Date: September 3, 2019

To: Ken Dagg, Chair, Kantara Identity Assurance Working Group

 Colin Wallace, Executive Director, Kantara Initiative

From: David Temoshok, Senior Policy Advisor, Applied Cybersecurity, NIST IT Laboratory

Subj.: Request for NIST Review and Action on Kantara Initiative’s Interpretation of NIST SP 800-63-3 Requirements

Thank you for your memorandum raising inquiries regarding NIST Special Publications 800-63A and -63B. We appreciate that the Kantara Initiative has developed a component of the Kantara Identity Assurance Framework (IAF) to address SP 800-63-3 requirements at IAL2 and AAL2. We see this as an important initiative to expand the scope of SP 800-63-3 beyond federal agencies to commercial service providers and industry.

We are happy to provide clarification and explanation of the requirements and text in SP 800-63-3, -63A and -63B to address the issues raised in the Kantara Initiative memo and Implementation Reports. However, we feel it is necessary to explain our authority and role in this capacity so there are no misunderstandings.

* NIST is responsible for issuing government-wide guidance for federal agencies in order to meet the statutory requirements of the Federal Information Security Modernization Act (FISMA). NIST IT Laboratory develops and issues Special Publications in the SP 800-XXX series to meet this responsibility. SP 800-63-3 *Digital Identity Guidelines* is one of the sets of information security guidelines issued by NIST to implement FISMA. Federal agencies are required to implement NIST SP-800-XXX guidelines to meet their requirements under FISMA. Non-federal entities may voluntarily adopt any of the NIST SP 800-XXX standards as information security requirements or security implementation guides.
* NIST Special Publications issued as final are normative. Errata may be subsequently published to make editorial corrections to published text. Special Publication errata may not create or modify any normative requirements in published text. The only way to change normative text in a Special Publication is to develop and issue a revision to the Special Publication.
* NIST IT Laboratory can respond to inquiries and information requests from federal and non-federal sources regarding NIST Special Publications. Responses to inquires must be informational and non-normative. NIST IT Laboratory publishes Frequently Asked Questions (FAQ) regarding SP 800-63-3 at: <https://pages.nist.gov/800-63-FAQ/>. Non-federal inquiries regarding NIST Special Publications, including SP 800-63-3, should be directed to the email address: <digcomm@nist.gov>.
* NIST does not have the authority to approve, authorize, or otherwise oversee federal agency implementation of NIST Special Publications. Federal agencies are responsible for the assessment, accreditation, and authorization of information technology systems and controls under FISMA. NIST is responsible for providing federal agencies with guidance, clarification and information associated with any of the NIST publications and guidelines.
* NIST does not have the authority to approve, authorize, or otherwise oversee non-federal agency implementation of NIST Special Publications. This includes non-governmental identity management trust frameworks such as the Kantara IAF. Outside of NIST evaluation and validation programs, NIST does not have authority to oversee non-federal voluntary implementation and/or interpretation of NIST Special Publications. Please see the attached Office of Management and Budget Policy Memorandum M-19-17 for additional clarification of these federal responsibilities and roles.

The Kantara Initiative has requested that NIST review five Implementation Reports and provide guidance “in the form of an erratum to the necessary clauses of the suite as a whole.” Please note that the five Implementation Reports do not present editorial corrections that can be made through the issuance of SP 800-63-3 Errata. Consistent with the foregoing explanation of responsibilities and authorities, we will present clarification and discussion of the issues presented in the Kantara Implementation Reports in terms of inquiries for NIST response (e.g., SP 800-63 FAQ).

1. Guidance on Selection of Authoritative Sources

A strict interpretation of the standard and the Service Assessment Criteria would lead to the conclusion that strong evidence could be validated only by a single authoritative source that either issued the evidence or had direct access to the issuer’s data.

To the best of our understanding, there is no commercially available service that can validate this strong evidence for the majority of the US population. The Driver’s Privacy Protection Act (CFR 18 U.S. Code § 2721) requires that DMVs treat photographs as “highly restricted information” not to be divulged without express consent or for some permissible uses (which do not include the issuance of digital identity credentials).

