Digital Identity Guidelines
aka NIST SP 800-63

March 1, 2017

Ken Klingenstein, Internet2

Topics

- 800-63 History and Current Revision process
- Caveats and Comments
- LOA Evolution
- Sections:
  - 800-63A (Enrollment and Identity Proofing)
  - 800-63B (Authentication and Lifecycle Management)
  - 800-63C (Federation and Assertions)
- Privacy and Usability
- Input mechanisms
- Discussion Starters

History of 800-63 and revision

- Original as a biblical reference
- The Revision Process
  - Preview version on Github
  - Formal review also now on Github - https://pages.nist.gov/800-63-3/
  - Final draft perhaps by July 1
- Has incorporated a lot of other efforts – e.g. IETF “Vectors of Trust”, Refeds

Caveats and comments

- A remarkably open process with significant influence from the R&E community
- Still a draft; already considerable change from the preview to the formal drafts
- Scoping to agencies with potential implications beyond
- There is a nest of related specifications (e.g. 800-53, 800-171) that could be affected
- A very, very large surface area with a lot of impacts
- Unclear on how it affects rough beasts already loose in the world

Evolution of LOA into distinct “vectors”

- *Identity Assurance Level (IAL) / Authenticator Assurance Level (AAL).*
- For federated systems, a third component, *Federation Assurance Level (FAL)*

- **IAL** refers to the identity proofing process and the binding between one or more authenticators and the records pertaining to a specific subscriber.
- **AAL** refers to the authentication process itself.
- **FAL** refers to the assertion protocol utilized in a federated environment to communicate authentication and attribute information (if applicable) to an RP.

Mapping Old M-04-04 to new Vectors

M-04-04 Level of Assurance (LOA)	Minimum Required Identity Assurance Level (IAL)	Minimum Required Authenticator Assurance Level (AAL)	Minimum Required Federation Assurance Level (FAL)
1	1	1	1
2	2	2	2
3	2	2	2
4	3	3	3

Changes since preview version of revision

All Documents	1. Decoupled LOA into its component parts 2. Included privacy requirements 3. Included usability considerations
SP 800-63A	1. Overhauled allowable identity proofing processes 2. Expanded options for in-person proofing
SP 800-63B	1. Revamped password guidance 2. Removed insecure authenticators (aka tokens) 3. Expanded allowable use of biometrics
SP 800-63C	1. Added new federation requirements and recommendations 2. Removed cookies as an assertion type 3. Modernized examples

Other changes from preview draft

All Documents	Renamed SP 800-63 to “Digitial Identity Guidelines”
SP 800-63-3	Provided decision trees to assist agencies in the selection of assurance levels
SP 800-63A	Included guidance for digital identity evidence to be supplied to prove physical identity
SP 800-63B	1. Added Verifier Compromise Resistance (i.e., is my secret safe?) 2. Added Authentication Intent (i.e., it really was me, not malware, attempting to authenticate) 3. Refined biometrics requirements 4. Clarified and improved requirements and limitations of SMS-based OTP
SP 800-63C	Reduced Federation Assurance Levels from 4 to 3

SP 800-63-3 *Digital Identity Guidelines*

- Provides an overview of general identity frameworks, using authenticators, credentials, and assertions together in a digital system, and a risk-based process of selecting assurance levels. *This document contains only informative material.*

- The roadmap for understanding the materials within the three sections
  - 800-63A Enrollment and Identity Proofing
  - 800-63B Authentication Lifecycle Management
  - 800-63C Federations and Assertions

SP 800-63A *Enrollment and Identity Proofing*

- Addresses how applicants can prove their identities and become enrolled as valid subjects within an identity system. It provides requirements for processes by which applicants can both proof and enroll at one of three different levels of risk mitigation in both remote and physically-present scenarios. *This document contains both normative and informative material.*

Identity Assurance Levels

- **IAL1** - There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as self-asserted.
- **IAL2** - Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. Attributes could be asserted by Credential Service Providers (CSPs) to RPs in support of pseudonymous identity with verified attributes.
- **IAL3** - Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.

