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

SP 800-63-3
Digital Identity Guidelines

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 Comment Period

January – May 2017

- 4900+ Views on Github
- 540+ Unique Visitors
- 1113 Comments
- ~800 Accepted
- ~142 Duplicates
- ~239 Decline/Noted
Significant Updates
Making 800-63 More Accessible

800-63-3
The Mother Ship

800-63A
Identity Proofing & Enrollment

800-63B
Authentication & Lifecycle Management

800-63C
Federation & Assertions

Streamlined Content & Normative Language

Privacy Requirements & Considerations

User Experience Considerations
SP 800-63-3
Digital Identity Guideline
In the beginning... OMB M-04-04

- Issued in 2003
- Established 4 LOAs
- Established Risk Assessment Methodology
- Established Applicability: Externally Facing Systems
- Tasked NIST with 800-63
- FIPS201/PIV Program Uses Same LOA Model
What are Levels of Assurance

Increased confidence in: vetting and credential use

LOA1
LOA2
LOA3
LOA4

We got a problem

LOA mitigates the risk associate of a potential authentication error
What’s wrong with LOA2?

SP 800-63-2

identity proofing  LOA2  ≡  LOA3

EO 13681

“…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.”
Not to mention…

OMB M-04-04:

LOA selected 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
A real example

Assessed at LOA1:

- No proofing
- Single factor authN

Should be:

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

Health Tracker Application

Old Model

Assess at LOA3 and unnecessarily proof individual

OR

Assess at LOA1 and use single-factor authN

New Model

Assess at IAL1 because agency has no need to know identity

AND

Assess at AAL2+ because the information shared is personal data (EO 13681)
The Plan

- OMB rescinds M-04-04
- 800-63-3 takes on digital identity risk management and becomes normative
- eAuth risk assessment goes away, Risk Management Framework ’adorned’ with identity risks and impacts
- Agencies have risk-based flexibility
- But if they take it, a digital identity acceptance statement is needed

*OMB reserves the right to change said plan
Robustness of the identity proofing process and the binding between an authenticator and a specific individual

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

Combines aspects of the federation model, assertion protection strength, and assertion presentation used in a given transaction into a single, increasing scale
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 (and a provision for attended remote)</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 authenticator</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>
So go ahead and mix-n-match

<table>
<thead>
<tr>
<th></th>
<th>AAL1</th>
<th>AAL2</th>
<th>AAL3</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAL1 without PII</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>IAL1 with PII</td>
<td>No</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>IAL2</td>
<td>No</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>IAL3</td>
<td>No</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
</tbody>
</table>
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.

- 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

2. Are you making personal data accessible?
   - no
   - yes

- AAL 1
- AAL 2
- AAL 3

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

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

Did you assess at moderate for personal safety?
- no
- yes

End

See federation recommendations.
Choose Your Own IAL

Discover Your Identity Assurance Level (IAL)

Start

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

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

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

IAL 1

IAL 2

IAL 3

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

5. Can you accept claims?
   - no
   - yes

End

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

See federation recommendations.
Including step-wise guidance

Figure 5-2 - Selecting IAL

The risk assessment and selection of IAL can be short circuited by answering this question first. If the service does not require any personal information, or if self-asserted information is not required, the service can be provided with all the personal information it requires.

Figure 5-1 - Selecting 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.

Step 1 asks agencies to look at the potential impacts of an authentication failure. In other words, what would occur if an unauthorized user accessed one or more valid user accounts. Risk should be considered from the perspective of the organization and to a valid user, since one may not be negatively impacted while the other could be significantly harmed. The risk assessment process of M-04-04 and any agency specific risk management process should commence from this step.

2. Are you making personal data accessible?

EO 13681 requires MFA when any personal information is made available online. Since the other paths in this decision tree already drive the agency to an AAL that requires MFA, the question regarding personal information is only raised at this point. That said, personal information release at all AALs should be considered when performing the risk assessment. An important point at this step is that the collection of personal information, if not made available online, does not need to be validated or require an AAL of 2 or higher. Release of even self-asserted personal information requires account protection via MFA. Even though self-asserted information can be falsified, most users will provide accurate information to benefit from the digital service. As such, self-asserted data must be protected appropriately.

3. Can you accept claims?

Step 5 focuses on whether the digital service can be provided without having access to full attribute values. This does not mean all attributes must be delivered as claims, but this step does ask the agency to look at each personal attribute they have determined they need, and identify which ones can suffice as claims and which ones need to be complete values. A federated environment is best suited for receiving claims, as the digital service provider is not in control of the attribute information to start with. If the application also performs all required identity proofing, claims may not make sense since full values are already under control of the digital service provider.

If the agency has reached Step 6, claims should be used. This step identifies the digital service as an excellent candidate for accepting federated attribute claims from a CSP (or multiple CSP’s), since it has been determined that complete attribute values are not needed to deliver the digital service.
SP 800-63A
Identity Proofing & Enrollment
The Identity Proofing Process

1. Resolution
   Core attributes and evidence collected

2. Validation
   Evidence validated

3. Verification
   Evidence verified

Individual uniquely distinguished among a given population or context

Linkage between claimed identity and real-life existence of subject presenting evidence confirmed and established

Subscriber
What’s new with ID Proofing

- Clarifies methods for resolving an ID to a single person
- Establishes strengths for 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
Knowledge Based Verification’s Role in Identity Proofing

- No restrictions in the resolution phase of ID Proofing
- Highly restrictive in verification phase
- Strict and clear rules on the use of KBVs
- Definition of proper/allowable data sources
- Prefers knowledge of recent Tx over static data
- Cannot be standalone
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 Devices
- Multi-Factor Cryptographic Software
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)

**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.”

Password Guidance Changes

- Same requirements regardless of AAL
- SHALL be minimum of 8 characters.
- SHOULD (with heavy leaning to SHALL) be:
  - Any allowable unicode character
  - Up to 64 characters or more
  - No composition rules
  - Won’t expire
  - 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
800-63-C
Federation & Assertions

1. Discusses multiple models & privacy impacts & requirements
2. Modernized to include OpenID Connect
3. Clarifies Holder of Key (HOK) for the new AAL 3
4. Attribute requirements
Anywhere assertions are used

Intra/inter-agency federated credentials

Commercial federated credentials

(but 800-63-3 remains agnostic to any architecture)
Attribute Claims vs. Values

Maturity Model

High

Low

No Federation

Over Collection

Federation

Over Collection

Federation

Just Values

Federation

Just Claims

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

Access Document

Preferred Method
- NIST pages on GitHub

Comment
- Submit GitHub issues

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

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>usnistgov</td>
<td></td>
</tr>
</tbody>
</table>

**Stable Version**

**Where to send pull requests**
What's Next

Public Draft Open Comment Period

- opens January 30, 2017
- closes May 1, 2017 (-3 only)

Final Document

- expected Summer 2017

Implementation Guidance

-~= Operations Manual/Implementation Guide v0.1 focused on proofing
Fostering Growth

Seeking new ways to engage our stakeholders in order to promote innovation and best practices, while reducing risk and avoiding an ever-constantly moving target.
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!
Backup
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