Publication Number: **NISTIR 8080**

Title: **Usability and Security Considerations for Public Safety Mobile Authentication**

Publication Date: **7/27/2016**

- Final Publication: http://dx.doi.org/10.6028/NIST.IR.8080 (which links to http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8080.pdf).
- Information on other NIST cybersecurity publications and programs can be found at: http://csrc.nist.gov/

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

The following information was posted with the attached DRAFT document:

Nov. 19, 2015

NIST IR 8080

DRAFT Usability and Security Considerations for Public Safety Mobile Authentication

In cooperation with the Public Safety Communications Research (PSCR) Program, NIST announces the release of NIST Interagency Report (NISTIR) 8080, Usability and Security Considerations for Public Safety Mobile Authentication. There is a need for cybersecurity capabilities and features to protect the Nationwide Public Safety Broadband Network (NPSBN), however, these capabilities should not compromise the ability of first responders to complete their missions. This report describes the constraints presented by the personal protective equipment, specialized gear, unique operating environments, and how such constraints may interact with public safety. The overarching goal of this work is analyzing mobile authentication technologies to explore which may be more appropriate and usable for first responders.

Deadline to submit comments is: **December 28, 2015**.
Email comments or questions to: nistir8080 <at> nist.gov

DRAFT NISTIR 8080

Usability and Security Considerations for Public Safety Mobile Authentication (DRAFT)

Yee-Yin Choong
Joshua M. Franklin
Kristen K. Greene

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

DRAFT NISTIR 8080

Usability and Security Considerations for Public Safety Mobile Authentication (DRAFT)

Yee-Yin Choong
Kristen K. Greene
Information Access Division
Information Technology Laboratory

Joshua M. Franklin
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge.

November 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Interagency Report 8080
40 pages (November 2015)

This publication is available free of charge.

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. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

Public comment period: *November 19, 2015* through *December 28, 2015*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: nistir8080@nist.gov

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

There is a need for cybersecurity capabilities and features to protect the Nationwide Public Safety Broadband Network (NPSBN). However, cybersecurity requirements should not compromise the ability of first responders to complete their missions. In addition, the diversity of public safety disciplines means that one solution may not meet the usability needs of different disciplines. Understanding how public safety users operate in their different environments will allow for usable cybersecurity capabilities and features to be deployed and used. Although first responders work in a variety of disciplines, this report is focused on fire service, emergency medical, and law enforcement. This report describes the constraints presented by the personal protective equipment, specialized gear, and unique operating environments and how such constraints may interact with mobile authentication requirements. The overarching goal of this work is analyzing mobile authentication technologies to explore which may be more appropriate and usable for first responders in a given environment.

Keywords

authentication; identity management; local authentication; public safety; remote authentication; usability; usable security

Acknowledgements

This publication was developed as part of the National Telecommunications and Information Administration / National Institute of Standards and Technology Public Safety Communication Research program with sponsorship from the Office for Interoperability and Compatibility at the Department of Homeland Security. The authors wish to thank their colleagues who reviewed drafts of this report and contributed to its technical content including Paul Grassi, Nelson Hastings, Ray Perlner, Andrew Regenscheid, and Mary Theofanos of NIST. The authors would also like to gratefully acknowledge our public safety subject matter experts for taking the time to share their knowledge and expertise with NIST staff.

Audience

This report is intended to support Nationwide Public Safety Broadband Network (NPSBN) research and implementation of identity management services for mobile devices. A wide audience may find this report of interest, including public safety decision makers, technology developers and implementers, and researchers. It is assumed that readers have some background knowledge in authentication and identity management and are familiar with public safety communications.

Table of Contents

1 Introduction 5
1.1 Purpose and Scope 5
1.2 Structure 6
2 Usability of Authentication for Public Safety 7
2.1 Why Usability Matters for Public Safety 7
2.2 Usability Research Methodology 7
2.3 Qualitative Data from Public Safety SMEs 8
3 Fire Service, EMS, and Law Enforcement 10
3.1 Fire Service 10
3.1.1 Current Authentication Practice 11
3.2 EMS 11
3.2.1 Current Authentication Practice 12
3.3 Law Enforcement 12
3.3.1 Current Authentication Practice 14
4 Authentication Methods Under Review 15
5 Usability and Technical Considerations of Authentication Methods 19
5.1 Knowledge-Based Authentication 19
5.2 Password 20
5.3 PIN 21
5.4 One-Time Password 22
5.5 One-Time Password Device 23
5.6 Gesture 24
5.7 Certificate-Based Authentication 24
5.8 Hardware Cryptographic Token 25
5.9 NFC-Enabled Smartcard with Software Token 26
5.10 Smartcard with External Reader 27
5.11 Proximity Token 28
5.12 Facial Recognition 28
5.13 Fingerprints 29

5.14 Iris Recognition 29
5.15 Keystroke Dynamics 30
5.16 Speaker Recognition 31
5.17 On-Body Detection 31
5.18 Location-Based Authentication 32
6 Discussion and Future Directions 33
6.1 Mobile Authentication Summary 33
6.2 Future Directions 37

List of Appendices

Appendix A— Acronyms 38
Appendix B— References 39

List of Tables

Table 1 - Analysis Summary of Authentication Methods for Fire Service, EMS, and Law Enforcement 36

1 Introduction

In the United States over 10 000 jurisdictions employ public safety personnel to respond to emergency situations every day. These first responders treat life-threatening injuries, keep natural disasters at bay, fight crime, and combat terrorism. To perform these duties, emergency responders must undergo unique training, utilize specialized equipment, and access a variety of information systems. The use of specialized tools, information systems, and protective equipment places first responders within a unique environment to perform their jobs.

Identifying methods to facilitate first responders' operations within their specialized environments can shorten response times and allow emergencies to be more effectively managed, hopefully saving more lives in the process. Surely, firefighters must be protected from heat, emergency medical technicians (EMTs) from bloodborne pathogens, and law enforcement from projectiles - but what other factors exist? To fully understand the requirements of public safety, it is necessary to analyze the various types of first responders, their job duties, and how they perform critical tasks, including their use of technologies.

With increasing proliferation of mobile devices and mobile applications, first responders have new mobile technologies to assist them in emergency situations. In the near future, these devices will access the forthcoming Nationwide Public Safety Broadband Network (NPSBN) [1] via long term evolution (LTE) technology, but may not be able to achieve their full potential if it is not understood how first responders will use these devices in the field. For instance, the first step in using a mobile device often involves authenticating to a device, service, or application, which can be quite a challenging task when wearing thick gloves and donning a protective mask. Most commercial off-the-shelf (COTS) mobile devices and applications are not designed with public safety and their unique constraints in mind. Solutions must be devised to ensure that first responders can take full advantage of current and emerging technologies while working under challenging conditions. Although the NPSBN will offer the ability to access new data and mobile applications in the field, it is important to evaluate the impact of mobile authentication on security and usability.

1.1 Purpose and Scope

This NIST Interagency Report (IR) explores mobile device authentication technologies that can be used in the face of constraints presented by the personal protective equipment, specialized gear, and the information systems that first responders must access in the field. The overarching goal of this work is analyzing which authentication solutions are the most appropriate and usable for first responders in a given context. This is an initial exploration of the mobile authentication usability space for public safety, and further research is necessary to validate the analyses presented in this report. Although first responders work in a variety of disciplines, this report is focused on fire service, emergency medical, and law enforcement.

Readers are highly encouraged to first read NISTIR 8014, Considerations for Identity Management in Public Safety Mobile Networks [11]. This document analyzes approaches to identity management for public safety networks in an effort to assist individuals developing technical and policy requirements for public safety. NISTIR 8014 explores many identity and authentication related issues pertaining to public safety. Topics such as authentication factors, local authentication versus remote authentication, and user and device identity are all addressed and act as a foundation for this effort. The topics of privacy and device identification, authentication, and authorization are out of scope.

