Digital Authentication Guideline

NIST 800-63-3 Preview

Bob Cowles

EUGridPMA, Abingdon U. K.

11 May 2016

Drill Down pages

- http://nstic.blogs.govdelivery.com/
  - https://pages.nist.gov/800-63-3/
    - https://pages.nist.gov/800-63-3/sp800-63a/cover.html
    - https://pages.nist.gov/800-63-3/sp800-63b/cover.html

Review process

- Comments solicited via GitHub
- Will respond and make edits continually over the summer
- After summer period; traditional 30/60 day comment period
- Trying to get technical content right
  - Focus on substantive comments; lean; discourage email or Excel files
  - Will get to grammatical issues later (unless you can’t resist)
  - Instructions available https://help.github.com/articles/creating-an-issue/
- Target is completed document by winter
- Built by community participation

Quick Summary

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

Some more details on changes

- LoA broken into independent parts
  - Identity proofing
  - Authenticators
  - Federated assertions
- Three levels each for Identity proofing and Authentication
- Guidance for compatibility with existing 4 levels (temporary)
- Guidance for in-person proofing over a “virtual channel”
- Clarified Knowledge Based Verification limited to proofing (never sufficient on its own)
- Emailing OTP is gone; SMS OTP is deprecated

Identity Assertion Level (IAL)

- Level 1 – self asserted
- Level 2 – remote or in-person identity proofing; same with attributes
- Level 3 – in-person proofing required; attributes must be verified by authorized representative of the certifying provider through examination of physical evidence

Authenticator Assurance Level (AAL)

- Level 1 – single factor; assurance of continuity; permits wide range of technologies; claimant must prove through a secure protocol possession/control of the authenticator
- Level 2 – at least two factors required; requires secure authentication protocol plus protection from verifier impersonation attacks; attribute transmitted similarly securely
- Level 3 – also requires proof of possession of a “hard” cryptographic authenticator (FIPS 140 level 2); in US, PIV card (FIPS 201) is OK
- Add’l attributes such as device or geo-location can reduce false-positives
- Fingerprint to unlock a device containing a key considered 2-factor
- Biometric single factor is not acceptable for authentication

Federation and Assertions

- Verifier of Authentication is separate from RP
- Assertions may be communicated directly to RP or through subscriber
- Verifier is responsible for for ensuring integrity of assertions
- RP authenticates the verifier and confirms integrity
- Examples: SAML; OpenID Connect; Kerberos tickets
- Federation Assurance Levels (proposed)
  - Level 1 – Bearer, shared secret between CSP and RP
  - Level 2 – Bearer, asymmetrically signed by CSPM
  - Level 3 – Holder of key, asymmetrically signed by CSP
  - Level 4 – Holder of key, encrypted with RP’s public key

“Now, please, go forth and contribute! We look forward to engaging with the community in this new process for 800-63-3 and developing effective, updated guidance.”

“Now is your chance to let us know: Did we miss anything? Have we gotten ahead of what is available in the market? Have we made appropriate room for innovations on the horizon?”