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

National Institute of Standards and Technology
U.S. Department of Commerce

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

The White House
Office of the Press Secretary

For Immediate Release October 17, 2014

Executive Order --Improving the Security of Consumer Financial Transactions

EXECUTIVE ORDER

- - - - - - -

IMPROVING THE SECURITY OF CONSUMER FINANCIAL TRANSACTIONS

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

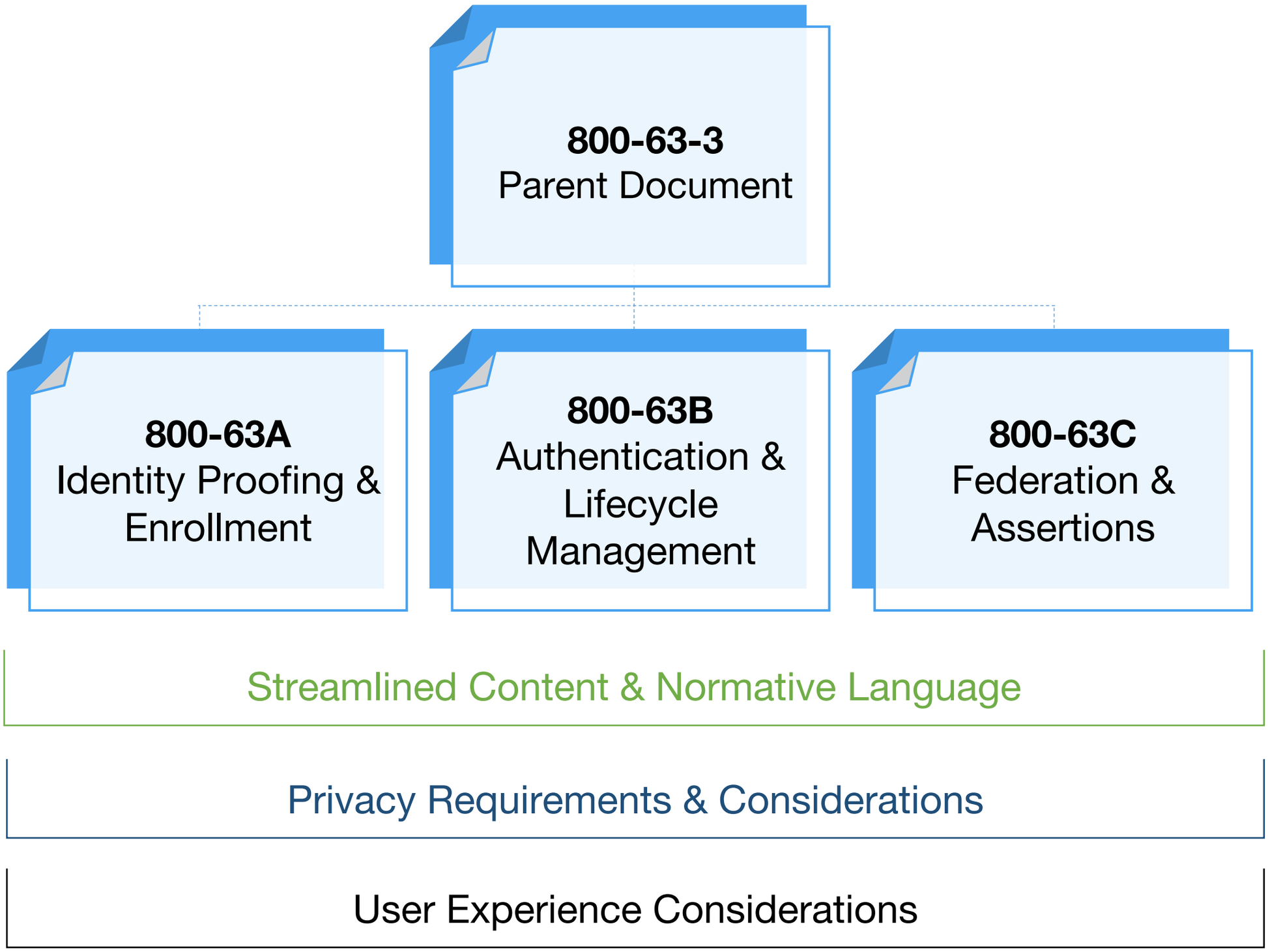
Significant Updates

Where we expect comments to focus on

SP 800-63-3

Digital Authentication Guideline

Making 800-63 More Accessible



Reference to Previous Versions of 800-63

800-63-2	New
Sections 1 – 4	800-63-3
Section 5	800-63A
Sections 6 – 8	800-63B
Section 9	800-63C

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

SP 800-63-2

identity proofing LOA2 ≅ LOA3

LOA1 ≅ LOA2 authenticators

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."