1.2 Structure

The remainder of this report is organized into the following major sections:

- Section 2, Usability of Authentication for Public Safety: Discusses why usability is critical for public safety, describes the usability research methodology, and explains qualitative data from public safety subject matter experts (SMEs).

- Section 3, Fire Service, EMS, and Law Enforcement: Briefly describes the Fire Service, Emergency Medical Services (EMS), and Law Enforcement, including specialized equipment for each. Discusses the current authentication practices for public safety personnel.

- Section 4, Authentication Methods Under Review: Describes a variety of authentication methods and whether they apply to a local or remote authentication scenario. Authentication methods are grouped into four categories: something you know, something you have, something you are, and other.

- Section 5, Usability and Technical Considerations of Authentication Methods: Discusses the usability and technical considerations of authentication methods under review. In many cases, the considerations are similar across Fire Service, EMS, and Law Enforcement disciplines.

- Section 6, Analysis and Future Directions: Summarizes the analysis of authentication methods for Fire Service, EMS, and Law Enforcement. Rates each method as impractical, challenging, or feasible for public safety. Discusses overarching concepts and identifies directions for future research.

The report also contains appendices with supporting material:

- Appendix A defines selected acronyms and abbreviations used in this report.
- Appendix B contains a list of references used in the development of this report.

2 Usability of Authentication for Public Safety

Although the public safety community acknowledges the need for cybersecurity capabilities and features to protect the Nationwide Public Safety Broadband Network (NPSBN), the cybersecurity requirements should not compromise the ability of first responders to complete their missions. In addition, the diversity of public safety disciplines means that one solution may not meet the needs of different disciplines. Understanding how public safety users operate in their different environments will allow for usable cybersecurity capabilities and features to be deployed and used.

2.1 Why Usability Matters for Public Safety

The human element is a critical yet often overlooked component during technology integration. The field of usability and human factors focuses on all aspects of human interaction. Usability is defined in ISO 9241-11 as the "Extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [2]. It is critical to understand users' primary goals, the characteristics of the users (both physical and cognitive attributes), and the context in which they are operating. Consider this example of a technology-driven solution that fails to consider user requirements: a handheld touchscreen device for situational awareness that does not accommodate users wearing heavy protective gloves working outdoors in sun glare.

User acceptance is critical to the success of emerging technologies and procedures. In order to meet the objectives of NPSBN, it is of utmost importance to understand emergency response practitioners' needs, key characteristics, tasks, and environments. Rather than considering a device or technology in isolation, a holistic approach that includes users in every element of the product development lifecycle is necessary, from initial user requirements to design, development, and testing. Such a holistic usability approach is referred to as user-centered design (UCD).

2.2 Usability Research Methodology

In order to achieve the objectives of UCD, usability research methods must be applied. There are a variety of qualitative and quantitative research methods, each appropriate at different phases of the product development lifecycle. Qualitative research methods include such techniques as contextual inquiry, user needs analysis, user profiling, behavioral observation, task analysis, workflow analysis, interviews, focus groups, and participatory design. Formal usability testing and laboratory experiments are examples of quantitative research methods that often use statistical analyses. Some methods, such as questionnaires and user modeling, can be both qualitative and quantitative.

It is common to begin with qualitative research to understand users' characteristics, needs, tasks, and environments. Qualitative research focuses on the rich and detailed information provided by smaller numbers of users rather than the statistical analyses from larger numbers of users in quantitative research [3]. An in-depth qualitative approach is especially crucial for domains with specialized personnel, such as public safety, given their challenging operating environments and interactions with specialized tools, technologies, and equipment. Given the exploratory nature of this effort to investigate the impacts of public safety mobile authentication, we chose to use a qualitative approach. Three NIST researchers met with six public safety subject matter experts (SMEs) in the areas of fire service, EMS, and law enforcement and gathered background information focused on public safety field operations. The individual semi-structured collegial discussions allowed for flexibility and the ability to follow SMEs' leads during the discussions.

2.3 Qualitative Data from Public Safety SMEs

Usability analyses and considerations in this report are based on background information gathered by NIST researchers from public safety SMEs. The information includes qualitative data about SME background and training; equipment carried in the field, either on their person (such as personal protective equipment, or PPE) or in their vehicle(s); technologies used; current authentication methods; and experience interacting with such equipment, technology, and authentication methods (including likes and dislikes). The remainder of this section is a summary of the qualitative data obtained from public safety SMEs.

Communication is vital for coordinating emergency response operations in the field among various disciplines and across jurisdictions. Currently, such coordination relies heavily on voice communication via land mobile radio (LMR) technology. However, the coordination can be difficult when there are different radio channels per jurisdiction and per discipline some of which may be encrypted. There may not always be one LMR for each first responder. For example, sometimes the buddy system is used, where an LMR is shared between two first responders. In addition, there may be transmission quality issues on shared channels. Coverage and signal penetration can also be a problem in and around certain structures, especially in very rural areas or underground metropolitan transportation tunnels. SMEs indicated that sometimes they used personal smartphones to supplement LMR communications. Unlike smartphones, LMRs are better secured physically (e.g., clipped or tethered) on a first responder's body, decreasing the chances they are going to be lost or stolen. There is a critical feature on LMRs, a panic button that enables first responders to radio instantaneously for assistance. Also, a key point is that LMRs do not require authentication.

In-vehicle computers are the most common in-field systems requiring authentication (e.g., the mobile data terminal (MDT) used in law enforcement vehicles). These in-vehicle computers typically require a user to log on only at the start of a shift. Many first responders carry a personal smartphone that they may use to facilitate their operations (e.g., use a language translation application to better communicate with non-English speaking patients, or a metronome application to assist in cardiopulmonary resuscitation, or CPR, compression rhythm). Therefore, they may also have to authenticate to their personal smartphones. The SMEs in these discussions indicated they had not been provided with an enterprise-owned smartphone (e.g., in a bring your own device scenario, or BYOD).

SMEs indicated that there are numerous public safety office systems that require authentication that are not used in the field, for example, systems for timekeeping, training, and other administrative tasks. SMEs indicated that they were struggling to keep up with their many passwords and accounts for the office systems. The systems often have different password requirements (e.g., rules for minimum length and complexity) and users are forced to change their passwords on different timescales. SMEs across disciplines expressed frustration with the number of passwords they must manage, stating that they often had to seek technical support to reset forgotten passwords.

The background information from SMEs was used to inform our analyses of mobile authentication methods and usability considerations, described in subsequent sections. In contrast to the many station systems requiring authentication, there is little to no authentication required for mobile in-field systems. Any additional in-field authentication requirements will not be well received by users, especially in high-stress situations. Although NPSBN will offer the ability to access new data and mobile applications in the field, it is important to evaluate the impact of additional mobile authentication on security and usability.

When examining authentication and usability for public safety, it is important to note that it is common for members of the fire service, EMS, and law enforcement disciplines to be "cross-trained" in other areas of expertise. For instance, firefighters often receive emergency medical education. Due to such cross-training, the mobile authentication and usability considerations across disciplines may be similar in many cases. Due to potentially extreme operating environments, many of the associated device considerations will be similar across disciplines. For example, devices must be able to operate in extreme environments, such as high heat and moisture.

3 Fire Service, EMS, and Law Enforcement

The following sections briefly describe the three public safety disciplines considered in this report. Much of this information was provided by public safety SMEs. However, this report is not intended to be a review of public safety disciplines. In order to evaluate the impact of new mobile authentication for NPSBN, it is important to first understand current public safety authentication practices. As described in Section 2, information on current authentication practices was provided by public safety SMEs.

3.1 Fire Service

Many fire situations require the coordination of all levels of government, federal, state, local, and tribal levels. For example, at the federal level, the United States Department of Agriculture (USDA) works with Federal Emergency Management Agency (FEMA) to suppress fire situations, which often involves responding to forest and wildfires. Fire stations exist throughout the country, often run at the county or local level with volunteer firefighters sometimes composing the majority of a county level fire service. This is especially true in rural areas. The general responsibilities of the fire service include:

- The prevention and suppression of fires,
- The application of emergency medical treatment as needed, and
- Assisting with search, rescue, and evacuation of structural fires.

Firefighters often carry additional equipment beyond the minimum personal protective equipment (PPE) required by National Fire Protection Association (NFPA) standards [NFPA]. A PPE ensemble usually consists of a coat, pants, boots, helmet, gloves, hood, self-contained breathing apparatus (SCBA), flashlight, and LMR and carrying a bail-out rope system. Additionally, firefighters are often dragging a hose or carrying a thermal imager, hand tools such as an axe and/or Halligan tool, a 6-foot-long pike pole, and/or a power saw, in addition to other items in their pockets. The total weight can be anywhere from 75 to 100 pounds or more of equipment [5]. Figure 1 shows an example of firefighter gear.

Firefighters receive specialized training and must operate in extreme environments that require quick decisions under high stress. Most members of the fire service are cross-trained for medical first aid, since fire fighters may respond to medical emergencies [6].

Figure 1 – Example Firefighter Gear

3.1.1 Current Authentication Practice

The most common and critical form of communication, voice communication via LMR, does not require authentication, as described in Section 2. If there is a mobile data computer in the cab of a fire truck, it may require authentication. In contrast to the limited in-field authentication required currently, there are numerous systems at the fire station that require authentication, for example, incident record systems, systems for logging hours, training systems, and in-house systems for unit deployment. As described in Section 2, SMEs indicated that there are significant challenges managing the many passwords required by different systems.

3.2 EMS

The activities falling under emergency medical services are broad and far ranging, including patient care, food and drug safety, mass fatality management, and guidance on waste disposal. For the purposes of this report, we consider EMS personnel defined as "the individuals who provide pre-hospital emergency medical care and patient transportation" [7].

General responsibilities include:

- Emergency patient care
- Emergency patient transport

First responder medical treatment covers the majority of the EMS profession, but other responsibilities exist, such as those working with decontamination. Depending on the amount of training completed, there are different levels of EMS certification, ranging from EMT basic to EMT paramedic (usually called EMT and Medic, respectively). EMS personnel must often wear protective gloves and masks [7]. Figure 2 shows an example of EMS gear. They must provide first responder medical care while in a moving vehicle, often an ambulance, but could also include helicopters, boats, and airplanes. EMS personnel must operate in high-stress environments that require fast decision-making.

Figure 2 – Example EMS Gear

3.2.1 Current Authentication Practice

The most common and critical form of communication, voice communication via LMR, does not require authentication, as described in Section 2. EMS personnel may have to authenticate to a laptop to fill out patient care reports after treatment. In contrast to the limited in-field authentication required currently, there are numerous systems at the hospital or fire station that require authentication, for example, systems for incident reporting, timekeeping, and training. As described in Section 2, SMEs indicated that there are significant challenges managing the many passwords required by different systems.

3.3 Law Enforcement

Law enforcement is a broad category for various types of public safety practices. Law enforcement officers (LEOs) exercise arrest and apprehension authority delegated by federal, state or local laws. LEOs observe, or respond to, reports of crimes ranging from simple rule violations to felonies, which may include but are not limited to capital crimes, emergency responses, rescue operations, crowd control, traffic control and acts of terrorism.

General responsibilities of law enforcement include:

- Protection of life and property
- Enforcement of laws, policies, and ordinances
- First aid on an ad hoc basis

A variety of roles exist for LEOs, for example patrol officers, riot police, motorcycle patrol, detectives, highway patrol, sheriffs, and mounted policemen. Many of these roles exist at varying levels of government (i.e., federal, state, local, tribal). LEOs face threats from potentially malicious intelligent adversaries on a daily basis. LEOs receive specialized training and must operate in hostile environments requiring quick decision-making under high stress.

LEOs often carry gear weighing between 15 and 40 pounds or more, such as a handgun, extra magazines, two sets of handcuffs, two flashlights, pepper spray, baton, portable radio, and small recorder. These items are generally affixed to a belt or body armor. Figure 3 shows an example of LEO gear. Additional systems and equipment are contained in police vehicles[1], such as a mobile data terminal (MDT), thermal printer, and dashboard camera(s).

[1] For ease of exposition, we use the term “police vehicle,” realizing that there are many types of police transportation, e.g., cruiser, motorcycle, Segway, bicycle, horse.

Figure 3 – Example LEO Gear

3.3.1 Current Authentication Practice

The most common and critical form of communication, voice communication via LMR, does not require authentication, as described in Section 2. LEOs are required to authenticate to their MDT at the beginning of a shift, which will keep them logged in for the duration of their shift. However, in order to access a variety of local and national law enforcement databases from their MDT (e.g., the National Crime Information Center or NCIC system [8]), LEOs must authenticate to each system separately. They may also need to authenticate to locally deployed equipment, such as mobile fingerprinting devices. Once fingerprints are captured from the person of interest, LEOs must then authenticate to a fingerprint database, such as the FBI's Integrated Automated Fingerprint Identification System (IAFIS) [9]. Additionally, LEOs must authenticate to systems at the police station, such as systems for training. As described in Section 2, SMEs indicated that there are significant challenges managing the many passwords required by different systems.

4 Authentication Methods Under Review

This section defines authentication methods under review in this report. These methods are analyzed in Sections 5 and 6 for the public safety disciplines of fire service, EMS, and law enforcement. Although not an exhaustive list, the authentication methods in this section are an expanded set of those presented in NIST Special Publication (SP) 800-63-2 [10] and NISTIR 8014, *Considerations for Identity Management in Public Safety Mobile Networks*, [11]. Topics such as identity management, authentication factors, and user and device identity are all addressed in NISTIR 8014, and act as a foundation for the current effort.

Although discussed in NISTIR 8014, the topics of local and remote authentication are sufficiently important to understand this project's subject matter that we will discuss them within this report. Local authentication occurs when the user is physically at the information system they are attempting to access—a network connection is not required. An example of local authentication is a user inputting a PIN or password into a tablet to unlock the homescreen. Remote authentication occurs when a user is authenticating to an information system over a network. In the context of public safety, an example of remote authentication occurs when a police officer in a vehicle authenticates to a criminal database via the internet or other network. The authentication methods presented within this report can be used for both local and remote authentication, although some are more appropriate for local authentication and others are more suitable for remote authentication.

It is possible that some data and information systems do not require authentication to gain access. Alternatively, there may be situations in which it is critical for public safety to access certain information, and without it a loss of life may occur, necessitating the removal of an authentication requirement.

- **Knowledge-Based Authentication:** Knowledge-based authentication (KBA) uses pre-registered knowledge tokens to perform authentication, which are pre-determined information and/or questions with answers already setup with a system. This type of authentication is sometimes used for identity proofing purposes, but this usage is not within the scope of this project.
- **PIN and Password:** Common examples include a password, Personal Identification Number (PIN), or passcode. NIST SP 800-63 refers to these as memorized secret tokens.
- **Gesture:** A gesture is a pattern drawn on a touchscreen connecting a series of points or shapes. Although gestures are not explicitly included within NIST SP 800-63, they fit within the definition of memorized secret tokens. The gesture authentication mechanisms analyzed within this document do not include the advanced behavioral measurements such as the speed, pressure, and trajectory of gesture entry.

- **One-Time Password Devices**: One-time password (OTP) devices are physical devices used to generate a password with a short lifespan.[2] A common method of using OTPs is to distribute physical pieces of paper containing multiple passwords, which are used in a sequence. The entity performing authentication knows both the passwords and the sequence in which they are to be used. Sub-classifications include *Software-based OTP* (e.g., a mobile application continuously generating new OTPs), and *One-Time Password Device* (e.g., RSA token). OTP devices are commonly deployed alongside memorized secret tokens to result in a multifactor solution.
- **Certificate-Based Authentication**: Certificate-based authentication uses public key cryptography to prove possession of a private key via digital signatures and certificates. Certificates can be used in a number of situations such as browser authentication, Personal Identity Verification (PIV) cards [17] [18] [19], and inter-application authentication (e.g., certificate pinning). Certificates are also commonly used to augment other authentication mechanisms to create multifactor scenarios.
- **Smartcard with External Reader:** Smartcards contain a processor capable of performing complex cryptographic operations and can be used to store credentials (e.g., digital certificates) that can be unlocked via a memorized secret token, such as a PIN. NIST SP 800-63 refers to smartcards used in this manner as multi-factor cryptographic tokens. Smartcard readers are generally too large to be built into mobile devices, which requires the use of an external smartcard reader to access stored credentials. Although integrated smartcard readers are common in the desktop computing environment, they are uncommon for mobile devices, especially smart phones, and are not included within our analysis.
- **Hardware Cryptographic Token:** Hardware security modules are physical devices providing trusted storage and other cryptographic operations such as trusted key storage. Smartcards, Universal Serial Bus (USB), and MicroSD security tokens are all common examples of these tokens, and can contain a processor providing capabilities similar to that of a smartcard. These hardware tokens may be removable, such is the case with the Universal Integrated Circuit Card (UICC), colloquially referred to as a Subscriber Identity Module (SIM) card. SIM cards reside within a mobile device, which can technically be removed from a device with some effort.
- **Near field Communication (NFC) Enabled Smartcard:** This approach achieves multifactor authentication without a bulky external card reader, addressing some usability concerns. Once a smartcard is placed within centimeters of an NFC-enabled device, the mobile device can wirelessly communicate with a smartcard to access its stored credential. The user would need to hold or place the card very near to the mobile device

[2] Referred to as a Look-up Secret Token described within NIST SP 800-63-2.

as they enter the PIN protecting the credentials stored on the smartcard. Protecting software tokens using software-based mechanisms potentially increases the risk that the credential could be stolen – hardware-based storage is preferred to software-based mechanisms for credential storage.

- **Proximity Token:** A proximity token allows a user to access a system based on the closeness of the token to the system a user is trying to access. These tokens may stay connected to a system, and revoke access when they lose connection. Proximity tokens can also be worn on a user's body, a subcategory we refer to as a wearable proximity token. These wearable proximity tokens, possibly using near field communication (NFC), radio-frequency identification (RFID), Bluetooth Low Energy (LE), or other wireless technologies, may be supported by the Universal 2nd Factor (U2F) open authentication standards from the FIDO Alliance. These wearable tokens could be worn as rings, on sleeves, or elsewhere on a user's body or equipment. Wearable tokens could also be combined with a memorized secret token or other software token to create a MF solution.

The following four biometric authentication methods all require initial enrollment(s), where a user's biometrics are taken and stored in the authentication system. These biometric modalities are more commonly used for individual identification. Per NIST SP 800-63 [10], biometrics are not authorized for use as primary authentication tokens for federal use in remote authentication scenarios. This document analyzes authentication approaches in both local and remote scenarios, necessitating the inclusion of authentication scenarios outside of the purview of NIST SP 800-63. For the purposes of public safety, we assume that the following biometric technologies would use sensors that are built into a mobile device, requiring no external sensors or peripherals. Authentication standards such as the Universal Authentication Framework (UAF) address mobile authentication with various types of biometrics.

- **Fingerprints:** Fingerprints are a common biometric used in modern mobile devices over the past several years. Multiple types of fingerprint sensors exist, such as optical, capacitive, and ultrasonic, each with unique ways of assessing characteristics of a biometric sample. In general, fingerprint scanners on mobile devices have a smaller surface area than traditional scanners, affecting resolution, which may impact accuracy.
- **Facial Recognition:** Facial recognition used locally employs a mobile device's camera to take a picture of a user's face and compare it against data of the same user's facial characteristics captured during enrollment/registration. This authentication mechanism is offered natively by some mobile device platforms and the necessary hardware sensors are built into many mobile devices.
- **Iris Recognition:** Iris recognition identifies patterns within an individual's iris, and is not natively offered in many current-generation mobile devices since a COTS video camera is often insufficient to perform iris scans.
- **Speaker Recognition:** Speaker recognition takes a voice sample of a user via the mobile device's microphone to identify and authenticate a user. The required sensors currently

exist within mobile phones, but this may not hold true for all mobile devices such as wearables and certain tablets.

In contrast to traditional methods of authentication mentioned above where authentication is typically performed at the initiation of system usage, new research areas are focusing on methods to authenticate users as they perform tasks on the system. A number of different characteristics can be used to continuously monitor and authenticate a user (e.g., a user's unique typing pattern, mouse usage, cognitive processing time) with this process being referred to as continuous authentication. Continuous authentication systems, also known as active authentication systems, require that users build a profile by interacting with the system they intend to use, and then a user's actions are compared against this known profile at the time of usage. The following are continuous authentication methods that we analyze for public safety.

- **Keystroke Dynamics:** By using the time intervals and pressure of keyboard presses, it is possible to authenticate an individual [20]. Although typically applied to traditional keyboards, it is possible that this could be used on mobile devices.
- **On-Body Detection:** This mechanism keeps a mobile device unlocked when a device's accelerometer is active (i.e., the device is affixed on a moving person), and locked when the accelerometer is inactive (i.e., not detecting movement).
- **Location-Based Authentication:** A user's "location" is used to authenticate an individual, which could be determined via a device's GPS location, IP address, or proximity to a specific wireless network. Depending on how it's deployed, it could be invisible to the user. This could be used as an additional "factor" when combined with other forms of authentication and would likely not be used on its own.

5 Usability and Technical Considerations of Authentication Methods

In the following section, we consider both the usability and technical considerations of a variety of authentication methods. The usability considerations are further divided into memory, physical, and environmental considerations. Several themes emerged when looking across authentication methods: usability issues with memorizing information, with the difficulty of text entry on mobile devices, the necessity of having access to a user's body for biometrics, and the theme of environmental issues that could negatively affect sensitive electronics. Although the analyses are focused on mobile authentication in the field, many of the same memory considerations would apply to systems used at the office.

5.1 Knowledge-Based Authentication

Memory Considerations:

This method relies on users remembering their KBA answers. When KBA uses questions with persistent answers (e.g., mother's maiden name, high school, first car), it is easier for users to recall their correct answers. However, when KBA uses questions about user preferences (e.g., favorite movie, favorite artist), these preferences can change over time. These changing preferences make it more difficult for users to recall their original responses. As the length of time increases between the initial KBA setup and the current authentication attempt, the recall difficulty is magnified.

Physical Considerations:

This method requires users to enter their KBA answers, usually via typing. Typing on mobile devices is significantly more error prone and time consuming than typing on a traditional keyboard for a desktop computer. The smaller the mobile device, the more difficult it is to type. Typing on small onscreen keyboards will not be possible for first responders wearing protective gloves.

