SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-63B (2017)

NIST SP 800-63B provides digital identity guidelines for authentication and lifecycle management.

What it is

NIST SP 800-63B — Digital Identity Guidelines: Authentication and Lifecycle Management is a federal cybersecurity standard that establishes best practices for authentication processes and the management of digital identity lifecycle events. It serves as a key reference for organizations seeking to mitigate identity-related risks and safeguard access to information systems.

Published by the National Institute of Standards and Technology (NIST), this guideline is used by federal agencies, regulated industries, and organizations implementing robust authentication mechanisms. NIST SP 800-63B addresses areas including secure password policies, multi-factor authentication, credential issuance, and ongoing identity proofing, supporting compliance with broader U.S. government cybersecurity requirements.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION Rev. 3
EFFECTIVE June 2017	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY Moderate

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

Why it matters

- **Strengthen identity assurance** Support verification and authentication processes that reduce unauthorized access and potential account compromise.
- **Enhance regulatory alignment** Facilitate adherence to federal and industry identity standards, simplifying compliance assessments and regulatory reporting.
- **Improve incident detection capabilities** Enable prompt identification and response to anomalous authentication activities, reducing impacts of credential-based attacks.
- **Promote consistent user experience** Establish uniform authentication requirements that minimize user confusion and improve usability across services.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-63B

Identity Assurance Requirement Library

Organize identity assurance levels (IAL), authenticator assurance levels (AAL), and federation assurance levels (FAL) requirements.

Authentication Policy Governance

Manage authentication policies, multi-factor authentication requirements, and credential lifecycle rules.

Identity Lifecycle and Access Management

Track identity creation, provisioning, modification, and deprovisioning activities across systems.

Authentication Evidence and Compliance Tracking

Capture authentication configuration evidence, testing results, and compliance documentation.

Identity Risk and Authentication Failure Tracking

Track identity-related risks, authentication failures, and security incidents involving credential misuse.

Identity Governance and Reporting

Provide dashboards showing authentication compliance, identity risks, and governance oversight.

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 is NIST SP 800-63B used for?

NIST SP 800-63B provides detailed requirements for digital authentication and identity proofing. It is used by organizations, especially those in the U.S. federal sector, to ensure secure user authentication and manage digital identities throughout their lifecycle. The guidelines help reduce risks related to unauthorized access, impersonation, and identity fraud.

Is NIST SP 800-63B required or certifiable?

NIST SP 800-63B is mandatory for U.S. federal agencies implementing digital authentication but is not a certifiable standard like ISO 27001. While private sector compliance is voluntary, many organizations adopt it as a best practice for strong authentication controls and alignment with federal expectations.

What is the scope of NIST SP 800-63B?

NIST SP 800-63B applies to any system where digital identity authentication and lifecycle management are necessary to protect information systems and resources. Its requirements address remote authentication, credential lifecycle management, and authentication assurance levels for applications handling sensitive data.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are the key concepts and artifacts in NIST SP 800-63B?

Key concepts include Authentication Assurance Levels (AALs), password and authenticator requirements, and lifecycle management of credentials. Artifacts generated can include authentication logs, identity proofing records, and documentation supporting adherence to defined assurance levels.

How is NIST SP 800-63B implemented in an organization?

To implement NIST SP 800-63B, organizations must classify applications by the required Authentication Assurance Level, deploy appropriate technical controls such as multi-factor authentication, and establish procedures for enrollment, credential issuance, and revocation. Ongoing monitoring and periodic review of authenticator management are also required.

How does NIST SP 800-63B relate to other frameworks?

NIST SP 800-63B aligns closely with broader cybersecurity standards like NIST SP 800-53 and complements identity management policies found in frameworks such as FIPS 201 (PIV). It can be integrated into overall risk management and compliance programs alongside other regulatory requirements.

What ongoing compliance activities are needed for NIST SP 800-63B?

Ongoing compliance includes periodic review of authenticators, monitoring for compromise, updating credentials as needed, and ensuring procedures for lost, stolen, or inactive authenticators are followed. Regular training, documentation, and audit activities help maintain adherence to the guidelines.

How would SmartSuite support NIST SP 800-63B?

SmartSuite can assist organizations in managing NIST SP 800-63B compliance by tracking authentication-related risks, mapping and managing control requirements, collecting and storing evidence of authentication events, and ensuring audit readiness. Detailed reporting and workflow automation enable continuous monitoring and documentation for lifecycle management and authentication compliance.

License included / downloadable: Yes NIST SP 800-63B is freely available for download from the NIST publications website. License included with platform

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