Draft NISTIR 8334

Using Mobile Device Biometrics for Authenticating First Responders

William Fisher
Don Faatz
Mark Russell*
Christopher Brown
Sanjeev Sharma
Sudhi Umarji
Karen Scarfone

** 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.8334-draft

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

Draft NISTIR 8334

Using Mobile Device Biometrics for Authenticating First Responders

William Fisher
Applied Cybersecurity Division
Information Technology Laboratory

Don Faatz
Mark Russell*
Christopher Brown
Sanjeev Sharma
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.8334-draft

June 2021

U.S. Department of Commerce
Gina M. 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 8334
34 pages (June 2021)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8334-draft

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: *June 2, 2021* through *July 19, 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

Many public safety organizations (PSOs) are adopting mobile devices, such as smartphones and tablets, to enable field access to sensitive information for first responders. Most recent mobile devices support one or more forms of biometrics for authenticating users. This report examines how first responders could use mobile device biometrics in authentication and what the unsolved challenges are. 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; biometrics; identity management; mobile devices; public safety organizations (PSOs).

Acknowledgments

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

Audience

This report is intended for personnel at PSOs who make technology decisions and for vendors of biometric authentication technologies for mobile devices. PSO personnel who are involved in technology acquisition may also find portions of this report useful.

Trademark Information

All registered trademarks or other trademarks belong to their respective organizations.

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

Public safety organizations (PSOs) face technology challenges that hinder their ability to accomplish their missions. A report from 2015 [1] explained one of these challenges:

> "In the explosion of technology supporting public mobility and ubiquitous connectivity, law enforcement, justice, and public safety agencies have been left behind: great difficulty still exists in making the connection to the last mile...the police officer, deputy sheriff, firefighter, and paramedic in a vehicle or in the field. These professionals—our colleagues—need immediate access to critical information from the wide variety of systems technology available (particularly portable computers, tablets, and smartphones) to make the best possible decisions and protect themselves and the public. Hand in hand with access challenges is the imperative to ensure robust internal controls on security […]."

To address these challenges, all PSOs need to improve their identity, credential, and access management (ICAM) capabilities. In a 2019 workshop conducted by the National Institute of Standards and Technology (NIST), PSO leaders and subject matter experts defined the following 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.

Many PSOs are adopting mobile devices to provide first responders with immediate access to the sensitive information they need from any location. However, authentication requirements meant to safeguard that information, like entering a complex password or retrieving a cryptographic token and reading a one-time password from it, can hinder access. Any delay—even seconds—could exacerbate an emergency.

Biometrics can help identify individuals based on their physical characteristics. Biometric capabilities for fingerprint and face scanning have become ubiquitous on commercial smartphones and tablets. Using biometrics with mobile devices could potentially help make authentication faster and easier, but there are challenges with mobile device biometrics in general and also specifically for first responders.

This report examines the potential use of mobile device biometrics by first responders and discusses the challenges in detail. The goal is to educate PSOs on the topic so that they can make better-informed decisions about first responder authentication.

Table of Contents

Executive Summary iv
1 Introduction 1
1.1 Purpose 1
1.2 Report Structure 1
1.3 Report Conventions 1
2 Biometrics and Biometric Authentication Basics 3
2.1 Authentication Factors 3
2.2 The Role of Biometrics in Authentication 4
2.3 Biometric Matching and Verification Model 4
2.4 Biometric System Components 6
2.4.1 Screen Unlocking 6
2.4.2 Local and Remote Biometric Verification 7
2.4.3 Fast Identity Online (FIDO) Alliance Authenticators 7
2.5 Biometrics and Privacy 8
3 Challenges in Biometric Efficacy 9
3.1 Errors and Metrics 9
3.2 Biometric Unlocking Performance 10
3.3 Public Safety Operational Considerations for Biometrics 11
4 Biometrics Use with Shared Mobile Devices 12
5 The Future of Biometrics 14
5.1 Three-Dimensional Measurements 14
5.2 Wearable Sensors 14
5.3 Behavioral Biometric Quality 15
5.4 Biometric Fusion 15
5.5 Challenges in Biometric System Evaluation 17
References 18

List of Appendices

Appendix A— FIDO Authentication Capabilities 20
A.1 What is FIDO2? 20
A.2 FIDO Authentication Use Cases 21
A.3 FIDO Authenticator AAL Considerations 22

A.4 FIDO Summary and Recommendations 24
Appendix B— Acronyms and Abbreviations 25

List of Figures

Figure 1: Callout Box Formats........ 2
Figure 2: Simplified Biometric Matching Model 5

List of Tables

Table 1: Authentication Factors........ 3
Table 2: Google Standards for Biometric Unlocking of Android Mobile Devices 10
Table 3: Authenticator Assurance Levels........ 23

1 Introduction

On-demand access to public safety data is critical to ensuring that first responders can deliver the needed care and support during an emergency. Many public safety organizations (PSOs) are adopting smartphones and tablets as a way of providing first responders with immediate access to the sensitive information they need from any location. However, authentication requirements meant to safeguard that information, like entering a complex password or retrieving a cryptographic token and reading a one-time password from it, can hinder access. Any delay—even seconds—could exacerbate an emergency.

PSOs are charged with implementing efficient and secure authentication mechanisms to protect access to sensitive information while meeting the demands of their operational environments.

1.1 Purpose

Biometrics can help identify individuals based on their physical characteristics. Biometric capabilities have become ubiquitous on commercial smartphones and tablets, including Apple's fingerprint and face scanning, Samsung's fingerprint, face, and iris scanning, and many others. Using biometrics with mobile devices could potentially help make authentication faster and easier, but there are challenges with mobile device biometrics in general and also specifically for first responders.

This report examines the potential use of mobile device biometrics by first responders and discusses the challenges in detail. The goal is to educate PSOs on the topic so that they can make better-informed decisions about first responder authentication.

1.2 Report Structure

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

- **Section 2** presents the basics of biometrics and biometric authentication based primarily on concepts from the National Institute of Standards and Technology (NIST) Digital Identity Guidelines and the Criminal Justice Information Services (CJIS) Security Policy.
- **Section 3** examines challenges with the accuracy of biometric authentication for mobile devices.
- **Section 4** discusses issues with biometric authentication on shared mobile devices.
- **Section 5** looks at the future of biometrics.
- The **References** section lists all references cited in the report.
- **Appendix A** introduces considerations for organizations that are interested in using Fast Identity Online (FIDO) authentication.
- **Appendix B** lists the acronyms and abbreviations used in the report.

1.3 Report Conventions

This report uses callout boxes to highlight certain types of information, as depicted in Figure 1. Callout boxes may 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 **Definition** box provides the definition of a key term. A **Note** box gives additional general information on a topic. A **Tip** box offers advice that may be beneficial to the reader.

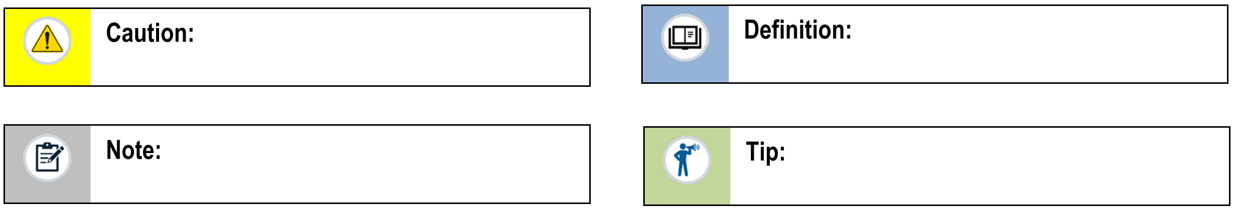

Figure 1: Callout Box Formats

2 Biometrics and Biometric Authentication Basics

This section provides an introduction to biometrics and biometric authentication. Much of the material in this section is based on concepts from the Digital Identity Guidelines [2] and the Criminal Justice Information Services (CJIS) Security Policy [3].

Definition: NIST's Digital Identity Guidelines define biometrics as "automated recognition of individuals based on their biological and behavioral characteristics." [2]

The Digital Identity Guidelines 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, the first responder community and others can also make use of their content. The Digital Identity Guidelines were written to be used as part of a risk-based approach to implementing digital identity services.

Public safety applications dealing with criminal justice information are also governed by the CJIS Security Policy, which provides "appropriate controls to protect the full lifecycle of CJI [criminal justice information], whether at rest or in transit [… and] guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI" [3]. It is based on a variety of best practices, including the Digital Identity Guidelines.

2.1 Authentication Factors

It is important to ensure that only authorized individuals are allowed access to sensitive information. *Authenticating* a user involves verifying evidence of one or more *authentication factors*, as described in Table 1.

Table 1: Authentication Factors

Authentication Factor	Description	Examples
Something you know	A *secret*—non-public information shared between an end user and a digital service.	Password Personal identification number (PIN)
Something you have	A physical device that stores a secret and is possessed by the end user and only the end user.	Cryptographic token
Something you are	A biometric. As Section 2.2 discusses, biometrics are *private*, not secret, so there are limitations on using "something you are" authentication factors.	Fingerprint Facial image Iris pattern

Multi-factor authentication (MFA)—authentication that uses a combination of two or more types of authentication factors—provides stronger authentication than single-factor authentication. Additionally, security policies such as the CJIS Security Policy require MFA for access to sensitive information.

One option for MFA is to require the end user to authenticate themselves with "something you have" that is activated by "something you know," so that the service has proof of possession of the physical device. Unfortunately, this is often difficult for first responders, who would need to memorize secrets and rapidly enter the correct secret during an emergency in order to get access to vital information.

Another option for MFA is to use “something you are” instead of “something you know” to activate “something you have.” For example, a first responder could use a fingerprint biometric instead of a PIN or password to activate a mobile device containing a well-protected, secret cryptographic key.

2.2 The Role of Biometrics in Authentication

Biometrics have been used in a wide range of authentication systems. They are used in both logical access control (controlling access to computer systems and applications) and physical access control (controlling access to physical buildings, facilities, and rooms), either by themselves or with other authentication factors in MFA schemes.

Using biometrics for authentication is often misunderstood. A common misconception is that biometrics are secret. A person’s biometric can be obtained online or by taking a picture of someone with a phone camera (e.g., facial images) with or without their knowledge, lifted from objects someone touches (e.g., latent fingerprints), or captured with high-resolution images (e.g., iris patterns). [4]

NIST has developed a detailed model of digital identity management in the Digital Identity Guidelines [2]. These guidelines address establishing a person’s identity, creating a digital identity for the person to use in online transactions, and authenticating a person’s right to use a particular digital identity.

> **Caution:** Although presentation attack detection (PAD) technologies (e.g., liveness detection) can mitigate the risk of someone using a captured biometric, additional trust in the sensor or biometric processing is required to ensure that PAD is operating in accordance with the needs of the organization.

The Digital Identity Guidelines require that authenticators contain a secret. Some secrets are known to both the person whose digital identity is being verified and the verifier, such as passwords (also referred to as *shared secrets*). Other secrets are only known to the person whose digital identity is being verified (or a client device in that person’s possession), such as a public/private encryption key pair. This limits how a biometric can be used as part of MFA because the biometric does not equate to a secret that is impractical for an attacker to guess or know. 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 used to access a secret cryptographic key stored on a mobile device.

2.3 Biometric Matching and Verification Model

Figure 2 shows the steps of a simplified biometric matching model for verifying a person’s identity. During enrollment, a new user’s biometric data is collected and stored for future use in verifying identity during authentication attempts. The top half of Figure 2 depicts these steps:

1. A biometric *sample* is collected by *capturing* an image (or some other likeness) of the biometric trait (also known as *presenting*) from the new user.
2. The biometric sample is processed into a *feature set* containing the features that are used to characterize the range of similarities and differences between samples.

3. The feature set is converted to a mathematical representation in a compact form called a *template*. The *enrollment template* is a sample that conforms to the quality requirements of the biometric system.
4. The enrollment template is stored as a *reference* for comparisons in future identity claims.

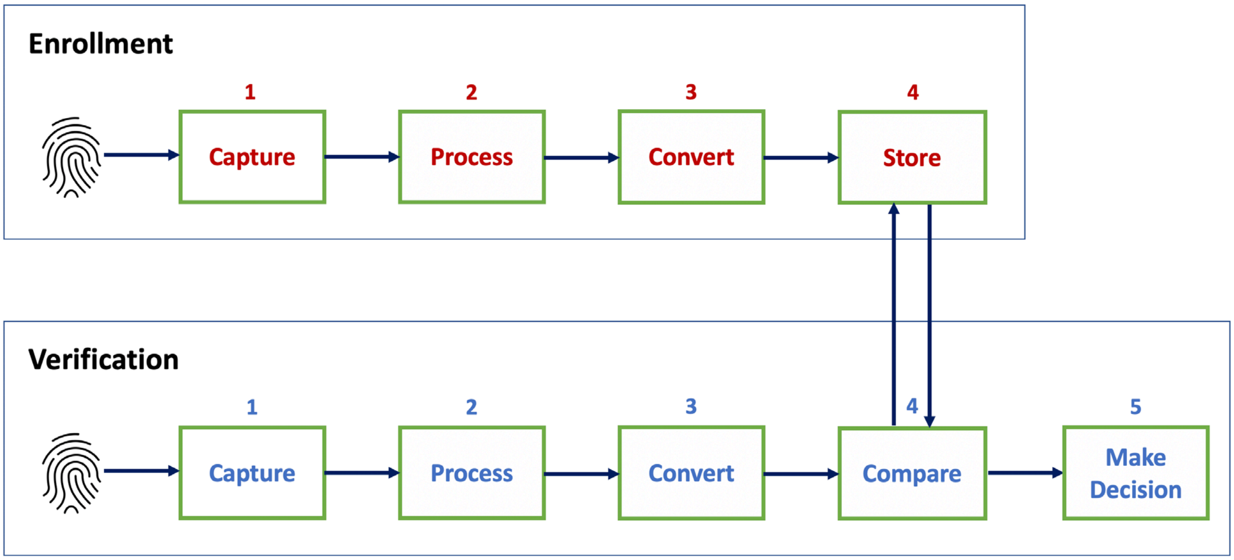

Figure 2: Simplified Biometric Matching Model

The bottom half of Figure 2 depicts the steps for verifying a claimed identity:

1. The user who is claiming the identity of the enrolled person presents a new sample of the previously registered biometric (e.g., fingerprint) to generate an *authentication sample* (also called a *probe*).
2. The authentication sample is processed into a feature set.
3. The feature set is converted into a template.
4. The template is then compared with the enrollment template for the claimed identity by a matching algorithm to generate a *similarity score*.
5. The similarity score is compared to a *threshold score* in order to make a decision about whether the two samples were from the same person and same finger.

> **Tip:** The steps in Figure 2 can also be used to identify an unknown person. The template to be verified could be compared against all the enrollment templates, not just one. However, it is important to note that images used for verification may perform differently when used for identification purposes.

The last two steps—generating a similarity score and comparing it to a threshold score—indicate what makes biometrics significantly different from other authentication factor types.

"Something you know" and "something you have" authentication factors use *deterministic* comparisons to verify identity. That is, when a user provides a password to authenticate, that password must exactly match the stored password against which it is compared. When a cryptographic key is used in an authentication protocol, the key must be exactly the key needed.

When biometrics are used in authentication, a current measurement of a characteristic or trait is compared to stored measurements. The new and stored measurements are not exactly the same, so the comparison of the measurements results in an assessment of the likelihood that they are measurements of the same person. Authentication using biometrics is *probabilistic*, not deterministic. Setting the threshold score correctly for a biometric system is critically important to the system's overall performance. The performance of some biometrics is not uniform across different demographic groups, so it is important to incorporate a representative sample of individuals in testing the performance of a biometric implementation.

> **Note:** Section 4 discusses errors that can affect the accuracy of verification in the biometric matching model.

2.4 Biometric System Components

The biometric matching model is implemented by a biometric system. A typical biometric system has several basic components, including the following:

- A *sensor* collects a sample; examples include fingerprint readers and cameras. Sensors are used for both enrollment and verification.
- An *extractor* converts the sample into a template.
- A *reference database* stores the enrollment templates.
- A *comparator* generates a score by comparing templates to be verified with stored references.
- A *matcher* generates a match result by checking the similarity score to the threshold score.

These components are not necessarily all in one place. Some biometric systems for mobile devices have all components within the mobile devices themselves, while other biometric systems have some components within the mobile devices and some components on remote servers. For example, the comparator could be within a mobile device, allowing comparisons to happen locally. Or it could be on a remote server, so the biometric captured by the local mobile device could be transferred to that server for comparison to stored references.

2.4.1 Screen Unlocking

The primary use case for the biometric capabilities provided by mobile device manufacturers is to enable the user to unlock the screen without entering a PIN or password. This capability is entirely local to the mobile device. The user's biometric templates are stored on the mobile device and typically cannot be exported. Enrollment and verification occur locally on the device and can occur when the device is offline.

> **Caution:** The Digital Identity Guidelines note that unlocking a device through biometric match *cannot* be considered an authentication factor.

Screen unlock does not inherently authenticate the user to any remote system or application, nor does it provide any assertion of the user's identity beyond the fact that the presented biometric matches a previously enrolled template on that specific device. Once unlocked, however, the device may grant the user access to remote systems and applications through stored credentials or active sessions and tokens. Screen unlock is an important security control, but the Digital Identity Guidelines note that unlocking a device through biometric match cannot be considered an authentication factor. It is generally not possible for the verifier to obtain any information on how, or whether, the device was unlocked.

2.4.2 Local and Remote Biometric Verification

The Digital Identity Guidelines advise that biometrics alone do not provide sufficient assurance of user identity, and they must be combined with a "something you have" factor in MFA. The Digital Identity Guidelines describe different types of MFA that could incorporate biometrics, including one-time password (OTP) devices and cryptographic devices in hardware and software forms. These authenticators typically require user verification with a biometric (or memorized secret) in order to activate the authenticator. Once activated, the authenticator performs its cryptographic function (e.g., it generates a one-time password or cryptographically signs an authentication challenge).

> **Caution:** The Digital Identity Guidelines advise that biometrics must be combined with a "something you have" factor in MFA.

When biometrics are used to activate a multi-factor authenticator in this way, the biometric validation is local (either on the user's device or on a hardware authenticator itself). The remote service or application to which the user is authenticating has no direct interaction with the biometric, but because the authenticator is known to require biometric activation, the cryptographic authentication process provides assurance that MFA has been performed.

As an alternative to local verification, the biometric measurement may be sent (typically in an abstracted form) to a remote server for verification. Server-side verification eliminates the need for users to enroll their biometrics on each mobile device, but it requires the aggregation of all users' biometric templates in a server-side database for verification, increasing the risk of a mass compromise of biometric templates. For this reason, the Digital Identity Guidelines states that local verification of biometrics is "preferred" and recommends additional security controls for remote verification. The CJIS Security Policy's Advanced Authentication requirements, on the other hand, only acknowledge authentication factors that are validated on the server side, so multi-factor authenticators that use local biometric activation would not meet these requirements.

Biometric mechanisms built into commercial mobile devices like Apple's Face ID are typically proprietary in design, only support local verification, and include controls to prevent the extraction of biometric data from the device. As a result, they cannot be used in a remote biometric verification scheme. Mobile app developers can still use mobile devices' cameras, and other sensors (but not built-in fingerprint sensors, due to the aforementioned controls) to implement biometrics that could support server-side verification.

2.4.3 Fast Identity Online (FIDO) Alliance Authenticators

The Fast Identity Online (FIDO) Alliance [5] is an industry consortium involving major cloud and web service providers, device vendors, and other members across finance and other industries. The FIDO Alliance has introduced a set of MFA standards. Apple, Google, and Microsoft are FIDO members and have built FIDO authentication functionality into iOS, Android, and Windows devices. Other vendors have produced a wide range of FIDO hardware authenticators that can be used with different client devices.

Tip: Appendix A contains technical information about FIDO authenticators.

FIDO authenticators can provide MFA by requiring verification with a biometric. Biometric verification occurs locally, activating a private key that is then used to sign an authentication challenge. For privacy reasons, the FIDO standards explicitly disallow the extraction of biometric information from the client device, so they cannot support server-side biometric verification. A FIDO authenticator could meet the requirements from NIST Special Publication (SP) 800-63B [6]—part of the Digital Identity Guidelines—for single or multi-factor hardware or software cryptographic authenticators, depending on the characteristics of the specific authenticator.

2.5 Biometrics and Privacy

The collection and use of biometric samples raises privacy concerns. Biometric data is inherently personal, and some types of biometrics can be abused to identify and track individuals. Some biometrics, like facial images, can be acquired at a distance without the subject's cooperation or knowledge. Identifiers like usernames or email addresses can be changed if they are exposed to unauthorized individuals, but biometrics are tied to innate characteristics of the subject and typically cannot be changed. Biometric data constitutes sensitive personally identifiable information (PII), which conveys an obligation to protect it from unauthorized access or disclosure. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), biometric data is also considered protected health information (PHI). The NIST Privacy Framework [7] provides a comprehensive resource for assessing and mitigating privacy risks.

As described in Section 2.4.2, biometric verification may occur locally (on the client device in the user's possession) or remotely. Using fingerprint or face recognition to unlock a mobile device is an example of local verification. On iOS and Android smartphones, biometric capabilities are integrated with the device hardware and use protected storage for biometric templates. These systems are designed to prevent extraction of registered biometric data from the device. Compromising the enrolled biometric data typically requires obtaining the physical device and defeating the software and firmware security mechanisms.

When remote verification is used, biometric templates are typically stored in a central database and the biometric image (or an abstract representation derived from it) is sent over the network. This introduces the risk of biometric data being intercepted in transit; in addition, if the verification database is compromised, this could enable the mass compromise of the biometric data of all individuals enrolled in the system. To mitigate these risks, NIST SP 800-63B [6] requires that biometric data be sent over an authenticated protected channel and that biometric template protections specified in International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 24745 [8] be implemented. ISO/IEC 24745 provides security and privacy requirements and guidelines for the handling of biometric data, including a mechanism for revoking an enrolled biometric.

3 Challenges in Biometric Efficacy

To use biometrics in authentication, reasonable confidence is needed that the biometric system will correctly verify authorized persons and will not verify unauthorized persons. This section describes errors that can affect verification. It also presents information on the biometric systems of mobile devices running Google's Android and Apple's iOS operating systems.

3.1 Errors and Metrics

Each component in a biometrics system introduces an error probability for the overall system:

- A *Failure to Capture (FTC)* occurs when a sensor cannot successfully detect a sample due to some limitation (e.g., bad lighting conditions).
- A *Failure to Extract (FTX*) occurs when the sample's quality is not good enough to generate a valid template.
- A *Failure to Enroll (FTE)* occurs when a template fails the enrollment policy (e.g., the template is not a uniquely distinguishable reference identifier).
- *False Match (FM)* errors occur when the matcher incorrectly decides that a newly collected template matches the stored reference, and *False Non-Match (FNM)* errors occur when it incorrectly decides that a newly collected template does not match the stored reference.

The combination of these errors defines the overall accuracy of the biometric system. Various metrics are used to describe the accuracy of biometric systems:

- The *False Accept Rate (FAR)* is the frequency of false matching. This occurs when an individual's sample is compared with another individual's reference and the comparison score exceeds the threshold, so a match is erroneously made.
- The *False Reject Rate (FRR)* is the frequency of false non-matching. This occurs when an individual's sample is compared with the same individual's reference and the comparison score is lower than the threshold, so a match is erroneously not made.
- The *Spoof Accept Rate (SAR)* is the frequency with which a biometric system accepts a previously recorded known good sample (e.g., a photograph or a recording of someone's voice) for comparison instead of an actual sample [9]. SAR is not an industry standard term, but is used in Google's documentation.

> **Caution:** Sometimes the term *False Match Rate (FMR)* is used instead of FAR, but these terms actually have slightly different meanings and shouldn't be interchanged.
>
> The FMR includes all samples, regardless of image quality issues, while the FAR only includes samples that can successfully be processed into templates.
>
> The same distinction is true for *False Non-Match Rate (FNMR)* and FRR.

Unfortunately, applying these metrics to compare the biometric capabilities of mobile devices is generally not feasible at this time. Manufacturers do not release performance data for any of the components of their biometric systems. The software used in the biometric system is proprietary, so independent evaluation of components such as the matcher are not possible. However, manufacturers do provide some information about the overall performance of their biometric systems.

3.2 Biometric Unlocking Performance

> **Tip:** See https://source.android.com/security/biometric/measure for detailed information on the Android evaluation processes for measuring face, iris, and fingerprint authentication.

Google has documented performance thresholds for biometric unlocking of mobile devices running Android. Android biometric implementations are designated as Class 1, 2, or 3 based on numerous requirements, including meeting the SAR, FAR, and FRR metrics presented in Table 2.[1] The Biometric Pipeline column is an assessment of the impact of an operating system compromise on the security of the biometric data. The pipeline is considered secure if such a compromise does not enable reading biometric data or injecting data that can influence an authentication decision. While Android mobile device manufacturers must test their devices against the requirements and satisfy compatibility requirements as well, they do not have to publish the results.

Table 2: Google Standards for Biometric Unlocking of Android Mobile Devices

Biometric Tier	Metrics			Biometric Pipeline
	SAR	FAR	FRR	
Class 3 (formerly Strong)	0 - 7%	< 0.002%	10%	Secure
Class 2 (formerly Weak) for new devices	7 - 20%	< 0.002%	10%	Secure
Class 2 (formerly Weak) for upgrading devices	7 - 20%	< 0.002%	10%	Insecure/Secure
Class 1 (formerly Convenience) for new devices	> 20%	< 0.002%	10%	Insecure/Secure
Class 1 (formerly Convenience) for upgrading devices	> 20%	< 0.002%	10%	Insecure/Secure

Apple provides some informal information about the performance of their biometric unlock capability on iOS devices. "The probability that a random person in the population could look at your iPhone or iPad Pro and unlock it using Face ID is approximately 1 in 1,000,000 with a single enrolled appearance. The statistical probability is different for twins and siblings that look like you and among children under the age of 13, because their distinct facial features may not have fully developed."[2] Fingerprints are unique, but their distinctiveness decreases if sensors capture only partial image of a finger, which can be the case with mobile devices because smaller sensors are used. According to Apple, "Every fingerprint is unique, so it's rare that even a small section of two separate fingerprints are alike enough to register as a match for Touch ID. The probability of this happening is 1 in 50,000 with a single, enrolled finger."[3]

---

[1] The information in the table is derived from https://source.android.com/security/biometric/measure#strong-weak-unlocks and https://source.android.com/compatibility/android-cdd.pdf.

[2] https://support.apple.com/en-us/HT208108

[3] https://support.apple.com/en-us/HT204587

Apple’s comment on Touch ID also makes clear that while an underlying feature such as a fingerprint may be distinctive, its efficacy has to be evaluated in conjunction with how much of that feature is actually utilized by a device’s biometric system.

Additionally, the efficacy of the overall biometric system in a mobile device can be assessed through laboratory testing. To augment manufacturers’ assertions, one can look to published research reports from testing laboratories. While different labs use different metrics to assess efficacy in biometric systems, the results from a reputable lab, such as a NIST National Voluntary Laboratory Accreditation Program (NVLAP)[4] accredited lab, can be trusted to provide a reasonable assessment of biometric system accuracy for the devices tested.

3.3 Public Safety Operational Considerations for Biometrics

Public safety operating environments frequently include environmental hazards that require public safety users to wear various forms of personal protective equipment (PPE) that may reduce the effectiveness of biometric authentication methods or preclude their use entirely. The latex gloves worn by paramedics and other medical staff typically prevent the use of fingerprints for authentication. Medical masks, face masks worn by firefighters, and other face coverings interfere with the use of facial recognition. PPE requirements for a given public safety user population must be considered when selecting biometric authentication methods. Accumulated dirt or other materials on fingers may also complicate fingerprint image capture.

PSOs adopting biometric authentication should identify and implement backup authentication factors such as memorized secrets that can be used when operational considerations preclude the use of biometrics. Most commercial mobile devices enable users to enter a PIN or password in lieu of using a biometric to unlock the device, for example.

4 https://www.nist.gov/nvlap

4 Biometrics Use with Shared Mobile Devices

There are use cases for first responders where mobile devices may need to be shared by multiple users. Examples of such use cases are:

- an ambulance with a single device shared by multiple emergency medical technicians (EMTs) on board. An EMT may record patient data and then pass the device off to a partner for another task.
- shift workers who check in/check out (CI/CO) a device for their shift
- large-scale events, such as the Super Bowl, where devices are checked out to first responders who may or may not be from the local area but need to use the device for the duration of the event

The challenge in these use cases is ensuring that the data on the device, such as session identifiers (IDs), access tokens, and logins, does not leak between users. Additionally, logs with information regarding each user's actions on the device may be required for auditing purposes.

Consumer mobile devices are primarily *single-user devices*—that is, the device uses a single digital identity and the person using the device authenticates as that digital identity. Google supports multiple users on Android devices, with digital identities that are each individually authenticated and isolated from each other.[6] By default multi-user support is disabled. Device manufacturers can enable it and define how many users are supported. Typically, the maximum number of users is five: one primary user, one guest user, and up to three secondary users. This creates an effective limit of three users because neither the primary user (typically the administrator) nor the guest user (a temporary secondary user) should be included.

> **Note:** Apple has general support for multiple users of iPad tablets. Apple also provides a "Shared iPad" capability for schools,[5] where each account is synced from the cloud and user data may be purged across sessions, but this is not a practical solution for public safety.

Adding multiple users to a mobile device may be constrained by the resources available on the device. Since the typical usage scenario is single-user, devices may not be equipped to handle more than one user. Each defined user profile uses storage on the device and all profiles run simultaneously in the background. This may adversely affect device performance. The details of if or how multi-user support is provided on a given Android device are vendor dependent.

Google's multi-user support provides biometric device unlock for all users. However, since the entire biometric system is implemented on the device, each user must individually enroll their biometric information on the device. Biometrics cannot be provisioned to the device using a mobile device management (MDM) system. This constraint has implications for some of the public-safety multi-user scenarios:

- For a device assigned to an ambulance, the limitation on the number of users supported on a device may make this impractical. If more than three people crew that ambulance

[5] https://developer.apple.com/education/shared-ipad/
[6] https://source.android.com/devices/tech/admin/multi-user

across shifts, a single device would not be able to simultaneously support all of the potential users. It is likely that each mobile device assigned to the ambulance would have to be reset at the start of each shift and set up for that shift's crew, including re-enrollment in each device's biometric system.

- The shiftwork use case is similar to the ambulance use case. If a device can be limited to three distinct users, then a multi-user device shared across shifts could be useful. However, if a device needs to support more than three users, it is likely impractical to share it.
- In the large-scale event use case, devices would need to be reset prior to distribution, and each user would need to individually configure the device they receive, including enrollment in the biometric system.

As it exists today, Android's multi-user functionality is sufficient to support the sharing of devices among small numbers of users with attended enrollment. Google has suggested that multi-user use of devices should only occur with "people you trust." Android also supports *ephemeral user* profiles, temporary user profiles that are added to the device and then deleted when the device is rebooted or switched to a different user profile. An MDM system could dynamically provision an ephemeral user profile along with any required apps and credentials to a shared device to support any number of users, circumventing the limited number of user profiles commonly supported on devices. MDMs have not yet integrated this functionality into their products, and it remains to be seen how they will make use of it.

> **Caution:** This discussion of shared device use on Android is based on using multiple Android user profiles on a device that supports them. Many devices allow a single user to enroll multiple biometrics (e.g., multiple fingerprints), so another option is to allow different users to register their biometrics under a single user profile.
>
> This does accommodate multiple users' biometrics on a shared device, but it doesn't enable mobile apps to determine which user has authenticated with the biometric – only that one of the enrolled users has authenticated. Therefore, this approach should be avoided in any use case where individual accountability and auditing are required.
>
> When multiple Android user profiles are used, as described in this section, each profile has its own set of biometric templates and only the active user's biometric is accepted for screen unlock or authentication.

5 The Future of Biometrics

Biometrics is an area of active research and development, with new and improved capabilities appearing regularly. This section mentions some areas where advances are being made or are still needed.

5.1 Three-Dimensional Measurements

Today's fingerprint sensors work by capturing a two-dimensional measurement of a fingerprint. These sensors are subject to several challenges, such as wet fingers that interfere with the capture. Some commercial vendors have developed ultrasonic sensors that capture three-dimensional measurements of a fingerprint. This includes measurements of fingerprint ridges and valleys, providing additional data that could potentially create a highly accurate model. Further, this technology may be able to accurately measure fingerprints in adverse conditions such as moisture or contamination. It is important to note that these theoretical benefits of ultrasonic fingerprint sensors have not yet been substantiated by research. While not currently implemented, it may be possible to read fingerprints through coverings such as latex gloves.

While the additional data provided by three-dimensional measurement could potentially improve the accuracy and usability of fingerprint biometrics, in at least one instance the introduction of new measurement techniques had unintended consequences. When Samsung introduced a new ultrasonic fingerprint reader on the Galaxy S10 smartphone in October 2019, some users reported that their phones could be unlocked by other (non-enrolled) users' fingerprints. Samsung discovered that with specific types of screen protectors installed on the device, the ultrasonic reader was detecting three-dimensional patterns in the screen protectors as part of the user's fingerprint during enrollment. Since these patterns were present regardless of the actual finger positioned over the reader, they created a high likelihood of false accept errors. Samsung resolved the issue with a software patch and advised all users to delete any enrolled fingerprints and re-enroll [10]. This episode demonstrates why new biometric technologies should generally be regarded with caution.

Similarly, sensors are being developed that can provide three-dimensional measurements of facial features with the promise of more accurate measurements.

5.2 Wearable Sensors

Smartwatches already contain sensors that can measure gait and heart rate. The newest smartwatches have sensors that can capture heart rhythms and oxygen saturation levels. These sensors are intended to provide health monitoring data to aid in detecting medical problems. However, they are biometrics which may be useful for other purposes. For example, suppose a wearable device uses fingerprint recognition to authenticate a person. When a person is authenticated via a fingerprint, the wearable could associate the identity with an electrocardiogram measurement. Through continuous monitoring of the electrocardiogram, the wearable could continuously authenticate the wearer. The combination of the electrocardiogram and the fingerprint scan could provide a form of PAD, making it more difficult for an attacker to use a manufactured fingerprint or other biometric without also spoofing the wearable authentication.

In addition to additional sensor types, wearables connected to a mobile device via Bluetooth or Near Field Communication (NFC) offer the potential for adding a "something you have" factor to the authentication process without creating the burden to carry another device. They offer potential functional benefits as well.

5.3 Behavioral Biometric Quality

Biometric systems can distinguish subjects based on physical (or biological) and behavioral characteristics. Some of the physical modalities include face, fingerprints, iris, vascular/vein pattern, hand geometry, and retina. Behavioral modalities include voice, signature, handwriting, keystroke, and gait dynamics. Many behavioral biometric technologies incorporate machine learning (ML) strategies that use an initial training period to build a model profile of the enrolled user. Once established, the profile can be compared to sensor inputs on an ongoing basis to produce a probability that the currently observed behavior matches the established profile. Because behavioral biometrics generally involve the collection of information over a period of time, they are more commonly used as part of a "continuous authentication" strategy to assess trust throughout a session rather than as an initial authentication method at the beginning of a session. This approach relies on the assumption that measurements taken during the learning phase are reliable (i.e., that they do not include measurements of different individuals). Some behavioral biometrics may be subject to "drift," in which the enrolled user's behavior changes over time, or sudden dramatic changes such as the effects of an injury or surgery on a user's gait.

Behavioral biometrics typically involve proprietary algorithms for interpreting sensor data, building profiles, and ongoing comparison, making it difficult to gauge their effectiveness in a standard, uniform way. NIST is engaged in both foundational and applied research on artificial intelligence (AI) and ML and can provide resources to PSOs interested in learning more about the capabilities, applications, and risks of AI technologies. [11]

From an implementation perspective, physical biometrics can be categorized as more of a science than an art. On the other hand, behavioral biometrics can be seen more as art than science. Less research has been done on the effectiveness of behavioral biometrics, and as discussed above, individual implementations are difficult to compare. PSOs should be skeptical of vendor claims of effectiveness in the absence of formal studies. However, behavioral biometrics are typically deployed alongside conventional authenticators, and they have the potential to augment security by providing additional risk signals. If an unlocked mobile device is stolen from an authorized user, for example, behavioral biometrics could potentially detect this and lock the screen or otherwise prompt for reauthentication with conventional PIN or password credentials.

5.4 Biometric Fusion

Current mobile device biometric systems typically use a single biometric modality. These systems can fail when the environment in which they are used changes. For example, over the last few years, high-end smartphone manufacturers have moved away from fingerprint readers to facial recognition for device unlock capabilities. Facial recognition may be easier to use in some circumstances and does not require the additional hardware of a fingerprint reader. This worked well until the COVID-19 pandemic resulted in users wearing masks that prevent facial recognition.

Another approach is to use *fused biometrics*—collect and use multiple biometrics. Many biometric fusion schemes have been and continue to be developed and tested. The challenge for fused biometrics is learning what traits to fuse, when to fuse the traits, and how to fuse the traits to achieve the best overall results. Fusion can occur in or across any of the components of a biometric system. Biometric measurements also may be fused with signals made available by other sensors on a client device, including behavioral biometrics and other contextual data such as location. For the purposes of this paper, "biometric fusion" refers to this broad concept of fusion in which physical biometrics, behavioral biometrics, and other contextual data or risk signals may be considered in an overall calculation of trust.

Mobile devices typically include a rich array of sensors, including user-facing cameras; cellular, Bluetooth, and Wi-Fi radios; Global Positioning System (GPS) receivers; and accelerometers. Physical and behavioral biometric modalities like face, voice, gait, and dynamics of device interactions (including the angle at which the user holds the device) can be measured using a combination of sensor inputs. In addition to biometrics, contextual attributes can be measured and analyzed. Contextual attributes might include connected devices (including wearables and other Bluetooth devices), available and connected networks (e.g., Wi-Fi), and GPS location. Any combination of these biometric and contextual attributes can be measured, analyzed, and used to build and continually update a composite "trust score" indicating the confidence that the device is being used by the authorized user. As with behavioral biometrics, this ongoing trust evaluation frequently leverages ML and evaluation against a trained model of expected behaviors and inputs.

As discussed in Section 5.3, behavioral biometric implementations tend to be proprietary. Their effectiveness is difficult to analyze and has not been extensively studied, and the further inclusion of contextual attributes has been studied even less. In a 2019 review of available research papers on fused biometrics, NIST concluded that fused biometrics had potential benefits, including making up for disparities in universality, uniqueness, and permanence of different biometric modalities and making presentation attacks more difficult. While many of the papers reviewed claimed increased accuracy when multiple biometrics were fused, most did not provide sufficient evidence to fully evaluate those claims.

While it is difficult to determine their precise accuracy and effectiveness, fused biometrics have potential advantages when used in conjunction with conventional authenticators. The composite trust score generated by fused biometrics could be used to relax authentication requirements for less-sensitive resources—for example, permitting access without requiring MFA when a trust score is high. As with behavioral biometrics, a composite trust score could be used to require additional or step-up authentication when the score is below a certain threshold or trigger a mobile device lock and require a complete reauthentication.

> **Note:** Since biometrics are probabilistic authenticators, even when multiple biometrics are fused, they do not meet the SP 800-63B requirements for Authenticator Assurance Level (AAL) 2. However, biometrics can support AAL2 when used as part of an MFA scheme that includes a physical authenticator that provides a possession factor.

5.5 Challenges in Biometric System Evaluation

It is currently challenging to understand the efficacy of a biometric system. The details of the biometric systems in mobile devices are considered proprietary. The systems themselves are not independently analyzed, and manufacturers do not provide verifiable information on error rates within the systems. While labs can test the mobile devices to get an overall sense of their performance, this black-box testing cannot identify potential weaknesses in components of the system.

For quite some time, the cryptographic community has recognized the value of open cryptographic algorithms that can be assessed in detail, ensuring that the security of a cryptographic algorithm does not depend on the secrecy of the algorithms itself. Additionally, such scrutiny can identify aspects of an algorithm that may expose it to weaknesses introduced through poor implementation. Confidence in mobile device biometric systems would increase if these systems could be independently verified.

742 # References

[1] ICAM National Strategy Summit (2015) Identity, Credential, and Access Management (ICAM): Wireless Mobility in Law Enforcement, Justice, and Public Safety National Strategy Summit. (U.S. Department of Homeland Security, Washington, DC). https://www.cisa.gov/sites/default/files/publications/ICAM_Summit_Report.pdf

[2] 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 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

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

[4] National Institute of Standards and Technology (2020) *NIST Special Publication 800-63: Digital Identity Guidelines Frequently Asked Questions (FAQ)*. Available at https://pages.nist.gov/800-63-FAQ/

[5] FIDO Alliance (2020) FIDO Alliance - Open Authentication Standards More Secure than Passwords. Available at https://fidoalliance.org

[6] Grassi PA, Fenton JL, Newton EM, Perlner RA, Regenscheid AR, 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 2, 2020. https://doi.org/10.6028/NIST.SP.800-63B

[7] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020

[8] International Organization for Standardization/International Electrotechnical Commission (2011) *ISO/IEC 24745:2011 – Information technology – Security techniques – Biometric information protection* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/52946.html

[9] Android Open Source Project (2020) Measuring Biometric Unlock Security. Available at https://source.android.com/security/biometric/measure.

[10] Samsung (2019) Statement on Fingerprint Recognition Issue. Available at https://news.samsung.com/global/statement-on-fingerprint-recognition-issue

[11] National Institute of Standards and Technology (2021) Artificial Intelligence. Available at https://www.nist.gov/artificial-intelligence

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

[13] 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

[14] 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/

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

[16] 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

[17] 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

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

Appendix A—FIDO Authentication Capabilities

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 and a commercial marketplace for authenticators. 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 PSOs is *WebAuthn Application Programming Interface (API)* [14], 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.

> **Note**: The second FIDO2 specification is named Client to Authenticator Protocol (CTAP) [12]. CTAP defines the interface language and the methods of communication between an authenticator and a web browser.
>
> Typically, CTAP will only 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, 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 PSOs [13], this document does not recommend a transport binding. However, PSOs should carefully consider their specific use case before adopting FIDO2 as an authentication solution.

A service that supports FIDO authentication is called a *FIDO relying party*. Any application can be a FIDO relying party, but FIDO is also frequently used in a single sign-on (SSO) architecture where a central Identity Provider (IdP) is the FIDO relying party and brokers individual application sessions using a federation protocol or other SSO technology. In this architecture, the IdP implements the set of verifier rules in conformance with the WebAuthn specification, with optional constraints that are created by the PSO. This is analogous to a custom password policy, such as password length, that an organization might create to align with the Digital Identity Guidelines.

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 relying party. The corresponding private portion of the keypair is kept secret and is never shared outside the boundary of the FIDO authenticator. In other words, no secret is exchanged between the PSO and the relying party. 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 IdP. In this process, the IdP provider sends a random string of data that the FIDO authenticator digitally signs with the private key. The IdP 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 [15].

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

- *Roaming authenticators* are external to a PSO'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 organizations 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 [6].

However, this still leaves FIDO authenticators susceptible to the threat of an attacker or authorized person using a lost or stolen authenticator. The FIDO2 specifications addresses this threat by defining a related, but distinct, concept of user *verification*. Verification distinguishes individual users by requiring *something you have* or *something you know* to activate the FIDO authenticator. This optional capability, when enabled by the IdP, 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 these best practices are beginning to be adopted by IdP software and Identity-as-a-Service (IDaaS) vendors, the maturity level amongst these implementations will vary, thus necessitating careful examination of an IdP'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* [16] considers the entire lifecycle of a physical authenticator, to include revocation and renewal events. These events are analogous to those described in the Digital Identity Guidelines (binding, authenticator compromise, expiration, and revocation).
- *Integrating FIDO & Federation Protocols* [17] discusses best practices for using FIDO together with federation protocols 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 IdP FIDO requirements that will assist in the evaluation of capabilities between multiple providers.

A.3 FIDO Authenticator AAL Considerations

The Digital Identity Guidelines specify an identity risk-based approach for selecting authenticators. It is based on the concept of *authenticator assurance levels (AALs)*, which indicate the relative strength of an authentication process: [2]

- **AAL1** requires single-factor authentication.
- **AAL2** requires two authentication factors (MFA) for additional security.
- **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 authenticator types 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 multi-factor authenticator types, or by using a memorized secret plus one of the five authenticator types specified in the rightmost column. AAL3 can only be achieved two ways: by using a multi-factor 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">Look-Up 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">Multi-Factor 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">Multi-Factor Cryptographic Software</td></tr>
<tr><td colspan="2">Multi-Factor Cryptographic Device</td></tr>
<tr><td rowspan="8">AAL2</td><td colspan="2">Multi-Factor OTP Device</td></tr>
<tr><td colspan="2">Multi-Factor Cryptographic Software</td></tr>
<tr><td colspan="2">Multi-Factor Cryptographic Device</td></tr>
<tr><td rowspan="5">Memorized Secret +</td><td>Look-Up 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">Multi-Factor Cryptographic Device</td></tr>
<tr><td>Memorized Secret +</td><td>Single-Factor Cryptographic Device</td></tr>
</table>

The FIDO mission is to completely replace the password as the primary authenticator; however, not all IdPs support this use case. Some IdPs may only support FIDO authenticators 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 a single-factor cryptographic device and the IdP meets Digital Identity Guidelines verifier requirements [6].

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. The IdP 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 been previously 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 IdP.

A.4 FIDO Summary and Recommendations

FIDO2 is an emerging set of authentication capabilities with broad industry support that can be utilized by PSOs. Within the context of the PSO community, FIDO2 has clear benefits. It reduces the amount of authentication time and failed attempts for first responders by eliminating complex passwords when FIDO authenticators are used in conjunction with biometrics. Also, FIDO2 enables authenticator flexibility for specific PSO 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. IdPs can assist in enabling these capabilities in alignment with the Digital Identity Guidelines.

PSOs considering FIDO authentication through an IdP 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 [18]. For PSOs, choosing an IdP that has not been certified by the FIDO Alliance could potentially introduce risks due to an incorrect implementation of the FIDO Alliance server specifications. The FIDO Alliance also performs biometric component certification using accredited independent labs to certify that biometric subcomponents of FIDO authenticators meet the FIDO Alliance requirements for biometric recognition performance and PAD.

Note that the FIDO Alliance allows for derivative server certifications for services such as IDaaS providers. A derivative certification relies upon existing certified implementations for conformance with FIDO specifications [18]. 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

Selected acronyms and abbreviations used in this paper are defined below.

AAL	Authenticator Assurance Level
AI	Artificial Intelligence
API	Application Programming Interface
CI/CO	Check In/Check Out
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
COVID-19	Coronavirus Disease of 2019
CTAP	Client to Authenticator Protocol
EMT	Emergency Medical Technician
FAQ	Frequently Asked Questions
FAR	False Accept Rate
FBI	Federal Bureau of Investigation
FIDO	Fast Identity Online
FM	False Match
FMR	False Match Rate
FNM	False Non-Match
FNMR	False Non-Match Rate
FOIA	Freedom of Information Act
FRR	False Reject Rate
FTC	Failure to Capture
FTE	Failure to Enroll
FTX	Failure to Extract
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act of 1996
ICAM	Identity, Credential, and Access Management
ID	Identifier
IDaaS	Identity as a Service
IdP	Identity Provider
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
ML	Machine Learning
NFC	Near Field Communication

NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OTP	One-Time Password
PAD	Presentation Attack Detection
PHI	Protected Health Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
PPE	Personal Protective Equipment
PSCR	Public Safety Communications Research
PSO	Public Safety Organization
SAR	Spoof Accept Rate
SP	Special Publication
SSO	Single Sign-On
USB	Universal Serial Bus
W3C	World Wide Web Consortium