Environment Considerations:

Typing while moving (e.g., while riding in a fire truck, ambulance, or police vehicle) will be more difficult than typing while stationary [12]. Although it may be possible to replace typing with voice entry, this will be difficult in noisy environments (e.g., riding in a fire truck, ambulance, or police vehicle with siren on). Additionally, entering KBA answers could be impacted by any environmental conditions that negatively affect sensitivity and functionality of the mobile device. Sun glare when using the device outdoors will negatively affect a user's ability to see and enter KBA answers on the screen.

Technical Considerations:

Before using a KBA authentication system, users will need to enroll themselves into the backend authentication system by providing answers to questions such as "What was the name of your first pet?" Providing the correct responses to these questions will form the basis for authentication. It's possible that users could engage in a more dynamic form of KBA by being asked questions about their history, taken from public and private information sources, for instance "What was your most recent address?" Questions and answers for dynamic KBA systems are not supplied by users during an enrollment process, and are only presented during the authentication process. KBA is often part of an identity proofing process and may not be suitable in the context of mobile authentication for public safety. The process of providing sufficient information (e.g., identity history, credentials, documents) to a Personal Identity Verification Registrar when attempting to establish an identity.

5.2 Password

Memory Considerations:

This method relies on users remembering their passwords. Password recall is becoming more difficult given increasingly stringent requirements for password length and complexity. The more passwords users have to manage, the more memory interference occurs (e.g. forgetting passwords, forgetting which password goes with which system). Password policies usually require regular password changes which places additional memory burden on users, especially when the change cycles differ between systems. For less frequently used passwords, these memory burdens are magnified [13].

Physical Considerations:

This method requires users to enter their passwords via typing. Typing on mobile devices is significantly more error prone and time consuming than typing on a traditional keyboard for a desktop computer. The smaller the mobile device, the more difficult it is to type. This is due to the size of the input device (i.e., a finger) relative to the size of the target (i.e., a single key on the onscreen keyboard) [14].

On mobile devices, it is necessary to switch back and forth between different onscreen keyboards to type numbers and special characters often required in complex passwords. Passwords are usually masked so users cannot see what they have typed. Furthermore, users cannot rely on predictive text algorithms during password entry. Typing on small onscreen keyboards will not be possible for first responders wearing protective gloves.

Environment Considerations:

Typing while moving (e.g., while riding in a fire truck, ambulance, or police vehicle) will be more difficult than typing while stationary [12]. Although it may be possible to replace typing with voice entry, this will be difficult in noisy environments (e.g., riding in a fire truck, ambulance, or police vehicle with siren on). Speaking complex passwords aloud would not be practical. For example, to enter the password “P@$$w0rd!”, a user would have to say “capital p, at sign, dollar sign, dollar sign, w, zero, r, d, exclamation mark.” Speaking longer passphrases (i.e., longer passwords consisting of words) may be more feasible. However, if a password or passphrase is spoken aloud in the company of others, then it would no longer be a secret. Entering passwords could be impacted by any environmental conditions that negatively affect sensitivity and functionality of the mobile device. Sun glare when using the device outdoors will negatively affect a user’s ability to see and enter passwords on the screen.

Technical Considerations:

Passwords can be used for both local and remote authentication and are often considered the default method of authentication for many information systems. Passwords used for remote authentication must be resistant to a variety of network-based attacks, and methods for assessing the strength and use of passwords in remote authentication situations are provided via NIST SP 800-63-2 [10] and discussed in NISTIR 8014 [11]. Unfortunately, the typical administrative problems with password registration, reset, and expiration are all transferred from desktop computing to the mobile form factor, since the device's small form factor and constant internet connection do nothing to allay these issues.

Passwords used for local authentication to a mobile device's lockscreen tend to be generated/managed by a user, and are shorter than passwords generated for remote authentication scenarios, since passwords for local authentication do not have to be resistant to the same set of threats. While there are many ways to measure the security of user generated passwords (e.g., [10] [The Benefits of Understanding Passwords]), the field of computer security lacks a universally agreed upon measurement standard with sufficient evidence to prove the merit of the standard. Using either authentication scenario, this method of authentication is vulnerable to shoulder surfing attacks.

5.3 PIN

Memory Considerations:

This method relies on users remembering their PINs. In comparison to passwords, PINs are generally shorter and less complex and therefore, easier to remember. The more PINs users have to manage, the more memory interference occurs (e.g. forgetting PINs, forgetting which PIN goes with which system). For less frequently used PINs, these memory burdens are magnified.

Physical Considerations:

This method requires users to enter their PINs, usually via typing. Typing on mobile devices is significantly more error prone and time consuming than typing on a traditional keyboard for a desktop computer. The smaller the mobile device, the more difficult it is to type. This is due to the size of the input device (i.e., a finger) relative to the size of the target (i.e., a single key on the onscreen keyboard) [14]. Typing on small onscreen keyboards will not be possible for first responders wearing protective gloves.

Environment Considerations:

Typing while moving (e.g., while riding in a fire truck, ambulance, or police vehicle) will be more difficult than typing while stationary [12]. Although it may be possible to replace typing with voice entry, this will be difficult in noisy environments (e.g., riding in a fire truck, ambulance, or police vehicle with siren on). Additionally, entering PINs could be impacted by any environmental conditions that negatively affect sensitivity and functionality of the mobile device. Sun glare when using the device outdoors will negatively affect a user's ability to see and enter PINs on the screen.

Technical Considerations:

PINs consist solely of numbers, are less complex, and are generated from a smaller character pool, possibly leading to a weaker overall authentication mechanism. Using PINS for local authentication to a mobile device may be easier than using a complex password. PIN setup, reset, and expiration are issues that still exist in the mobile form factor. NIST SP 800-63 recommends a 4 digit randomly generated PIN for use at Level of Assurance 1, and a 6 digit randomly generated PIN for use at Level of Assurance 2 [10]. This method of authentication is vulnerable to shoulder surfing and smudge attacks.

5.4 One-Time Password

Memory Considerations:

This method relies on users remembering to bring their OTP with them (e.g., paper, email containing their assigned OTP). If users are using a mobile application to obtain their OTP, they may need to remember the OTP when switching back and forth between applications.

Physical Considerations:

This method requires users to enter their OTP, usually via typing. Typing on mobile devices is significantly more error prone and time consuming than typing on a traditional keyboard for a desktop computer. The smaller the mobile device, the more difficult it is to type. This is due to the size of the input device (i.e., a finger) relative to the size of the target (i.e., a single key on the onscreen keyboard) [14].

On mobile devices, it is necessary to switch back and forth between different onscreen keyboards to type numbers and special characters often required in complex passwords [16]. Passwords are usually masked so users cannot see what they have typed. Furthermore, users cannot rely on predictive text algorithms during password entry. Typing on small onscreen keyboards will not be possible for first responders wearing protective gloves.

Environment Considerations:

Typing while moving (e.g., while riding in a fire truck, ambulance, or police vehicle) will be more difficult than typing while stationary [12]. Although it may be possible to replace typing with voice entry, this will be difficult in noisy environments (e.g., riding in a fire truck, ambulance, or police vehicle with siren on). Additionally, entering OTPs could be impacted by any environmental conditions that negatively affect sensitivity and functionality of the mobile device. Sun glare when using the device outdoors will negatively affect a user's ability to see and enter OTPs on the screen.

Technical Considerations:

OTP systems require a shared secret with a backend system (that may not be digital) to generate passwords, and also inherit the typical problems with password setup, reset, expiration, and complexity. In general, OTP systems are more commonly used for remote authentication scenarios alongside a device, but could be used for local authentication. This method of authentication is vulnerable to shoulder surfing attacks, alongside theft of the medium containing the list of OTPs (e.g., a piece of paper).

5.5 One-Time Password Device

Memory Considerations:

This method relies on users remembering to bring their OTP device with them.

Physical Considerations:

This method requires users to enter their OTP, usually via typing. Typing on mobile devices is significantly more error prone and time consuming than typing on a traditional keyboard for a desktop computer. The smaller the mobile device, the more difficult it is to type. This is due to the size of the input device (i.e., a finger) relative to the size of the target (i.e., a single key on the onscreen keyboard) [14].

On mobile devices, it is necessary to switch back and forth between different onscreen keyboards to type numbers and special characters often required in complex passwords [16]. Passwords are usually masked so users cannot see what they have typed. Furthermore, users cannot rely on predictive text algorithms during password entry. Typing on small onscreen keyboards will not be possible for first responders wearing protective gloves.

In addition to the demands of typing passwords, having to carry an extra device (i.e., OTP device) may make this a difficult method of authentication, especially since OTP devices are often small and may be easily lost or crushed.

Environment Considerations:

Typing while moving (e.g., while riding in a fire truck, ambulance, or police vehicle) will be more difficult than typing while stationary [12]. Although it may be possible to replace typing with voice entry, this will be difficult in noisy environments (e.g., riding in a fire truck, ambulance, or police vehicle with siren on). Additionally, using an OTP device could be impacted by any environmental conditions that negatively affect sensitivity of the touchscreen or functionality of the OTP device. Depending on the type of screen an OTP device has, when using the device outdoors sun glare may negatively affect a user’s ability to see and enter OTPs on the screen.

Technical Considerations:

OTP devices require a shared secret with a backend system to generate passwords, and also inherit the typical problems with password setup, reset, expiration, and complexity. OTP devices are typically deployed alongside a memorized secret token (e.g., password, PIN) in remote authentication scenarios. Although they have a long battery life, OTP devices will eventually run out of power and may need to be discarded or repaired. This method of authentication is vulnerable to shoulder surfing attacks and theft of the OTP device.

A special case of OTPs is software-based OTP systems. A mobile application could provide a user with an OTP to provide to a remote authentication system. This likely would not be used for local authentication, unless a user had a second device to run the OTP application.

5.6 Gesture

Memory Considerations:

This method relies on users remembering their gestural patterns. More complex gestural patterns are more difficult to remember, especially for less frequently used gestures.

Physical Considerations:

This method requires users to move their finger(s) across the surface of a mobile device to complete their gestural pattern. More complex gestural patterns are more difficult to execute. The smaller the mobile device, the more difficult it is to gesture accurately. Gestural input will not be possible for first responders wearing protective gloves.

Environment Considerations:

This method could be impacted by any environmental conditions that negatively affect sensitivity and functionality of the mobile touchscreen. Sun glare when using the device outdoors will negatively affect a user's ability to see and enter gestures on the screen. Entering a gesture while moving (e.g., while riding in a fire truck, ambulance, or police vehicle) will be more difficult than entering a gesture while stationary.

Technical Considerations:

Gesture based passwords inherit much from traditional passwords, including gesture setup, reset, and expiration. The gesture analogues of strength metrics are not as well researched and understood for gestures. There is an additional complication of "smudge attacks", where cameras operating under specific lighting situations can view the residue left by a user's skin on the screen of the device to infer information about the gesture in order to bypass the lockscreen.

5.7 Certificate-Based Authentication

Note: Certificates are commonly used in MFA situations alongside a PIN or password, and in this situation, would inherit the usability considerations and technical considerations from using the PIN or password, or any other second factor that is implemented.

Memory Considerations:

If certificate-based authentication is set up such that authentication happens automatically, then there may be few if any memory considerations for users. If there is only one certificate to select, again, there would be minimal memory considerations for users. However, if users are required to select from a list of certificates, then this would place memory burdens on users. Since certificates are not set up and named by individual users, certificates do not generally have meaningful and descriptive names. Therefore, users would have to recognize and recall which certificate to use for which authentication task. This task would be impacted by differences in the user interfaces for certificate selection, which vary from device to device and browser to browser.

Since digital certificates can be used for many different activities beyond authentication (e.g., encrypt emails, digitally sign documents), it may be difficult for users to learn and remember which procedures are required for which activities.

Physical Considerations:

If certificate-based authentication happens automatically, then there would be few if any physical considerations for users. However, if users must select from a list of certificates, then this will not be possible for first responders wearing protective gloves. Even without gloves, the physical size of the device may also be a factor. The smaller the mobile device, the more difficult it is to select items from a list. This is due to the size of the input device (i.e., a finger) relative to the size of the target (i.e., a single item on the UI) [14]. In addition to variability in physical surface size, UIs also vary from device to device and browser to browser.

Environment Considerations:

If certificate-based authentication happens automatically, then there would be few environmental considerations for the user. However, if users must interact with an interface to select from a list of certificates while moving (e.g., while riding in a fire truck, ambulance, or police vehicle), then this will be more difficult than doing so while stationary. Although it may be possible to replace touchscreen interaction with voice entry, this will be difficult in noisy environments (e.g., riding in a fire truck, ambulance, or police vehicle with siren on). When using the device outdoors sun glare may negatively affect a user's ability to see and select a certificate.

Technical Considerations:

There are a number of ways in which certificate-based authentication can be implemented on mobile devices. Certificate-based authentication may be best suited for remote authentication, instead of local authentication to a mobile device's lockscreen. Digital certificates must be part of a PKI, and the certificate model used on the public internet could be used, but a private PKI system could also be constructed. Reuse of the federal PKI is a possible avenue to pursue for certificate-based authentication.

5.8 Hardware Cryptographic Token

Memory Considerations:

There are different memory considerations depending on whether the hardware cryptographic token is integrated (e.g., a SIM card) or removable (e.g., a USB or MicroSD security token). If it is a removable token, a user must remember to bring the token. If it is integrated, a user does not have to remember to bring a token. In both cases, a user must generally remember and enter a PIN with the token. The more PINs users have to manage, the more memory interference occurs (e.g. forgetting PINs, forgetting which PIN goes with which system). For less frequently used PINs, these memory burdens are magnified.

Physical Considerations:

This method requires users to enter their PINs, usually via typing. Typing on mobile devices is significantly more error prone and time consuming than typing on a traditional keyboard for a desktop computer. The smaller the mobile device, the more difficult it is to type. This is due to the size of the input device (i.e., a finger) relative to the size of the target (i.e., a single key on the onscreen keyboard) [14]. Typing on small onscreen keyboards will not be possible for first responders wearing protective gloves.

Environment Considerations:

First responders would have no environment-related requirements prohibiting them from storing credentials in hardware tokens *per se*, but the use of a PIN or other credential to access the credential would be problematic for gloved use. Typing while moving (e.g., while riding in a fire truck, ambulance, or police vehicle) will be more difficult than typing while stationary [12]. Although it may be possible to replace typing with voice entry, this will be difficult in noisy environments (e.g., riding in a fire truck, ambulance, or police vehicle with siren on). Additionally, entering PINs could be impacted by any environmental conditions that negatively affect sensitivity and functionality of the mobile device. Sun glare when using the device outdoors will negatively affect a user's ability to see and enter PINs on the screen.

