Kantara Implementation Guidance Report

**ID:** 2018-K-01 ver. 2.0

**Subject:** Guidance on Permitting “Commodity” Hardware for Unsupervised Remote Identity Proofing

**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 800-63B, §5.3.2, which is captured in KIAF-1440 as follows:

|  |  |
| --- | --- |
| **SP 800-63B §5.3.2 Use of biometrics** | **KIAF-1440** |
| An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established and … | ***63B#1310****The CSP SHALL establish an authenticated protected channel between the sensor (or an endpoint containing a sensor that resists sensor replacement) and the verifier.* |
| … and the sensor or endpoint authenticated prior to capturing the biometric sample from the claimant. | ***63B#1320****The CSP SHALL ensure that the sensor or endpoint is authenticated prior to capturing the biometric sample from the Claimant.* |

It should be noted that although this section resides in SP 800-63B, which deals with authentication, the requirements in this clause are invoked from SP 800-63A under the identity proofing requirements.

In the context of proofing, Kuma’s interpretation of the above requirements is that photograph-based identity verification requires authentication of the camera or endpoint capturing the photograph. This is due to the following reasoning:

* IAL2 requires strong verification of the binding of the identity to the evidence (SP 800-63A §4.4.1.4)
* Strong verification requires either physical comparison of the applicant to the photograph on their strongest evidence, or biometric validation of the same (SP 800-63A Table 5-3)
* In either case the verification process is required to conform to SP 800-63B §5.2.3.
* The referenced section requires the establishment of an “authenticated protected channel” between the camera capturing the image of the applicant, or the endpoint containing that camera.

Because there is no universal authentication scheme for consumer-owned equipment such as laptops and mobile phones, this requirement is not achievable in a model whereby applicants register for service via their own equipment.

On 2018-05-31, NIST published Frequently Asked Questions about SP 800-63 rev.3, and one of the responses shed some light on this topic. Question A2 asked “*What is the difference between supervised remote identity proofing and unsupervised remote identity proofing?*” The answer points out that SP 800-63A §5.3.3.2 includes a number of requirements for supervised remote that distinguish it from unsupervised remote. The FAQ response includes the following rationale:

* Supervised remote identity proofing uses a video connection to a human operator, made over an agency-owned device, not the applicant’s personal phone.
* If the above and other controls are met, the supervised remote identity proofing achieves IAL3.
* Unsupervised remote identity proofing “typically involves commodity hardware and services”.

From the first two bullets it is clear that supervised remote identity proofing that uses applicant-owned devices could achieve IAL2. The reference to “commodity hardware” also indicates that applicant-owned devices are permissible for unsupervised remote identity proofing.

Based on the reasoning above, 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.

**Recommendation for Kantara:**

Update the Kantara SAC 63B#1310 and 63B#1320: Change the first word “The” to “When using biometrics for authentication, the”.

See also 2018-K-03 which recommends that the method of identity proofing be stated in the public service description of the S3A.

**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.