MITRE

MITRE Response to Pre-Draft Call for Comments: NIST SP 800-63-4

Author:
Christopher J. Brown

August 2020

Document No:
MP200648

Table of Contents

Contributors

This document contains comments and feedback from subject matter experts across MITRE, including:

- Lorrayne Auld
- Ronna ten Brink
- Chris Buchanan
- Russ Reopell
- Rebecca Scollan
- Jim Thomson
- Mary Yang

Introduction

MITRE's mission is to solve problems for a safer world. We work across the whole of government, through the federally funded research and development centers (FFRDCs) we manage and numerous public-private partnerships, to tackle difficult problems that challenge the safety, stability, and well-being of our nation. Our unique role and perspective allow us to provide innovative, practical solutions for some of our nation's most critical challenges in defense and intelligence, aviation, civil systems, financial systems, homeland security, the judiciary, healthcare, and cybersecurity.

MITRE has performed independent research, such as developing a methodology, detailed processes, and practice statement templates to proof digital identities at high assurance levels to help advance the state of the possible in the Identity, Credential, and Access Management (ICAM) domain. We also have experience assisting multiple federal agencies as they address prior and current ICAM requirements, and through our support for our sponsors, we have gained insight into private sector adoption of identity standards and technologies' capabilities to meet ICAM requirements. We thus welcome this opportunity to draw on our technical knowledge and broad operational experience to respond to National Institute of Standards and Technology's (NIST's) pre-draft call for comments for the next revision of the *Digital Identity Guidelines*, NIST Special Publication 800-63-3.

Since publication in 2017, the *Digital Identity Guidelines* have had significant adoption within all branches of the U.S. government and modest adoption (voluntarily) within private organizations. MITRE has also observed commercial identity service providers use their alignment with 800-63-3 as a competitive advantage in their marketing strategy. However, we believe opportunity exists for further adoption of the *Digital Identity Guidelines* across critical sectors of the U.S. economy to increase the security of online transactions that continue to be vulnerable. Modest changes to the *Digital Identity Guidelines* that continue and expand on the multidisciplinary and collaborative approach—to include the Privacy Framework, User Experience (UX), Cybersecurity Framework 1.1, accessibility, and biometrics—will facilitate the continued adoption of the guidance and contribute to securing the nation's critical resources.

The upcoming sections of this document highlight cross-cutting topic areas applicable to the development of 800-63-4. The final three sections discuss specific areas that address each volume of the current guidance.

Accessibility

Throughout 800-63-3 it is stated, "Accessibility differs from usability and is out of scope for this document. Section 508 was enacted to eliminate barriers in information technology and require federal agencies to make their electronic and information technology public content accessible to people with disabilities. Refer to Section 508 law and standards for accessibility guidance."

MITRE asserts the line between accessibility and usability need not be so stark; we do not recommend completely striking accessibility out of scope. Because Section 508 provides guidance on achieving at least minimum acceptable accessibility, in these documents, consider including considerations on usability for people with disabilities, which goes beyond basic accessibility and has much in common with existing usability considerations.

Often, designing with "edge case" users in mind, like users with disabilities, creates innovative solutions that are more usable for everyone, including users without disabilities. For example, the Usability Considerations in 800-63B include suggestions to offer alternate authentication options, to write for a low literacy level, and to use high-contrast and 12+ size fonts (800-63B, Section 10.1). These suggestions are also inclusive of people with a variety of disabilities, people with cognitive disabilities, and people with color deficiency or vision loss, respectively.

Additionally, Section 508 is important for accessibility, but it does not necessarily correspond to a usable, accessible experience for all people. New or novel interactions might not be covered in 508, and regardless, we recommend testing with people with disabilities. Just as usability heuristics do not stand in for usability testing, using Section 508 design guidelines does not stand in for testing with actual users with disabilities.

MITRE also recommends suggesting usability testing with targeted populations, especially when using interactions that may be new to some users. For example, interactions that include camera positioning on a mobile phone could pass 508 standards but not be accessible to blind or low-vision users.

Artificial Intelligence/Machine Learning

Commercial cloud identity service providers have begun advertising artificial intelligence (AI) or machine learning (ML) capabilities as part of their solutions and to enhance the security of authentication transactions. MITRE recommends speaking to these capabilities in the next version of 800-63, as a supplemental technique for credential service providers (CSPs) to detect attacks, or to otherwise enhance an authentication transaction. We also recommend communicating the risk of utilizing AI capabilities: vulnerabilities can be created from adversarial AI/ML, and services that use AI/ML methods for authentication and readers of 800-63 should be aware of those vulnerabilities.

