Articles

What are the NIST 800-63 Digital Identity Guidelines?

As the world continues to move online, digital identity proofing is a key pillar of making sure that transactions and interactions are safe. Digital identity proofing is critical to stopping rampant identity theft and online fraud attempts that have arisen in recent years.

The National Institute of Standards and Technology (NIST) is a federal agency that establishes industrial measurements and standards, including for cybersecurity and digital identity. Released in June 2017, the NIST Special Report 800-63-3 defines requirements for federal agencies implementing digital identity services.

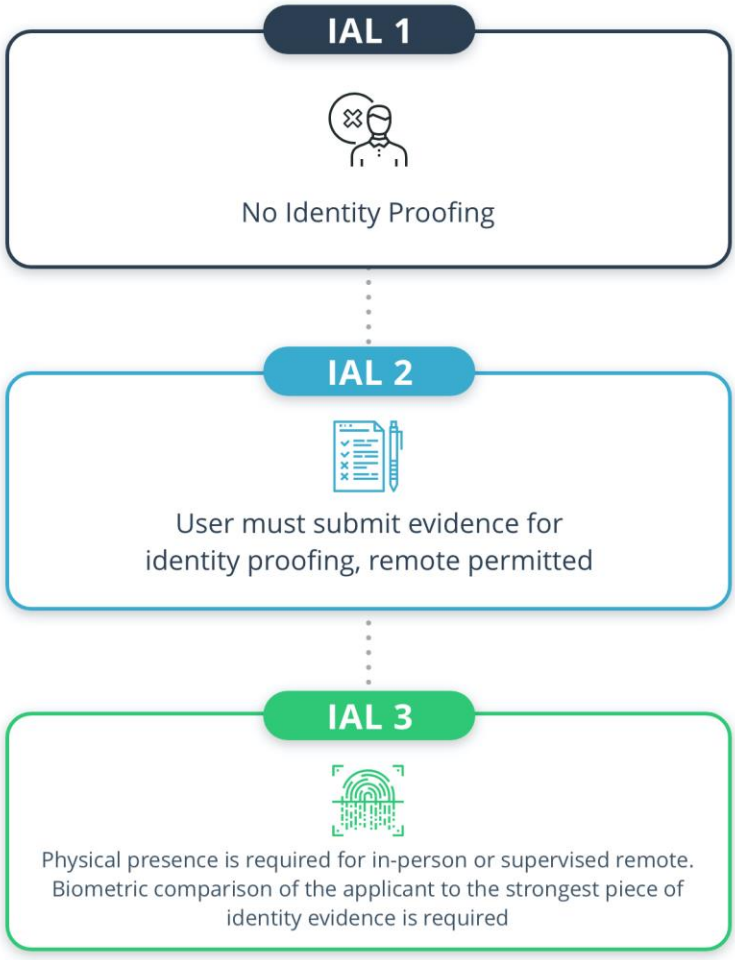
These NIST standards are primarily concerned with ensuring that **someone is who they say they are** before granting them access to a digital service. These digital identity standards and other cybersecurity frameworks are part of a larger government strategy to reduce identity theft and fraud.

NIST 800-63-3 is divided into three components:

- Enrollment and Identity Proofing (NIST SP 800-63A)
- Authentication and Lifecycle Management (NIST SP 800-63B)
- Federation and Assertions (NIST SP 800-63C)

The higher the risk of someone accessing an account they shouldn't, the more confidence the organization must have in the accuracy of the requestor's identity. Organizations garner increased confidence by adding further checks that an individual must pass before having their identity verified. Those checks are outlined in the levels of assurance defined by NIST: Identity Assurance Levels (IAL), Authenticator Assurance Levels (AAL), and Federation Assurance Levels (FAL).

Identity Assurance Levels



There are three IALs defined in NIST SP 800-63A – IAL1, IAL2, and IAL3 – which require progressively stricter requirements.

IAL1: Does not require mapping the claimed identity to a real person, or ensuring that the user actually owns the claimed identity. IAL1 is the least strict level and does not require actual identity proofing – the digital service does not need to map the person creating an account to a real-life identity. The attributes of the identity are self-asserted by the user, rather than verified, so they do not need to submit pieces of evidence.

