NIST Update
Draft SP 800-63-4

Federal Cybersecurity and Privacy Professionals Forum

September 1, 2022

David Temoshok

Applied Cybersecurity

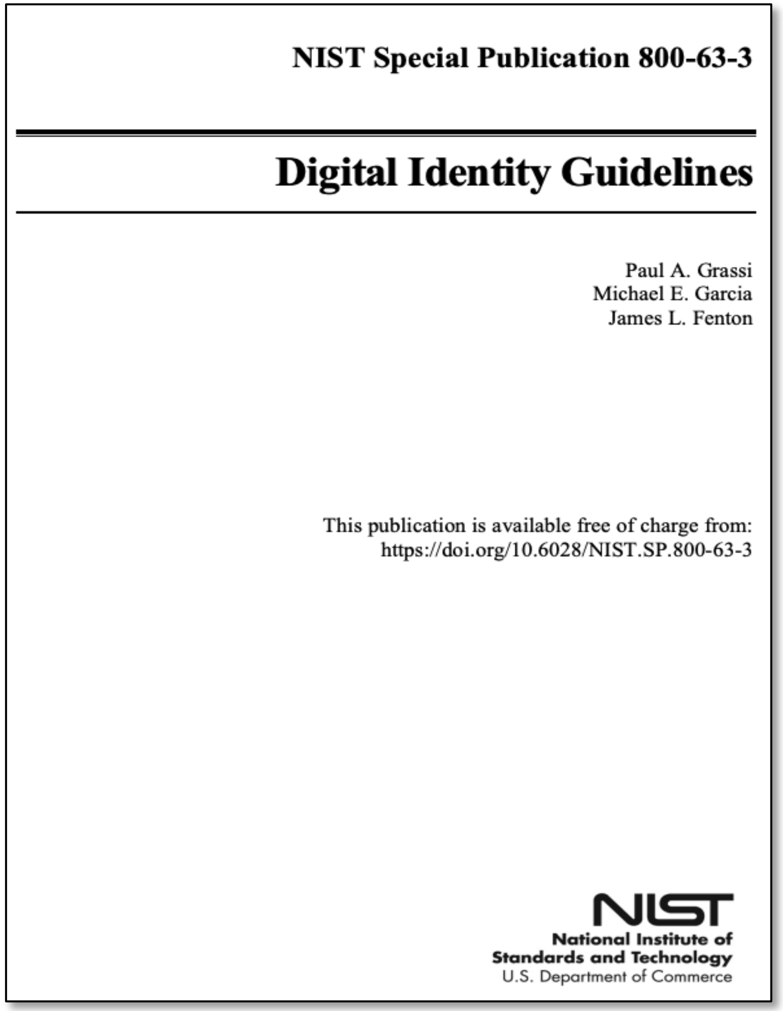
NIST IT Laboratory

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

Celebrating 50 years of Cybersecurity at NIST

NIST SP 800-63-4: Digital Identity Guidelines

- **NIST SP 800-63 rev. 4 represents an update to all 4 volumes of the standard.**
- **Update follows 2 separate public comment and discussion periods, multiple meetings with federal agencies and industry.**
- **Retains 3 assurance level model for IAL, AAL and FAL and basic organizational structure.**
- **Key objectives for rev. 4:**
  - Increased flexibility for identity service implementation
  - Enhanced fraud resilience
  - Equity considerations
  - Enhanced agency flexibility for digital identity risk management and alignment with RMF.



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

Volume Overview – Substantive Changes

Base Document	Identity Proofing & Enrollment	Authentication & Lifecycle Mgt.	Federation & Assertions
Digital Identity Risk Assessment: revised content to address equity impacts, privacy and usability For digital identity risk assessment to better align to RMF/FISMA **xAL Selection:** Updated xAL selection approach to better address impacts to equity, privacy, and usability. **Subscriber Account**: Added requirements for maintenance of subscriber accounts to govern retention of PII, authenticators, and consent agreements. (Normative requirements in A, B, C)	**IAL 1:** Incorporated controls for IAL1 identity proofing to support lower risk applications. **Trusted Referee & Applicant Reference:** expanded content on Trusted Referee and introduced the concept of "Applicant References" to expand access and risk based options for agencies. **Digital Evidence:** Added more explicit language to support use of digital evidence in proofing. **Privacy Risk Assessments:** Added requirements for privacy risk assessments for PII collection, retention, use, and consent.	**Phishing Resistance:** Added definition and requirements for phishing resistant authenticators. **Biometric Performance Requirements**: Updated biometric performance requirements and metrics and included discussion of equity impacts. **Account Recovery**: Provided additional context on account recovery options to account for users with limited access to multiple authenticators. **Wireless Connections**: Guidance and requirements for wireless direct connections for cryptographic authenticators.	**Redefined FALs**: clarified requirements to make compliance more understandable, particularly at FAL3. **Provisioning & Identity APIs**: Added content to include providing requirements for Relying Parties and a identity APIs used to passe identity attributes and data. **Bound Authenticators**: Added language for the use of ”bound authenticators” in support of high assurance federation use cases (e.g., FAL3). **Federation Agreements:** Expanded guidance and requirements for Federation Agreements and IDP & RP responsibilities.

Questions/Comments?

David Temoshok

Applied Cybersecurity

NIST IT Laboratory

dig-comments@nist.gov

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