Authentication at Scale

As more transactions and engagements move online, being able to authenticate large groups (e.g., millions of diverse individuals) quickly with a measurable or high-level of assurance (based on the transaction's risk) will only become more important. The current COVID-19 pandemic highlights the need and urgency of this issue, though "authentication at scale" is not a new concern. Google identified the issue and coined this phrase back in 2013, documenting their perspective in IEEE Security & Privacy [1].

Strong authentication at scale is an issue for both the public and private sectors. Numerous federal agencies support citizen and non-citizen online transactions that may consist of accessing or transmitting personally identifiable and sensitive information. With COVID-19, this list of agencies is only growing; prior to the pandemic, many federal agencies were pushing to move in-person or paper-based processes and transactions online to support digital modernization efforts and improve efficiencies. With the pandemic, these efforts have only accelerated. Private sector organizations, such as banks, have adopted some technologies that enable strong authentication at scale, but wide-scale adoption across diverse communities continues to lag.

While authentication technologies have advanced since 2013, secure implementations to support authentication at scale based on standards remain, at best, ambiguous. Identiverse 2020 hosted a panel session [2] on this topic, and the discussion illustrated the lack of clarity surrounding it. A

clearer definition of "authentication at scale," general use cases, and guidance on how organizations can address these concerns should be considered as additions to a revision of 800-63.

Decentralized Identity

Self-Sovereign or Decentralized Identity (DID) is the next evolutionary step in creating and managing identities on the internet from current stove-piped centralized identity and federated models. The ability to record, track, and manage identity on a blockchain [3] has the potential to vastly improve the efficiency and minimize the cost of identity management across all U.S. sectors; an immutable, trusted source of identity will make it difficult to steal, hack, modify, or otherwise damage reputation, or compromise identity to steal real assets or perpetrate fraud.

Technology vendors and the private sector are beginning to investigate implementing DID more earnestly. Gartner's recent report on 2020 identity and access management (IAM) technologies and trends [4] indicated that DID is likely to see a strong surge in adoption. With its broad private and public sector research and engagement, Gartner analysts noted, "Decentralized identity is making a debut in 2021, and will disrupt traditional methods of access for many providers, as it will be used for 25% of all bring your own identity (BYOI) logins by 2023." Beyond Gartner, other technology companies and NIST partners, such as Microsoft and IBM, also publicly support and advocate for DID.

Standards for identity management using blockchain are not yet set, and best practices are still being developed. Research is needed into the blockchain's ability to protect private information. Once information is recorded on the blockchain, it remains accessible to all parties in the network, so users must be aware to minimize any private information.

While public blockchains, designed to operate in a trust-less environment, provide the most security, government users will be most interested in a permissioned blockchain. However, the nature of a permissioned blockchain requires careful planning and governance to establish the parties participating in the consensus process.

Further, consider the inclusion of discussion of an additional volume, or other supplemental publication to provide guidance that addresses DID that builds upon the NIST whitepaper *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*. DID would represent a paradigm shift from the current framework described in 800-63, in that access control is changed from a direct authentication activity from the subscriber to the verifier, to a verification of the subscriber's credentials. At a minimum, this guidance could apply current Identity Assurance Level (IAL) concepts to DID issuance, and Authenticator Assurance Level (AAL) concepts to DID wallets, addressing phishing attacks against wallets themselves.

Finally, given the potential industry shift to DID, we recommend NIST consider becoming a member of two foundations created to foster collaboration in the DID community: the Trust over IP Foundation and the Sovrin Foundation. Established in May 2020, the mission of the Trust over IP Foundation is to "simplify and standardize how trust is established online so that everyone can feel safe, secure, and private in all of our digital interactions—whether between individuals, businesses, governments, or any "thing" on the Internet of Things." [5] The Sovrin Foundation supports "the creation of the internet's long-missing identity layer and the global adoption of self-sovereign identity (SSI)" [6]. As a member, NIST can work closely with industry partners to shape the governance and technical standards as they are developed.

Privacy

MITRE was pleased to see the official release of the NIST Privacy Framework in early 2020. As part of the introduction to the Privacy Framework, NIST notes that ensuring privacy is challenging because "individuals may not be able to understand the potential consequences for their privacy as they interact with systems, products, and services." IAM is a key component of these interactions, as many systems and services require some identity proofing or authentication as part of process to utilize a system or service.

MITRE recommends providing specific guidance on privacy and digital identity in a revision of 800-63. Much of this could draw on existing work in the Privacy Framework, of which IAM experts may not be aware or understand how to use. This guidance could help IAM technology vendors identify paths to incorporating privacy engineering and privacy concepts into their products.

