Draft Special Publication
800-63-3
Digital Identity Guideline
(formerly known as Electronic Authentication Guideline)

SP 800-63-3
Digital Authentication Guideline

SP 800-63A
Identity Proofing & Enrollment

SP 800-63B
Authentication & Lifecycle Management

SP 800-63C
Federation & Assertions

https://pages.nist.gov/800-63-3
http://csrc.nist.gov/publications/PubsDrafts.html#800-63-3
Why the update?

• Implement Executive Order 13681: *Improving the Security of Consumer Financial Transactions*
• Align with market and promote (adapt to) innovation
• Simplify and provide clearer guidance
• International alignment
Highlights from the Public Preview

May – September 2016

- 12,000+ Views on Github
- 3,600+ Unique Visitors
- 250+ Comments
- 200 Pull Requests
- 30 Contributors
- 503 Commits
Significant Updates

Where we expect comments to focus on
SP 800-63-3
Digital Authentication Guideline
# Reference to Previous Versions of 800-63

<table>
<thead>
<tr>
<th>800-63-2</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sections 1 – 4</td>
<td>800-63-3</td>
</tr>
<tr>
<td>Section 5</td>
<td>800-63A</td>
</tr>
<tr>
<td>Sections 6 – 8</td>
<td>800-63B</td>
</tr>
<tr>
<td>Section 9</td>
<td>800-63C</td>
</tr>
</tbody>
</table>
New Model

Old

LOA
Level of Assurance

New

IAL
Identity Assurance Level

Robustness of the identity proofing process and the binding between an authenticator and a specific individual

AAL
Authentication Assurance Level

Confidence that a given claimant is the same as a subscriber that has previously authenticated

FAL
Federation Assurance Level

Combines aspects of the federation model, assertion protection strength, and assertion presentation used in a given transaction into a single, increasing scale
Why change LOA?

OMB M-04-04:

LOA determined by “determining the potential impact of authentication errors”

However, an authentication error is not a singleton:

1: Authentication error = attacker steals authenticator
2: Proofing error = attacker proofs as someone else

…and...

Requiring authN and proofing to be the same could be inappropriate
Which also means LOA2 is gone

Identity proofing \(\equiv\) LOA2 \(\equiv\) LOA3

“...consistent with the guidance set forth in the 2011 National Strategy for Trusted Identities in Cyberspace, to ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate.”
Identity Assurance Levels (IALs)

Refers to the robustness of the identity proofing process and the binding between an authenticator and a specific individual

<table>
<thead>
<tr>
<th>IAL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Self-asserted attribute(s) – 0 to n attributes</td>
</tr>
<tr>
<td>2</td>
<td>Remotely identity proofed</td>
</tr>
<tr>
<td>3</td>
<td>In-person identity proofed</td>
</tr>
</tbody>
</table>
Authenticator Assurance Levels (AALs)

Describes the robustness of confidence that a given claimant is the same as a subscriber that has previously authenticated.

<table>
<thead>
<tr>
<th>AAL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Single-factor authentication</td>
</tr>
<tr>
<td>2</td>
<td>Two-factor authentication</td>
</tr>
<tr>
<td>3</td>
<td>Two-factor authentication with hardware token</td>
</tr>
</tbody>
</table>
Federation Assurance Levels (FALs)

Combines aspects of the federation model, assertion protection strength, and assertion presentation used in a given transaction into a single, increasing scale

<table>
<thead>
<tr>
<th>FAL</th>
<th>Presentation Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bearer assertion, signed by IdP</td>
</tr>
<tr>
<td>2</td>
<td>Bearer assertion, signed by IdP and encrypted to RP</td>
</tr>
<tr>
<td>3</td>
<td>Holder of key assertion, signed by IdP and encrypted to RP</td>
</tr>
</tbody>
</table>
If you love M-04-04…

<table>
<thead>
<tr>
<th>M-04-04 Assurance</th>
<th>IAL</th>
<th>AAL</th>
<th>FAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2 or 3</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>2 or 3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
…but, digital services today

