementations are PKI or self-assertion.
- Financial institutions will also have difficulty verifying these sources. Negotiating individual contracts with different states for driver's license validation would expand costs considerably, if it were even possible.

Technical challenges to document verification

a) While current technology does exist to allow the digital capture of a document and then compare that image to a 'selfie' image of an individual, it is a very cumbersome and much more costly procedure. In addition, it can be inaccurate depending on quality of document as well as the capability of person trying to capture image. As such, this will result in a much lower success rate of Identity Proofing and which will increase user friction. It is Kantara's position that many agencies and organizations are not looking to provide more friction for their clients.

b) Kantara also believes that this approach requires clients to provide documentation that they may not feel comfortable in providing (e.g., Driver's License or Passport). Many document verification solutions also are limited to the types of documents that can be scanned or captured and these are typically Driver's Licenses and Passports. Kantara also believes that there is a limited population that has access to these types of documents. Many younger as well as the older demographic may not have a driver's license and less than 50% [1] of the U.S. population has a passport. If services are restricted to only these two forms of identification then the population able to use

[1] The Expeditioner, "How Many Americans Have a Passport" December 2016, http://www.theexpeditioner.com/2010/02/17/how-many-americans-have-a-passport-2/

services may be significantly restricted.

***Recommendation**:* Document verification should not be a requirement for every remote identity proofing transaction. Kantara suggests that there is a need for intermediate verification options that don't require the full rigor of IAL2 (remote + document verification).

Kantara believes that document verification can and should play a role in the identity proofing process. Document verification would be a viable solution in situations where it would be necessary to provide an extra layer of verification (i.e., there might be limited data available).

Issuing Source

GitHub comment #1069 – March 31, 2017

References: 4.4.1.2; 4.5.2; 5.2.1.1 Table 5-1; 5.2.2.1 Table 5-2

NIST has classified the levels of evidence that can be used into four categories (Weak, Fair, Strong, and Superior). Each category indicates that information is validated against the "issuing source". Most data validations today are not performed directly against an issuing source (such as a bank for credit card or a DMV for driver's license) but against an authoritative source (such as a credit bureau) that affirms the information and assumes that the process the "issuing source" used to create the data performed proper vetting of identification at the time the data was created. For example, the process of obtaining a new Driver's license requires in-person verification along with providing many forms of identification before the new Driver's License is issued. Kantara believes requiring validations using the "issuing source" is unrealistic and many Identity Proofing solutions will not be able to provide this level of validation.

As mentioned above, document verification will be required for all IAL2 transactions. In today's environment, the pieces of documentation that contain both PII and photo/image/biometric data are extremely limited. For the majority of the U.S. consumers, that would be either a driver's license or a passport or possibly a US Resident Card. Although information contained in these documents can be validated, today the data typically cannot be verified directly against the issuing source. Meaning there is not a method of directly going to neither the state that issued the Driver's License nor the State Department that issued the Passport document. Document verification technology today is looking at the 'correctness' of the document, meaning it is looking at format, holographic images, watermarks, positioning of text and abnormalities of the physical document. It is not looking at the PII data and comparing it directly against a database (of sorts) to confirm that the state or country actually issued

this document.

Recommendation:

NIST should either provide further clarification on this requirement or make prevision for the use of an authoritative source for verification of PII information contained in the document. Using an authoritative source allows verification of the PII using validated and verified data to confirm that the PII information is accurate while still allowing the document verification technology to verify the validity of the document.

Reduced Assurance Levels from 4 to 3

GitHub comment #1070 – March 31, 2017

Reference: Section 7

- The simplification of the levels from four to three may have made it more difficult to obtain the levels. Kantara believes that it removes the lower cost category and increases the cost to comply.
- In order to achieve IAL level 2 would require that at least one piece of STRONG evidence be used. By definition, a STRONG level of evidence must contain a photo/image/biometric of the individual. NIST has confirmed this to mean that some form of remote document verification technology would be required in order to verify the photo/image/biometric. Kantara feels that this is too restrictive and does not provide agencies and organizations enough flexibility to determine the level of Identity Proofing needed for given situations. Kantara further believes that having only one level of remote identity proofing (IAL2) which, as it currently is written, requires document verification, creates an undue burden on agencies and organization to have to provide this level of proofing for every remote transaction. Kantara believes that this would significantly increase the cost and user friction as well as reducing the performance (pass rate) of existing solutions – particularly those that currently leverage LOA2.

