



National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3: Analysis and Recommendations

Joseph W. Grubbs, Ph.D.
IMSAC Staff Analyst

Presentation to the Identity Management
Standards Advisory Council
June 30, 2016



NIST SP 800-63-3 Documents

- SP 800-63-3 *Digital Authentication Guideline*
- SP 800-63A *Enrollment and Identity Proofing*
- SP 800-63B *Authentication and Lifecycle Management*
- SP 800-63C *Federation and Assertions*

Accessible on GitHub at <https://pages.nist.gov/800-63-3/>



Public Review Process

- “Public Review” version of NIST SP 800-63-3 and companion documents published on GitHub in May 2016
- NIST opted for a Public Review process over a formal Public Comment to allow flexibility
- Public Review will feature multiple iterations of review with each being approximately 2 weeks in length
- NIST editors will make approved edits for 2-3 weeks following each comment period



Major Changes

- Level of Assurance (LOA) decoupled into component parts
- Complete revamp of identity proofing
- New password guidance
- Removal of insecure authenticators (aka tokens)
- Federation requirements and recommendations
- Broader applicability of biometrics
- Updated definitions
- Privacy requirements (under construction)
- Usability considerations (under construction)



Primary Updates to 800-63-2

- Terminology changes, primarily the use of authenticator in place of token to avoid conflicting use of the word token in assertion technologies
- Updates to authentication and assertion requirements to reflect advances in both security technology and threats
- Requirements on the storage of long-term secrets by verifiers
- Restructured identity proofing model
- Updated requirements regarding remote identity proofing
- Clarification on the use of independent channels and devices as “something you have”
- Removal of pre-registered knowledge tokens (authenticators), with the recognition that they are special cases of (often very weak) passwords
- Requirements regarding account recovery in the event of loss or theft of an authenticator
- Expanded discussion of reauthentication and session management
- Expanded discussion of identity federation; restructuring of assertions in the context of federation



Identity Assurance Level (IAL)

- Identity Assurance Level 1 – Attributes provided in conjunction with the authentication process, if any, are self-asserted.
- Identity Assurance Level 2 – IAL 2 introduces the need for either remote or in-person identity proofing. IAL 2 requires identifying attributes to have been verified in person or remotely using, at a minimum, the procedures given in SP 800-63A.
- Identity Assurance Level 3 – At IAL 3, in-person identity proofing is required. Identifying attributes must be verified by an authorized representative of the CSP through examination of physical documentation as described in SP 800-63A.



Authenticator Assurance Level (AAL)

- Authenticator Assurance Level 1 - AAL 1 provides single factor digital authentication, giving some assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. AAL 1 allows a wide range of available authentication technologies to be employed and requires only a single authentication factor to be used. It also permits the use of any of the authentication methods of higher authenticator assurance levels. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she possesses and controls the authenticator.



Authenticator Assurance Level (AAL)

- Authenticator Assurance Level 2 – AAL 2 provides higher assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. Two different authentication factors are required. Various types of authenticators, including multi-factor Software Cryptographic Authenticators, may be used as described in SP 800-63B. AAL 2 also permits any of the authentication methods of AAL 3. AAL 2 authentication requires cryptographic mechanisms that protect the primary authenticator against compromise by the protocol threats for all threats at AAL 1 as well as verifier impersonation attacks. Approved cryptographic techniques are required for all assertion protocols used at AAL 2 and above.



Authenticator Assurance Level (AAL)

- Authenticator Assurance Level 3 – AAL 3 is intended to provide the highest practical digital authentication assurance. Authentication at AAL 3 is based on proof of possession of a key through a cryptographic protocol. AAL 3 is similar to AAL 2 except that only “hard” cryptographic authenticators are allowed. The authenticator is required to be a hardware cryptographic module validated at Federal Information Processing Standard (FIPS) 140 Level 2 or higher overall with at least FIPS 140 Level 3 physical security. AAL 3 authenticator requirements can be met by using the PIV authentication key of a FIPS 201 compliant Personal Identity Verification (PIV) Card.



LOA-IAL-AAL Crosswalk

| Level of Assurance | Identity Assurance Level | Authenticator Assurance Level | Federation Assurance Level |
|--------------------|--------------------------|-------------------------------|----------------------------|
| 1 | 1 | 1, 2 or 3 | TBD |
| 2 | 1 or 2 | 2 or 3 | TBD |
| 3 | 1 or 2 | 2 or 3 | TBD |
| 4 | 1, 2 or 3 | 3 | TBD |



Allowable IAL-AAL Combinations - Enrollment

| | IAL 1 | IAL 2 | IAL 3 |
|-------|---------|-------------|-------------|
| AAL 1 | Allowed | Not Allowed | Not Allowed |
| AAL 2 | Allowed | Allowed | Allowed |
| AAL 3 | Allowed | Allowed | Allowed |



Alignment with Other Standards

| | | | | | | |
|-----------|----------|----------|-------------|------------|-----------|----------------------|
| SP 800-63 | [GPG 45] | [RSDOPS] | STORK 2.0 | 29115:2011 | ISO 29003 | Government of Canada |
| N/A | N/A | Level 01 | N/A | N/A | N/A | N/A |
| AAL/IAL 1 | Level 1 | Level 1 | QAA Level 1 | LoA 1 | LoA 1 | IAL/CAL 1 |
| AAL/IAL 1 | Level 2 | Level 2 | QAA Level 2 | LoA 2 | LoA 2 | IAL/CAL 2 |
| AAL/IAL 2 | Level 3 | Level 3 | QAA Level 3 | LoA 3 | LoA 3 | IAL/CAL 3 |
| AAL/IAL 3 | Level 4 | N/A2 | QAA Level 4 | LoA 4 | LoA 4 | IAL/CAL 4 |

[GPG 45] UK Cabinet Office, Good Practice Guide 45, Identity proofing and verification of an individual, November 3, 2014, available at: <https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual>.

[RSDOPS] UK Cabinet Office, Good Practice Guide 43, Requirements for Secure Delivery of Online Public Services (RSDOPS), November 3, 2014, available at: <https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services>.



Recommendations

- Revise draft guidance documents on trust frameworks and identity proofing & verification to reflect NIST SP 800-63-3 and companion documents
- Document edits as part of the public record on the draft review and comment process
- Complete the public review and comment process pursuant to § 2.2-437 and the Administrative Process Act
- Bring to IMSAC for approval at September 2016 meeting



For More Information

Joseph W. Grubbs, Ph.D.

IMSAC Staff Analyst

Virginia Information Technologies Agency

Phone: (804) 467-7729

Email: Joseph.Grubbs@vita.virginia.gov