MITRE also recommends NIST consider restarting or refining the National Cybersecurity Center of Excellence's Privacy-Enhanced Identity Federation project. This project would likely need to be reviewed and revised based on the NIST Privacy Framework; however, it can provide applied guidance at the intersection of privacy and digital identity that can be helpful to both the public and private sectors. This project can potentially serve as an exemplar of both guidance publications. This is especially relevant today with existing social logins and cloud services that market themselves as a "broker." Related standards work is emerging in the health sector with privacy manifest proposal and OpenID Connect Federation.

800-63A

Considering recent events surrounding the COVID-19 pandemic, MITRE recommends adding content regarding how agencies should make data-driven decisions for situations where physical presence is required but temporarily not allowable due to the physical environment. This would also present an opportunity to update the remote identity threat model. Two such threats—synthetic identities and deep fakes—have gained traction since the guidelines have been published. As AI advances and becomes more attainable for non-nation state attackers, MITRE predicts deep fakes will become a particularly difficult threat for agencies to defend against. Financial services organizations are tracking synthetic identity as a growing area of fraud and cybercrime; NIST could begin exploring this topic by engaging in industry conversations about growth of the use of synthetic identities, impact to the organization and/or industry, and mitigations.

In the remainder of this section, we summarize the findings of a study conducted by MITRE that are relevant to Enrollment and Identity Proofing Requirements 800-63A. This study was sponsored by a U.S. government agency that has a portfolio of growing online services, including those that offer citizens access to their personal, sensitive information. Thus, the agency faced a challenge of offering a digital identity solution that is highly secure, usable, and accessible to its wide audience.

MITRE conducted a qualitative study to investigate tech-savvy and non-tech-savvy citizen perceptions of new digital identity technologies: remote identity proofing, two-factor authentication, and CSPs. We examined their trust, comprehension, and satisfaction around these new concepts and looked to identify potential usability and accessibility issues. MITRE's analysis revealed that, despite their concerns, both audiences are willing to use these services.

Most tech-savvy users interviewed were very concerned about security and had a false assumption that their image and biometrics were being captured and stored in an experimental "selfie" verification process. Non tech-savvy users had the same false assumption that their image was being stored in the selfie verification process. Non-tech-savvy users also preferred not to have a choice of CSPs, but despite prioritizing registering directly with the agency in question, they were willing to use a third party.

This study suggests a need for more research into improving comprehension and awareness through the design of future versions of online services, and further user research on new digital identity concepts such as selfie verification and liveness testing. In addition, measuring citizen perceptions can unveil additional areas for research into the intersection of privacy and identity management.

800-63B

When published, the *Digital Identity Guidelines* attracted significant media attention through restricting the use of short message service (SMS)-based one-time passwords (OTPs). This decision has borne out to be prescient—SMS-based attacks have proliferated since its restriction in 2017. However, the use of SMS-based OTPs is still prevalent in the private sector and among various agencies, regardless of the threat. MITRE has also observed SMS-based OTP marketed among commercial cloud identity services, with insufficient discussion of the threats presented by this capability. Therefore, MITRE recommends the complete deprecation of SMS-based OTPs and urges the transition to other types of authenticators, such as FIDO2 (single-factor cryptographic device) or the combination of a memorized secret with a single-factor OTP device.

Additionally, achieving an AAL-3 authentication transaction, outside the use of Personal Identity Verification (PIV) credentials, continues to be challenging for implementers. We recommend NIST explore alternative mechanisms to assist organizations that lack a smartcard infrastructure, such as collaborating on use case documentation and prototyping with efforts like OpenID's Enhanced Authentication Profile.

The remainder of this section provides comments for authenticators and processes described in Part B.

Memorized Secrets

Considering the accessibility of password managers to non-technical users from commercial, open source projects, and built-in capabilities within major web browsers, MITRE recommends the next version of the guidelines provide official guidance on the usage of password managers. Per the 800-63 FAQ the use of password managers is not explicitly recommended in 800-63B, but MITRE has observed the universal adoption of recommended password policy, such that they are less complex (i.e., memorable), has been slow among agencies. We believe explicitly allowing password managers that allow the subscriber to store passwords generated by the verifier or assist the subscriber in generating a password that aligns with a verifiers' password complexity policy would ease the transition from long, complex passwords to the current guidance. Guidance in this area should also describe the risk decision for agencies presented by cloud versus local password manager synchronization.

Out-of-band Device

As the *SP 800-63-3 Implementation Resources* document notes, many different implementations of out-of-band authenticators exist. Regarding the security of out-of-band authenticators the document also notes the transfer or verification of a secret between the primary and secondary channels avoids the opportunity for an attacker with good timing to obtain authentication of a different session controlled by them. However, some industry implementations have chosen instead to display primary channel authentication information, such as location, time, and IP address, to the secondary channel—in the form of a push notification. While such an implementation does not share a "secret," the user compares the consistency of the primary channel transaction to the information presented in the secondary channel. We recommend the next revision of the guidelines allow agencies to accept the risk of this type of implementation, with additional user training mitigations to detect when the primary channel authentication may have been compromised.