Identity Assurance Levels (IALs)

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

IAL	Description
1	Self-asserted attribute(s) – 0 to n attributes
2	Remotely identity proofed
3	In-person identity proofed

Authenticator Assurance Levels (AALs)

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

AAL	Description
1	Single-factor authentication
2	Two-factor authentication
3	Two-factor authentication with hardware token

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

FAL	Presentation Requirement
1	Bearer assertion, signed by IdP
2	Bearer assertion, signed by IdP and encrypted to RP
3	Holder of key assertion, signed by IdP and encrypted to RP

If you love M-04-04…

M-04-04 Assurance	IAL	AAL	FAL
1	1	1	1
2	2	2 or 3	2
3	2	2 or 3	2
4	3	3	3

…but, digital services today

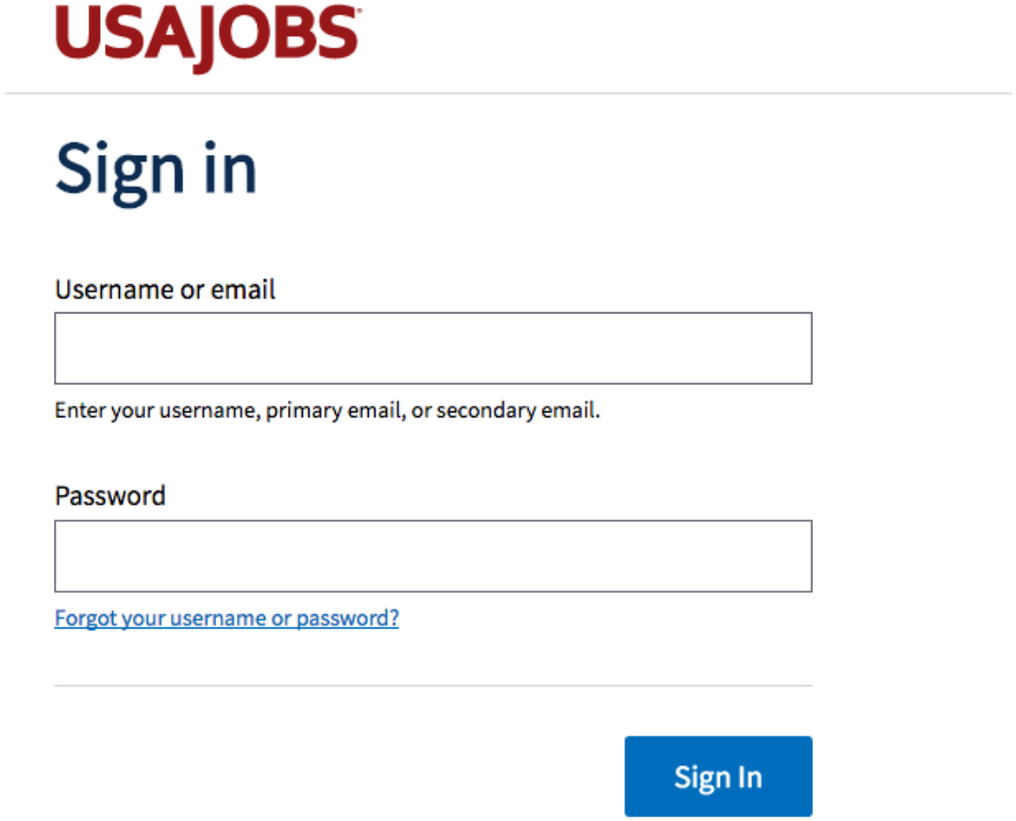
M-04-04 Assurance	IAL	AAL	FAL
1	1	1, 2 or 3	1, 2, 3, or 4
2	1 or 2	2 or 3	2 or 3
3	1 or 2	2 or 3	2 or 3
4	1, 2 or 3	3	3

