NIST Digital Identity Guidelines Update

David Temoshok, Connie LaSalle, Ryan Galluzzo

Digital Identity Team, Information Technology Lab

October 2022

What is the state of digital identity today?

- **Rapid Digital Transformation** – the pandemic accelerated the transition to or creation of new digital services to support previously analog or manual service mandating new methods for identity verification

- **New Vectors and Opportunities for Nefarious Actors** – rapid digitalization plus maturation of bad actors has given rise to new opportunities to exploit benefits programs such as COVID 19 relief programs

- **Advanced and Scaled Threats** – attackers are leveraging increasingly complex attacks to enable fraud and unauthorized access including phishing, ransomware, synthetic identities, automated attacks, and the use of industrialized criminal forums and market places

- **Outdated Techniques** – despite known issues, many techniques such as Knowledge Based Verification (KBV) remain in place as components of identity proofing processes

- **Limited Alternatives** – modern, secure, scalable, and remote pathways to verification are limited in the current market and revolve around often controversial technology such as biometrics (e.g., facial image)

- **Changing Consumer and Public Sentiment** – surging awareness and concern around data privacy, bias, and usability are coming into conflict with security principles and concepts

- **Constrained Interoperability** – though standards, protocols, and technology support greater portability of identity technology it if often constrained by policy, operations, and business motivations

What is NIST's Role in Identity Management?

NIST

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 in conjunction ISO/IEC 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 meeting the digital identity management

- Describes identity risk management process and assurance level selections (identity, authentication, federation assurance)

- Provides considerations for enhancing privacy 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?

Publication Structure
- There will remain 4 volumes each focused on their respective aspects of digital identity

Decoupled Assurance Levels (IAL/AAL/FAL)
- 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 equitable access!

What Are We Changing?

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

What Are We Changing?

NIST

Authentication & Lifecycle Management (Volume B)	Federation & Assertions (Volume C)
• Defines and elaborates on phishing resistance (channel binding and domain binding)	• Redefines and clarifies all of the FALs
• Differentiates MFA using shared secrets from stronger, phishing-resistant authentication protocols	• Adds guidance for the use of provisioning & identity APIs
• Updates biometric performance requirements	• Adds concept of bound authenticators for high assurance federation
• Elaborates on account recovery options	• Introduces requirements for federation agreements, including dynamic federation agreements
• Adds guidance on wireless connection to cryptographic authenticators	
• Shifts password "should" to "shalls" (complexity, rotation, and password manager support)	
• Enumerates authentication-related equity considerations	

Targeted Issues for Comment/Feedback

NIST intends to target specific issues for public comment on the Draft of SP 800-63-4, such as:

➢ 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 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:

David Temoshok

Ryan Galluzzo

Connie LaSalle

or

dig-comments@nist.gov