Single-Factor One-Time Password Device

Organizations that have chosen to implement OTP devices as an authenticator often use one of the numerous mobile applications available in free and paid versions. Users of these applications often encounter a poor user experience when upgrading or otherwise changing their devices: they are forced to reenroll the application because the secret seed is not transferred to the new device. This scenario is worsened if the user does not have a backup authenticator that can facilitate self-re-enrollment. Cloud identity services have addressed this issue by implementing an optional cloud "backup" feature that allows the secret to be moved from device to device. While useful to the end user, it introduces risk to the verifier if application secrets are exposed to hackers. We recommend NIST provide mitigation guidance to protect cloud secrets for agencies that choose to offer this capability to subscribers.

800-63C

Overall, the term *federation* is used for a very narrow concept; NIST 800-63C details what would better be described as *credential translation,* as described in the GSA FICAM Architecture [7]. The dictionary definition of federation implies that members fall under no central authority but agree to trust each other. The concept of federation in the ICAM world is much larger than what is in 800-63C, encompassing trust agreements between participating entities. The concepts of an indirect verifier and passing of authentication assertions and attributes (claims) are a component of federation; however, the 800-63 model defines federation as a simple redirect—one that might exist within even a small disconnected enterprise that wants to offload authentication from the applications.

MITRE acknowledges that the term *federation* and the concept of Federation Assurance Level (FAL) cannot be easily changed to wording that more precisely conveys a credential translation. However, we recommend the next revision provide additional context that acknowledges a true federation has more considerations than those described within 800-63C. The additional context would help address the practical problem MITRE has observed among agencies in that the term is understood by some to encompass the broader view and by some as the current pattern in 800-63C.

MITRE also recommends qualifying uses of *Assertion* to *Authentication Assertion*. While the context of 800-63C is authentication, and thus *authentication assertion* is implied, MITRE has observed the use of unqualified *assertion* leads to some confusion among the agencies we support, because not all assertions claim a successful authentication. For example, assertions can provide attribute information, and emerging standards work is leading to other types of assertions such as policy assertion.

Finally, current guidance allows the use of *front-channel* assertions; OpenID Connect defines this as the *implicit* use case where the access token is transmitted though web browser redirects. OAuth 2.0 Security Best Current Practice (draft) and OAuth 2.1 Authorization Framework (draft) deprecates the implicit grant, due to multiple weaknesses in the transaction. We recommend the removal of *front-channel* assertions in the next version of guidance to align with current security best practice.

Federation Relationships

The manual registration model described in the Federation Models section states “federation relationships SHALL establish parameters regarding expected and acceptable IALs and AALs in connection with the federated relationship.”

MITRE recommends NIST develop additional context for agencies, perhaps in the form of non-normative implementation guidance. This guidance should address best practices for the enforcement of such relationships—from the perspective of the identity provider and the relying party. Additionally, the guidance should include strategies for informing the subscriber that they are inadequately credentialed or identity proofed.

References

[1] IEEE, "IEEE XPlore," 13 December 2012. [Online]. Available: https://ieeexplore.ieee.org/document/6381399.

[2] J. Fontana, L. Auld, B. Hall and S. Weeden, "Scaling Strong Authentication," in *Identiverse Virtual*, n/a, 2020.

[3] D. Bryson, D. Goldenberg, D. Penny and G. Serrao, "Blockchain Technology for Government," MITRE, McLean, Virginia, 2017.

[4] Gartner, "Information Technology Research," Garnter, n/a, 2019.

[5] Trust Over IP Foundation, "Trust Over IP Foundation," 5 May 2020. [Online]. Available: https://trustoverip.org/wp-content/uploads/sites/98/2020/05/toip_introduction_050520.pdf.

[6] Sovrin, "Join Sovrin," 2020. [Online]. Available: https://sovrin.org/join-sovrin/.

[7] U.S. General Services Administration, "Federal Identity, Credential, and Access Management Architecture," [Online]. Available: https://arch.idmanagement.gov/services/federation/.

Abbreviations and Acronyms

Term	Definition
AAL	Authenticator Assurance Level
AI	Artificial Intelligence
BYOI	bring your own identity
CSP	credential service providers
DID	Decentralized Identity
FAL	Federation Assurance Level.
FFRDC	federally funded research and development centers
IAL	Identity Assurance Level
IAM	identity and access management
ICAM	Identity, Credential, and Access Management
ML	Machine Learning
NIST	National Institute of Standards and Technology
OTP	one-time password
PIV	Personal Identity Verification
SMS	short message service
UX	User Experience