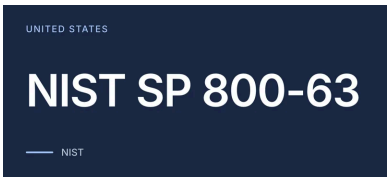
SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-63-4, Digital Identity Guidelines (July 2025)

NIST SP 800-63-4 (July 31, 2025) is NIST's Digital Identity Guidelines base volume: the digital identity model, the five-step DIRM process and the IAL, AAL and FAL assurance levels.



What it is

NIST SP 800-63-4, Digital Identity Guidelines, is the base volume of NIST's four-volume suite on the identity proofing, authentication and federation of users (employees, contractors or private individuals) who interact with government information systems over networks. NIST published it as final on July 31, 2025, after drafts in June 2020, December 2022 and August 2024; it supersedes SP 800-63-3 of June 2017 (updated March 2, 2020), which NIST withdrew on August 1, 2025. Section 3 is normative and binding on federal relying parties: federal RPs SHALL implement the Digital Identity Risk Management (DIRM) process for all online services, while private-sector organizations and state, local and tribal governments may consider the guidelines where appropriate (Section 1.1).

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION Revision 4 (SP 800-63-4, July 31, 2025)
EFFECTIVE July 31, 2025	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: csrc.nist.gov/pubs/sp/800/63/4/final

Why it matters

- **A defined process with mandatory outcomes** Section 3 requires organizations to execute and document each of the five DIRM steps and their normative outcomes, whatever internal process or tool they use.
- **Three independent assurance levels** IAL, AAL and FAL are selected separately for each user group (Section 1.2), and the final implemented xALs do not all need to be at the same level (Section 3.4.4).
- **Tailoring with a record** Section 3.4 lets an organization modify an initially assessed assurance level or add compensating and supplemental controls after privacy, customer experience and threat assessments, and Section 3.4.4 requires the Digital Identity Acceptance Statement to record the result.
- **Continuous evaluation** Section 3.5 asks for performance metrics (Table 4), evaluation inputs and redress processes, so the selected controls are checked against fraud rates, user impacts and new threats rather than set once.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST SP 800-63

Online Service Register (Section 3.1)

Record each online service's functional scope, user groups, available transactions and impacted entities, the outcome Section 3.1 requires before any assurance level is chosen.

Impact Assessment (Section 3.2)

Hold the impact categories, potential harms and impact levels per user group and the combined low, moderate or high result that drives the initial xAL selection.

Assurance Level Selection (Section 3.3)

Track the initial IAL, AAL and FAL for each user group and the baseline controls identified from SP 800-63A-4, 63B-4 and 63C-4.

Digital Identity Acceptance Statement (Section 3.4.4)

Keep the DIAS for every service with its minimum contents: impact assessment results, initial and tailored xALs with rationale, compensating controls with comparability or residual risk, and supplemental controls.

External Services and Providers

Prepare the DIAS Section 3.4.4 requires for external online services, including software-as-a-service offerings, and review the DIAS of each CSP or IdP the organization relies on.

Evaluation Metrics and Redress (Sections 3.5 and 3.6)

Record the Table 4 performance metrics, evaluation inputs and redress cases, and the DIAS adjustments that follow from them.

Common framework mappings

ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5

Official resources

NIST SP 800-63-4: Digital Identity Guidelines

The umbrella volume of Revision 4 (July 2025): digital identity risk management and the assurance levels for identity proofing, authentication and federation.

pages.nist.gov/800-63-4/sp800-63.html

NIST SP 800-63A-4: Identity Proofing and Enrollment

Outlines the processes for validating identities and enrolling subscribers at each Identity Assurance Level.

pages.nist.gov/800-63-4/sp800-63a.html

NIST SP 800-63B-4: Authentication and Authenticator Management

Describes authenticator requirements, including syncable authenticators (passkeys), and lifecycle management at each Authentication Assurance Level.

pages.nist.gov/800-63-4/sp800-63b.html

NIST SP 800-63C-4: Federation and Assertions

Provides guidance for identity federation, assertions and subscriber-controlled wallets at each Federation Assurance Level.

pages.nist.gov/800-63-4/sp800-63c.html

Frequently asked questions

What changed from NIST SP 800-63-3 to SP 800-63-4?

SP 800-63-4 was published as final on July 31, 2025 and SP 800-63-3 was withdrawn on August 1, 2025. Section 1.3.1 says the revision repurposes IAL1 as a new assurance level, updates authentication risk and threat models, adds options for phishing-resistant authentication, introduces requirements to prevent automated attacks against enrollment, and prepares for mobile driver's licenses and verifiable credentials. Section 1.3.3 adds two concepts, control tailoring and continuous improvement programs, which Section 3 turns into the DIRM process.

What are IAL, AAL and FAL?

Section 1.2 requires an assurance level for each digital identity function: the Identity Assurance Level for identity proofing, the Authentication Assurance Level for authentication, and the Federation Assurance Level for federated transactions between a relying party and a CSP or IdP. Each has three levels, described in Section 3.3.2 and summarized with control objectives and user profiles in Tables 1 to 3; the normative requirements are in SP 800-63A-4, 63B-4 and 63C-4.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What is the Digital Identity Risk Management (DIRM) process?

Section 3 defines five steps: define the online service (3.1), conduct an initial impact assessment for each user group (3.2), select initial assurance levels and baseline controls (3.3), tailor and document the assurance levels (3.4), and continuously evaluate and improve (3.5). Federal RPs SHALL implement it for all online services, and every organization that uses it SHALL execute and document each step and its outcomes, whatever its own processes or tools.

What is a Digital Identity Acceptance Statement?

Section 3.4.4 requires organizations to develop a DIAS for each online service they manage and for each external online service they use, including software-as-a-service offerings. At a minimum it records the initial impact assessment results, the initially assessed xALs, any tailored xAL with its rationale, all compensating controls with their comparability or residual risks, and all supplemental controls. Federal agencies SHOULD include it in the RMF authorization package, and CSPs and IdPs prepare their own DIAS when they deviate from the normative guidance.

Who must follow NIST SP 800-63-4?

Section 1.1 applies the guidelines to all online services for which some assurance in a digital identity is required, primarily services for external users but also federal systems used by employees and contractors, where FIPS 201 extends them. Section 3 is normative for federal relying parties. National security systems are excluded, and private-sector organizations and state, local and tribal governments may consider the standards where appropriate. Section 1.3.1 adds that the controls augment but do not replace the FISMA and RMF controls an agency already has.

License included / downloadable: Yes NIST SP 800-63-4 and its companion volumes are available free of charge from NIST, and the assurance level structure is included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-63

 © 2026 SmartSuite Inc. All rights reserved.