NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Digital Identity Webinar Series: Future of Authentication

NIST Information Technology Laboratory

16 March 2023

Welcome

David Temoshok, Digital Identity Guidelines Lead

Why are we here today?

Purpose:

- ➢ Continue our public engagement on the DRAFT of NIST SP 800-63-4
- ➢ Provide an opportunity to get insight from a panel of subject matter experts on relevant topics to the update
- ➢ Provide an opportunity for the public to engage in discussion around specific aspects of the guidance

Outcomes:

- ✓ Reinforce the intended updates to the DRAFT of NIST SP 800-63B-4 *Authenticator and Lifecycle Management*
- ✓ Get insights from across different communities and sectors
- ✓ Initiate a public dialogue that will extend across the three sessions

****** NOTE: Participating in this session is not a replacement for comments! Please engage both here and through the established NIST process.***

A Quick Announcement!

To allow for continued engagement and additional input from across diverse communities we will be extending our comment period!

The new Deadline will be 11:59pm on April 14th !

Details for how and where to submit comments remains the same and can be found at the end of this presentation

Some Notes on Engagement

NIST

On Webex, Andrew will host a moderated panel of experts featuring:

- John Bradley, *Senior Principal Architect, Yubico*
- Libby Brown, *Senior Program Manager- Cloud Authentication, Microsoft*
- Christine Owen, *Director, Guidehouse*
- Mike Prorock, *CTO and Founder, mesur.io*

On Slack we will host an open discussion where:

- Everyone can respond to the questions posed to our panel…
- Everyone can engage in discussion, debate, and constructive feedback…
- Everyone can submit questions for NIST team members and panelists (we may not get to all of them…)
- But that is ok, because the Slack will remain open through the close of the comment period on March 24th
- Looking for the invite to the slack? We have posted in the Webex chat over here*

* Accuracy of arrow not guaranteed…

Slack Rules of the Road

Be polite and be respectful!

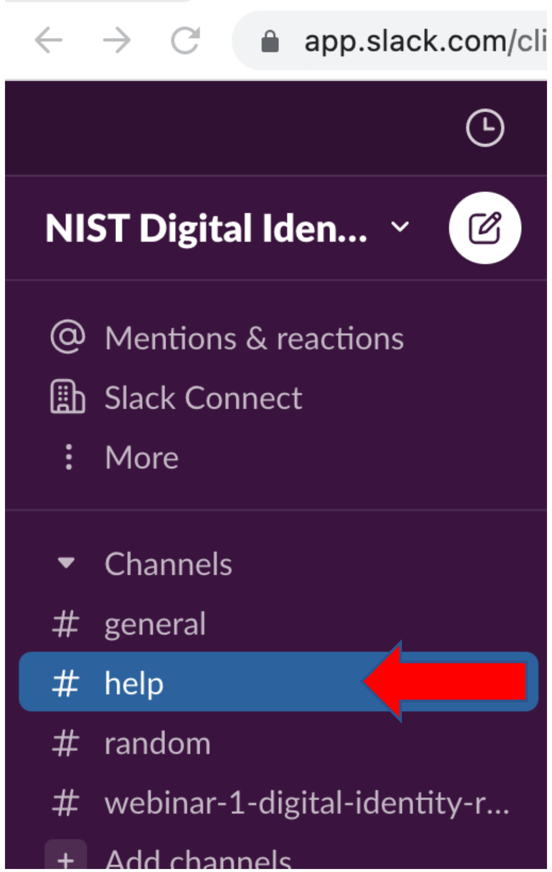
Be constructive!

No spam, no marketing!

Debate, discussion, and questions are encouraged!

Webex Captioning

Our panel will be simulcast with live captioning. The link to access this is posted in the Webex Chat and in the "help" section of Slack



app.slack.com/cli

NIST Digital Iden...

Mentions & reactions

Slack Connect

More

Channels

general

help

random

webinar-1-digital-identity-r...

