Kantara Implementation Guidance Report

**ID:** 2018-K-02 ver 2.0

**Subject:** Guidance on Selection of Authoritative Sources

**Date:** 2019-06-27  
**To:** Kantara Assurance Review Board, Kantara Identity Assurance Working Group

**CC:** NIST, GSA

**From:** Kuma LLC

**Co-signed:** ID.me, Zygma

**Background:**

Certain requirements within NIST SP 800-63 rev.3 appear to be very difficult for commercial service providers, and likely most CSPs operating under the auspices of agencies, to fulfill. Such a case would be a specific part of SP 800-63A, §4.4.1.3, which is captured in KIAF-1430 as follows:

|  |  |
| --- | --- |
| **SP 800-63A §4.4.1.3 Validation Requirements** | **KIAF-1430** |
| Evidence for more information on validating identity evidence. | ***63A#0230*** *The CSP SHALL document its justification, for each form of evidence it recognises and collects in fulfilling its CrP and these criteria, of how the strength of validation of the evidence it collects satisfies the qualities identified in Table 5‑2 [see worksheet 63A\_T5-2].* |
| **Table 5-2 [STRONG/SUPERIOR]** 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). | ***63A-T5-2#strg/supr b)*** *The CSP can demonstrate that the evidence which it has collected has had all personal details and evidence details confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).* |

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. Furthermore, there are reasons to believe that no such service could emerge under current law. 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).

Based on guidance from the Kantara ARB, the assessor considered possible compensating controls that could be used when the strict definition of authoritative sources was not available. The result of this analysis was that we expect two features in the necessary compensating controls – geolocation verification, and risk scores based on transaction history.

We noted that strong evidence includes physical or biometric features, which requires that the issuer capture those features from the applicant during a face-to-face enrollment process. We believe that this face-to-face enrollment is an intended feature of the standard; because it provides assurance that the applicant has physically appeared in the jurisdiction in which the license was issued.

Based on that analysis, one could conclude that in the absence of an authoritative source that can directly access issuer data for strong evidence, compensating controls could include some form of geolocation verification.

Furthermore, Drivers Licenses are subject to inconsistency of policies and procedures between the states. Most jurisdictions permit reissuance of licenses without an in-person transaction, so the face-to-face nature of the enrollment process can be based on an event that occurred a decade or more in the past.

**Recommendation for Kantara:**

Based on the reasoning above, the assessors recommend updating the criteria such that a service may select alternate authoritative sources that do not have direct access to strong evidence issuer data, provided that compensating controls are in place, such as checking geolocation against address of record, and calculation of risk scores based on transaction history.

See also 2018-K-03 which recommends that the selection of authoritative source be stated in the Service Definition / CrP.

**Request to NIST**:

Please review the above and provide the community with a formal response against which application of SP 800-63 rev.3 can be confidently effected, e.g.in the form of an erratum to the necessary clauses of the suite as a whole.