ITL BULLETIN FOR AUGUST 2017

UNDERSTANDING THE MAJOR UPDATE TO NIST SP 800-63: DIGITAL IDENTITY GUIDELINES

Mike Garcia, Paul Grassi, Kristina Rigopoulos, Larry Feldman,[1] and Greg Witte,[1] Editors
Applied Cybersecurity Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

Digital identities are used in nearly every aspect of our online activities each day. A digital identity is the unique representation of a subject that is engaged in an online transaction. This bulletin outlines updates that NIST recently made in its four-volume Special Publication (SP) 800-63, *Digital Identity Guidelines*, which provide agencies with technical guidelines regarding the digital authentication of users to federal networked systems.

Rather than being a single, monolithic guideline, SP 800-63-3 has been separated in multiple parts – each representing a distinct component of digital identity services. This way, organizations can choose the document that applies to the digital identity services they want to offer. This approach makes applying the guidelines easier for agencies—and also sets the stage for a nimble continuous improvement process. Also, NIST can quickly release key updates, rather than delivering in two or three year cycles.

This bulletin will describe the components of digital identity – identity proofing, authentication, and federation – and explain how federal agencies can use them to protect the digital identities of their employees. It also provides an overview of the NIST documents that describe these digital identity components and explains how the information in them is organized.

Understanding Digital Identity

A digital identity is always unique when using a digital service, but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known. Support for digital identities involves several components that help to verify and validate an entity. These components include the following:

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.

- **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.

How has SP 800-63-3 evolved?

Since the last revision of this document in 2013, NIST SP 800-63-2, digital identity components have evolved substantially. To better align with market-driven business models and innovation, the new revision replaces levels of assurance (LOAs) with ordinals for individual parts of the digital identity flow, providing implementers with more flexibility in their design and operations:

- **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; and
- **Federation Assurance Level (FAL):** the assertion used in a federated environment to communicate authentication and attribute information to a RP.

SP 800-63 is a suite of four documents: SP 800-63-3 (the parent document; your starting point for all things digital identity and risk) and three additional documents – SP 800-63A, 800-63B, and 800-63C – which cover the various components of a digital identity system. These documents are described below:

- SP 800-63-3, *Digital Identity Guidelines*, provides an overview of general identity frameworks, guidance regarding use of authenticators, credentials, and assertions together in a digital system, and a risk-based process of selecting assurance levels;
- SP 800-63A, *Enrollment and Identity Proofing*;
- SP 800-63B, *Authentication and Lifecycle Management*; and
- SP 800-63C, *Federation and Assertions*.

Identity Proofing

Strengthening identity proofing while expanding options for remote and in-person proofing is arguably the most difficult part of digital identity. Identify proofing is the focus of NIST SP 800-63A, the first of the three additional documents—which provides guidelines that clarify methods for resolving an identity to a single record. This guidance enables RPs to evaluate and determine the strength of identity evidence. No longer will agencies be required to ask for "one government-issued ID and a financial account." The proofing guidance moves away from a static list of acceptable documents and instead describes "characteristics" for the evidence necessary to achieve each IAL. Agencies can now pick the evidence that works best for their stakeholders.

In fact, the document no longer differentiates between physical evidence (such as a passport) and digital evidence (for example, a mobile driver's license or an assertion from another identity provider). You would no longer think "plastic is good" and "digital is bad" for presented evidence; what matters is the process used to validate and verify the evidence.

The three IALs reflect the options from which agencies may select, based on their risk profile and the potential harm caused by an attacker making a successful false claim of an identity. The IALs are as follows:

- **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 SP 800-63A opens the door for a diverse array of proofing options, including virtual in-person (also known as "supervised remote") and trusted referees (e.g., notaries). It offers clearer guidelines on document checking and address confirmation.

Authentication

The ongoing authentication of subscribers is central to the process of associating them with their online activity. Subscriber authentication is performed by verifying that the claimant controls one or more *authenticators* (called *tokens* in earlier versions of SP 800-63) associated with a given subscriber. Successful authentication results in the assertion of an identifier – whether or not this person uses a false name – and, optionally, other identity information, to the RP.

NIST SP 800-63B provides recommendations on the types of allowable authenticators that may be used at various AALs, how account recovery should be performed, and when it is necessary to reauthenticate an individual. This technical guideline applies to the digital authentication of subjects to systems over a network. It does not address the authentication of a person for physical access (e.g., to a building), though some credentials used for digital access may also be used for physical access authentication. This technical guideline also requires that federal systems and service providers participating in authentication protocols be authenticated to subscribers.

