NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Digital Identity Guidelines Update

Ryan Galluzzo & David Temoshok

Applied Cybersecurity Division

December 2022

What is NIST’s Role in Identity Management?

NIST’s role is to…

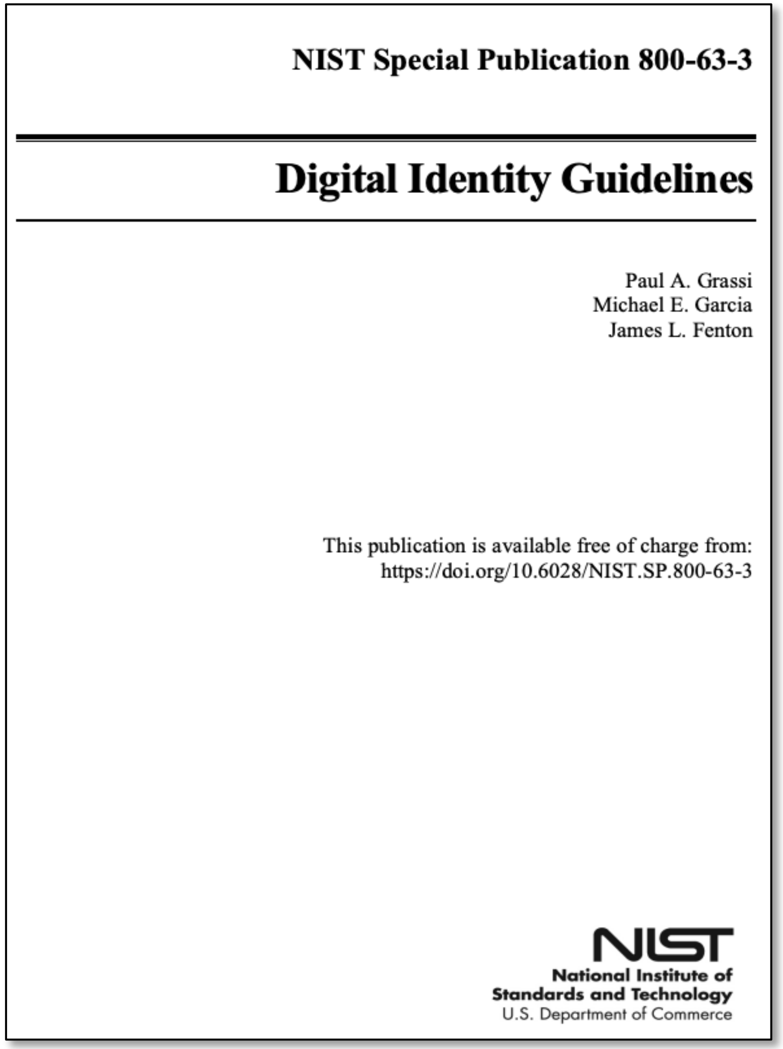
- **Create Guidelines by way of** NIST Special Publication 800 series – for example NIST Special Publication 800-63: Digital Identity Guidelines. These are mandatory for federal agencies and widely adopted by commercial entities
- **Develop Standards** such as Federal Information Processing Standards (FIPS) and contribute to international standards such as those developed in ISO, IETF, W3C, FIDO, and IETF
- **Conduct foundational and applied research** to advance knowledge of Digital Identity Technology and Processes and bridge the gap between standards, guidance, and implementation

NIST’s ongoing projects include…

- Updating NIST SP 800-63, *Digital Identity Guidelines* and NIST 800-157, *Guidelines for Derived Personal Identity Verification Credentials* to address new technology and challenges
- Creating new guidelines for PIV Federation to promote greater cross agency interoperability
- Developing Mobile Driver’s License standards (e.g., ISO/IEC 18013) to advance deployment and adoption of the technology
- Researching Identity Verification and Attribute Validation technology to set the foundation for future guidelines and standards engagement
- Developing Zero Trust reference implementations to advance critical national cybersecurity priorities

What are the Digital Identity Guidelines?

