NIST Special Publication 800-63-3

IGTF Discussion

JAN 2018

DARKMATTER

GUARDED BY GENIUS

CONTENTS

NIST SP800-63-3: An Introduction

- NIST recently (June 2017) released its four-volume Special Publication (SP) 800-63, *Digital Identity Guidelines*
  - The new Guideline has 4 volumes instead of one all inclusive guide
  - SP 800-63-3 : the parent document containing definitions and starting point for all things digital identity and risk
  - SP 800-63A : *Enrollment and Identity Proofing*
  - SP 800-63B : *Authentication and Lifecycle Management*
  - SP 800-63C : *Federation and Assertions*
  - A fifth volume (SP 800-63D) is also underway to detail efforts to align with international technical specifications for interoperable identity in federations

NIST SP800-63-3: An Introduction

- Some Definitions from the Guidelines:
  - **Identity proofing** is the process used to verify a subject's association with their real-world identity, establishing that a subject is who they claim to be.
  - An **authenticator** is something the subject possesses and controls (typically, a cryptographic module or password) that is used to authenticate the subject's identity.
  - **Digital authentication** is the process of determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate. Successful authentication provides reasonable risk-based assurances that the subject accessing the service today is the same that previously accessed the service.
  - **Federation** is when the relying party (RP) and identity provider (IdP) are not a single entity or not under common administration. Federation enables an IdP to proof and authenticate an individual and provide identity assertions that RPs can accept and trust.

NIST SP800-63-3: What Changed from V2?

- The new version drops a single scale of 4 Levels of Assurance in favor of 3 different vectors of assurance each with their own ordinal scale
  - **Identity Assurance Level (IAL):** the identity proofing process and the binding between one or more authenticators and the records pertaining to a specific subscriber
  - **Authenticator Assurance Level (AAL):** the authentication process, including how additional factors and authentication mechanisms can impact risk mitigation
  - **Federation Assurance Level (FAL):** the assertion used in a federated environment to communicate authentication and attribute information to a RP

NIST SP800-63-3: What Changed from V2?

- **Identity Proofing Levels (IAL)**
  - **IAL1:** No requirement is made 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 such (including attributes a credential service provider (CSP) asserts to a RP).
  - **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 can be asserted by 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 can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.

NIST SP800-63-3: What Changed from V2?

- ## Authenticator Assurance Levels (AAL)

  - **AAL1:** provides some assurance that the claimant controls an authenticator registered to the subscriber. AAL1 requires single-factor authentication, using a wide range of available authentication technologies. Successful authentication requires that the claimant proves possession and control of the authenticator through a secure authentication protocol.

  - **AAL2:** provides high confidence that the claimant controls an authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through secure authentication protocol(s).

  - **AAL3:** provides high confidence that the claimant controls an authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through secure authentication protocol(s).

NIST SP800-63-3: What Changed from V2?

- **Federation Assurance Levels (FAL)**
  - **FAL1:** Bearer assertion, signed by IdP. E.g. FAL 1 maps to the OpenID Connect Basic Client profile or SAML Web SSO Artifact Binding profile, with no additional features.
  - **FAL2:** Bearer assertion, signed by IdP and encrypted to RP. E.g. FAL 2 additionally requires that the OpenID Connect ID Token or SAML Assertion be encrypted to a public key representing the RP in question.
  - **FAL3:** Holder of key assertion, signed by IdP and encrypted to RP. E.g. FAL 3 requires the presentation of an additional key bound to the assertion (for example, the use of a cryptographic authenticator) along with all requirements of FAL 2. Note that the additional key presented at FAL 3 need not be the same key used by the subscriber to authenticate to the IdP.

NIST SP800-63-3: What Changed from V2?

- **Federation Assurance Levels (FAL) suggested mapping for federal agencies:**
  - NOTE:FAL levels in the right column can be used to meet LoA requirements in the left column

M-04-04 Level of Assurance	Federation Assurance Level
1	1, 2, or 3
2	2, or 3
3	2, or 3
4	3

NIST SP800-63-3

Questions?

Scott.Rea@DarkMatter.ae

THANK YOU

DARKMATTER

GUARDED BY GENIUS