SP 800-63A 4.4.1.3. Validation Requirements states: *Each piece of evidence SHALL be validated with a process that can achieve the same strength as the evidence presented*. SP 800-63A and Table 5-2 Validating Identity Evidence require that identity evidence be validated at STRONG strength by examination that the evidence is confirmed as genuine and that *all personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).*

As stated, this requirement would include the comparison of pictures on state driver’s licenses to DMV records or another authoritative source.

**RGW** – given the provisions of the Driver’s Privacy Protection Act, no such comparison is going to be possible. And DHS doesn’t offer any such facility wrt PP photo matches / release.

When this confirmation is not possible, the CSP must confirm the validity of other personal and evidence details as valid with the issuing or authoritative sources.

**RGW** – notwithstanding the pre-amble, is this a formal statement interpretive statement of the cited -63A clause on which Kantara might rely?

***If so it effectively removes the need to perform any photo-matching since if it is acceptable that it can be omitted if it is just too tough then it may as well be omitted for all, since the net proofing assurance will always be determined by the LCD*** (effectively the opposite to FIPS 199’s approach with establishing security requirements).
**This is a key point in trying to gain any value from this response.**

The CSP must also examine the evidence (the driver’s license) to confirm that it has not been tampered with, including both the photo and other evidence details.

**RGW** – this can be accomplished by some smart online apps, but the ‘also’ is the rider which makes the

A strict interpretation of the standard and the Service Assessment Criteria would lead to the conclusion that strong evidence could be validated only by a single authoritative source that either issued the evidence or had direct access to the issuer’s data.

SP 800-63-3 defines the term authoritative source as: *An entity that has access to, or verified copies of, accurate information from an issuing source such that a CSP can confirm the validity of the identity evidence supplied by an applicant during identity proofing. An issuing source may also be an authoritative source. Often, authoritative sources are determined by a policy decision of the agency or CSP before they can be used in the identity proofing validation phase.*

This does not limit validation of strong evidence to a single authoritative source, although, as noted, the CSP may establish this limitation by policy decision. The authoritative source should have direct access or verified copies of the evidence or otherwise be able to demonstrate traceability to the issuing source. If an entity has information that came directly from an issuing source or can trace the information path back to the issuing source, then it may be considered authoritative.

**RGW** – accepted that it is not correct to say “could be validated only by a single authoritative source” – potentially multiple auth srcs could be used, but I think the intention of the original point was that only one of them needs to meet the requirements of the definition of ‘auth src’, which ultimately requires that the auth src has access to the issg src. The definition does not allow for the authoritative source to gain its authority by any depth of corroboration.

Essentially, by definition, the only possible relationships are:
 **CSP <= => Issg Src** or
 **CSP <= => Auth Src <= => Issg Src**

So the problem remains that, e.g. a DL or a PP, while all sorts of alternative validations and corroborations can be performed, a CSP cannot, universally, gain verification from the issg src. Hence the key point above remains the stumbling block.

1. Impasse on KBV approval for IAL2

In an effort to evaluate compliance with the NIST 800-63-3 and determining the feasibility of KBV to pass compliance for IAL2, the latest Kantara Service Assessment Criteria V3 (filename “KIAF 1430 NIST SP 800-63A Service Assessment Criteria v3.0.pdf”) does not give a pathway for success and presents an impasse.

This inquiry appears to be asking for a way to leverage Knowledge Based Verification (KBV) to meet identity proofing requirements at IAL2. NIST SP 800-63A section 5.3 specifies that KBV can only be used for identity resolution and for identity verification of a single piece of identity evidence at the “fair” level (on the scale of unacceptable, weak, fair, strong, and superior). This restriction stems from the wide availability of the KBV answers to potential impostors, and therefore presents very limited strength to the verification process. SP 800-63A section 5.3.2 presents restrictions and guidance for how KBV can be used for these very limited purposes. The objective of the verification phase in identity proofing is to bind the validated identity evidence from the validation phase of identity proofing to the real-world identity of the applicant. SP 800-63A section 5.3 and Table 5-3 present a graduated scale for methods that may be used to bind validated identity evidence to the claimed identity. Therefore, KBV could never be used exclusively for verification of such binding. Additional verification of such binding is always required for identity evidence beyond KBV in order to meet IAL2 for SP 800-63A.

**RGW**: RQ has commented on this and I have nothing to add.

1. Consistency of terms describing proofing types

The Kantara Implementation Report cites confusion with the terms in the table below.

|  |  |  |
| --- | --- | --- |
| **Ref** | **term / phrase** | **§ ref** |
| **1** | **remote** or **in-person** identity proofing | 4.4, 4.4.1.5 |
| **2** | **in-person proofing (physical or supervised remote)** | 4.4.1.6 (4) |
| **3** | **remote proofing (unsupervised)** | 4.4.1.6 (5) |
| 4 | In-person proofing … either … physical [or] remote | 5.5.3 |
| 5 | Supervised Remote In-Person Proofing | 5.3.3.2 |
| 6 | in-person … same physical location | 5.3.3.2 |
| 7 | Supervised remote identity proofing | 5.3.3.2 |

The terms “remote” and “in-person” are used as dictionary-defined terms and, as such, are not further defined in SP 800-63-3. Remote identity proofing represents an identity proofing session where the CSP and the applicant are in separate locations, not meeting face-to-face, with communications over a network. In-person identity proofing is a face-to-face session in the same location between the CSP and the applicant.

The term remote proofing (unsupervised) represents an identity proofing session where the CSP and the applicant are in separate locations with communications over a network and the controls for “supervised remote identity proofing” specified in SP 800-63A section 5.3.3.2 are not required or applied.

The use of the term “supervised” has special meaning when it is used to define identity proofing in SP 800-63A. The term “supervised remote identity proofing” means that the requirements and controls for identity proofing sessions specified in SP 800-63A section 5.3.3.2 Requirements for Supervised Remote In-Person Proofing are applied. SP 800-63A section 5.3.3.2 requires specific physical, technical and procedural controls so that supervised remote identity proofing can be considered equivalent to an in-person identity proofing session and, therefore, meet the in-person presence requirement for IAL3.

SP 800-63-3 Definitions presents the following definition for supervised remote proofing:

*A remote identity proofing process that employs physical, technical and procedural measures that provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process.*

Please note that this question is addressed in SP 800-63-3 FAQ A2 posted at <https://pages.nist.gov/800-63-FAQ/>.

**Q-A2:**

What is the difference between supervised remote identity proofing and unsupervised remote identity proofing?

**A-A2:**

[Supervised remote identity proofing](https://pages.nist.gov/800-63-3/sp800-63a.html#supervised) is an equivalent approach to in-person proofing and requires a robust set of features. This includes high-resolution video monitoring through an agency-controlled device (e.g., not an applicant’s personal phone), a trained operator on the other end of the video, and a number of other security controls. If those controls are all met, supervised remote identity proofing can achieve IAL3. Supervised remote identity proofing is also perfectly fine for IAL2. Unsupervised remote proofing can be used for IAL2 but not IAL3. It does not require that a remote operator participate in the session with the applicant, and typically involves commodity hardware and services that users and agencies can easily access.

**RGW**: this wasn’t looking for an explanation of what the types of proofing were. The point was that more consistent usage of terms would avoid a degree of inconsistent terminology, i.e. use one term for one thing and don’t mix it (which the SP undoubtedly does) but evidently that is not seen to be a matter of concern.

1. Scope and Application of ‘Trusted Referees’

Given the vagueness of the requirements and the mixed terms used, one could conjecture on a TR being realized in two different ways. One is where the TR has antecedent knowledge of the applicant, e.g. is the applicant’s neighbor, accountant, physician, … In this case, the TR is more of an Applicant’s Referee who would act on behalf of the applicant to persuade the proofing CSP as to the applicant’s claims of identity being true.