SP 800-63B *Authentication and Lifecycle Management*

- Addresses how an individual can securely authenticate to a CSP to access a digital service or set of digital services. *This document contains both normative and informative material.*

Authentication Assurance Level

- **AAL1** - Provides some assurance that the claimant controls the authenticator registered to a subscriber. AAL1 requires at least single-factor authentication using a wide range of available authentication technologies. Successful authentication requires a secure authentication protocol through which the claimant demonstrates possession and control of the authenticator(s).
- **AAL2** - Provides high confidence that the claimant controls authenticators registered to a subscriber. In addition to requirements of AAL1, two different authentication factors are required. Approved cryptographic techniques are required at AAL2 and above.
- **AAL3** - Provides very high confidence that the claimant controls the authenticator registered to a subscriber. In addition to requirements for AAL2, authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a “hard” cryptographic authenticator that provides verifier impersonation resistance.

SP 800-63C *Federation and Assertions*

- Provides requirements on the use of federated identity architectures and assertions to convey the results of authentication processes and relevant identity information to an agency application. In addition, this guideline offers privacy enhancing techniques to share information about a valid, authenticated subject, as well as describing methods that allow for strong multi-factor authentication (MFA) while the subject remains pseudonymous to the digital service. *This document contains both normative and informative material.*

Federation Assurance Levels

- **FAL1** - Allows for the subscriber to enable the RP to receive a bearer assertion. The assertion is signed by the IdP using approved cryptography.
- **FAL2** - Adds the requirement that the assertion be encrypted using approved cryptography such that the RP is the only party that can decrypt it.
- **FAL3** - Requires the subscriber to present proof of possession of a cryptographic key referenced in the assertion in addition to the assertion artifact itself. The assertion is signed by the IdP and encrypted to the RP using approved cryptography.

- These guidelines are agnostic to the vast array of identity services architectures that agencies can develop or acquire, and are meant to be applicable regardless of the approach an agency selects. However, where possible federation is encouraged, and the ability to mix and match IAL, AAL, and FAL is simplified when federated architectures are used. In addition, federation is a keystone in the ability to enhance the privacy of agency constituents as they access valuable government digital services.

Privacy and Usability Components Throughout 800-63-3

- Minimizing tracking and profiling
- Notice and Consent
- Data minimization
- Revocation and Redress
- Blinding in Federated Proxies

Usability considerations

- For attribute sharing, consider the following:
  - Provide a means for users to verify those attributes and attribute values that will be shared. Follow good security practices (see Section 6).
  - Enable users to consent to a partial list of attributes, rather than an all or nothing approach. Allow users some degree of online access, even if the user does not consent to share all information.
  - Allow users to update their consent to the list of attributes shared.
  - Minimize unnecessary information presented to users. For example, do not display system generated attributes such as pairwise pseudonymous identifiers, even if they are shared with the RP as part of the authentication response.
  - Minimize user steps and navigation. For example, build attribute consent into the protocols—so they're not a feature external to the federated transaction. Examples can be found in standards such as OAuth or OpenID Connect.
  - Provide effective and efficient redress methods such that a user can recover from invalid attribute information claimed by the IdP (see Section 6).
  - Minimize the number of times a user is required to consent to attribute sharing. Balancing the frequency of consent requests avoids user frustration with multiple requests to share the same attribute.
- For example, only request attributes from the user that are relevant for the current transaction, not for all possible transactions a user may or may not access at the RP.

Input mechanisms

- Internet2 Trust and Identity Consultation Feedback page on the wiki by March 15th: https://spaces.internet2.edu/pages/viewpage.action?pageId=108987144
- NIST Github issue reporting directly by March 31
  - https://github.com/usnistgov/800-63-3/issues/

Discussion Starters

- PII release requires MFA. What is your MFA population?
- Do your remote identity proofing needs get addressed?
- Are you planning on user consent?
- How important is 800-63-3 in our lives?