<table>
<thead>
<tr>
<th>M-04-04 Assurance</th>
<th>IAL</th>
<th>AAL</th>
<th>FAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1, 2 or 3</td>
<td>1, 2, 3, or 4</td>
</tr>
<tr>
<td>2</td>
<td>1 or 2</td>
<td>2 or 3</td>
<td>2 or 3</td>
</tr>
<tr>
<td>3</td>
<td>1 or 2</td>
<td>2 or 3</td>
<td>2 or 3</td>
</tr>
<tr>
<td>4</td>
<td>1, 2 or 3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
A real example

Assessed at LOA1:

- **No proofing** (Green check)
- **Single factor authN** (Red cross)

Should be:

- **IAL1: No proofing** (Green check)
- **AAL2 (or higher): Multifactor authN** (Green check)
A future example

Health Tracker Application

Old Model

1. Assess at LOA3 and unnecessarily proof individual
   OR
2. Assess at LOA1 and use single-factor authN

New Model

1. Assess at IAL1 because agency has no need to know identity
   AND
2. Assess at AAL2+ because the information shared is personal data (EO 13681)
Choose Your Own AAL

Discover Your Authenticator Assurance Level (AAL)

1. What are the risks (to the organization or the subject) of providing the digital service? Perform the OMB M-04-04 risk assessment.

<table>
<thead>
<tr>
<th>Inconvenience, distress, or damage to standing or reputation</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial loss or agency liability</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Harm to agency programs or public interests</td>
<td>N/A</td>
<td>Low-Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Unauthorized release of sensitive information</td>
<td>N/A</td>
<td>Low-Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Personal safety</td>
<td>N/A</td>
<td>Low</td>
<td>Moderate-High</td>
</tr>
<tr>
<td>Civil or criminal violations</td>
<td>N/A</td>
<td>Low-Moderate</td>
<td>High</td>
</tr>
</tbody>
</table>

Did you assess at moderate for any of the remaining categories?

No → Did you assess at high for any of the above?

Yes → Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?

No → AAL 1

Yes → Did you assess at moderate for personal safety?

No → AAL 2

Yes → AAL 3

Are you making personal data accessible?

No → AAL 1

Yes → AAL 2

End

See federation recommendations.
Discover Your Identity Assurance Level (IAL)

1. To provide the service, do you need any individual attribute information?
   - no
   - yes

2. To complete the transaction, do you need the information to be validated?
   - no
   - I don’t know.
   - yes

3. What are the risks (to the organization or the subject) of providing the digital service?
   Perform the OMB M-04-04 risk assessment.
   - Inconvenience, distress, or damage to standing or reputation
     - Low
     - Moderate
     - High
   - Financial loss or agency liability
     - Low
     - Moderate
     - High
   - Harm to agency programs or public interests
     - N/A
     - Low-Moderate
     - High
   - Unauthorized release of sensitive information
     - N/A
     - Low-Moderate
     - High
   - Personal safety
     - N/A
     - Low
     - Moderate-High
   - Civil or criminal violations
     - N/A
     - Low-Moderate
     - High

4. Did you assess at moderate for any of the remaining categories?
   - no
   - yes

5. Did you assess at high for any of the above?
   - no
   - yes

6. Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?
   - no
   - yes

7. IAL 1
8. IAL 2
9. IAL 3

4. Do you need to resolve an identity uniquely?
   - yes
   - no

5. Can you accept claims?
   - yes
   - no

6. Use claims if you can complete the transaction or offer the service without complete attribute values.

Choose Your Own IAL
Including step-wise guidance
SP 800-63A
Identity Proofing & Enrollment
A Stronger Identity Proofing Process
Components of Stronger ID Proofing

- Clarifies methods for resolving an ID to a single person
- Establishes strengths evidence, validation, and verification
  - Unacceptable, Weak, Fair, Strong, Superior
- Moves away from a static list of acceptable documents and increases options for combining evidence to achieve the desired assurance level
- Visual inspection no longer satisfactory at higher IAL
- TFS-related requirements are gone
- Reduced document requirements in some instances
- Clearer rules on address confirmation
Expanding & Clarifying Identity Proofing Options

✓ Virtual in-person proofing counts as in-person

✓ Remote notary proofing

✓ Remote selfie match

✓ Trusted referees (e.g., notaries)
Knowledge Based Verification’s Role in Identity Proofing

• No restrictions in the resolution phase of ID Proofing

• Highly restrictive in verification phase
  o Strict and clear rules on the use of KBVs
  o Definition of proper/allowable data sources
  o Prefers knowledge of recent Tx over static data
  o Cannot be standalone
SP 800-63B
Authentication & Lifecycle Management
Authenticators

