



1

2

NIST Special Publication NIST SP 800-63-4 ipd

3

Digital Identity Guidelines

4

Initial Public Draft

5

David Temoshok

6

Diana Proud-Madruga

7

Yee-Yin Choong

8

Ryan Galluzzo

9

Sarbari Gupta

10

Connie LaSalle

11

Naomi Lefkovitz

12

Andrew Regenscheid

13

This publication is available free of charge from:

14

<https://doi.org/10.6028/NIST.SP.800-63-4.ipd>

15

16 NIST Special Publication
17 NIST SP 800-63-4 ipd
18 Digital Identity Guidelines
19 Initial Public Draft

20 David Temoshok
21 Ryan Galluzzo
22 Connie LaSalle
23 Naomi Lefkovitz
24 *Applied Cybersecurity Division*
25 *Information Technology Laboratory*

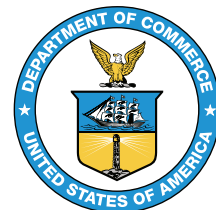
26 Andrew Regenscheid
27 *Computer Security Division*
28 *Information Technology Laboratory*

29 Yee-Yin Choong
30 *Information Access Division*
31 *Information Technology Laboratory*

32 Diana Proud-Madruga
33 Sarbari Gupta
34 *Electrosoft*

35 This publication is available free of charge from:
36 <https://doi.org/10.6028/NIST.SP.800-63-4.ipd>

37 December 2022



39 U.S. Department of Commerce
40 Gina M. Raimondo, Secretary

41 National Institute of Standards and Technology
42 Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at <https://csrc.nist.gov/publications>.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

[Copyright, Fair Use, and Licensing Statements](#)
[NIST Technical Series Publication Identifier Syntax](#)

77 **Publication History**

78 Approved by the NIST Editorial Review Board on YYYY-MM-DD [will be added upon
79 final publication]

80 **How to Cite this NIST Technical Series Publication**

81 Temoshok D, Proud-Madruga D, Choong YY, Galluzzo R, Gupta S, LaSalle C, Lefkovitz
82 N, Regenscheid A (2022) Digital Identity Guidelines. (National Institute of Standards and
83 Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63-4 ipd.
84 <https://doi.org/10.6028/NIST.SP.800-63-4.ipd>

85 **Author ORCID iDs**

86 David Temoshok: 0000-0001-6195-0331
87 Diana Proud-Madruga: 0000-0002-8972-7809
88 Yee-Yin Choong: 0000-0002-3889-6047
89 Ryan Galluzzo: 0000-0003-0304-4239
90 Sarbari Gupta: 0000-0003-1101-0856
91 Connie LaSalle: 0000-0001-6031-7550
92 Naomi Lefkovitz: 0000-0003-3777-3106
93 Andrew Regenscheid: 0000-0002-3930-527X

94 **Public Comment Period**

95 December 16, 2022 - March 24, 2023

96 **Submit Comments**

97 <mailto:dig-comments@nist.gov>

98 **All comments are subject to release under the Freedom of Information Act**
99 **(FOIA).**

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government information systems over networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions. This publication will supersede NIST Special Publication 800-63-3.

Keywords

authentication; authentication assurance; authenticator; assertions; credential service provider; digital authentication; digital credentials; identity proofing; federation; passwords; PKI.

Note to Reviewers

The rapid proliferation of online services over the past few years has heightened the need for reliable, equitable, secure, and privacy-protective digital identity solutions.

Revision 4 of NIST Special Publication 800-63, Digital Identity Guidelines, intends to respond to the changing digital landscape that has emerged since the last major revision of this suite was published in 2017 — including the real-world implications of online risks. The guidelines present the process and technical requirements for meeting digital identity management assurance levels for identity proofing, authentication, and federation, including requirements for security and privacy as well as considerations for fostering equity and the usability of digital identity solutions and technology.