# Kantara Initiative Identity Assurance Work Group: Analysis and position on “Address of record” usage in NIST 800-63

2024-02-08

## Background

SP 800-63 formally defines “Address of Record” as “***the validated and verified location (physical or digital) where an individual can receive communications using approved mechanisms.***”[[1]](#footnote-1)

This is in contrast with a “Claimed Address” which is formally defined as - ***the physical location asserted by a subject where they can be reached. It includes the individual’s residential street address and may also include their mailing address. For example, a person with a foreign passport living in the U.S. will need to give an address when going through the identity proofing process. This address would not be an “address of record” but a “claimed address.”***[[2]](#footnote-2)

The described nature and permitted usages of different kinds of addresses are conflated and are confusing for CSP and Assessors. To improve clarity for stakeholders, the Identity Assurance Work Group (IAWG) offers this analysis and position on the use of “address” in SP 800-63.

# Identity Assurance Work Group Position on “Address”

The Kantara Initiative Identity Assurance Work Group (IAWG) shall treat “Address of Record” and “Claimed Address” as defined in NIST SP 800-63-4 ipd as “a means to communicate with the Applicant or Subscriber”.

“Address of Record” and “Claimed Address” shall not be considered as evidence supporting a claimed identity.

The correct term for checking ownership or possession of an address is “Address Confirmation” rather than verification or validation.

## Analysis

As an address or address of record primarily serves as a means for the CSP to communicate with individuals, its validation and verification should specifically assess its suitability as a communication location for a particular applicant. While confirming the existence of a a possessive attribute such as an address does not inherently validate it as belonging to a real-life identity, applicants should be able to validate and verify an address by demonstrating ownership or possession.

Ownership is demonstrated when an address is included in the applicant's identity evidence, such as the address on a driver’s license, or confirmed through an authoritative source, such as a mobile carrier confirming ownership of a phone number.[[3]](#footnote-3) For physical addresses, a credible source aggregating identity information could be used for validation.[[4]](#footnote-4) In both cases, the address is a relevant attribute for identity resolution and is verified through the verification of the general identity.[[5]](#footnote-5)

If an address is not in the identity evidence or cannot be validated through a credible source, an applicant can still demonstrate possession. This is particularly relevant to email addresses, where providers generally don't validate the owner's identity. In such cases, possession can be demonstrated by returning an enrollment code sent to the address, validating its association with an identity and verifying it as a part of their identity.[[6]](#footnote-6) Although the address is not a relevant attribute for identity resolution, it would be relevant as a part of the confirmed identity.[[7]](#footnote-7) This approach should also be acceptable for validating mobile phone numbers or physical addresses.[[8]](#footnote-8)

This approach is supported by this notion that a proofing notification must be sent to an address of record that is preferably not the one that received the enrollment code and that proofing notifications but not enrollment codes are required for IAL2 identity proofing.[[9]](#footnote-9) These imply that an address can be validated via a method that does not necessarily prove possession, ownership.[[10]](#footnote-10)

A concern with this approach, however, is that the standards seem to mandate sending enrollment codes to a previously validated address, implying an additional validation before sending the code.[[11]](#footnote-11) This approach makes sense if the address is being used to resolve the identity but not if the address is merely being added as part of the confirmed identity.

We therefore recommend that the standards distinguish ownership and possession validation and verification methods from each other and expressly allow for either method of address validation and verification.

1. Line 1607 of 800-63-4 ipd [↑](#footnote-ref-1)
2. Line 1773 of 800-63-4 ipd [↑](#footnote-ref-2)
3. See the requirements for authoritative sources in Sec. 4.3.4.4 of of 800-63A-4 ipd. [↑](#footnote-ref-3)
4. See the requirements for credible sources namely those beginning on line 653 of Sec. 4.3.4.4 of 800-63A-4 ipd [↑](#footnote-ref-4)
5. Per Sec. 5.1.1(4) of 800-63A-4 ipd, identity information that is used to resolve the claimed identity to a single unique individual would be considered a core attribute. [↑](#footnote-ref-5)
6. See Sec. 5.1.6 of 800-63A-4 ipd. [↑](#footnote-ref-6)
7. Per Sec. 5.1.1(4) of 800-63A-4 ipd, core attributes also includes information that is conveyed to relying parties as part of the confirmed identity. [↑](#footnote-ref-7)
8. Per the requirements Sec. 5.1.6 of 800-63A-4 ipd that allow for the use of enrollment codes for postal addresses, phone numbers, and email addresses. [↑](#footnote-ref-8)
9. Sec. 5.1.7(1) of 800-63A-4 ipd requires proofing notifications to preferably be sent to a different address than the one used for an enrollment code. Also, the new standards require a proofing notification for IAL2 in Sec. 5.4.5 of 800-63A-4 ipd but do not require an enrollment code. [↑](#footnote-ref-9)
10. As the standards do not offer another method for proving possession of an address other than an enrollment code. [↑](#footnote-ref-10)
11. See Sec. 5.1.6(1) of 800-63A-4 ipd. [↑](#footnote-ref-11)