SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management (July 2025)

NIST SP 800-63B-4 (July 31, 2025) sets the authentication requirements for AAL1, AAL2 and AAL3: permitted authenticators, password rules, phishing resistance, timeouts and sessions.



What it is

NIST SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management, is the volume of NIST's SP 800-63-4 suite that sets the technical requirements for authenticating subjects who interact with government information systems over networks, at each of the three Authentication Assurance Levels (AALs). NIST published it as final on July 31, 2025, after drafts of December 16, 2022 and August 21, 2024; it supersedes SP 800-63B of June 2017 (updated March 2, 2020), whose subtitle, Authentication and Lifecycle Management, this page's title still carries. The SP 800-63-4 base volume explains how an organization chooses the AAL a service needs; this volume says what that AAL requires of authenticators, verifiers and sessions.

Sections 2 to 5 and Appendix B are normative. Section 2 defines the AALs: AAL1 gives basic confidence through single-factor or multi-factor authentication; AAL2 gives high confidence through two distinct factors with approved cryptography, and verifiers SHALL offer at least one phishing-resistant option; AAL3 gives very high confidence through a cryptographic authenticator with a non-exportable private key that provides phishing resistance, and syncable authenticators SHALL NOT be used there.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION SP 800-63B-4 (Revision 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/b/4/final

Why it matters

- **Password rules with a rationale** Section 3.1.1.2 lists nine verifier requirements, from the 15-character minimum for single-factor use and the blocklist of commonly used, expected or compromised values to the ban on hints, security questions and periodic changes, with Appendix A explaining why.
- **Phishing resistance by level** Table 1 summarizes it: not required at AAL1, recommended at AAL2 where a phishing-resistant option SHALL be available, required at AAL3 (Section 3.2.5 defines the property).
- **An AAL ladder with timeouts** Each AAL fixes permitted authenticator types, FIPS 140 expectations and reauthentication limits, from a recommended 30-day overall timeout at AAL1 to 12 hours overall and 15 minutes of inactivity at AAL3.
- **Rules for the authenticator's life** Section 4 covers binding at enrollment and afterward, subscriber-provided authenticators, renewal, account recovery by IAL and AAL, loss, theft and compromise, expiration, invalidation and account notifications.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-63B

AAL Assignment by Service

Record the AAL selected for each online service and user group from the base volume's Digital Identity Acceptance Statement, and the Section 2.1 to 2.3 requirement set it triggers.

Authenticator Inventory (Section 3.1)

Hold every authenticator type in use, the AALs it is permitted at, its FIPS 140 validation status and whether it is phishing-resistant, replay-resistant or syncable.

Password Policy Verification (Section 3.1.1.2)

Check each verifier against the nine rules: 15- or 8-character minimums, 64-character maximum allowed, no composition rules, no periodic change, forced change on compromise, no hints or security questions, full verification and the blocklist.

Phishing-Resistant Rollout (Sections 2.2.2 and 3.2.5)

Track which services offer a phishing-resistant option at AAL2 and which staff, contractor and partner populations have moved to phishing-resistant authentication.

Authenticator Events (Section 4)

Log binding, renewal, account recovery, loss, theft, compromise, expiration and invalidation events with the notifications sent to subscribers.

Sessions, Privacy and Redress (Sections 2.4 and 5)

Record reauthentication and inactivity timeouts per AAL, session binding methods, the SAOP analysis, SORN and PIA where triggered, and redress cases.

Common framework mappings

CIS Controls v8.1 | FedRAMP Rev. 5 | GDPR | ISO 27001:2022 | ISO 27002:2022 | ISO 27701 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

NIST SP 800-63B: Digital Identity Guidelines

Defines technical requirements and best practices for digital identity systems, including authentication and lifecycle management.

pages.nist.gov/800-63-3/sp800-63b.html

NIST SP 800-63B Implementation Guidance

Provides detailed implementation guidance to assist organizations in applying digital identity guidelines.

csrc.nist.gov/publications/detail/sp/800-63/3/final

NIST Identity Guidelines Overview

Describes the structure and purpose of the NIST digital identity guidelines series.

pages.nist.gov/800-63-4

Frequently asked questions

What are the password rules in NIST SP 800-63B-4?

Section 3.1.1.2 requires verifiers and CSPs to demand at least 15 characters when a password is the only factor and at least eight when it is part of multi-factor authentication, to allow at least 64 characters, printing ASCII, spaces and Unicode, and to check new passwords against a blocklist of commonly used, expected or compromised values. They SHALL NOT impose composition rules, require periodic changes, store hints visible to unauthenticated claimants or use security questions, and they SHALL verify the entire password and force a change on evidence of compromise. Section 3.1.1 adds that passwords are not phishing-resistant.

Is phishing-resistant authentication mandatory under SP 800-63B-4?

It depends on the level. Section 2.2.2 says verifiers SHALL offer at least one phishing-resistant option at AAL2 and that federal agencies SHALL require their staff, contractors and partners to use phishing-resistant authentication to access federal information systems. Section 2.3.2 requires a phishing-resistant cryptographic authenticator with a non-exportable private key at AAL3. Table 1 summarizes it as not required at AAL1, recommended and available at AAL2, required at AAL3.

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

What changed from SP 800-63B (2017, updated 2020) to SP 800-63B-4?

Appendix E lists the changes: memorized secrets are renamed passwords, the minimum length for single-factor passwords is increased, AAL3 requires a non-exportable cryptographic authenticator rather than a hardware-based one and a lower FIPS 140 validation level, fraud indicators replace pre-authentication checks, VoIP numbers are no longer prohibited for out-of-band authentication, multi-factor out-of-band authenticators and subscriber-controlled wallets are recognized, presentation attack detection is required for facial recognition and voice comparison is prohibited, and syncable authenticators gain requirements in Appendix B. The final version was published July 31, 2025, and the subtitle changed to Authentication and Authenticator Management.

Can passkeys or other syncable authenticators be used, and at which AAL?

Yes at AAL1 and AAL2, under Appendix B, which is normative: keys SHALL be generated with approved cryptography, stored in the sync fabric only in encrypted form, used for private-key operations on the local device, protected by access control and by AAL2-equivalent multi-factor authentication to the fabric, and the policy SHALL be documented; federal enterprise keys SHALL sit in sync fabrics with FISMA moderate protections. Section 2.3.2 says syncable authenticators SHALL NOT be used at AAL3 because AAL3 requires a non-exportable private key.

How often must users reauthenticate at each AAL?

Section 2 sets two timeouts, an overall limit on the session and an inactivity limit. At AAL1 the overall timeout SHOULD be no more than 30 days and no inactivity timeout is required (2.1.3). At AAL2 the overall timeout SHOULD be no more than 24 hours and the inactivity timeout no more than 1 hour, with reauthentication by password or biometric plus the session secret allowed after inactivity (2.2.3). At AAL3 the overall timeout SHALL be no more than 12 hours and the inactivity timeout SHOULD be no more than 15 minutes, with full AAL3 authentication required (2.3.3).

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

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