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)

Choose Your Own AAL

Discover Your Authenticator Assurance Level (AAL)

Start

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

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

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

2 Are you making personal data accessible?

no

yes

Did you assess at high for any of the above?

no

yes

Did you assess at moderate for personal safety?

no

yes

AAL 1

AAL 2

AAL 3

AAL

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 → 2
   - yes → 2
2. To complete the transaction, do you need the information to be validated?
   - no → IAL 1
   - I don't know. → 3
   - yes → 3
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 → 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 → IAL 1
    - yes → IAL 2
  - yes → IAL 2
- Did you assess at high for any of the above?
  - no → Did you assess at moderate for personal safety?
    - no → IAL 2
    - yes → IAL 3
  - yes → IAL 3

IAL

4. Do you need to resolve an identity uniquely?
   - yes → End
   - no → 5
5. Can you accept claims?
   - no → End
   - yes → 6
6. Use claims if you can complete the transaction or offer the service without complete attribute values. → End

See federation recommendations.

Including step-wise guidance

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 verified to 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.

Figure 5-2 - Selecting IAL

1. To provide the service, do you need any individual attribute information?

The risk assessment and selection of IAL can be short circuited by answering this question first. If the service does not require any personal

required, or if self-asserted
ed to accept attributes that have
e digital service with self-

e potential impacts of an identity
ailure an agency may encounter
on. In addition, proofing, when
ttribute information when not
1 and 2 incorrectly, realizing they
he organization and to the user,
nt process of M-04-04 and any

unique identity. In other words,
access, even with a few
rocess can end. However, the
e risk of over collecting and

5. 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.