Technical Considerations:

In order to leverage hardware cryptographic capabilities, a device must have these hardware cryptographic modules and functionality built into it. Therefore, devices must be purchased with these capabilities, and cannot be added on after the fact. PINs are often required to access credentials stored in a hardware cryptographic module. PINs consist solely of numbers, are less complex, and are generated from a smaller character pool, possibly leading to a weaker overall authentication mechanism. For memorized secret tokens, NIST SP 800-63 recommends a 4 digit randomly generated PIN for use at Level of Assurance 1, and a 6 digit randomly generated PIN for use at Level of Assurance 2 [10]. NIST 800-157 recommends a 6-character password as a minimum to protect a derived PIV credential [17]. Using PINs for local authentication to a mobile device may be easier than using a complex password. PIN setup, reset, and expiration are issues that still exist in the mobile form factor.

5.9 NFC-Enabled Smartcard with Software Token

Memory Considerations:

This method relies on users remembering to bring their smartcard with them and have the NFC interface turned on and properly configured. Because users must enter their PIN to unlock the credentials stored on the smartcard, this method relies on users remembering their PINs. The more PINs users have to manage, the more memory interference occurs (e.g. forgetting PINs, forgetting which PIN goes with which system). For less frequently used PINs, these memory burdens are magnified.

Physical Considerations:

Users must be able to raise their NFC-enabled smartcard to their mobile device to enable the transfer of the credential from the smartcard to the device. This method requires users to enter their PINs, usually via typing. Typing on mobile devices is significantly more error prone and time consuming than typing on a traditional keyboard for a desktop computer. The smaller the mobile device, the more difficult it is to type. This is due to the size of the input device (i.e., a finger) relative to the size of the target (i.e., a single key on the onscreen keyboard) [14]. Typing on small onscreen keyboards will not be possible for first responders wearing protective gloves.

Environment Considerations:

Typing while moving (e.g., while riding in a fire truck, ambulance, or police vehicle) will be more difficult than typing while stationary [12]. Although it may be possible to replace typing with voice entry, this will be difficult in noisy environments (e.g., riding in a fire truck, ambulance, or police vehicle with siren on). Any environmental conditions that negatively affect sensitivity and functionality of the mobile device or physical NFC card could impact this authentication method. Sun glare when using the device outdoors will negatively affect a user's ability to see and enter PINs on the screen.

Technical Considerations:

An example of an NFC-enabled smartcard is the PIV card distributed to every US federal employee containing multiple credentials [18]. The PIV series of standards is widely promulgated and are actively maintained. PIV cards are generally not distributed to state and local governmental entities although a separate effort known as PIV-I is working to define a mechanisms to do so [19].

5.10 Smartcard with External Reader

Memory Considerations:

This method relies on users remembering to bring their smartcard and external reader with them. Because users must enter their PIN protecting the credentials stored on the smartcard, this method relies on users remembering their PINs. The more PINs users have to manage, the more memory interference occurs (e.g. forgetting PINs, forgetting which PIN goes with which system). For less frequently used PINs, these memory burdens are magnified. Additionally, after using the smart card, a user must remember to remove their card from the reader.

Physical Considerations:

This method requires users to enter their PINs, usually via typing. Typing on mobile devices is significantly more error prone and time consuming than typing on a traditional keyboard for a desktop computer. The smaller the mobile device, the more difficult it is to type. This is due to the size of the input device (i.e., a finger) relative to the size of the target (i.e., a single key on the onscreen keyboard) [14]. Typing on small onscreen keyboards will not be possible for first responders wearing protective gloves. A typical usage scenario would also require two hands; one to hold and swipe or insert the smartcard and another to hold the mobile device steady. The size of the card reader is also a consideration, as they may be bulky.

Environment Considerations:

Typing while moving (e.g., while riding in a fire truck, ambulance, or police vehicle) will be more difficult than typing while stationary [12]. Although it may be possible to replace typing with voice entry, this will be difficult in noisy environments (e.g., riding in a fire truck, ambulance, or police vehicle with siren on). Additionally, entering PINs could be impacted by any environmental conditions that negatively affect sensitivity of the touchscreen or functionality of the smartcard reader. Sun glare when using the device outdoors will negatively affect a user's ability to see and enter PINs on the screen.

Technical Considerations:

While external smartcard readers can enable strong MF authentication, there are drawbacks that must be considered and mitigated, e.g., the bulkiness of the readers, before they are deployed for public safety. External card readers that correctly interoperate with large swaths of mobile devices would need to be tested to ensure they function correctly before they are purchased, and then they must be distributed. These readers would also use a small amount of power, and could either pull energy from the mobile device via a communications port (e.g., micro-USB), or be externally powered by an onboard or rechargeable battery.

5.11 Proximity Token

Memory Considerations:

This method relies on users remembering to bring and properly affix their wearable proximity token. If the proximity token is externally powered, then a user will need to remember to charge the device, or simply obtain a new one if they are disposable.

Physical Considerations:

Depending on the specific token and its placement on a user's body or gear, it could interfere with first responder operations if lost, damaged, or is physically bulky.

Environment Considerations:

This method could be impacted by any environmental conditions that negatively affect functionality of the wearable proximity token, such as electromagnetic radiation.

Technical Considerations:

Proximity tokens, specifically wearable proximity tokens, are not widely deployed, posing a distribution challenge. There are many types of proximity tokens, including rings, bracelets, and watches, etc. These tokens may establish and maintain a connection to mobile device, keeping it unlocked, or may need to be activated by touching an NFC-enabled mobile device to the token. Proximity tokens can use different wireless technology to communicate and run very basic operating systems, or use modern mobile operating systems (e.g., Android, iOS). Current implementations of these devices operate at short to medium ranges, using NFC, WiFi, or Bluetooth, all of which are vulnerable to jamming attacks. The more feature-rich wearables need to be recharged at least every 1 - 2 days, while low-power wearables may last much longer.

5.12 Facial Recognition

Memory Considerations:

Users must remember whether they wore any artifacts, such as glasses, during enrollment because it affects facial recognition accuracy.

Physical Considerations:

This method may be difficult to use if users are in a confined space, since there must often be a certain distance between a user's face and the sensor. This method would not be possible for a user whose face is occluded by protective equipment such as self-contained breathing apparatus (SCBA), protective goggles, or medical masks. Additionally, the time elapsed between the time of facial recognition for authentication and the time of the initial enrollment can affect the recognition accuracy as a user's face changes naturally over time. A user's weight changes (e.g. weight gain or loss) may also be a factor.

Environment Considerations:

Using facial recognition while moving (e.g., while riding in a fire truck, ambulance, or police vehicle) will be more difficult than using it while stationary because a user will have increased difficulty aligning his/her face with the sensor. Facial recognition could be impacted by any environmental conditions that negatively affect sensitivity and functionality of the facial recognition sensor, such as dim lighting conditions. Sun glare may make it difficult for a user to use this authentication mechanism.

Technical Considerations:

Current facial recognition technology would not be viable for a first responder whose face is occluded by protective equipment. Non-masked first responders may be able to use facial recognition for local authentication. In cases where facial recognition does not work, an alternative authentication method would need to be in place and functioning. This technology would not require additional sensors other than what is provided by common smart phones.

5.13 Fingerprints

Memory Considerations:

Users must remember which finger(s) they initially enrolled with.

Physical Considerations:

This method would not work for gloved users. Depending on the finger(s) required, this method would not work for users with missing or temporarily injured fingers. The amount of moisture on the finger(s) affects the sensor's ability for successful capture.

Environment Considerations:

This method could be impacted by any environmental conditions that negatively affect sensitivity and functionality of the fingerprint sensor (e.g., extreme temperatures, dust, moisture).

Technical Considerations:

If a first responder injures his/her enrolled finger(s), an alternative authentication method would need to be in place and functioning. For gloved first responders, this authentication method would be unviable. First responders often perform intense physical tasks with their hands that might degrade their fingerprints, further complicating the use of this technology.

