2019-10-31 Meeting Minutes - Meeting with NIST

Attendees

Invited Guests: Jim Fenton, David Temoshok (NIST), Scott Shorter
Non-voting participants: Andrew Hughes, Roger Quint, Ahmed Naeem
Voting participants: JJ Harkema, Ken Dagg, Martin Smith, Mark Hapner, Richard Wilsher

Staff: Colin and Ruth

Quorum: 4 of 7. There was quorum

Agenda

1. Administration:
   a. Roll Call
2. Discussion: NIST Response to Kantara Implementation Guidance Reports on 800-63-3

Discussion on NIST Response (Key discussion items)

- DT walked the IAWG through the written responses provided before the meeting, see NIST Responses
- DT said that NIST appreciates Kantara's work offering a Trust Framework based on NIST 800-63-3 (A and B criteria), which is a valuable service for the industry and for the Agencies.
- RW added that IAWG expectation is a more definite response to guide us on the implementation of the criteria. He would like to know how Kantara will apply the responses we received, to live with the uncertainties or to apply our own interpretation?
- DT clarified that NIST can respond to inquiries from industry or gov agencies, but they cannot add text or change normative requirements. However, they can clarify terms and text. In addition, NIST is working on implementation resources, FAQ, informative text/material that is not included in the normative text and could help on the implementation, which will be published in the coming year.
- RW remarked that the Kantara Reports address issues on implementing or applying the criteria, for instance cases when it is extremely difficult to meet the criteria, thus one of the goals of the Reports is to get guidance or some kind of alternative interpretation to the criteria.
- RW said that in relation to requirements for validating evidence, SP 800-63A 4.4.1.3., he has an observation on NIST response "this requirement would include the comparison of pictures on state driver's licenses to DMV records or another authoritative source". He stressed that there are no other authoritative sources for comparing a picture on the driver license, other than issuing DMV, given the provisions of the Driver's Privacy Protection Act (you cannot access to the DMV records), no such comparison is going to be possible and Dep. of State does not offer any such facility to match a photo on a passport. If I cannot match a driver license photo with the issuing DMV, is it sufficient to only match the text info on the driver license? DT answered that the photo match and biometrics match requirements are in the verification of the identity evidence to the applicant in the identity proofing process, whether that comparison to the validated identity evidence is performed through a biometric or comparison match is required for verification and it binds the applicant to the validated id evidence. JF added that the purpose of validation evidence is to make sure that the evidence that was presented is genuine and that the evidence applies to the applicant, thus we use the photo for the latter and not for the former. DT clarified that "validation" is validating the genuineness of the identity evidence; "verification" is verifying the binding of that validated evidence to the applicant.
- AH asked if as verification it is allowed to compare a selfie to the photo on the driver license. DT responded that for remote identity proofing, that form of verification may be required. JF added that it would be better to have a liveness detection, like a video chat. AH stressed that in unsupervised remote identity proofing, from a design perspective it is difficult to compare a photo of the driver license with some sort of scan of the person using her/his phone.
- JF pointed out that 63A provides a mid-point for AL2, a balance between achievability and security, but there is not too much 63A can do to improve the security of remote proofing given the limitation of the evidence that people have.
- MH asked if someone qualifies for AL2 using driver license with remote proofing. AH answered that for instance, Idemia does.
- DT remarked that if a person cannot complete the remote identity proofing it needs to go through an in-person identity proofing session. RW added that for some people, a supervised remote identity proofing or physical proofing would be very expensive to accomplish.
- MH asked which other credential could be used for remote identity proofing, DT said immigration documents. RW pointed out that those also raise issues accessing to the issuing source. JF provided another interpretation of authoritative source, it is who you can explain the path back to the issuing source, it does not mean that you need to talk to the issuing source but you need to explain where you get the information from. JF sustained that the weakness is the collection of the selfie, how do you know the selfie is the person sitting behind the computer or mobile? RW said that in those cases we can apply liveness tests, but he is concerned that we cannot access the issuing source for a significant part of the population.
- DT said that the verification is against the identity evidence being presented in the identity proofing session. If the evidence is presented with a photograph, a driver license, in the verification you compare the applicant to that photograph on the validated identity. The entire piece of evidence is validated, verification is always evidence vs applicant.
- RW asked which other parties are involved in interpreting 800-63-3 criteria and using the standard. DT answered that NIST has regular sessions with Federal Agencies that need to authenticate or identity proof the public in order to offer their services, accordingly 800-63-3 is an ongoing dialogue with them. RQ asked if there is a way to benefit from the ongoing dialogue with US Federal Agencies, DT responded that they will incorporate that information on the FAQ and informative material as part of the implementation guidance resources.
- MH asked which agency do AL2 Remote, DT replied Records Administration Agency.
- It was agreed to set up another session to continue the discussion with NIST. Ruth to work with David to schedule the next session.