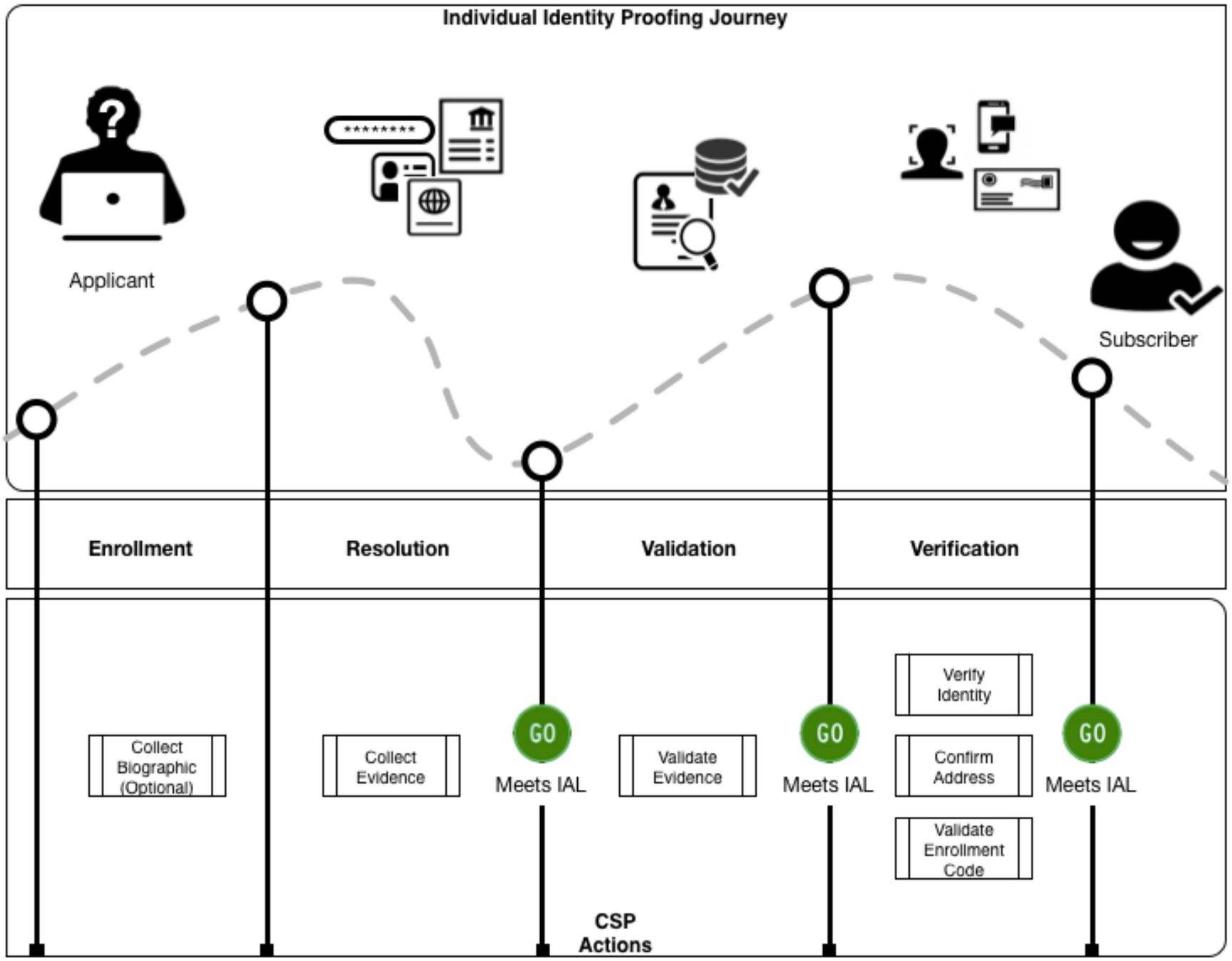
6. Use claims if you can complete the transaction or offer the service without complete attribute values.

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

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
  - 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

