SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-63-3

NIST SP 800-63 provides risk-based guidelines for digital identity proofing, authentication, and credential management to secure online access.

What it is

NIST SP 800-63 is a federal digital identity guideline that helps organizations assess and manage the assurance of user identities in online environments. The framework provides a risk-based approach to digital identity and authentication, supporting secure access to systems and protecting sensitive information.

Published by the National Institute of Standards and Technology (NIST), NIST SP 800-63 is used by federal agencies and public sector entities, as well as private organizations seeking to align with government cybersecurity and privacy best practices. It covers areas including identity proofing, authentication processes, credential management, and federation protocols to reduce identity-related risks.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION NIST SP 800-63 (Digital Identity Guidelines — current revision)
EFFECTIVE June 2017	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY Moderate

Source: https://pages.nist.gov/800-63-3/

Why it matters

- **Strengthen identity assurance** Enable organizations to verify user identities with higher confidence, helping to prevent unauthorized access and fraud.
- **Support regulatory compliance** Align digital identity management with federal requirements and recognized best practices for audit and reporting obligations.
- **Enhance data protection** Reduce the risk of data breaches by ensuring only authenticated and authorized users can access sensitive information.
- **Promote operational resilience** Minimize operational disruptions by ensuring reliable and secure authentication processes across digital services.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST SP 800-63

Identity Requirements and Assurance Levels

Track IAL/AAL/FAL targets by system and document the rationale.

Identity Proofing and Onboarding Workflows

Manage proofing procedures, approvals, and evidence for identity verification.

MFA and Authentication Governance

Track MFA rollout, enforcement, exceptions, and coverage reporting.

Privileged Access and Lifecycle Controls

Manage joiner/mover/leaver workflows, access reviews, and privilege governance.

Monitoring and Abuse Detection Evidence

Centralize logging, alerting, and investigation records for identity events.

Identity Program Reporting

Report assurance posture, gaps, and remediation by system and user group.

Common framework mappings

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

Official resources

NIST SP 800-63-3: Digital Identity Guidelines

Defines guidelines for digital identity management, providing a framework for identity proofing and authentication.

pages.nist.gov/800-63-3

NIST SP 800-63A: Enrollment and Identity Proofing

Outlines the processes for validating identities and issuing credentials securely.

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

NIST SP 800-63B: Authentication and Lifecycle Management

Describes methods for managing digital authentication systems and maintaining identity integrity.

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

NIST SP 800-63C: Federation and Assertions

Provides guidance for identity federation and the usage of assertions in digital identity systems.

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

Frequently asked questions

What is NIST SP 800-63 used for?

NIST SP 800-63 is used to establish assurance levels for digital identities and authentication processes in online environments. Its guidelines help organizations manage identity-related risks and strengthen secure access for users, particularly in federal and regulated sectors.

Is NIST SP 800-63 mandatory or certifiable?

NIST SP 800-63 is mandatory for federal agencies but not certifiable in the same way as ISO standards; private organizations may choose to align with its requirements to meet regulatory or contractual obligations. Adherence is often driven by organizational risk management and compliance needs.

Who does NIST SP 800-63 apply to?

NIST SP 800-63 primarily applies to U.S. federal agencies that provide digital services but can also be adopted by state agencies and private entities seeking to align with federal security and privacy best practices. Its applicability is determined by the level of identity assurance required for a system or process.

What are the key concepts or artifacts required under NIST SP 800-63?

Core concepts include Identity Assurance Level (IAL), Authenticator Assurance Level (AAL), and Federation Assurance Level (FAL). Required artifacts include documented risk assessments, identity proofing procedures, authentication mechanisms, and evidence of compliance with each lifecycle stage.

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

How does an organization implement NIST SP 800-63?

Implementation starts by conducting a risk assessment to determine appropriate assurance levels, followed by selection and deployment of suitable identity proofing, authentication, and federation controls. Integration with IAM systems and ongoing monitoring are essential to meet NIST SP 800-63 requirements.

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

NIST SP 800-63 complements broader frameworks such as the NIST Risk Management Framework (RMF) by providing specific guidance on digital identity management. It integrates with organizational cybersecurity and privacy policies to enhance data protection and regulatory compliance.

What are the ongoing compliance requirements for NIST SP 800-63?

Ongoing compliance involves regular review of risk assessments, monitoring authentication events, maintaining current documentation, and implementing incident response measures for identity-related threats. Periodic audits and continuous improvement of identity controls are recommended.

How would SmartSuite support NIST SP 800-63?

SmartSuite enables organizations to operationalize NIST SP 800-63 by mapping guideline requirements to control libraries, tracking risks, and managing policy governance. The platform supports evidence collection, compliance tracking, and remediation workflows, facilitating audit readiness and comprehensive reporting for digital identity management.

License included / downloadable: Yes NIST SP 800-63 is published by the National Institute of Standards and Technology and is publicly available through official NIST publications.

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