From: Vishal Gupta
Sent: Thursday, July 30, 2020 12:26 PM
To: dig-comments-RFC <dig-comments-rfc@nist.gov>
Cc: Per Jirstrand
Subject: Submissions for NIST Special Publication 800-63A (DRAFT)

Submissions for NIST Special Publication 800-63A

(DRAFT)

Under IAL2, the Address confirmation requirement an enrolment code needs to be sent to the physical address.

Comments

The IAL3 requirement is almost similar or rather confusing.

Sending an enrolment code is expensive, time consuming and difficult particularly for international verification.

Suggestion

Standard should consider online verification from utility companies that have physical delivery like water, heating, telephone, cable, electricity with a current invoice. This will make the verification solid, instant and can be carried out internationally. Further a provision may be made to have the name of the person or at least the surname be present on the utility bill.

On the contrary the enrolment code is vulnerable to be stolen from mail delivery which the online utility verification can prevent.

Under Table 5-3 Verifying Identity evidence – poses risk of identity fraud and does not cover latest developments in verification technologies.

Strong (strength) – provides only two options

1. physical comparison of photograph (local or remote)
2. Biometric comparison (local or remote)

Comment

The current guidelines do not solve the epidemic of identity takeover because:

- Technology to create deep-fakes is becoming common place. The current AI can not detect if the photo has been replaced or contains a face that has been mixed with another face.
- Authoritative sources do not provide confirmation of photographs or biometric data therefore the binding remains vulnerable.
- The remote verification input stream does not use a trusted device and therefore always remains vulnerable.

This creates a huge vulnerability in the system.

Suggestion

- At minimum allow for impersonation checks to be carried out using derived credentials from, third-party sources like banks, utility companies or identity databases based on successful logins.
- The remote impersonation check should contain one or more sources of authentication from credible third parties depending on the level of verification required. (this address photograph spoofing or synthetic identity creation).

Hope this feedback helps.

Vishal Gupta