- Memorized Secrets
- Look-up Secrets
- Out-of-Band Devices
- Single Factor OTP Device
- Multi-Factor OTP Devices
- Single Factor Cryptographic Devices
- Multi-Factor Cryptographic Software
- Multi-Factor Cryptographic Devices
Authenticator Guidance

Changes

“Token” is out
“Authenticator” is in

Greater allowance for biometrics, but with rules

SMS OTP Requirements

OTP via email is out

Pre-registered knowledge tokens are out
New authenticators at AAL3 (aka LOA4)

<table>
<thead>
<tr>
<th>FIPS 140-2</th>
<th>Level 1/Physical Level 3</th>
<th>Level 2/Physical 3</th>
</tr>
</thead>
</table>

### Why it matters

- M-05-24 Applicability (*Action Item 1.3.2*)
- Derived PIV Credentials (*Action Item 1.3.2*)
- Consumers already have these (*Action Item 1.3.1*)
- PIV Interoperability should expand beyond PKI (*Action Item 1.3.2*)

*Action Item 1.3.2: The next Administration should direct that all federal agencies require the use of strong authentication by their employees, contractors, and others using federal systems.

“The next Administration should provide agencies with updated policies and guidance that continue to focus on increased adoption of strong authentication solutions, including but, importantly, not limited to personal identity verification (PIV) credentials.”

- *Commission on Enhancing National Cybersecurity, Report on Securing and Growing the Digital Economy, December 1, 2016*
Password Guidance Changes

• Same requirements regardless of AAL
• SHALL be minimum of 8 characters.
• SHOULD (with heavy leaning to SHALL) be:
  o Any allowable unicode character
  o Up to 64 characters or more
  o No composition rules
  o Won’t expire
  o Dictionary rules
• SHALL - Storage guidance to deter offline attack (salt, hash, HMAC)
## Reauthentication

<table>
<thead>
<tr>
<th>AAL</th>
<th>Description</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Presentation of any one factor</td>
<td>30 days</td>
</tr>
<tr>
<td>2</td>
<td>Presentation of any one factor</td>
<td>12 hours or 30 minutes of activity</td>
</tr>
<tr>
<td>3</td>
<td>Presentation of all factors</td>
<td>12 hours or 15 minutes of activity</td>
</tr>
</tbody>
</table>
SP 800-63C
Federation & Assertions
| 1 | Discusses multiple models & privacy impacts & requirements |
| 2 | Many SHOULDs – document needs to be agnostic |
| 3 | Modernized to include OpenID Connect |
| 4 | Clarifies Holder of Key (HOK) for the new AAL 3 |
| 5 | Attribute requirements |
Attribute Claims vs. Values

Maturity Model

High

No Federation Over Collection

Federation Over Collection

Federation Just Values

Federation Just Claims

Low

Old

Give me date of birth.

Give me full address.

New

I just need to know if they are older than 18.

I just need to know if they are in congressional district X.

New Requirements

**CSP** SHALL support claims and value API

**RP** SHOULD request claims
Retaining the New Development Approach

Iterative – publish, comment, and update in a series of drafting sprints

2. Collect public comments via GitHub.
3. Adjudicate comments on GitHub.
4. Update draft documents on GitHub.
5. Close public comment period.
Contributing During Public Comment

Preferred Method
- NIST pages on GitHub

Supported Method
- PDF on CSRC.nist.gov
- Email using comment matrix

Comment
- Submit GitHub issues

All email comments will be made into GitHub issues.
Advanced Contribution Option

<table>
<thead>
<tr>
<th>Owners</th>
<th>Feb</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Stable Version

Where to send pull requests
What’s Next

Public Draft Comment Period
- opens January 30, 2017
- closes March 31, 2017

Final Document
- expected Q2 FY17

Implementation Guidance
- ~= Operations Manual/Implementation Guide v0.1 focused on proofing
In Closing

01 Major Update
Biggest update since original version. Did we get it right?

02 Innovation
Focused on private sector capabilities. Did we future-proof it?

03 International
Need 1 less of these than # of countries. OK? Use cases?

04 Participate
Not our document. It’s yours. Participate!