The strength of an authentication transaction is characterized by an ordinal measurement, defined as the Authenticator Assurance Level (AAL). Stronger authentication, or a higher AAL, requires malicious actors to have better capabilities and use greater resources to subvert the authentication process. In other words, authentication at higher AALs can more effectively reduce the risk of attacks than authentication at lower AALs.

The technical requirements for each AAL can be summarized as follows, from least effective (AAL1) to most effective (AAL3):

- **Authenticator Assurance Level 1 (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.

- **Authenticator Assurance Level 2 (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).

- **Authenticator Assurance Level 3 (AAL3)** provides very high confidence that the claimant controls an authenticator(s) registered to the subscriber. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 also requires a hardware-based cryptographic authenticator and an authenticator that provides verifier impersonation resistance.

The new guidelines also enable server-side biometric matching (the process of comparing a biometric sample provided by the user during authentication to a biometric template collected during enrollment) and include a comprehensive set of biometric performance and security requirements. Because biometric sensors have already been implemented in numerous devices – and their number is growing – it was important to provide guidelines that can prevent unreliable or weak biometric approaches from sneaking their way into federal digital services while allowing these powerful tools to play a large role in doing digital identity properly.

Federation

Federation allows users to establish a digital identity with an IdP and to use that digital identity at a host of RPs that are completely unrelated to the IdP (for example, obtaining a digital identity from a mobile phone carrier and using that identity to log into an eCommerce site). Federation enables a RP to reduce costs by outsourcing identity proofing and authentication management to a third party IdP.

NIST SP 800-63C lays out the details of identity federation and identity assertions for organizations that chose the implementation of a federation architecture. NIST SP 800-63C expands federation guidelines from previous versions of 800-63, provides greater detail on how assertions should be used, and includes a host of privacy-enhancing requirements that can make federation appealing to users.

An assertion used for authentication is a packaged set of attribute values or attribute references about an authenticated subscriber, or associated with him or her, that is passed from the IdP to the RP in a federated identity system. Assertions contain a variety of information, including: assertion metadata, attribute values and attribute references about the subscriber, and other information that the RP can leverage (such as restrictions and expiration time).

While the assertion's primary function is to authenticate the user to a RP, the information conveyed in the assertion can be used by the RP in a variety of ways — for example, to authorize or personalize a website. These guidelines do not restrict the many ways in which a RP is used—nor the type of protocol or data payload used to federate an identity—assuming the chosen solution meets all mandatory requirements.

Since the federated authentication process involves coordination among multiple components, including the CSP, which now acts as an IdP, attackers have more opportunities to compromise federated identity transactions. NIST SP 800-63C summarizes many of the attacks and mitigations applicable to federation (such as assertion replay or tampering).

Federation involves the transfer of personal attributes from a third party that is not otherwise involved in a transaction — the IdP. Federation also potentially gives the IdP broad visibility into subscriber

activities, which is why NIST SP 800-63C addresses specific privacy requirements associated with federation.

Next Steps

With the completion of updates to the four volumes, we are now preparing to implement guidance to help agencies deploy solutions that meet requirements in SP 800-63. The first set of solutions will focus on identity proofing, and further guidance will be released over the course of the year.

Also, we have started working on a new publication (SP 800-63D), which will detail efforts to align with international technical specifications for interoperable identity in federations, including Security Assertion Markup Language (SAML) profiles and an International Government Assurance Profile (iGov) working group's OpenID Connect/OAuth profile (which was developed in partnership with industry and international governments).

Additionally, we soon plan to release information on new password guidance for use across the Federal Government.

Additional Resources

NIST SP 800-63-3, *Digital Identity Guidelines*
https://pages.nist.gov/800-63-3/sp800-63-3.html

SP 800-63A, *Enrollment & Identity Proofing*
https://pages.nist.gov/800-63-3/sp800-63a.html

SP 800-63B, *Authentication & Lifecycle Management*
https://pages.nist.gov/800-63-3/sp800-63b.html

SP 800-63C, *Federation & Assertions*
https://pages.nist.gov/800-63-3/sp800-63c.html

Mic Drop — Announcing the New Special Publication 800-63 Suite:

http://trustedidentities.blogs.govdelivery.com/2017/06/22/mic-drop-announcing-the-new-special-publication-800-63-suite/

Trusted Identities Group Twitter account:

https://twitter.com/TrustedIDsNIST

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov