Draft NISTIR 8335

Identity as a Service for Public Safety Organizations

William Fisher
Christopher Brown
Mark Russell
Sudhi Umarji
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8335-draft

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8335

Identity as a Service for Public Safety Organizations

William Fisher
Applied Cybersecurity Division
Information Technology Laboratory

Christopher Brown
Mark Russell*
Sudhi Umarji
The MITRE Corporation
McLean, VA

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

** Former employee; all work for this publication was done while at employer.*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8335-draft

June 2021

U.S. Department of Commerce
Gina Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8335
38 pages (June 2021)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8335-draft

Public comment period: June 16, 2021 through August 2, 2021

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: psfr-nccoe@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

On-demand access to public safety data is critical to ensuring that public safety and first responder (PSFR) personnel can protect life and property during an emergency. The increasing use of cloud technologies can improve data access but also causes authentication challenges. The objective of this report is to inform public safety organizations (PSOs) about identity as a service (IDaaS) and how they can benefit from using it. This report also lists questions that PSOs can ask IDaaS providers when evaluating their services to ensure that the PSOs' authentication needs are met and the risk associated with authentication is mitigated properly. This report was developed in joint partnership between the National Cybersecurity Center of Excellence (NCCoE) and the Public Safety Communications Research (PSCR) Division at NIST.

Keywords

authentication; identity, credential, and access management (ICAM); identity as a service (IDaaS); multifactor authentication; public safety and first responders; public safety organization (PSO).

Audience

This document is intended for PSFR personnel who make technology decisions and also for affiliated technology providers (e.g., an authorized public safety digital service for criminal justice information access). The reader should have a basic understanding of identity, credential, and access management (ICAM) concepts, specifically authentication and access control capabilities that are found in a typical enterprise environment. PSFRs who are involved in acquisition program planning may also find this document useful.

Acknowledgments

The authors of this report thank all who have contributed to its content and provided feedback.

Trademark Information

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: psfr-nccoe@nist.gov

Executive Summary

Over the past several years, researchers from the National Institute of Standards and Technology (NIST) have worked closely with public safety organizations (PSOs) on a wide array of cybersecurity topics, including wearables, mobile devices, and identity, credential, and access management (ICAM). In 2019, NIST's National Cybersecurity Center of Excellence and Public Safety Communications Research Division hosted an invitation-only workshop with subject matter experts and decision makers from PSOs to address pressing, community-wide cybersecurity challenges [1]. Workshop participants made recommendations on a vision for data sharing in PSOs and agreed on this vision statement:

Getting the correct data to the correct people at the correct time with the correct protections and only if it is for the proper reason and in an efficient manner.

This document builds on the key findings from the workshop and focuses on authentication methods for PSOs. Specifically, PSOs have asked for technical guidance on how cloud solutions can be integrated into existing and new information technology (IT) architectures while aligning with NIST's *Digital Identity Guidelines* [2] and the Criminal Justice Information Services (CJIS) Security Policy [3]. This document is intended as a first step in establishing that guidance by examining the topic of identity as a service (IDaaS).

Today, IDaaS providers offer ICAM services, such as authentication, to customers through a software-as-a-service (SaaS) cloud-service model. PSOs could acquire IDaaS to provide authentication services for their own applications. This would allow the PSOs to offload some of their authentication responsibilities to the IDaaS provider.

The following are key recommendations from the report:

- Depending on the nature of a public safety application, such as the sensitivity of the data it uses and the types of devices and locations it is accessed from, stronger forms of authentication may be needed. PSOs are encouraged to use resources like the *Digital Identity Guidelines* [2] and the CJIS Security Policy [3], in addition to the recommendations in this document, for guidance on selecting authentication methods while taking risk into account.

- PSOs should perform a risk assessment for all of their applications that might use IDaaS authentication services before selecting an IDaaS provider. This allows PSOs to ask IDaaS providers specific questions about the forms of authentication that they need the provider to support.

- Most PSOs are unlikely to want to shift all authentication to the cloud immediately, so they should consider taking a hybrid IT approach—a mix of on-premises/data center and cloud-based authentication services. IDaaS providers typically support this type of deployment with software tools that can synchronize credentials (e.g., password hashes) and/or associated attributes. This allows PSOs to take advantage of IDaaS as they gradually transition from on-premises to cloud.

Table of Contents

List of Appendices

List of Tables

1 Introduction

On-demand access to public safety data is critical to ensuring that public safety and first responders (PSFRs) have the information they need to protect life and property during an emergency. Modern authentication services offer a significant operational advantage by providing access to mission-critical information and services while deployed in the field, during training and exercises, or when participating in day-to-day business and preparing for emergencies during nonemergency periods. These advantages can be limited if poorly implemented authentication requirements hinder PSFRs, especially when a delay—even seconds—is a matter of containing or exacerbating an emergency. Public safety organizations (PSOs) are challenged with implementing efficient and secure authentication mechanisms to protect access to this sensitive information while meeting the demands of their operational environments.

PSOs are increasingly using cloud applications that enable access to public safety data to ensure delivery of proper care and support during an emergency. It is common for these applications to issue their own credentials, often usernames and passwords, to users of the application. As the number of credentials that need to be managed grows across stovepiped applications, most PSOs, especially smaller ones with fewer resources, face increased challenges in managing these credentials and ensuring secure authentication practices. Here are some examples of common challenges:

- Password-based authentication practices vary among cloud providers. Some cloud applications may store passwords in an insecure manner or enforce needlessly complex password rules that negatively affect usability.
- PSOs operate in a variety of environments with different authentication requirements.
- A PSO may determine that a multifactor authentication mechanism is necessary to provide stronger protection for sensitive data stored within cloud applications but implementing multifactor authentication can be complex and may be outside the scope of expertise in the organization.
- Digital identities are not frequently shared across jurisdictional boundaries, and there is no single management or administrative hierarchy spanning all PSOs.
- A PSO's existing organizational identity, credential, and access management (ICAM) services may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult [4].
- When a user leaves an organization, the best practice is for their accounts to be deleted or otherwise disabled. Often this is a manual process subject to human error or not done at all.

> **Note:** The FirstNet Authority has identified ICAM as one of the key technology areas that compose secure information exchange.

PSOs can address these challenges by using cloud services dedicated to providing ICAM services as a core competency. Cloud-based ICAM can include some or all of the parts of identity assurance—identity proofing, authentication, and federation. Cloud-based ICAM services can augment and, in some cases, completely replace on-premises or data-center-centric implementations of ICAM services.

Identity as a service (IDaaS) is an informal term used by some cloud service providers. For the purposes of this document, an IDaaS provider offers ICAM services, such as authentication, under the software-as-a-service (SaaS) cloud-service model [5]. This means that the cloud consumer—the PSO—offloads some of the responsibility for ICAM software creation, installation, and maintenance to the IDaaS provider, while the PSO is still responsible for ICAM functions, such as maintaining the authenticator lifecycle as well as maintaining the applications that rely on the IDaaS provider's services.

The following are some of the benefits that PSOs may derive by transitioning to IDaaS:

- IDaaS providers enable authentication services that are flexible, efficient, and interoperable. The need for authentication flexibility is key for PSOs due to the diverse set of operational environments.
- IDaaS providers rely on standards to securely authenticate end users and to assert information about users to SaaS applications. IDaaS providers typically offer a catalog of customizable pre-built integrations for applications that use standards as the mechanism for interoperability. This growing ecosystem of interoperable SaaS applications and IDaaS providers can reduce the risk of cloud vendor lock-in while also easing the integration of identity services in customized PSO applications.
- IDaaS providers capture the mission benefits of cloud adoption by supporting organizational cybersecurity requirements. These benefits may include overall cost savings and increased agility that allow organizations to respond quickly to emerging cybersecurity threats.

1.1 Purpose

This document educates PSOs about what IDaaS is and how it can benefit them. It defines questions that a PSO can ask an IDaaS provider when procuring IDaaS to objectively determine the costs and benefits of moving to IDaaS, validate performance claims, and compare services from multiple providers. This document also presents considerations for determining what authenticator or combination of authenticators to use for an IDaaS deployment based on a risk assessment.

1.2 Scope

This document focuses on technology drivers when choosing an IDaaS provider for authentication needs. IDaaS providers may offer additional capabilities, such as identity proofing or access control capabilities, but those are out of scope for this document. Other facets of evaluating IDaaS providers and calculating the total cost of ownership when adopting cloud services are also out of scope.

Authentication in the context of this document is a (human) user-to-application transaction that occurs across a network such as the open internet or within an enterprise—for example, a user who authenticates to an email service through a web browser. Local authentication to a workstation or mobile device is out of scope, as are machine-to-machine authentications.

1.3 Report Structure

The rest of this report contains the following sections and appendices:

- **Section 2** presents the fundamentals of authenticators for IDaaS usage based on concepts from the *Digital Identity Guidelines* and the Criminal Justice Information Services (CJIS) Security Policy. It also discusses how PSOs can select IDaaS authenticators based on an identity-based risk assessment.
- **Section 3** explores additional considerations for IDaaS adoption.
- **Section 4** provides recommendations and other guidance to PSOs on selecting authenticators for IDaaS usage.
- The **References** section lists all references cited in the report.
- **Appendix A** introduces considerations for PSOs that are interested in using Fast Identity Online (FIDO) authentication for IDaaS.
- **Appendix B** lists the acronyms and abbreviations used in the report.

1.4 Report Conventions

This report uses callout boxes to highlight certain types of information, as depicted in Figure 1. Except for **Definition** boxes, which repeat the definitions of key terms, callout boxes usually contain new material that is not covered elsewhere in the report. A **Caution** box provides a warning of a potential issue with doing or not doing something. A **Note** box gives additional general information on a topic. A **Tip** box offers advice that may be beneficial to the reader.

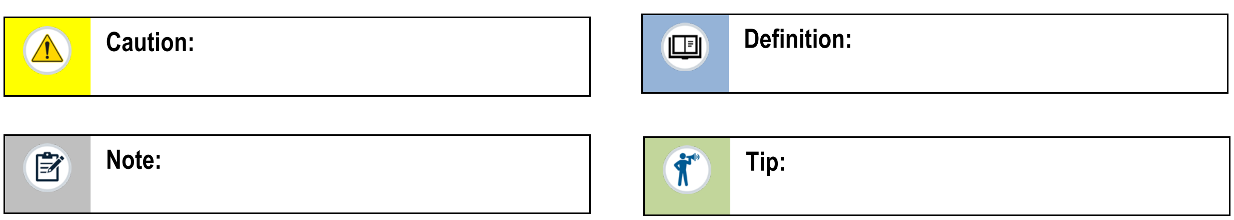

Figure 1: Callout Box Formats

2 Fundamentals of Authenticators for IDaaS Usage

This section explains the fundamentals of authenticators for IDaaS usage. It is based on concepts from the *Digital Identity Guidelines* [2] and the CJIS Security Policy [3].

> **Note:** This document is meant to supplement and describe how the *Digital Identity Guidelines* could be used to align with the CJIS Security Policy. PSOs that require access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and criminal justice information (CJI) are subject to the CJIS Security Policy which specifies the necessary controls to protect CJI from creation through dissemination, whether at rest or in transit. PSOs subject to this requirement should consult with their CJIS representative for specifics of implementing the CJIS Security Policy.
>
> The CJIS Security Policy is underpinned by Presidential and FBI directives and NIST recommendations, including *Digital Identity Guidelines* (NIST SP 800-63) and *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53). Readers should refer to the NIST website for the latest versions of these publications.
>
> The CJIS Security Policy is tailored and governed by the CJIS Advisory Policy Board. The security policy is currently undergoing a modernization process that will align with national information assurance methodology that is implementable by both large and small agencies charged with protecting criminal justice information. Readers should refer to the FBI website for the latest versions of the CJIS Security Policy.

2.1 Authentication Factors

Authenticating a user involves verifying evidence of one or more authentication factors:

- ***Something you know*** means a *secret*—nonpublic information shared between an end user and a digital service. Common examples are passwords and personal identification numbers (PINs) that can be created by either the end user or the digital service.
- ***Something you have*** means a physical device that stores a secret and is possessed by only the end user. During authentication, the user proves they are in control of the secret through a challenge and response transaction.
- ***Something you are*** means a fingerprint or other biometric data. As Section 2.4.4 discusses, biometrics are *private*, not secret, so there are limitations on using something you are authentication factors.

Many digital services use two or more authentication factors in combination to authenticate users. An example is a user entering a password into a PSO website, which causes the user's mobile device to receive a login code that the user enters in the website to gain access to their account. These techniques are sometimes referred to as advanced authentication, two-step verification, login verification, two-factor authentication, or multifactor authentication (MFA). This document uses the term MFA. MFA must use factors in two or more authentication factor categories for greater strength, so requiring a password and a PIN (e.g., both something you know) without any other factors (something you have or something you are) would not qualify as MFA [6].

For digital services, one option for MFA is to require an end user to authenticate themselves with something you have that is activated by something you know so that the service has proof of possession and control of the physical device. Note that for this option, the physical device must be activated only by something you know and must have additional protections against attacks such as PIN guessing in case the physical device is stolen or lost. Another possible option for MFA is to use something you are—for example, a biometric—to activate something you have.

2.2 Concepts from the *Digital Identity Guidelines*

Published in 2017, the National Institute of Standards and Technology's (NIST's) *Digital Identity Guidelines* [2] are a suite of publications that provide technical requirements for federal agencies implementing digital identity services. While the primary audience for these guidelines is federal agencies, PSOs and others can also use their content. The *Digital Identity Guidelines* were intended to be part of a risk-based approach to implementing digital identity services.

Note: This document attempts to be consistent with the terms and definitions used in the *Digital Identity Guidelines*. Readers should also use the guidelines' Definitions and Abbreviations for terms that are not explicitly defined in this document.

Table 1 lists the publications comprising the *Digital Identity Guidelines*. For simplicity, this document uses the term *Digital Identity Guidelines* to refer to the suite of publications. Where appropriate, a single document in the suite will be indicated by specifying its reference number as listed in Table 1.

Table 1: *Digital Identity Guidelines* Publications

NIST Special Publication (SP)	Title and Reference	Description
NIST SP 800-63-3	*Digital Identity Guidelines* [7]	Provides an overview of general identity frameworks by using authenticators, credentials, and assertions together in a digital system, and a risk-based process for selecting assurance levels.
NIST SP 800-63A	*Digital Identity Guidelines: Enrollment and Identity Proofing* [8]	Addresses how applicants can prove their identities and become enrolled as valid subscribers within an identity system.
NIST SP 800-63B	*Digital Identity Guidelines: Authentication and Lifecycle Management* [9]	Addresses how an individual can securely authenticate to a credential service provider to access a digital service or set of digital services.
NIST SP 800-63C	*Digital Identity Guidelines: Federation and Assertions* [10]	Provides requirements when using federated identity architectures and assertions to convey the results of authentication processes and relevant identity information to an agency application.

The *Digital Identity Guidelines* separate identity assurance into three discrete components:

- **Identity Assurance Level** refers to the identity proofing process, which is the process used to verify a user's association with their real-world identity for issuing the user a credential.
- **Authenticator Assurance Level (AAL)** refers to the authentication process.
- **Federation Assurance Level** refers to the strength of an assertion in a federated environment, which is used to communicate authentication and attribute information (if applicable) to a relying party. A *relying party* is an entity that relies upon the user's authenticator(s) and credentials or a verifier's assertion of a user's identity, typically to process a transaction or grant access to information or a system.

Tip: As NIST incorporates feedback on the current *Digital Identity Guidelines* into the next revision, interested readers can follow the progress. The Frequently Asked Questions page [11] is another recommended resource for digital identity implementers.

The rest of this report concentrates on AALs and the IDaaS authentication services that are used to achieve them. These are some of the authentication-related roles that an IDaaS provider can perform:

- **credential service provider:** A *credential* binds an identity to an issuing authority, and a *credential service provider (CSP)* manages the life cycle of a credential. In the physical world, a credential could be a first responder's identification card or badge issued by their local jurisdiction. However, in the digital world, a credential can be a record that links a user's identity to a username and password.
- **verifier:** A *verifier* validates a user's identity by verifying their possession and control of one or two authenticators by using an authentication protocol. In the digital world, this is commonly accomplished by challenging the user to authenticate with an *identifier* (username) and *shared secret* (password). The IDaaS provider then verifies that the submitted username links to a valid user and the submitted password matches the password that the IDaaS provider has stored.

In this example, the IDaaS provider authenticates the user by a username and password. IDaaS providers usually support additional ways of authenticating besides single-factor username and password, with increasing levels of assurance.

2.3 Authenticator Types from the *Digital Identity Guidelines*

There are many possible types of authenticators, and several are viable for commercially available IDaaS platforms. The *Digital Identity Guidelines* specify the authenticator types listed in Table 2, which can be used alone, or in combination for MFA and define guidance for the authenticator and the verifier for each type. An IDaaS provider may offer only a subset of these authenticators that are compatible with their service.

Table 2: Authenticator Types from the *Digital Identity Guidelines*

Authenticator Type	Authenticator Description	Verifier Description
memorized secret 	A secret value intended to be chosen and memorized by the user, such as a password or PIN	The user remembers the secret value and manually enters it (types it into the application).
lookup secret 	A secret value shared between the user and the CSP that is stored in a physical or electronic record	The user looks up the secret value and manually enters it.
out-of-band device 	A physical device that is possessed and controlled by the user	The device is uniquely addressable—that is, it can unambiguously identify itself over an insecure network—and it communicates securely with the verifier over a distinct communications channel to share a secret value.
single-factor OTP device 	A one-time password (OTP) generator in a specialized hardware device or in software installed on devices such as mobile phones. It has an embedded secret that is used as the seed for generating OTPs.	The user views the OTP and manually enters it.

Authenticator Type	Authenticator Description	Verifier Description
multifactor OTP device 	An OTP generator that is activated only after authenticating the user	The user authenticates to the OTP device through a different authentication factor type (something you know or something you are). The user then views the OTP and manually enters it.
single-factor cryptographic software 	Software that performs cryptographic operations by using protected cryptographic key(s) stored on disk or some other "soft" media, and provides the authenticator output directly to the verifier	The verifier generates a challenge nonce, sends it to the authenticator, and uses the authenticator output to verify possession of the cryptographic software.
single-factor cryptographic device 	A hardware device that performs cryptographic operations using protected cryptographic key(s), then provides the authenticator output directly to the verifier	The verifier generates a challenge nonce, sends it to the authenticator, and uses the authenticator output to verify possession of the cryptographic device.
multifactor cryptographic software 	Same as single-factor cryptographic software, except the software requires activation through a second factor of authentication	The user authenticates to the cryptographic software through a different authentication factor type (something you know or something you are). Then the verifier generates a challenge nonce, sends it to the authenticator, and uses the authenticator output to verify possession of the cryptographic software.
multifactor cryptographic device 	Same as single-factor cryptographic device, except the hardware device requires activation through a second factor of authentication	The user authenticates to the cryptographic device through a different authentication factor type (something you know or something you are). Then the verifier generates a challenge nonce, sends it to the authenticator, and uses the authenticator output to verify possession of the cryptographic device.

2.4 The Strength of Authentication Processes

The authentication risks inherent to digital services must be managed as part of a PSO's risk management program. To assist in this process, the *Digital Identity Guidelines* [2] and the CJIS Security Policy [3] both define approaches for selecting authenticators. These approaches are described below.

2.4.1 Authenticator Assurance Levels (AALs)

The *Digital Identity Guidelines* specify an identity risk-based approach for selecting authenticators. It is based on the concept of *AALs,* which indicate the relative strength of an authentication process [7]:

- **AAL1** requires single-factor authentication and is permitted with any authenticator type listed in Table 2.
- **AAL2** requires two authentication factors (MFA) for additional security, with each factor of a type listed in Table 2.

- **AAL3** is the highest authentication level. In addition to meeting the AAL2 requirements, one of its factors must be a hardware-based authenticator, and the authentication process must be resistant to verifier impersonation.

Table 3 shows how the authenticator types from Table 2 can be used alone or in combination to achieve the AALs defined in the *Digital Identity Guidelines*. For example, AAL2 can be achieved by using any of the multifactor authenticator types or by using a memorized secret plus one of the five authenticator types specified in the rightmost column. AAL3 can be achieved only two ways: by using a multifactor cryptographic device or by using a memorized secret plus a single-factor cryptographic device.

Table 3: Authenticator Assurance Levels

<table>
<tr><th>AAL</th><th colspan="2">Permitted Authenticator Type(s)</th></tr>
<tr><td rowspan="9">AAL1</td><td colspan="2">memorized secret</td></tr>
<tr><td colspan="2">lookup secret</td></tr>
<tr><td colspan="2">out-of-band device</td></tr>
<tr><td colspan="2">single-factor OTP device</td></tr>
<tr><td colspan="2">multifactor OTP device</td></tr>
<tr><td colspan="2">single-factor cryptographic software</td></tr>
<tr><td colspan="2">single-factor cryptographic device</td></tr>
<tr><td colspan="2">multifactor cryptographic software</td></tr>
<tr><td colspan="2">multifactor cryptographic device</td></tr>
<tr><td rowspan="8">AAL2</td><td colspan="2">multifactor OTP device</td></tr>
<tr><td colspan="2">multifactor cryptographic software</td></tr>
<tr><td colspan="2">multifactor cryptographic device</td></tr>
<tr><td rowspan="5">memorized secret +</td><td>lookup secret</td></tr>
<tr><td>out-of-band device</td></tr>
<tr><td>single-factor OTP device</td></tr>
<tr><td>single-factor cryptographic software</td></tr>
<tr><td>single-factor cryptographic device</td></tr>
<tr><td rowspan="2">AAL3</td><td colspan="2">multifactor cryptographic device</td></tr>
<tr><td>memorized secret +</td><td>single-factor cryptographic device</td></tr>
</table>

Section 2.5 provides guidance on how to select the appropriate AAL for a particular situation based on the results of a risk assessment.

2.4.2 Authentication Categories from the CJIS Security Policy

The CJIS Security Policy provides the minimum set of “appropriate controls to protect the full lifecycle of CJI [criminal justice information], whether at rest or in transit.” It further provides “guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI” [3]. The CJIS Security Policy defines requirements for authenticating users of digital services in its Policy Area 6. It specifies two categories of authentication and provides examples from each category, as explained in Table 4.

Table 4: Authentication Categories from CJIS Security Policy

Category	Examples of Authenticator Type(s)	
standard	password or PIN	
	hard or soft token	
	biometric	
	one-time password	
advanced	password +	biometric system
		user-based digital certificate
		smart card
		software token
		hardware token
		paper (inert) token
		out-of-band authenticator
		risk-based authentication

Note: The CJIS Security Policy and the *Digital Identity Guidelines* both use the term "risk-based authentication" but with different meanings. Risk-based authentication is broadly used terminology and may have different meanings depending on the context.

At this time, the **CJIS Security Policy** defines risk-based authentication as including "a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions."

The ***Digital Identity Guidelines*** define it as a technique that may be used to reduce the likelihood that an attacker will lock the legitimate claimant out because of rate limiting. In other words, in the context of the *Digital Identity Guidelines,* risk-based authentication supplements an authentication transaction but cannot be a factor.

2.4.3 Authenticator Requirement Differences

While the CJIS Security Policy and the *Digital Identity Guidelines* have many similarities in their authenticator requirements, there are also noteworthy differences. Table 5 lists some of these.

Table 5: Differences Between CJIS Security Policy and *Digital Identity Guidelines*

Authenticator	CJIS Security Policy	Digital Identity Guidelines
Short Message Service (SMS)	SMS messages are acceptable as part of an out-of-band authenticator transaction.	Restricts but does not prohibit the use of SMS-based OTPs.
Biometrics	Specifies a biometric plus a password as an example of advanced authentication.	Supports biometrics as part of MFA only when used in combination with a physical authenticator. Refer to Section 2.4.4 for more information.
Memorized secrets	Categorizes memorized secrets into *basic* and *advanced* password standards. Advanced password standards are similar to the *Digital Identity Guidelines'* memorized secret guidelines, except that the CJIS policy specifies a minimum length of 20 characters.	Has one set of guidelines for memorized secrets. Refer to Section 4.1 for further discussion.

Authenticator	CJIS Security Policy	Digital Identity Guidelines
PINs	A PIN serves two roles in CJIS policy: as a standard authenticator and when used in conjunction with a certificate or token. When used to activate a certificate or token, the PIN has a minimum of six digits. There is no stipulation about PIN digits being random.	Permits the use of six-digit memorized secrets that are random and are created by the IDaaS provider.
Hardware- and software-based authenticators	Permits the use of hardware and software-based authenticators.	Distinguishes between hardware- and software-based authenticators corresponding to an AAL.

2.4.4 Biometrics and Authentication

Using biometrics for authentication is often misunderstood. While the *Digital Identity Guidelines* support the use of biometrics, there are limitations [11]. A common misconception is that biometrics constitute a secret. Although biometrics are *personally identifiable information*—that is, information that can link to a specific person—they are private but not secret. A person's biometric can be obtained via an online attack, by taking a picture of the person with a camera phone (e.g., facial images) with or without their knowledge, lifted from objects that the person touches (e.g., latent fingerprints), or captured with high-resolution images (e.g., iris patterns) [11]. While presentation attack detection (PAD) technologies (e.g., liveness detection) can mitigate the risk of these types of attacks, additional trust in the sensor or biometric processing is required to ensure that PAD is operating in accordance with the needs of the CSP and the user.

One of the notable changes between NIST SP 800-63 revisions 2 and 3 is that biometrics are no longer considered a secret; therefore, the NIST identity guidelines prohibit them from being an authenticator type on their own. In other words, a PSO cannot accept a biometric as a single factor at AAL1 in an authentication transaction because the biometric does not equate to a secret that is impractical for an attacker to guess, such as a password. Similarly, a biometric cannot be combined with a shared secret to achieve AAL2 or above.

A biometric can, however, be used as part of MFA in conjunction with a specific physical authenticator (something you have). For example, this could be a fingerprint (or other biometric) used to unlock a secret such as a cryptographic key. As the *Digital Identity Guidelines Frequently Asked Questions* [11] note, a PSO verifier that accepts the risk of using a biometric in combination with a physical authenticator must ensure that the biometric readers meet the *Digital Identity Guidelines*' normative requirements for biometric systems [9].

Biometrics are commonly used to unlock commercial mobile devices. While a mobile device may have a biometric reader that meets the performance requirements of the *Digital Identity Guidelines,* the guidelines note that unlocking a device through biometric match cannot be considered an authentication factor because it is generally not possible for the verifier to obtain any information on how or whether the device was unlocked.

> **Tip:** PSOs interested in using mobile device biometrics for MFA should examine IDaaS provider claims and ensure the following are all true:
>
> - A biometric factor does not rely on device unlock.
> - Any underlying mobile application uses the official operating system biometric application programming interfaces (APIs).
> - The IDaaS provider can discern the make and model of mobile devices to assure that the biometric reader meets *Digital Identity Guidelines* performance requirements.

2.4.5 Protecting Secrets

In the example MFA scenario earlier in this section, the second authentication factor was an unpredictable, secret numeric code being transmitted to a mobile device that was registered with the digital service. Protecting this code while in transit is important so that attackers cannot steal the code and reuse it to impersonate the actual user.

The *Digital Identity Guidelines* restrict but do not prohibit use of the most commonplace method—SMS, also known as text messages—due to threats against the public switched telephone network. This introduces challenges because most users accept and understand SMS-based authentication factors, but the active threats against this method increase impersonation risk. Likewise, email-based distribution of codes is not recommended because the user does not have to prove possession of a device. An attacker could take control of a poorly secured email account and retrieve the secret codes. The *Digital Identity Guidelines* define a method of code distribution where these risks can be mitigated, and it is discussed further in Section 4.4.

In addition to stealing secrets sent by SMS or emails, it has also become commonplace for attackers to steal secrets from service providers that do not follow best practices for protecting them. For example, passwords can be stolen from a weakly protected database.

Another way that attackers acquire secrets is by tricking a user into supplying their password at a website that impersonates a legitimate digital service provider. Once stolen, these secrets are used in broader-scale attacks against other service providers by using techniques such as credential stuffing and password sprays. Credential attacks such as these present challenges for service providers to protect against, especially for organizations with limited cybersecurity expertise. The likelihood of a successful attack can be reduced by outsourcing authentication service to a third party that has committed to adopting the *Digital Identity Guidelines*.

2.5 Authenticator Type Selection

To help organizations decide what authenticator type(s) would offer the necessary strength for a particular scenario, the *Digital Identity Guidelines* [2] and the CJIS Security Policy [3] both provide decision trees. A decision tree asks a series of questions, and the answer to each question determines the next part of the path through the tree. Table 6 compares noteworthy characteristics of both decision trees, using language taken directly from the source documents, to help explain their fundamental differences.

Table 6: Comparing Decision Trees for Authenticator Type Selection

Characteristic	*Digital Identity Guidelines*	CJIS Security Policy
Applicability	any data	CJI
Possible outcomes	• AAL1 • AAL2 • AAL3	• Use advanced authentication • Don't use advanced authentication
Relies on risk assessment results?	Yes—must estimate the maximum potential impact (N/A, Low, Moderate, High) of an authentication failure for each of the following: • Inconvenience, distress or damage to standing or reputation • Financial loss or agency liability • Harm to agency programs or public interests • Unauthorized release of sensitive information • Personal safety • Civil or criminal violations What could happen if an unauthorized user accessed one or more valid user accounts?	No—since it only applies to CJI, there is not a wide range of possible impacts to consider
Considers factors other than risk assessment results?	Yes: • Whether or not personal data is being made accessible	Yes: • Whether the request is direct or indirect • Whether or not the request originates from within a physically secure location • Whether or not the request is from a location or organization that has all required technical controls implemented • Whether or not the request is from an organization-issued and controlled smartphone or tablet with approved compensating controls implemented

PSOs subject to the CJIS Security Policy must ensure that adequate safeguards are in place to secure ICAM functions, such as authentication, when SaaS applications are used to access CJI. PSOs that use IDaaS to centralize identity services to comply with this policy must use the CJIS authentication decision tree to determine if advanced authentication is required.

> **Note:** For the purposes of this document, it is assumed that **advanced authentication is required** to access CJI over an untrusted network.

If a PSO determines that advanced authentication is needed, this indicates that either AAL2 or AAL3 is needed. Therefore, the PSO should also assess their authentication risk based on the *Digital Identity Guidelines*' AAL decision tree to determine whether to use AAL2 or AAL3.

PSOs that are considering an AAL3 implementation with an IDaaS provider should carefully examine whether AAL3 is appropriate for some or all authentication transactions, given the technical considerations. Suppose that a PSO performs a risk assessment for an online case creation and retrieval system. The assessment reveals that unauthorized access to especially sensitive case information would have a severe adverse effect on PSO operations and thus a high impact that requires AAL3. Here are some of the considerations for an AAL3 implementation:

- The IDaaS provider may not support AAL3. Among the technical requirements for AAL3 is a strong verifier impersonation resistance authentication protocol—that is, the ability to mitigate the risk of a phishing attack that could fool an unwary PSFR into authenticating to an impostor IDaaS provider. In practical terms, this means the IDaaS provider must support a mutually authenticated version of Transport Layer Security (TLS) protocol where the client authenticator (in this case, possessed by a PSFR) and the server (IDaaS provider) authenticate each other at the same time. Please refer to Section B.4.2.6, Verifier Impersonation Resistance, of NIST SP 800-63-3, *Implementation Resources* [12], for an extended discussion of this topic.
- If the IDaaS provider supports AAL3, this should include supporting the use of hard cryptographic tokens. PSOs should also consider the form factor of the cryptographic token for a particular use case. For example, a ruggedized Universal Serial Bus (USB) token may be a more appropriate choice for PSFRs in the field than a conventional smart card.

3 Additional Considerations for IDaaS Adoption

As organizations continue to move workloads to the cloud, IDaaS providers have responded with integration options that can support various cloud maturity levels. For example, a greenfield identity solution deployment may benefit from an IDaaS provider with comprehensive native ICAM services. Such a provider offers not only authentication services but also other identity management core components such as identity governance, centralized access management, and federation services.

In a more likely scenario, a PSO has legacy systems and applications that will not shift to the cloud immediately. Consider an organization with a legacy authentication service, either on-premises or in a data center, that uses memorized secrets as the primary authenticator and requires an MFA capability to support CJIS advanced authentication. Memorized secrets could be supplemented with an OTP or push notification to target MFA at AAL2.

In this scenario, PSOs should take a hybrid IT approach to support a transition to the cloud. IDaaS providers typically support this type of deployment with a software tool that synchronizes credentials from an on-premises identity repository to the cloud provider. This type of solution enhances the user experience because the enterprise password for legacy services is the same as for cloud applications that are integrated with the IDaaS provider, which reduces the number of passwords that are managed by the end user. This approach also has the benefit of allowing an enterprise to manage identities through legacy processes while outsourcing authentication services to the cloud.

> **Definition:** *Hybrid IT* is "the use of traditional internal IT systems integrated with cloud environments. This includes the participation of external partners systems and services simultaneous with the participation of traditional internal IT processes and systems" [13].

> **Tip:** When evaluating a potential IDaaS provider, a PSO should get answers to questions such as these:
>
> - What authenticator types do you support?
> - For each supported authenticator type:
>   - What secret or private information is associated with it?
>   - How is the secret or private information protected?
>   - How is the secret or private information verified?
>   - How is the authenticator provisioned?

PSOs should also consider if IDaaS providers support the System for Cross-Domain Identity Management (SCIM) [14]. SCIM is an open standard to securely automate exchange of identity data. Additionally, IDaaS providers may provide web-based APIs that offer deeper integration into their identity services. For PSOs with the technical expertise to leverage APIs, APIs represent an opportunity to customize the authentication experience and align more closely to NIST guidance.

Finally, mature cloud-first organizations that use tooling to orchestrate application deployments to a platform-as-a-service (PaaS) cloud-service model should consider identity software that can support this type of deployment. Sometimes referred to as *continuous integration/continuous deployment (CI/CD)*, this approach allows organizations to automatically upload changes to services or applications on a frequent basis. Some identity-based software vendors create portable, reusable packages called *containers* that organizations can incorporate into their CI/CD processes [15]. This model is especially useful for organizations that require customization beyond typical IDaaS provider capabilities.

3.1 Risk Assessment and Acceptance

Before selecting an IDaaS provider, a PSO should perform a risk assessment for all of its applications that might use IDaaS authentication services, in accordance with Section 6.2 of the *Digital Identity Guidelines*. This will result in assigning an AAL commensurate with risk for each application. The PSO can then be mindful of its AALs and the authentication types that may be feasible for each application when asking potential IDaaS providers about the forms of authentication they support.

It is important to make risk-based decisions regarding IDaaS authenticators. Many security frameworks, such as NIST's Risk Management Framework (RMF), are built on the principle of risk-based decision-making. From the NIST RMF: "The selection and specification of security controls for a system is accomplished as part of an organization-wide information security program that involves the management of organizational risk—that is, the risk to the organization or to individuals associated with the operation of a system" [16].

In addition to performing a risk assessment, the *Digital Identity Guidelines* recommends developing a Digital Identity Acceptance Statement to provide risk accountability for the PSO. The statement should include a section that describes compensating controls and the acceptance of risk by the PSO when the complete set of NIST SP 800-63 security controls are not implemented. PSOs may not have the resources necessary to implement every digital identity guideline requirement and may prefer a phased approach to implementation. This is also particularly useful for PSOs that use IDaaS providers that may not implement all the digital identity guideline requirements for an AAL. Such providers may describe adequate compensating controls that should be documented within this statement.

4 Recommendations for Authenticator Selection

This report has highlighted common capabilities of cloud services that market themselves as IDaaS providers and has documented considerations for PSOs. In summary, while some IDaaS providers offer a mature suite of ICAM services (federation capabilities, for example), others offer supplemental authentication services for existing identity solutions. Thus, PSOs, especially those of smaller size without ICAM expertise, that are moving toward enhancing their authentication capabilities face a difficult task of procuring a satisfactory IDaaS provider.

This section presents guidance to PSOs on selecting authenticators that are typically supported by IDaaS providers—memorized secrets (passwords), out-of-band devices (push notifications), and single-factor OTP devices—as well as common supplemental capabilities marketed by IDaaS providers. For example, IDaaS providers may include out-of-band device and single-factor OTP device capabilities in one mobile application to simplify deployment.

This section is not intended as exhaustive. Readers are encouraged to also refer to the *Digital Identity Guidelines* described in Section 2.1 and their related supporting documents, particularly NIST SP 800-63-3*, Implementation Resources* [12]; and *Conformance Criteria for NIST SP 800-63A Enrollment and Identity Proofing and NIST SP 800-63B Authentication and Lifecycle Management* [18]. The conformance criteria may be particularly useful to PSOs as a method for an IDaaS provider to communicate its alignment with the *Digital Identity Guidelines* requirements in NIST SP 800-63B [9]. The National Security Agency has also published criteria, based on the *Digital Identity Guidelines,* to consider when selecting a multifactor authentication solution [19].

Caution: The authenticators in this section require exchange of a secret value between the user's computing device and the IDaaS provider. It is important that the secret is protected from interception by attackers. This can be done by a NIST-recommended authenticated protected channel, such as TLS [17].

4.1 Memorized Secrets

Memorized secrets (passwords) are commonly used in combination with another factor to achieve MFA at AAL2 (refer to Section 2.4.5 for a full discussion). In a change from previous password requirements, the *Digital Identity Guidelines* shift the burden of password management from the user to authentication services (i.e., IDaaS providers) in important ways. The threat model used by the *Digital Identity Guidelines* is intended to protect against *online* password attacks rather than *offline*. The password security model has been validated by research from one of the largest commercial IDaaS providers, whose password recommendations [20] are in alignment.

Most notably, the *Digital Identity Guidelines* remove complexity requirements. Instead, the user is required to create a password with a minimum length of eight characters, which makes it more memorable for the user, yet hard for attackers to compromise. For example, a user could create a password with four words that have meaning for them (correct horse battery staple) but are sufficiently random that an attacker could not predict them. Also, there are no password expiration requirements. That is, the user should not be required to change their passwords arbitrarily at regular intervals (e.g., 90 days, six months).

Removing password complexity and expiration requirements is acceptable because of controls implemented by the IDaaS provider. For example, the IDaaS provider checks the user's password against known compromised accounts and easily guessable passwords via a restricted-password list. This check happens when the user initially creates their password, and if the password is on the restricted list, the user is asked to create a different password. The check is similarly repeated during the password's lifetime. If a compromised password is detected, the user's account may be locked until a suitable replacement password is chosen. Further, the IDaaS provider implements controls such as rate limiting to mitigate online attacks, transport-level encryption, and supplemental techniques discussed in Section 4.3.

Tip: PSOs should consider asking IDaaS providers the following questions regarding memorized secrets:

- What password policy customization options are available for cloud consumers?
- What security controls does your service implement to protect memorized secrets while in transit and at rest? Please specify rate-limiting capabilities, encryption algorithms (at rest and in transit), and offline attack resistance measures (salt and hash implementations).
- What restricted-password capabilities are available for cloud consumers? Detail any automated and consumer-controlled capabilities.

4.2 Out-of-Band Devices

Out-of-band authenticators are something you have, usually a mobile device, that the user proves possession of via an application. Out-of-band authenticators are typically used in combination with passwords to achieve MFA at AAL2. The *Digital Identity Guidelines* define three possible methods of operation for out-of-band authenticators, which are described below. In each method, the *primary channel* is typically a web browser, and the *secondary channel* is created via a mobile application. Significantly, the primary and secondary channels may occur on the same mobile device or separate computing device (e.g., laptop) and a mobile device.

1. The user transfers a secret received by the out-of-band device via the secondary channel to the verifier using the primary channel. For example, the user may receive the secret on their mobile device and type it (typically a six-digit code) into their authentication session.
2. The user transfers a secret received via the primary channel to the out-of-band device for transmission to the verifier via the secondary channel. For example, the user may view the secret on their authentication session and either type it into an application on their mobile device or use a technology such as a barcode or Quick Response (QR) code to complete the transfer.
3. The user compares secrets received from the primary channel and the secondary channel, then confirms the authentication via the secondary channel.

IDaaS providers will typically direct users to download a specific application to their mobile device that facilitates at least one of the three methods of operation. Contrast this with single-factor OTP devices (Section 4.4) that use open protocols supported by multiple applications, including mobile applications that the user may already have.

In all out-of-band authentication methods, the mobile device must be securely and uniquely authenticated via a secret. Commonly used out-of-band devices satisfy this requirement by generating a public/private key pair in the secure storage area of the device via the associated application. The public portion of the key is registered with the IDaaS provider, and the private portion never leaves the device and is unlocked by the user using a biometric or PIN.

Later, during the authentication transaction, the associated application accesses the private portion of the key pair to digitally sign a message that approves the transaction or to convey the secret from the primary channel. The IDaaS provider can positively identify the device through the properties of public key cryptography.

Caution: For PSOs considering an out-of-band device implementation, note that some IDaaS providers may use a variation of the third method of operation in which the mobile application uses contextual data (example below), such as the location and Internet Protocol (IP) address from the primary authentication channel in lieu of a visible secret.

In this case, this risk should be mitigated with security awareness training that reminds users to confirm that the information in the push notification is accurate.

Tip: PSOs should consider asking IDaaS providers the following questions regarding out-of-band authenticators:

- Which of the three scenarios from Section 5.1.3 of the *Digital Identity Guidelines* [7] does your out-of-band device authenticator solution support?
- How does your service verify that the user has physical control of the out-of-band authenticator?
- If your solution uses cryptographic key pairs to verify control of the device, where is the key pair stored, and how do you implement key management?

4.3 Supplemental Authentication Controls

A PSO may have a use case to implement a dynamic authentication policy for its user population that incorporates contextual attributes or behavioral profiles to reduce friction in the authentication transaction. IDaaS providers can provide contextual or behavioral capabilities to assist PSOs in creating a risk-driven authentication policy. The *Digital Identity Guidelines* do not include risk-based or contextual authentication systems as an authentication factor, but they recommend these technologies as an additional control against online guessing attacks such as password spray [21]. Risk-based authentication techniques, however, are commonly marketed by

IDaaS providers and allow PSOs to create an MFA policy based on signals such as IP addresses, geolocation, and other variances from a user's baseline behavior.

PSOs with limited ICAM experience may benefit from risk-scoring capabilities offered by IDaaS providers. To simplify authentication policy creation, some IDaaS platforms support a risk-score metric that can enhance authentication policy. This technique allows an organization to align its risk tolerance with authentication policy by using predetermined algorithms that incorporate the signals. Some IDaaS providers offer additional functionality in this space by allowing customization of the signal weights used to calculate a risk score. For example, if an organization is concerned about users authenticating from a location, a geolocation signal could be weighted more heavily than other signals in the calculation.

Further, these platforms can incorporate threat intelligence into a risk score. *Threat intelligence* is threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making. In the context of IDaaS providers, an example of threat intelligence could be automated blockage of IP addresses known to be involved in phishing, password spraying, or other authentication-related attacks. In contrast to legacy, on-premises solutions, IDaaS providers are uniquely positioned to detect large-scale attacks to reduce risk for users.

> **Tip:** Some IDaaS providers market "step-up" authentication, which increases the threshold of an authentication transaction (e.g., AAL2 to AAL3) when a user accesses a sensitive resource. This approach is static. A risk-based authentication can incorporate resource sensitivity as a dynamic risk-score signal, which is preferable.

Additionally, as zero-trust security models gain popularity, IDaaS providers are responding with mobile device health capabilities. One of the pillars associated with zero trust is the real-time cybersecurity posture and trustworthiness of a device [22]. In the context of an authentication transaction, a zero-trust model ensures that devices that access an organization's resources are in an acceptable state. The state of the device can incorporate factors such as examinations of compromise, version of the running operating system, and encryption status. Some IDaaS providers additionally incorporate device health into an authentication risk-score calculation.

> **Tip:** PSOs should consider asking IDaaS providers the following questions when evaluating risk-based authentication capabilities:
>
> - What risk-based capabilities for authentication transactions are supported? Please include capabilities that are marketed as contextual, behavioral, or adaptive.
> - What are the signals used to calculate the risk score? If the calculation is weighted, can it be customized?
> - Does the service provide a native capability to derive endpoint health status, such as with Enterprise Mobility Management (EMM)? Can the service integrate with third-party EMM or endpoint protection platform services?

4.4 Single-Factor OTP Device

Like out-of-band devices, single-factor OTP device authenticators are typically used in combination with passwords to achieve MFA at AAL2. A single-factor OTP device may be a distinct physical device or an application installed on a mobile device. For the purposes of this section, distinct physical devices are out of scope because application-based single-factor OTP devices are most used by IDaaS providers.

The workflow of a single-factor OTP device via a mobile application as part of an MFA authentication transaction typically consists of prompting the user to launch the OTP application after successfully submitting a password. The user then submits the displayed six-digit OTP associated with the IDaaS provider. The OTP proves the user is in control of the pre-registered mobile device and is protected from brute force attacks because it has been generated using a secret value that was exchanged during the mobile device registration process. The transfer of the secret is typically implemented during the mobile device registration process via a scan of a QR code.

The *Digital Identity Guidelines* recommend using time-based OTP (TOTP) or hash-based message authentication code OTP (HOTP) generation protocols in mobile applications. As a result of using an open standard, there are multiple applications that support TOTP and HOTP protocols and are not tied to any specific IDaaS provider. However, an IDaaS provider may choose to tell users to install a specific application that is directly supported.

Tip: PSOs should consider asking IDaaS providers the following questions regarding single-factor OTP device authenticators:

- Which OTP protocols are supported (TOTP or HOTP)?
- For third-party mobile applications that support TOTP or HOTP, are there other requirements that would inhibit interoperability between the applications and the service?

4.5 OTPs via SMS

The *Digital Identity Guidelines* formally deprecate the use of SMS, or text messaging, as an OTP transport mechanism, as discussed in Section 2.4.5 of this document. Nevertheless, many non-governmental IDaaS customers use OTP via SMS, so IDaaS providers typically support SMS-based OTP authentication as a second factor, regardless of the potential security implications. Organizations that choose to accept the risk of using SMS-based OTPs typically do so for one or more of the following reasons:

- Nearly all mobile devices have an SMS capability, even so-called feature phones that lack the ability to install mobile applications. Contrast this with other OTP-based solutions that require the user to install a compatible application. Application distribution can be difficult for organizations that do not have direct control over user mobile devices.
- The absence of hardware purchases for devices, such as hardware-based OTP authenticators, results in reduced costs for organizations.
- Business-to-consumer services' use of SMS-based OTP as a second authentication factor has become common, hence more accessible for the nontechnical person.

Phishing and subscriber identity module (SIM) swap attacks against SMS OTPs have persisted since publication of the *Digital Identity Guidelines,* increasing the risk of compromised authentication transactions for organizations. For this reason, PSOs should assess, understand, and accept the risk associated with implementing or continuing the use of an SMS-based solution. Any form of authentication using SMS or another technology that relies on the public switched telephone network is considered a restricted authenticator to indicate its reduced reliability. The *Digital Identity Guidelines Frequently Asked Questions* [11] provide the following recommendations that are relevant for PSOs:

- Offer subscribers at least one alternative authenticator that is not restricted.
- Provide subscribers with meaningful information on the security risks of the restricted authenticator and availability of alternatives. The user's account and personal information are at risk, so the user needs to participate in the risk determination process as well.
- Include in its risk assessment any additional risk to subscribers.
- Develop a migration plan for the possibility that the restricted authenticator is no longer acceptable at some point.

If an SMS-based solution is a requirement, at a minimum PSOs should support mobile application TOTPs or HOTPs as an alternative authenticator. These solutions provide a similar experience to SMS-based OTPs, with mobile applications available from IDaaS providers and third-party alternatives available from commercial services and open-source projects. While still phishable, software-based OTPs are not susceptible to SIM swap-style attacks. An alternative mechanism to SMS-based authenticators takes on greater importance if the PSO determines that individuals within its subscriber population are at higher risk of targeted attacks. Additionally, PSOs should use user experience customization capabilities offered by IDaaS providers to communicate to subscribers the risk of using SMS-based authenticators.

References

[1] National Institute of Standards and Technology (2019) NIST Identity, Credential, and Access Management (ICAM) Workshop Outcomes. https://www.nist.gov/system/files/documents/2019/11/01/nist_identity_credential_and_access_management_icam_workshop_outcomes.pdf

[2] National Institute of Standards and Technology (2017) *Digital Identity Guidelines*. Available: https://www.nist.gov/itl/tig/projects/special-publication-800-63

[3] Federal Bureau of Investigation (FBI) Criminal Justice Information Services Division (2020) Criminal Justice Information Services (CJIS) Security Policy (Version 5.9). https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

[4] Healthcare Information and Management Systems Society (2015) Cloud Computing Toolkit. http://s3.amazonaws.com/rdcms-himss/files/production/public/HIMSSorg/Content/files/PrivacySecurity/CS03_Cloud_PS_101_Final.pdf

[5] Simmon E (2018) Evaluation of Cloud Computing Services Based on NIST SP 800-145. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 500-322. https://doi.org/10.6028/NIST.SP.500-322

[6] National Institute of Standards and Technology (2019) *Back to basics: Multi-factor authentication (MFA)*. Available: https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication

[7] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[8] Grassi PA, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Enrollment and Identity Proofing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63A, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63A

[9] Grassi PA, Newton EM, Perlner RA, Regenscheid AR, Fenton JL, Burr WE, Richer JP, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63B, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63B

[10] Grassi PA, Nadeau EM, Richer JP, Squire SK, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Federation and Assertions. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63C, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63C

[11] National Institute of Standards and Technology (2021) *NIST Special Publication 800-63: Digital Identity Guidelines Frequently Asked Questions*. Available at https://pages.nist.gov/800-63-FAQ/

[12] National Institute of Standards and Technology (2020) NIST Special Publication 800-63-3 Implementation Resources. https://www.nist.gov/system/files/documents/2020/07/02/SP-800-63-3-Implementation-Resources_07012020.pdf

[13] Open Alliance for Cloud Adoption (2018) Open Alliance for Cloud Adoption Usage Manual: Cloud Maturity Model, Rev. 4.0. https://www.oaca-project.org/wp-content/uploads/2018/10/CloudMaturityModelUMv4-0.pdf

[14] Li K et al. (2015) System for Cross-domain Identity Management: Definitions, Overview, Concepts, and Requirements, Internet Engineering Task Force (IETF), IETF Request for Comments (RFC) 7642. https://doi.org/10.17487/RFC7642

[15] Souppaya MP, Scarfone KA, Morello J (2017) Application Container Security Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-190. https://doi.org/10.6028/NIST.SP.800-190

[16] National Institute of Standards and Technology (2021) *NIST Risk Management Framework*. Available at https://csrc.nist.gov/projects/risk-management/about-rmf

[17] McKay KA, Cooper DA (2019) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-52, Rev. 2. https://doi.org/10.6028/NIST.SP.800-52r2

[18] National Institute of Standards and Technology (2020) Conformance Criteria for NIST SP 800-63A Enrollment and Identity Proofing and NIST SP 800-63B Authentication and Lifecycle Management. https://www.nist.gov/system/files/documents/2020/07/02/800-63B%20Conformance%20Criteria_0620.pdf

[19] National Security Agency (2020) Selecting Secure Multi-factor Authentication Solutions. https://media.defense.gov/2020/Sep/22/2002502665/-1/-1/0/CSI_MULTIFACTOR_AUTHENTICATION_SOLUTIONS_UOO17091520.PDF

[20] Hicock R (2016) *Password Guidance,* Microsoft. Available at https://www.microsoft.com/en-us/research/publication/password-guidance/.

[21] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (2018) *Brute Force Attacks Conducted by Cyber Actors,* Alert TA18-086A. Available at https://www.us-cert.gov/ncas/alerts/TA18-086A

[22] American Council for Technology-Industry Advisory Council (2019) Zero Trust Cybersecurity Current Trends. https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf

[23] FIDO Alliance (2020) *FIDO2: Web Authentication (WebAuthn)*. Available at https://fidoalliance.org/fido2/fido2-web-authentication-webauthn

[24] FIDO Alliance (2020) *FIDO® Certified*. Available at https://fidoalliance.org/certification/fido-certified-products/

[25] FIDO Alliance (2019) Client to Authenticator Protocol (CTAP). https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.pdf

[26] World Wide Web Consortium (2019) Web Authentication: An API for accessing Public Key Credentials, Level 1. https://www.w3.org/TR/2019/REC-webauthn-1-20190304/

[27] National Cybersecurity Center of Excellence (2018) Mobile Application Sign-On: Improving Authentication for Public Safety First Responders. (National Institute of Standards and Technology, Gaithersburg, MD). https://www.nccoe.nist.gov/sites/default/files/library/fact-sheets/psfr-mobile-sso-fact-sheet.pdf

[28] FIDO Alliance (2021) *How FIDO® Works*. Available at https://fidoalliance.org/how-fido-works/

[29] FIDO Alliance (2018) Enterprise Adoption Best Practices: Managing FIDO Credential Lifecycle for Enterprises. https://media.fidoalliance.org/wp-content/uploads/Enterprise_Adoption_Best_Practices_Lifecycle_FIDO_Alliance.pdf

[30] FIDO Alliance (2017) Enterprise Adoption Best Practices: Integrating FIDO & Federation Protocols. https://media.fidoalliance.org/wp-content/uploads/Enterprise_Adoption_Best_Practices_Federation_FIDO_Alliance.pdf

[31] FIDO Alliance (2021) *Functional Certification*. Available at https://fidoalliance.org/certification/functional-certification/

Appendix A—Fast Identity Online (FIDO) Authentication Capabilities

Fast Identity Online, or FIDO, is a set of industry-led authentication specifications with the goal of eliminating passwords from digital transactions. In addition to a passwordless experience, FIDO also supports an MFA use case in which passwords or biometrics are used in conjunction with FIDO authenticators. FIDO specifications are open and written by an alliance of industry participants. This collaborative effort ensures consistent behaviors between online services (verifiers) and clients that implement FIDO specifications.

The FIDO Alliance has increased adoption within industry since its inception with major browser support [23] and a commercial marketplace [24] for authenticators. However, FIDO capabilities among IDaaS providers can vary, which can introduce challenges for IDaaS consumers. This section introduces considerations for a PSO interested in a FIDO authentication solution and contextualizes FIDO in terms of the *Digital Identity Guidelines*.

A.1 What Is FIDO2?

FIDO2 is comprised of two specifications that work together to secure authentication transactions. The specification of greater relevance for IDaaS consumers is *WebAuthn Application Programming Interface (API)* [26], which is published by the World Wide Web Consortium (W3C). The WebAuthn API is used to define the contract, or set of rules, between the verifier and client. While any software program could conform to the WebAuthn API as a client, in the context of this document a client is a web browser. An IDaaS provider implements the set of verifier rules in conformance with the WebAuthN specification with optional constraints that are created by the IDaaS consumer. This is analogous to a custom password policy, such as password length, that an IDaaS consumer might create to align with the *Digital Identity Guidelines*.

> **Note:** The second FIDO2 specification is named Client to Authenticator Protocol (CTAP) [25]. CTAP defines the interface language and the methods of communication between an authenticator and a web browser.
>
> Typically, CTAP only will be relevant to web browser developers and manufacturers of FIDO authenticators, but it is mentioned here to highlight the methods of communication or transport bindings defined by CTAP: USB, Near-Field Communication (NFC), and Bluetooth. USB FIDO authenticators are plugged directly into a client device, while NFC and Bluetooth authenticators do not require direct contact with the client device.
>
> Due to the broad range of working conditions that present unique challenges to PSFRs [27], this document does not recommend a transport binding. However, PSOs should carefully consider their specific use case before adopting FIDO2 as an authentication solution.

FIDO authenticators are something you have: a public-private cryptographic keypair created by the authenticator. In the context of the *Digital Identity Guidelines,* they are considered single-factor cryptographic device authenticators. FIDO2 leverages properties of public key cryptography (not public key infrastructure) by storing the public portion of the key with the IDaaS provider. The corresponding private portion of the key pair is kept secret and is never shared outside the boundary of the FIDO authenticator. In other words, no secret is exchanged between the PSFR and the IDaaS provider. This process is described in the WebAuthN specification as *registration*.

After the public key has been registered, the possessor of the FIDO authenticator can authenticate to the IDaaS provider. In this process, the IDaaS provider sends a random string of data that the FIDO authenticator digitally signs with the private key. The IDaaS provider then uses the registered public key associated with that user to validate the digital signature. Refer to the FIDO Alliance website for a full description of the registration and authentication process [28].

There are two defined categories of FIDO authenticators: roaming and platform.

- *Roaming authenticators* are external to a PSFR's client device (e.g., laptop, mobile device), which allows usage across multiple devices. They are either inserted directly into the device or used through a wireless method in accordance with the CTAP specification.
- *Platform authenticators* are built into the client device and leverage hardware-level protections to store the cryptographic keypair.

Each category presents advantages and challenges for the IDaaS consumer when deploying to a user population. For example, platform authenticators may offer a quicker authentication process than roaming because there is no need to insert the authenticator into a port or hold it near a wireless reader. However, roaming authenticators offer greater flexibility for the user. For example, when the user is deployed in the field without access to their primary workstation, a roaming authenticator is capable of being used with most computing devices.

Unlike passwords, FIDO authenticators are resistant to automated attacks such as credential stuffing because they require a human presence to activate the authentication process. That is, if a human is not in physical possession of the FIDO authenticator, it will not work. Typically, for roaming authenticators, presence is established by the gesture of simply touching the FIDO authenticator. This is described as an *authentication intent* by the *Digital Identity Guidelines* [9].

However, this still leaves FIDO authenticators susceptible to the threat of an attacker or an authorized person using a lost or stolen authenticator. The FIDO2 specifications address this threat by defining a related but distinct concept of *user verification*. Verification distinguishes individual users by requiring something you are or something you know to activate the FIDO authenticator. This optional capability, when enabled by the IDaaS consumer, aligns with the *Digital Identity Guidelines* definition of a multi-factor cryptographic device authenticator.

A.2 FIDO Authentication Use Cases

FIDO is often associated with securing authentication services of individual consumers versus the enterprise use case. This has begun to change with the publication of emerging best practices for the enterprise use of FIDO authenticators. While IDaaS providers are beginning to adopt these best practices, the maturity level among these implementations will vary, thus necessitating careful examination of an IDaaS provider's FIDO capabilities.

The FIDO Alliance has published two documents to assist enterprise FIDO implementers. These documents discuss interrelated considerations beyond registration and authentication events defined in the FIDO specification.

- *Managing FIDO Credential Lifecycle for Enterprises* [29] considers the entire lifecycle of a physical authenticator, including revocation and renewal events. These events are analogous to those described in the *Digital Identity Guidelines* (binding, authenticator compromise, expiration, and revocation) [9].

- *Integrating FIDO & Federation Protocols* [30] discusses best practices for using FIDO together with federation protocols that an organization may already use with other types of authenticators.

While federation is outside the scope this document, PSOs should use the FIDO Alliance best-practice publications to define IDaaS provider FIDO requirements that will assist in evaluating capabilities among providers.

A.3 FIDO Authenticator AAL Considerations

The FIDO mission is to completely replace the password as the primary authenticator; however, not all IDaaS providers support this use case. Some IDaaS providers may support FIDO authenticators only as a secondary factor in combination with a password. The distinction in these use cases affects the AAL and the user experience during an authentication transaction.

Consider an authentication transaction targeted at AAL1 where any authenticator defined in the *Digital Identity Guidelines* is acceptable. A FIDO passwordless experience is possible in this scenario if the authenticator is considered a single-factor cryptographic device and the IDaaS provider meets *Digital Identity Guidelines* verifier requirements [9].

However, a passwordless FIDO experience targeted at AAL2 would require a *multi-factor cryptographic device*—a FIDO authenticator that is capable of user verification via biometrics or a memorized secret. Given the specificity of the FIDO authenticator required for this scenario, a conventional enterprise deployment model is recommended where the FIDO authenticator is pre-loaded with credentials and distributed to the user population via a secure mechanism. This ensures that the correct FIDO authenticator is bound to the correct user. However, the IDaaS provider would need to support this specific deployment model.

Alternatively, an AAL2-targeted authentication transaction can be satisfied with the combination of a password and a FIDO authenticator. In this flow, the user is typically prompted for a username and password as the primary authenticator. If successful, the user is then prompted to authenticate with a FIDO authenticator that has previously been registered. While this flow inherits the challenges of password management for the PSO, it may be the only option that is natively supported by the IDaaS provider.

> **Caution:** At this writing, a targeted authentication transaction fully aligned with AAL3 would present challenges for the implementer. AAL3 introduces the concepts of *verifier compromise resistance* and *verifier impersonation resistance*.
>
> As previously discussed, FIDO2 relies on public key cryptography, which removes the need to share secrets between the IDaaS provider and the FIDO authenticator in alignment with verifier compromise resistance requirements. However, verifier impersonation resistance requires specific protocol protections against phishing attacks.
>
> While FIDO2 does have inherent protections against phishing attacks, aligning with verifier impersonation resistance requirements requires security capabilities that have not been adopted by any commonly used web browsers.

A.4 FIDO Summary and Recommendations

FIDO2 is an emerging set of authentication capabilities with broad industry support that can be utilized by PSOs. It reduces the amount of authentication time and failed attempts for PSFRs by eliminating complex passwords when FIDO authenticators are used in conjunction with biometrics. Also, FIDO2 enables authenticator flexibility for specific PSFR contexts. Some PSOs may prefer to use FIDO2 as the primary authenticator for a passwordless workflow, while others may determine that using FIDO2 authenticators works best to enable MFA in conjunction with a password. IDaaS providers can assist in enabling these capabilities in alignment with the *Digital Identity Guidelines*.

PSOs considering FIDO authentication through an IDaaS provider should first examine the provider's FIDO Alliance certification status. The FIDO Alliance has created a functional certification program to ensure interoperability between the products and services that support FIDO specifications [31]. For PSOs, choosing an IDaaS provider that has not been certified by the FIDO Alliance could potentially introduce risks due to an incorrect implementation of the FIDO Alliance server specifications.

Note that the FIDO Alliance allows for derivative server certifications for services such as the IDaaS providers. A derivative certification relies upon existing certified implementations for conformance with FIDO specifications [31]. With this in mind, it is possible that an IDaaS provider leverages a certified server implementation but chooses not to publicize this fact. Therefore, PSOs should inquire about an IDaaS provider's certification status or other attestation to conformance with the FIDO Alliance server test suite.

Appendix B—Acronyms and Abbreviations

AAL	Authenticator Assurance Level
API	Application Programming Interface
CI/CD	Continuous Integration/Continuous Deployment
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
CSP	Credential Service Provider
CTAP	Client to Authenticator Protocol
EMM	Enterprise Mobility Management
FBI	Federal Bureau of Investigation
FIDO	Fast Identity Online
FOIA	Freedom of Information Act
HOTP	Hash-Based Message Authentication Code-Based One-Time Password
ICAM	Identity, Credential, and Access Management
IDaaS	Identity as a Service
IETF	Internet Engineering Task Force
IP	Internet Protocol
IT	Information Technology
ITL	Information Technology Laboratory
MFA	Multifactor Authentication
NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
OTP	One-Time Password
PaaS	Platform as a Service

PAD	Presentation Attack Detection
PIN	Personal Identification Number
PSFR	Public Safety and First Responder
PSO	Public Safety Organization
QR	Quick Response
RFC	Request for Comments
RMF	Risk Management Framework
SaaS	Software as a Service
SCIM	System for Cross-Domain Identity Management
SIM	Subscriber Identity Module
SMS	Short Message Service
SP	Special Publication
TLS	Transport Layer Security
TOTP	Time-Based One-Time Password
USB	Universal Serial Bus
W3C	World Wide Web Consortium