Example

Consider social media accounts, like Facebook or Twitter – you don't have to submit proof of your identity to set up an account registered to your name.

IAL2: Requires the user to submit evidence that they are the owner of the identity they are claiming. IAL2 requires identity proofing, which can be completed remotely or in person. The person requesting access to an asset must provide evidence that they are the owner of the identity they are claiming. Biometrics, like a face scan or fingerprints, can be collected.

Example

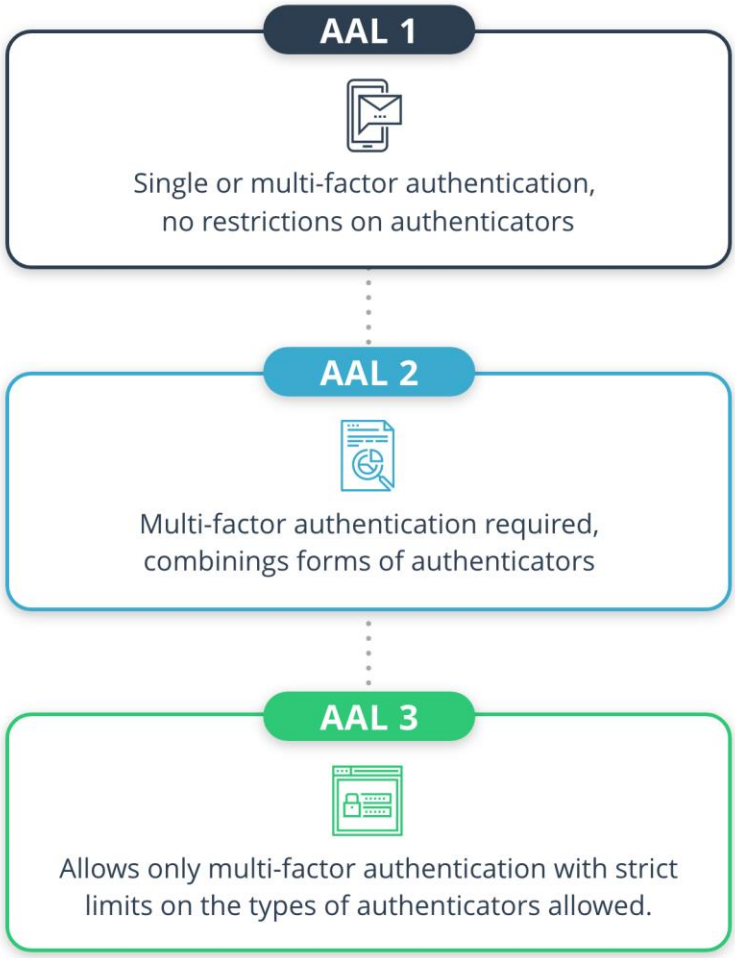
Consider accounts that hold information already registered to a certain person, such as a government account linked to a social security number. To request access to that information, you first have to provide evidence that you are the owner of that identity, potentially by using a passport or driver's license.

IAL3: IAL3 is the strictest level of NIST 800-63-3 identity verification. Physical presence is required, whether in-person or supervised remote. Biometric comparison of the applicant to the strongest piece of identity evidence is required.

Example

Consider how DMVs require people to show up in-person for certain services, including applying for a driver's license and upgrading to a REAL ID. These forms of ID not only confer the authority to drive a vehicle, but also serve as a form of identification in and of themselves. As a result, the confidence level in the identity of the applicant must be extremely high.

Authenticator Assurance Levels



There are three AALs defined in NIST SP 800-63B – AAL1, AAL2, and AAL3 – which require progressively stricter requirements.

AALs define the requirements for authentication. For online services that someone needs to access repeatedly, authentication is used to ensure that they are the same person who previously verified their identity on that account.