SP 800-63B

Authentication & Lifecycle Management

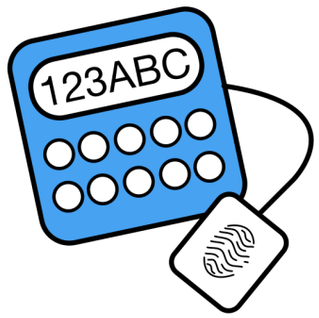
Authenticators

Memorized Secrets

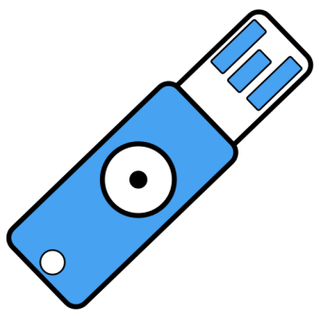
Look-up Secrets

Out-of-Band Devices

Single Factor OTP Device



Multi-Factor OTP Devices



Single Factor Cryptographic Devices

Multi-Factor Cryptographic Software

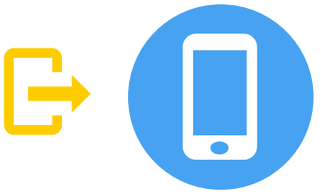
Multi-Factor Cryptographic Devices

Authenticator Guidance Changes

"Token" is out
"Authenticator" is in

Greater allowance for biometrics, but with rules

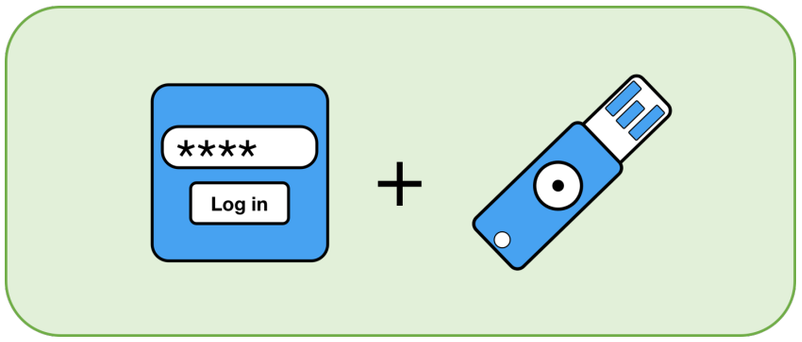
SMS OTP Requirements



OTP via email is out

Pre-registered knowledge tokens are out

New authenticators at AAL3 (aka LOA4)



FIPS 140-2	Level 1/Physical Level 3	Level 2/Physical 3

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:
  - 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

AAL	Description	Timeout
1	Presentation of any one factor	30 days
2	Presentation of any one factor	12 hours or 30 minutes of activity
3	Presentation of all factors	12 hours or 15 minutes of activity

SP 800-63C

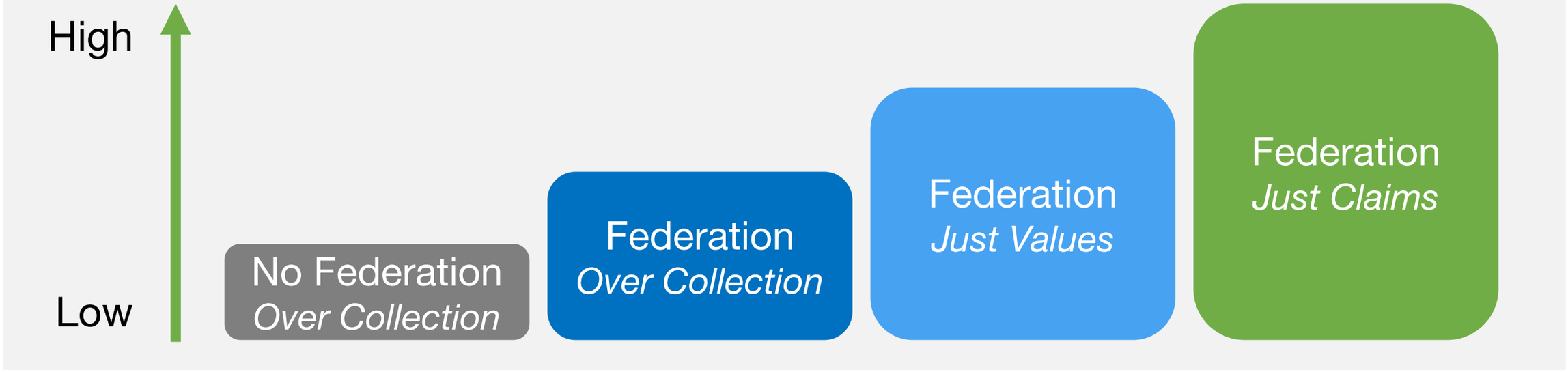
Federation & Assertions

800-63-C
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



Old	New
Give me date of birth.	I just need to know if they are older than 18.
Give me full address.	I just need to know if they are in congressional district X.

