Draft Cover Letter -Final

Aaron Miri

Health Information Technology Advisory Committee

Dear Mr. Miri:

We, the undersigned, would like to make the HITAC aware of a worrisome identity assurance disconnect that we recently uncovered and have documented in the attached report. As independent SMEs, who have been working in the patient identity space for many years and involved in several associations (HIMSS, Kantara, IDESG, CARIN Alliance and others) we felt it was important to raise this issue to the fore. We submit this analysis, entitled “*Alignment Around Identity Assurance Levels*”, in hopes that you would make this concern known to the members of the Health IT Advisory Committee and specifically to the members of Trusted Exchange Framework Task Force.

As you are aware, the healthcare IT sector does not currently have a single regulatory authority that could adjudicate and judge which process for identity assurance is correct and should be closely followed as a “best practice” example in the private sector, despite widespread tax supported subsidies and reimbursement. It is our hope that before the TEFCA design is put in motion that the HITAC weighs in on what elements constitute a trusted and reliable IAL2 design. Otherwise, we are concerned that different authoritative agencies will determine what works best for their constituents resulting in different rigor being applied to the process of identity proofing. It also raises a serious challenge to the NIST SP 800-63.3C at the Federated Level where the Relying Party is the credential exchange hub that provides secure access to PHI. Without a consistent interpretation of how 800-63 is to be implemented, it will be impossible for independent healthcare entities to trust each other’s identification protocol and TEFCA will not function optimally with such a security vulnerability.

Once again, please recognize that we are signing this document and supporting the need for improvement as individuals with extensive experience and not representing any views of the aforementioned associations nor our employment groups.

Please feel free to reach out to Dr. Tom Sullivan or any of the undersigned, should you have any questions regarding this matter.

Sincerely,

<signature lines for Dr. Tom, Jim Kragh, Catherine Schulten, Barry Hieb, MD, Michael Magrath…others?>

Thomas e Sullivan, MD

Chair, IDESG/Kantara Healthcare Committee

Chief Strategic Officer, Chief Privacy Officer

 DrFirst.com, Inc.

(978) 729-5075 (M)

tsullivan@drfirst.com

sullivan@massmed.org

Catherine Schulten

VP Product

LifeMed ID

(954) 290-1991 ©

Catherine.schulten@lifemedid.com

Barry Hieb, M.D.

Chief Scientist

Global Patient Identifiers, Inc.

520-320-6220

bhieb@vuhid.org

Jim Kragh

Compliance Consultant

Chair User Compliance/IDEF

Secretary: Healthcare Working Group

c 407-415-1645

Alignment Around Identity Assurance Levels

**When is LOA3/ial2 not LOA3/IAL2**

A recent analysis of applicant identity assurance has revealed some incongruity around the processes used to achieve confidence that the person is who they say they are. Two entities – Direct Trust and Kantara – have interpreted the NIST 800-63-2 specifications for identity proofing in different ways with Direct Trust opting in favor of verifying the applicant’s SSN and utility account ownership and Kantara adhering to the inspection and verification of the applicant’s identity evidence.

The NIST SP 800-63-2 and version -3 describe the elements needed to establish strong identity assurance.  Specifically, one of the elements cited requires that the applicant’s *identity evidence* (such as their driver’s license or passport) be validated either by a person or electronically.

**800-62-2, LOA3:**



**800-63-3, IAL2:**



In both versions, -2 and -3, the NIST publication explains that the applicant needs to provide a piece of unexpired identity evidence with their photo on it and the evidence needs to be strongly confirmed as being authentic and belonging to the applicant.

**Exceptions**

Sec 5.3.2 of the 800-63-2 SP contains some special directions for non-federal agencies and explains that some organizations (like a healthcare organization) can leverage existing relationships with individuals (like their professional staff) to assist in the confirmation their identity.

*“The strength of these relationships and the obligations of organizations to know identities vary considerably, for example employers have legal obligations to withhold and pay taxes on employees and are regulated by a variety of local, state and Federal entities, but the certainty enforced in many employment situations is not high. Retail stores are not broadly required to know their customers, but financial institutions are. Healthcare organizations are regulated at many levels and are expected to know the identities and professional qualifications of their professional staff, as are legal and accounting firms. This section identifies several areas where these organizations may leverage their existing relationships with individuals to act as CAs or CSPs for those individuals and issue credentials for use with Federal entities.”*

Since Patients aren’t the same type of role as Licensed Professional Staff – this exception does not appear to apply.

**Direct Trust Identity Assurance Process:**

The Direct Trust process for assuring the identity of a patient has the individual providing their SSN and not a piece of identity evidence. This attribute is checked against a 3rd party reference data base to confirm that a person with that name and DOB has that SSN. At the same time the identity service performing the proofing process checks to see if a utility is in the name of the applicant. The applicant does not provide an account number for a specific utility in their name, instead the verifying service checks a 3rd party reference database to determine if a person with this name, DOB, address has a utility in their name.

If both checks “pass” then the applicant is deemed appropriately proofed for LOA3.

Following are a set of screen shots from a Health Information Services Provider (HISP) certified to perform identity proofing for patients seeking a Direct Email Address.