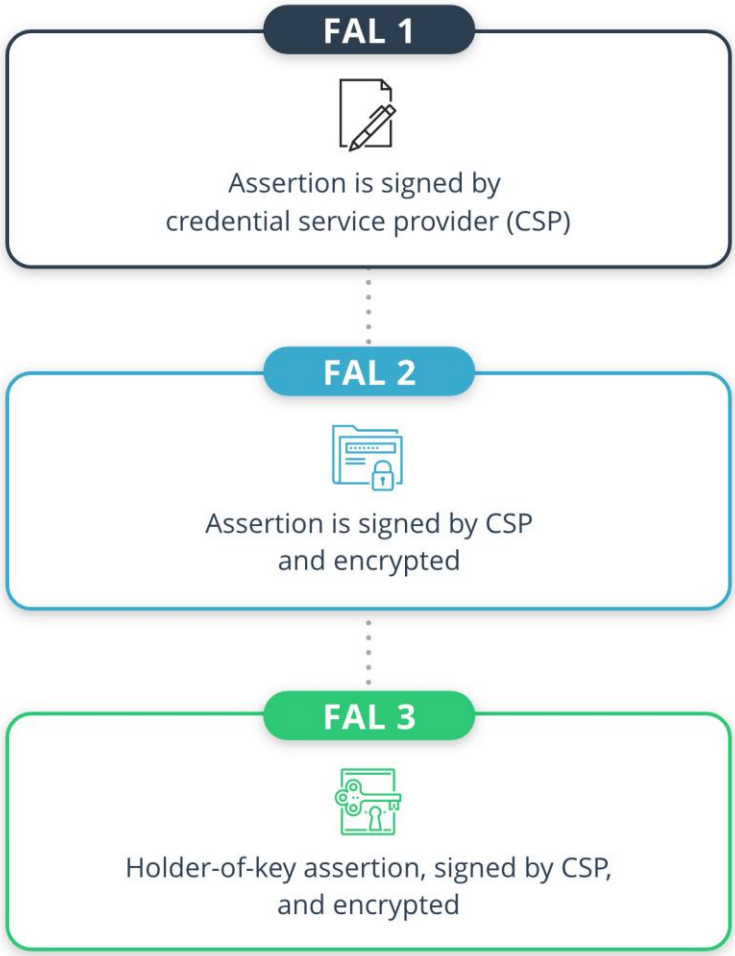
To authenticate, people must demonstrate that they are in control of an *authenticator* that has previously been tied to the account. A password is a common example of an authenticator.

AAL1: Allows single or multi-factor authentication, with little restriction on the type of authenticators accepted.

AAL2: Allows only multi-factor authentication, where a combination of two categories of authenticators must be used.

AAL3: Allows only multi-factor authentication with strict limits on the types of authenticators allowed. Two of the three authenticator categories – something you know, something you have, and something you are – must be represented. The "something you have" authenticator must be a hardware key while the "something you are" authenticator must be impersonation resistant.

Federation Assurance Levels



FAL standards for Federation Assurance Level. It is part of the NIST 800-63-3 Digital Identity Guideline.

Federation is used when one system needs to send packages of information, called assertions, to another system. In the case of identity credentials, those assertions include information about the user's credential. The credential service provider (CSP), which completes the identity verification, must pass

the important parts of the user's identity to the organization that controls the digital service, called the relying party (RP).
There are three FALs defined in NIST SP 800-63C – FAL1, FAL2, and FAL3 – which require progressively stricter requirements.

FAL1: Assertion is signed by credential service provider (CSP)

FAL2: Assertion is signed by CSP and encrypted

FAL3: Holder-of-key assertion, signed by CSP, and encrypted

ID.me's digital identity network can strengthen your business

Proving a user's digital identity is an important measure for businesses and government agencies. ID.me's team can help you build a robust, scalable, and efficient solution. We provide a complete identity platform featuring NIST 800-63-3 IAL2 and AAL2 aligned capabilities with identity proofing and a flexible identity broker.
ID.me is compliant at NIST IAL2/AAL2 by the Kantara Initiative and also can also provide secure credentialing at NIST IAL1 for lower-risk logins. In addition, ID.me offers authentication options that meet AAL3, should your organization choose to strengthen authentication requirements.

https://insights.id.me/article/what-are-the-nist-800-63-digital-identity-guidelines/