Add channels

NIST SP 800-63B-4: *Authenticator and Lifecycle Management*

Andrew Regenscheid, NIST

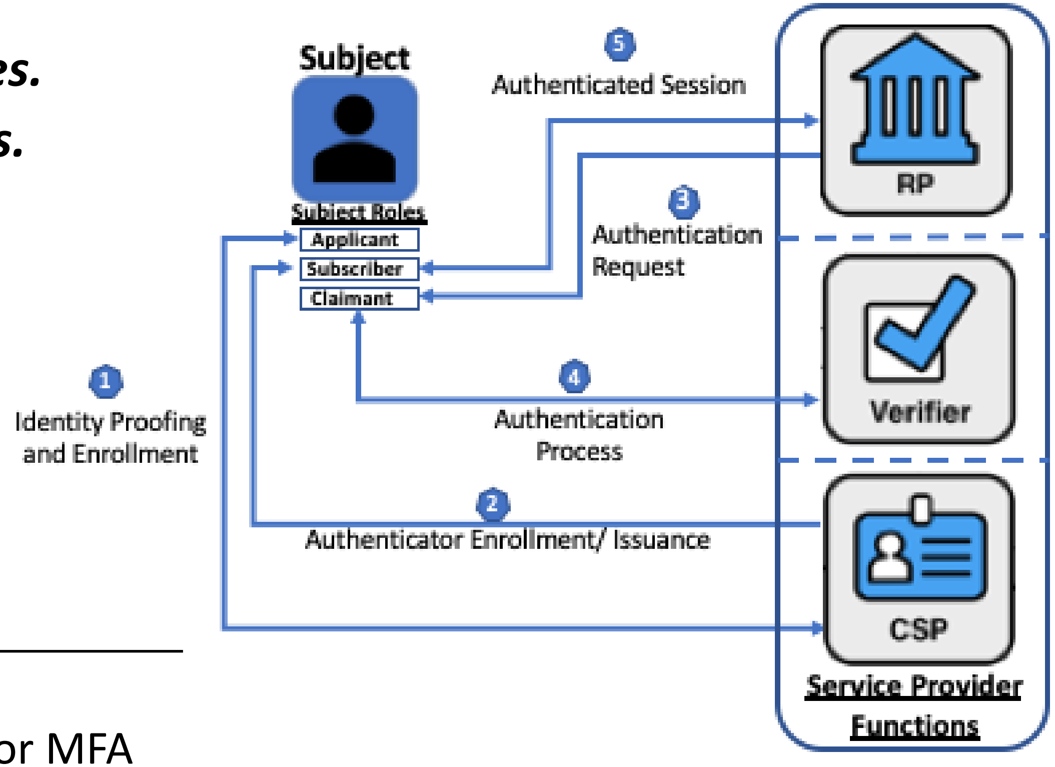
SP 800-63B Overview

Scope: Authentication and Lifecycle Management

- Authenticators to authenticate ***subjects*** to ***relying parties.***
- Authentication processes and protocols used by ***verifiers.***
- Lifecycle:
  - Authenticator Selection and equity considerations
  - Authenticator Binding/Issuance
  - Session management
  - Account recovery

Authentication Assurance Levels

AAL1	• Single-factor authentication
AAL2	• Multifactor authentication • Supports implementation of EO 14028 and EO 13681 for MFA
AAL3	• Hardware-based, cryptographic multifactor authentication • Phishing resistant in support of OMB M -22-09 • Supported by PIV at federal agencies, consistent with HSPD-12



Highlights – 800-63B

- **Phishing Resistance** – Able to be achieved through one of two techniques: Channel Binding (such as mutual TLS) and Verifier Name Binding (WebAuthn/FIDO).
- **Password Guidelines** – Advances previous recommendations by requiring the removal of complexity, arbitrary rotation requirements, and allowing for password managers.
- **Activation Secrets** – Splits out requirements for secrets used for activation of a device (e.g., mobile phone) from requirements from those that are remotely verified over a network.
- **Biometric Requirements** – Biometrics remain allowable as part of an MFA scheme that includes a physical authenticator but performance metrics have been updated to align to new industry standards (FMR 1:10,000)
- **Out-of-Band Changes** – Removed the option for push notifications that do not require the user to enter a secret to account for prevalence of MFA exhaustion attacks.
- **Wireless Authenticators** – includes new requirements for the connection of wireless (e.g., bluetooth, NFC) authenticators for use in an MFA scheme.
- **Equity Considerations for Authenticators and Recovery** – Provides recommendations for account recovery options where users may not have the ability bind multiple authenticators. Also considers the need to maintain widely available authenticators - such as SMS - to provide MFA for diverse populations.
- **Cryptographic Authenticators** – Removes the restriction on “facilitating cloning” to allow for synching and back of keys. Maintains “non-exportability” at AAL3. *Still evaluating the potential impact of Passkey*.

Panel of Experts

Meet the Panel

John Bradley
Senior Principal Architect,
Yubico

Libby Brown
Senior Program Manager,
Cloud Authentication,
Microsoft

Christine Owen
Director,
Guidehouse

Mike Prorock
CTO and Founder,
mesur.io

Closing

David Temoshok, Digital Identity Guidelines Lead

Comment Period

- Where can I find the documents?
  - 800-63-4: Base Volume
  - 800-63A-4: Identity Proofing and Enrollment
  - 800-63B-4: Authentication and Lifecycle Management
  - 800-63C-4: Federation and Assertions
- How do I submit comments?
  - Email them to: dig-comments@nist.gov
- What format should my comments be in?
  - The preferred format is the comment sheet available here: Comment template (xls)
- What kind of comments are most helpful?
  - All of them!
  - Reference our Note to Reviewers for specific questions
  - Please do not send marketing material

- What if I have questions before I submit comments?
  - Email any questions or requests for clarifications you may have to: dig-comments@nist.gov
  - We will do our best to respond to as many questions as possible
- Will my comments be made public?
  - Yes! Our process is open and transparent and we will post all comments as issues on our GitHub repository
- How can I keep up to speed on any changes?
  - There will not be changes to the text between now and the close of the comment period
  - But, if we get frequent comments or areas where clarification is regularly requested, we will post them to our "Ongoing Updates" page
  - Follow along at: https://pages.nist.gov/800-63-4/

Comment period extended!

COMMENTS ARE DUE APRIL 14th