The other case is where the TR has no antecedent knowledge of the applicant and is acting on behalf of the CSP (and potentially an agency, where that is managed by the CSP).

Please note that this issue is addressed in SP 800-63-3 FAQ A1 posted at <https://pages.nist.gov/800-63-FAQ/>.

**Q-A1:**

What is the difference between the conventional proofing process and using a trusted referee at IAL2?

**A-A1:**

We recognize that the language in the document is somewhat confusing. In our attempt to use standards-based terms like SHALL and SHOULD, avoiding terms like “unless” and “if,” this section got a little bloated. The requirement, in layman’s terms, is that agencies should make every effort to proof individuals according to the [conventional proofing process](https://pages.nist.gov/800-63-3/sp800-63a.html#normal) laid out in Section 4.4.1 of SP 800-63A. However, we know there are scenarios where the conventional proofing process, either remote or in person, is not going to work for all constituents. In other words, some individuals will just not be able to pass the conventional process or even have the identity evidence required by the conventional process. Nonetheless, we don’t want this to be a barrier for, say, a homeless veteran with no, or a lack of, documentation. This is why we added the ability to use “[trusted referees](https://pages.nist.gov/800-63-3/sp800-63a.html#referee),” such as notaries, that can assist agencies in establishing a digital identity for the applicant. This gives agencies greater flexibility to determine what works best for their stakeholders and their risk tolerance. Ultimately the agency needs to define a process, but there is a catch or two. First, trusted referees can be used to achieve IAL2, but not IAL3. Second, as an individual builds, or rebuilds, evidence of their identity, we want agencies to regularly attempt to re-proof any individual who has completed the trusted referee process via the conventional process.

In addition to the posted response, it is intended that the use of trusted referees will involve applicants (particularly members of the public) that are not able to complete enrollment, potentially as the result of a disability or other circumstance that makes conventional identity proofing difficult or infeasible. The use of and procedures for trusted referees is intentionally flexible in SP 800-63A to allow CSPs to determine the most appropriate processes to meet the needs of their intended applicants.

**Therefore, trusted referees may be representatives of the CSP or representatives for the applicant, depending on the CSP’s intended applicants and defined procedures.**

**RGW**: This appears to be a definitive statement that a TR covers both the types conjectured in Kantara’s report. I think there might be scope for clarification of Kantara’s requirements for a TR, depending on the mode of participation/representation of the TR, e.g. ‘Applicant’s TR’, ‘CSP’s TR’, since I think that more specific criteria could be devised to govern the two different modes of TR involvement?

1. Guidance on Permitting “Commodity” Hardware for Unsupervised Remote Identity Proofing

Kuma concludes that applicant-owned (i.e. ‘commodity’) hardware is permissible for unsupervised remote identity proofing at IAL2. The wording of the FAQ seems to imply that applicant-owned hardware would also be permissible for supervised remote identity proofing at IAL2, but not at IAL3. Therefore, we recommend removing this provision by limiting the respective criteria to biometric authentication, not for identity verification.

The verifier is still required to make a determination of camera/endpoint performance, integrity and authenticity, but other methods are permitted aside from authentication of the endpoint.

To clarify, it is correct that applicant-owned devices (e.g., commodity hardware) are permitted for remote identity proofing (unsupervised) at IAL2. As discussed under item #3, The use of the term “supervised” has special meaning when it is used to define identity proofing in SP 800-63A. The term “supervised remote identity proofing” always means that the requirements and controls for identity proofing sessions specified in SP 800-63A section 5.3.3.2 Requirements for Supervised Remote In-Person Proofing are applied.

Therefore, applicant-owned devices are not permitted for supervised remote identity proofing but are permitted for remote identity proofing (unsupervised) at IAL2.
**RGW**: So this confirms Scott’s finding and established that as acceptable practice.

We recognize the challenges associated with authentication of the end point for identity verification purposes and are examining this SP 800 63A requirement for a potential change.

**RGW**: So why are other challenges not also being examined, e.g. DL/PP verification?