  Recommendation:
  NIST to return to 4 levels of IALs to provide more flexibility with the following structure:

  - IAL1 – No Identity Proofing required (Self-Asserted)

  - IAL2 – Remote Identity Proofing using verification of government ID and financial/utility account (this utilizes current LOA3 Identity Proofing

capabilities)

- IAL3 – Remote Identity Proofing at IAL2 level plus the addition of document verification

- IAL4 – In-person Identity Proofing

SP 800-63B

Reference: Sections 2 and 4.

GitHub comment # 1071 – March 31, 2017

1) Kantara believes that there is inconsistency in the use of the term "digital service" in the introduction to SP-800-63-B. Section 4 uses the term as if it refers to the Credential Service Provider, whereas the introductory text uses the term as if means the Relying Party.
   Recommendation: Clarify the term.

GitHub comment #1072 – March 31, 2017

2) Subscriber vs subject, lack of clarity of the concepts.
   - Part of the model inconsistency is differences in how the verb "authenticate" is applied. For example, does the subscriber authenticate or does the CSP do the authentication?
   - There is extensive reference to the "subscriber" whereas other schemes include "subscriber" and a "subject". While the “subject” and the "subscriber" may be the same individual, there are many use cases where the subscriber is the individual or organization that wants credentials issued for one or more subjects (e.g., power of attorney, tax preparation firms, old age homes).
   - There are inconsistencies in the overall lifecycle model in different sections of the text. You become a subscriber because you have enrolled, the definition of enrollment doesn't include the definition of a service account. Since they are unclear on the enrollment process it is not clear what the subscriber is.

   Recommendation:
   Define subscriber and subject and ensure those terms are used consistently in the text in alignment with recognized international sources (e.g., ETCI, Kantara Initiative Inc., international standards).

GitHub comment #1073 – March 31, 2017

3) The state model for transitions between non-authenticated and authenticated states is not clear - a diagram would be helpful.
   Recommendation: Create a state model to show how entities go from non-authenticated to authenticated state, verifiers in pre-authenticated to post-authenticated state.

GitHub comment #1074 – March 31, 2017

4) In items 4.1.4, 4.2.4, 4.3.4 there are references to 800-53 "or an equivalent industry standard". However, no method of judging what an equivalent standard is identified.
   Recommendation: Provide the criteria to determine an equivalent standard in all relevant places in the document.

GitHub comment #1075 – March 31, 2017

5) Section 4.5, summary of requirements: there are not rows for records retention or privacy requirements.

   Recommendation: Add to the summary records retention and privacy requirements.

GitHub comment #1081 – March 31, 2017

6) There are currently no normative usability requirements, is this intentional?

Typos, language, title and others

GitHub comment #1076 – March 31, 2017

1) Item 4.2 of SP 800-63C - requirements on federal agencies.

   Recommendation: Include it in an annex instead of including in the rest of the flow of the document. The agency guidance at the end of the privacy section is a non sequitur with respect to the rest of the document

GitHub comment #1078 – March 31, 2017

2) Need to uniquely identify clauses in the requirements. Uniqueness of requirements clauses is great assistance to implementers and assessors alike.

Recommendation: Use numbers instead of bullets, so that requirements could be uniquely identified.

GitHub comment #1079 – March 31, 2017

3) The documents are called "guidance" but they contain requirements. The documents are a mixture of explanatory material, guidance material and requirements material. ***Recommendation***: Change of title and adopt a normative style.

GitHub comment # 1087 - March 31, 2017

4) The shift towards normative language in the requirements is appreciated. However, the phrasing of some requirements makes it difficult to have certainty that an implementation meets those requirements. As assessors there is also uncertainty about how to evaluate conformity. Uncertainty then leads to inconsistency. ***Recommendation***: Clean up the text to separate (i.e., have in separate paragraphs) normative requirements and non-normative suggestions.

GitHub comment #1080 – March 31, 2017

5) Audience section of 800-63-3 is blank. ***Recommendation***: Add an audience section.