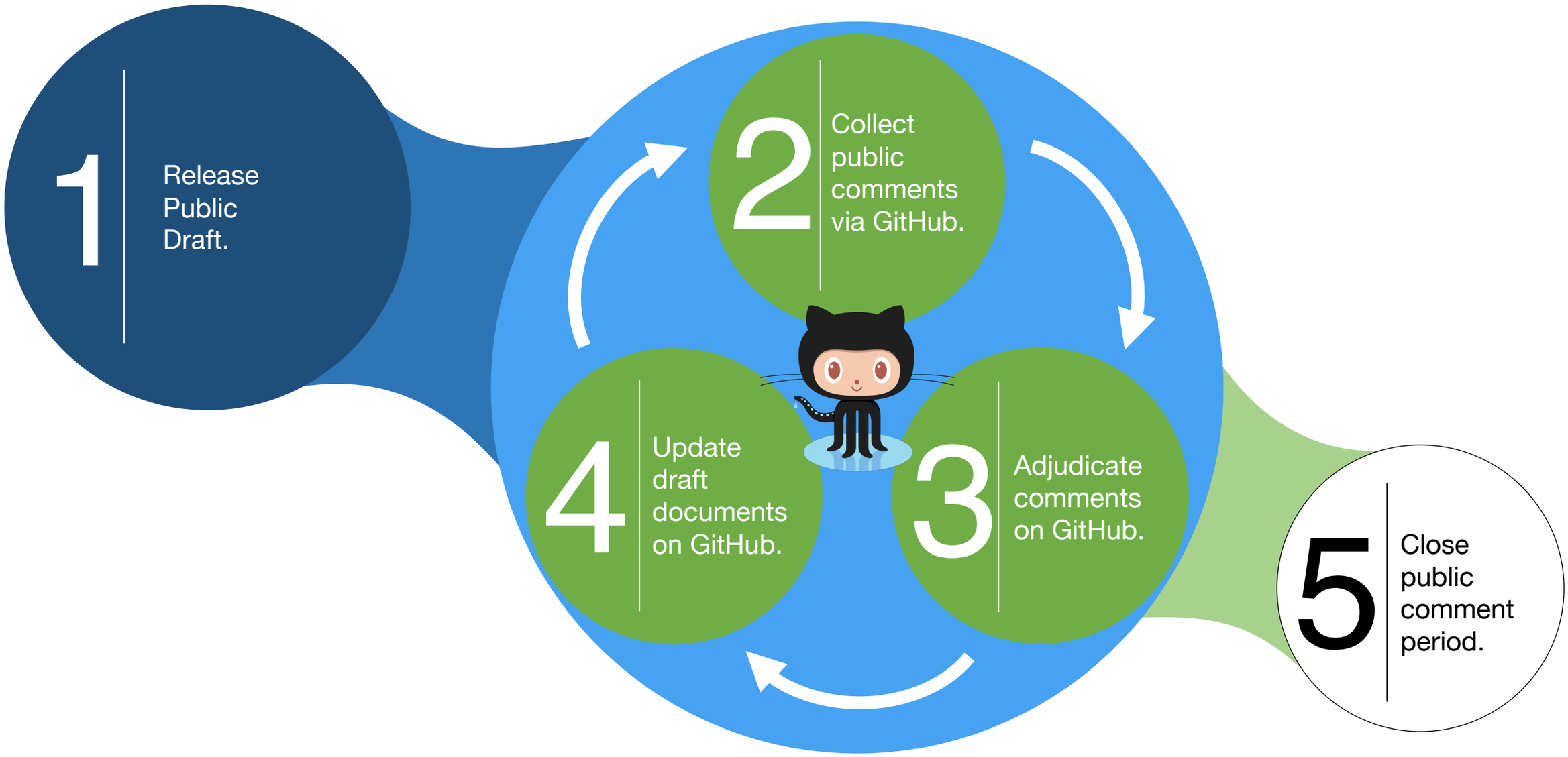
New Requirements

CSP SHALL support claims and value API

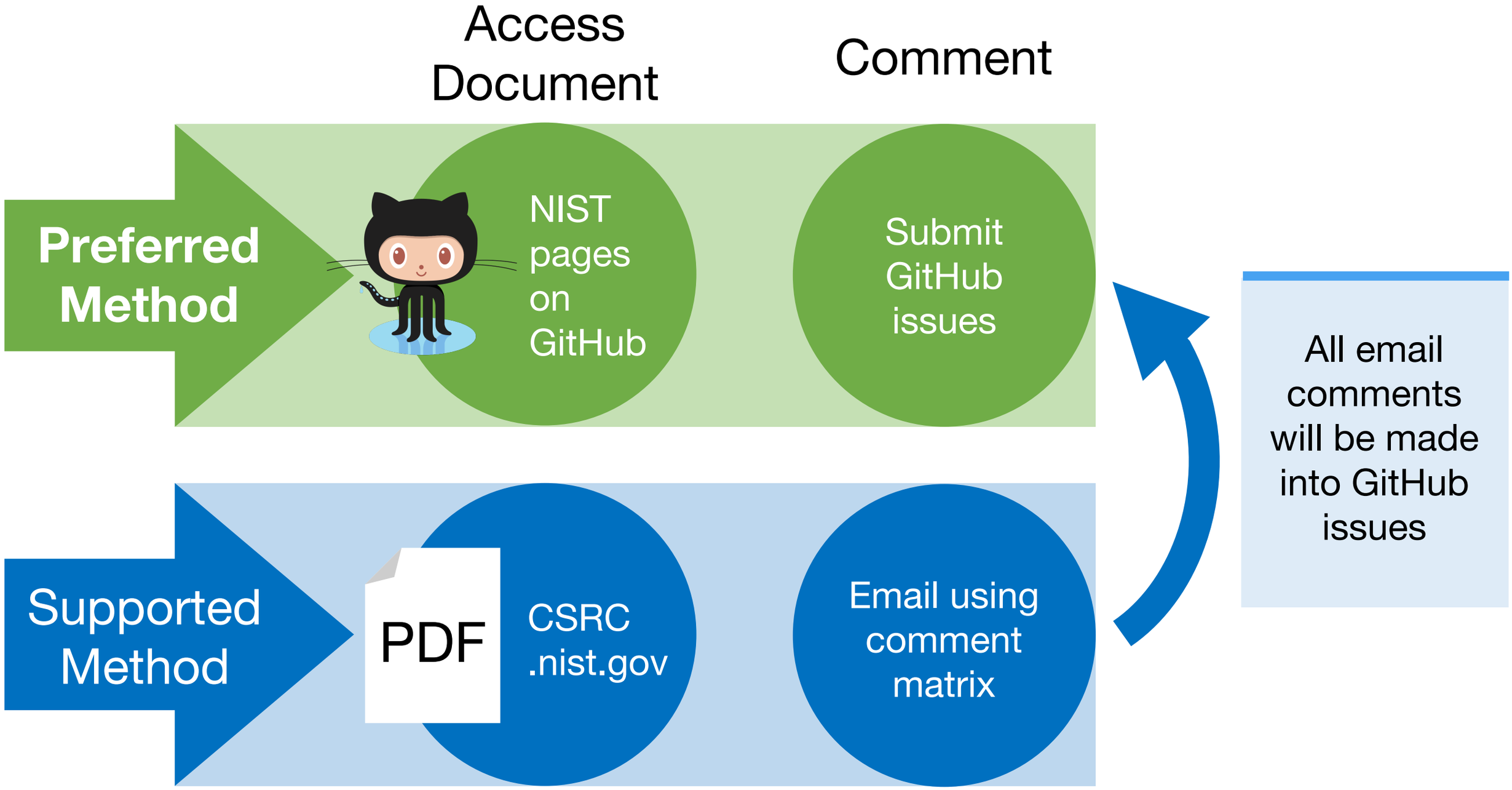
RP SHOULD request claims