- Details the process and technical requirements for digital identity management
- Describes identity risk management process and assurance level selections (identity, authentication, federation assurance)
- Provides considerations for enhancing privacy and usability of digital identity solutions and technology.
- Inclusive of 4 volumes
  - Base – Digital Identity Model and Risk Management
  - A – Identity Proofing & Enrollment
  - B – Authentication & Lifecycle Management
  - C – Federation & Assertions
- Last major revision was in June of 2017



NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Why are we making changes?

In conjunction with feedback from our 2020 Call for Comments, NIST focused on a few core “design principles” to drive our updated requirements and considerations:

- **Advance equity**
- **Emphasize optionality and choice for individuals**
- **Deter phishing, fraud and advanced threats**
- **Address lessons learned through real-world implementations**
- **Emphasize multi-disciplinary risk management processes**
- **Clarify and consolidate requirements where needed**

OUR WORLD HAS CHANGED IN PROFOUND WAYS SINCE 2017; IT IS TIME FOR OUR GUIDANCE TO CHANGE TOO…

What aren’t we changing?

- **Structure -** there will remain 4 volumes each focused on their respective aspects of digital identity
- **Decoupled assurance levels -** there will still be three different types of assurance levels (identity, authentication, and federation) with three levels of assurance each.
- **Privacy, usability, and security –** there will still be emphasis on balancing risks to each of these critical components of identity and solution delivery and volumes continue to include specific requirements and considerations…we’ve just taken things one step further to consider equity!

What ARE we changing?

Base Document	Identity Proofing & Enrollment
➢ Revamps risk management to integrate equity & mission delivery ➢ Considers risk to individuals and communities alongside risks to organizations ➢ Updates digital identity model to address new deployment patterns (federated, non-federated) ➢ Updates assurance level selection and introduces ”tailoring” ➢ Introduces continuous evaluation and emphasizes integration with fraud, cyber, and program integrity	➢ IAL 1 – a whole new assurance level (kind of)!! ➢ Clarifies Trusted Referee role & introduces “Applicant Reference” ➢ Expands the use of digital evidence ➢ Provides biometric performance requirements ➢ Expands options for proofing that don’t require the use of face recognition ➢ Introduces concept of “Subscriber Account” ➢ Requires assessment of impacts to equity in addition to privacy and usability

What ARE we changing?

Authentication & Lifecycle Mgt.

- Defines and elaborates on phishing resistance (channel binding and domain binding)
- Differentiates MFA using shared secrets from stronger, phishing-resistant authentication protocols
- Updates biometric performance requirements
- Elaborates on account recovery options
- Adds guidance on wireless connection to cryptographic authenticators
- Shifts password “should” to “shalls” (complexity, rotation, and password manager support)
- Enumerates authentication-related equity considerations

Federation & Assertions

- Redefines and clarifies all of the FALs
- Adds guidance for the use of provisioning & identity APIs
- Adds concept of bound authenticators for high assurance federation
- Introduces requirements for federation agreements, including dynamic federation agreements

What can you do? Comment on the draft!

We will release the draft for public comments soon and are seeking specific input on some of the following areas:

- What technologies or methods can be applied to develop a remote, unattended IAL2 identity proofing process that demonstrably mitigates the same risks as the current IAL2 process?

- What methods exist for integrating digital evidence into identity proofing at various identity assurance levels?

- What are the impacts, benefits, and risks of specifying a set of requirements for CSPs to establish and maintain fraud detection, response, and notification capabilities?

- Are emerging authentication models and techniques – such as FIDO passkey, Verifiable Credentials, and mobile driver’s licenses – sufficiently addressed and accommodated, as appropriate, by the guidelines?

- Are the controls for phishing resistance as defined in the guidelines for AAL2 and AAL3 authentication clear and sufficient?

- Are current testing programs for liveness detection and presentation attack detection sufficient for evaluating the performance of implementations and technologies?

How can you get in touch?

Send your questions or comments to: dig-comments@nist.gov

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
UNITED STATES DEPARTMENT OF COMMERCE
100 Bureau Drive