In speaking with this HISP I learned that SSN submission along with checking for a utility in the applicant’s name was considered an equal measure as validation of the patient’s government issued/photo identity evidence.  I was told that the HISPs under Direct Trust have a different set of instructions they need to follow for this element of the proofing requirement.  Identity Document Verification is not needed to be deemed LOA3 for the applicant to get a Direct Email Address.  As the founder and CEO of Direct Trust, Dr. David Kibbe recently put context around this “disconnect” or different interpretation of NIST 800-63-2 and the bottom line was that Direct applied a different set of requirements for their needs because it was felt that the -2 SP – while appropriate for federal agencies and the like – did not meet the needs of consumer/patient identity.

Validating the identity evidence strictly as described in -2 SP, would be an obstacle due to several factors including, the process by which such an activity could occur, and in particular, the cost and time to achieve it.

**Kantara Identity Proofing Process:**

Kantara’s documentation for their CSPs directs that the in-person identity proofing process include inspection of the applicant’s Government Picture ID and that the photo on the card matches the card bearer (this process can be done by a person or electronically).

Next, a “*record check with the specified issuing authority or through similar databases that:*

* *Establishes the existence of such records with matching name and reference numbers;*
* *Corroborates date of birth, current address of record, and other personal information sufficient to ensure a unique identity;*
* *Provides all reasonable certainty that the identity exists and that it uniquely identifies the applicant”*

Kantara’s instructions around remote identity proofing has the applicant submitting reference of and attesting to current possession of a primary Government ID (notice that the requirement for a photo on the ID is omitted) along with:

*a) a second Government ID;*

*b) an employee or student ID number;*

*c) a financial account number (e.g., checking account, savings account, loan, or credit card), or;*

*d) a utility service account number (e.g., electricity, gas, or water) for an address matching that in the primary document. Ensure that the applicant provides additional verifiable personal information that at a minimum must include: e) a name that matches the referenced photo-ID;*

*f) date of birth;*

*g) current address [omitted]. Additional information may be requested so as to ensure a unique identity, and alternative information may be sought where the enterprise can show that it leads to at least the same degree of certitude when verified.*

Kantara’s process has the applicant providing a utility service account number with an address matching that in the primary evidentiary document. *(this instruction is a bit confusing since some document evidence like the* ***SSN card*** *does not contain the individual’s address and a* ***passport*** *only has a space for the individual to write in their address…if SSN and a utility account number were provided, the address aligned with the applicant for that utility could be verified, however the utility address could not match the “primary document” since the SSN card has no address on it.)*

**The Difference**

The Direct Trust process has the applicant providing some essential PII including their SSN. The Kantara process also has the same requirement for essential PII with the SSN being an enumerator from “primary Government ID” that doesn’t contain a photo. However, the 2nd element required in Kantara’s process would have the applicant supplying a “utility service account number”. The difference occurs around how this verification is conducted. Direct Trust allows the CSP to perform a scan to find a utility in the applicant’s name/address while Kantara has the applicant supplying a utility account number first and then having the CSP performing the steps needed to confirm that utility in in the applicant’s name at that address.

The Direct Trust process is more vulnerable to fraud since a bad actor could easily steal a small set of identity details (name, address, DOB, email, SSN) from another person and achieve LOA3 identity assurance.

Because the Kantara process requires the applicant to provide a utility account number the ability for the bad actor to achieve LOA3 is made more challenging.

**Equitable?**

Are Direct Trust’s and Kantara’s identity proofing requirements equitable?

Is the same degree or assurance in the identity of the individual achieved via Direct’s v. Kantara’s process?

Would a relying party have equal risk if they were to accept an individual’s Direct Trust LOA3 claim as a Kantara’s LOA3 claim?

**NIST 800-63-3, IAL2 Specifications**

Direct Trust has not yet published instructions for their HISPs around the process they will need to apply to perform identity assurance to achieve IAL2.

Kantara has published their service assessment criteria for this version and has had a CSP achieve 800-63-3 conformance for in-person and facilitated remote identity assurance.

To achieve industry alignment and trust between and among relying parties, it is important that Direct Trust, Kantara and any other entity that certifies CSPs, do so in a manner that doesn’t allow one certifying organization to support a “less strict” option to achieve the same result or level of confidence that a person is truly who they claim to be.

**In conclusion**, as eCommerce explodes worldwide, the importance of trustworthy online identities has also increased “pari passu”. Members of the Identity Ecosystem Group Healthcare committee (IDESG), recently affiliated with the Kantara Initiative, believe that it is worth reminding both experts and the public that a true identity is inherently resilient to theft or any compromise. It is the **Identifiers** that are vulnerable (SSNs etc.). Thankfully, since there are hundreds and many thousands of human identifiers – particularly leveraging biometrics, behavioral and molecular resources, resilience is real, and remedies can be applied.

A good ecosystem that builds upon strictly following NIST SP 800-63-3 as a point of departure, along with other recognized standards promoting appropriate levels of assurance, authentication and the federation of identifiers can help remedy the current global epidemic of dishonesty, fraud and theft.