Retaining the New Development Approach

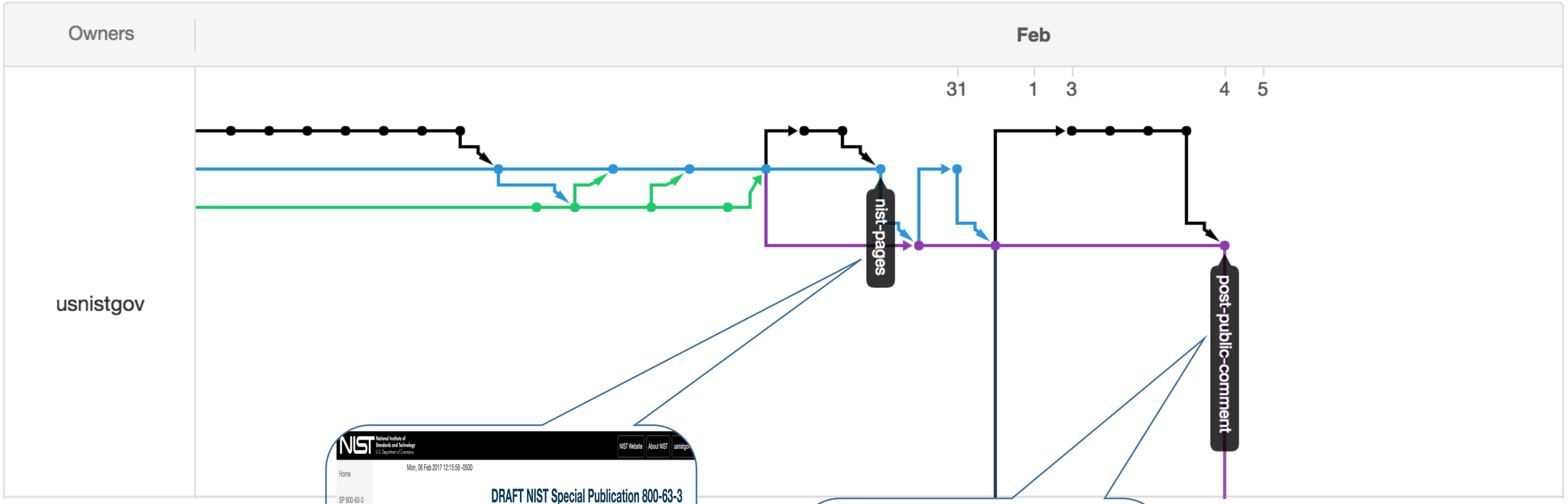
Iterative – publish, comment, and update in a series of drafting sprints

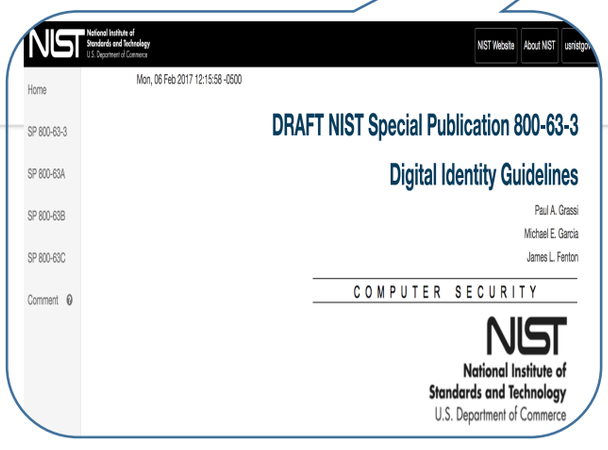


Contributing During Public Comment

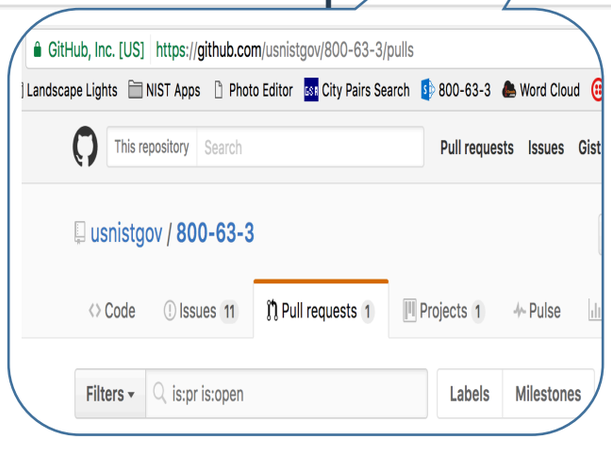


Advanced Contribution Option





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!