5.14 Iris Recognition

Memory Considerations:

If single iris recognition is implemented, users must remember which iris they initially enrolled with, so first responders may need to enroll the iris of both eyes. Otherwise, there are no identified human memory considerations for iris recognition.

Physical Considerations:

There must often be a certain distance between a user's eyes and the sensor, which may be difficult in extremely confined spaces. This method would not be possible for first responders whose eyes are occluded by protective equipment. Users wearing colored contacts have the potential to affect the iris recognition accuracy.

Environment Considerations:

Using iris recognition while moving (e.g., while riding in a fire truck, ambulance, or police vehicle) will be more difficult than using it while stationary because a user will have increased difficulty aligning his/her eyes with the sensor. Iris recognition could be impacted by any environmental conditions that negatively affect sensitivity and functionality of the mobile device's camera (e.g., dim light, extreme temperatures, dust, moisture).

Technical Considerations:

It's unclear if there's a benefit of using iris recognition over facial recognition, when both technologies are relying upon the same camera built into the mobile device. Additionally, iris recognition is not available on all major mobile operating systems, making a third-party application necessary, using a mobile device's camera to capture an image of the iris. Iris recognition may not work for people who have had eye surgery, or for people with very light-colored irises. In cases where iris recognition does not work, an alternative authentication method would need to be in place and functioning.

5.15 Keystroke Dynamics

Memory Considerations:

There would not be any memory considerations as long as this method does not require users to recall and type specific text.

Physical Considerations:

This method requires users to type. Typing on mobile devices is significantly more error prone and time consuming than typing on a traditional keyboard for a desktop computer. The smaller the mobile device, the more difficult it is to type. This is due to the size of the input device (i.e., a finger) relative to the size of the target (i.e., a single key on the onscreen keyboard) [14]. Typing on small onscreen keyboards will not be possible for first responders wearing protective gloves. In addition, injured hands may alter the "dynamics" as well as which hand (or both) is used.

Environment Considerations:

Typing while moving (e.g., while riding in a fire truck, ambulance, or police vehicle) will be more difficult than typing while stationary [12]. Although it may be possible to replace typing with voice entry, this will be difficult in noisy environments (e.g., riding in a fire truck, ambulance, or police vehicle with siren on). Additionally, keystroke dynamics could be impacted by any environmental conditions that negatively affect sensitivity and functionality of the mobile device (e.g., extreme temperatures, dust, moisture). Sun glare when using the device outdoors will negatively affect a user's ability to see and enter text on the screen.

Technical Considerations:

The viability of this method of authentication on mobile devices is unclear, since this technology is not widely implemented or deployed. An enrollment process would still need to occur and it's unclear what other infrastructure would be necessary. The enrollment must take place on the same mobile device as will be used for authentication since keystroke dynamics on a computer keyboard differ from the way a user types the same text on a mobile touchscreen.

5.16 Speaker Recognition

Memory Considerations:

There would not be any memory considerations as long as this method does not require users recall and speak a specific phrase.

Physical Considerations:

The speaker must be sufficiently close to the microphone for speaker recognition to work. This method would be unviable for a first responder whose mouth is occluded by protective equipment.

Environment Considerations:

This method could be impacted by any environmental conditions that negatively affect sensitivity of the microphone (e.g., extreme temperatures, moisture). This will be difficult in noisy environments, such as when many individuals are speaking loudly at the same time, or when riding in a fire truck, ambulance, or police vehicle with siren on.

Technical Considerations:

Voice processing would need to be performed on the mobile device's hardware making it more suitable for local rather than remote authentication. This method of authentication is not available on all major mobile operating systems, making a third-party application necessary. If a user is unable to speak, or lost their voice, an alternative authentication method must be available.

5.17 On-Body Detection

Memory Considerations:

There would not be any human memory considerations with this method.

Physical Considerations:

The mobile device must be affixed to the user in some manner (e.g., requiring a device holster, pockets). Depending on the specific device and its placement on a user's body, it could interfere with a first responder’s duties in the field.

Environment Considerations:

This method could be impacted by any environmental conditions that negatively affect sensitivity of the device accelerometer (e.g., extreme temperatures, moisture).

Technical Considerations:

This technology is not natively implemented on all major mobile operating systems. Additionally, on-body detection does not identify or authenticate a specific user, instead it prevents anyone from accessing the phone if the phone is not in motion. With this in mind, on-body detection would not be suited as a method of authentication, the capability of using a mobile device’s accelerometer to detect if a first responder is vertical or not is useful in and of itself as it may be an indicator that a first responder is down and needs assistance.

5.18 Location-Based Authentication

Memory Considerations:

There would not be any memory considerations with this method. Since this is only one factor in a multifactor authentication solution, memory considerations for the remaining factor(s) would apply, as described above.

Physical Considerations:

There would not be any physical considerations with this method. Since this is only one factor in a multifactor authentication solution, physical considerations for the remaining factor(s) would apply, as described above.

Environment Considerations:

There would not be any environmental considerations with this method. Since this is only one factor in a multifactor authentication solution, environmental considerations for the remaining factor(s) would apply, as described above.

Technical Considerations:

The technical considerations for any location-based authentication system would be extremely dependent on how location of the device is determined, and there are a multitude of methods of doing this. Common methods include use of the Global Positioning System (GPS), triangulation via cellular base stations, and proximity to known wireless access points (e.g., WiFi) or Bluetooth beacons.

6 Discussion and Future Directions

Smartphones go beyond traditional LMR voice communication and offer access to and storage of richer and more varied data types (e.g., photos, videos). The data will in many cases be sensitive, e.g., personally identifiable information (PII), that must be protected from unauthorized access and disclosure. Protecting such data will require appropriate authentication (more sensitive data may require additional authentication mechanisms) but must not overburden first responders. Similarly to the way in which first responders currently use LMRs without authentication for voice communication, they should not be required to authenticate to voice communication functions on their new mobile devices. Furthermore, core mobile communication capabilities such as texting or video calling should not require authentication.

It is assumed that the mobile devices first responders will use on the future NPSBN—as is the case with their existing LMR devices—will remain under the physical control of first responders for the duration of their shifts. These devices are often affixed to them via a physical tether. Therefore, allowing core communication functions to be accessed without authentication seems reasonable. This is not completely atypical as many modern mobile operating systems allow users to access certain features without first authenticating. Common examples include accessing the camera, performing emergency calls, and viewing notifications from a variety of applications (e.g., texting). With that concept in mind, compensating controls may be necessary to mitigate threats raised by this security configuration, especially accidental device loss or theft. These controls may include auditing and logging which entities access certain resources, and the ability to remotely wipe a portion, or the entire contents, of a mobile device’s storage locations.

If first responders are forced to authenticate even for basic communication, this may negatively affect their willingness to embrace new technology. User acceptance is critical to fully realizing the benefits of any new technology; in order for first responders to accept any of the new functionality offered by smartphones, the core communication functionality that they are accustomed to must remain intact. Since many first responders already carry their personal smartphones with them, any enterprise-issued mobile devices need to work as well as personal devices do. For example, mobile features such as voice calling, texting, and video calling are commonly used for personal communication and therefore must work as users expect on an enterprise-issued mobile device. Shifting from personal to enterprise devices should be a seamless user experience. First responders already carry a significant amount of required equipment; any new device must fit physically with their current equipment ensembles. The discussion and analyses in this section should help begin to identify which authentication methods are more promising for first responders given the current state of COTS technology.

6.1 Mobile Authentication Summary

Mobile authentication should be behind-the-scenes and invisible to the user. User effort during authentication should be minimal. As previously discussed in Sections 5, any authentication method requiring text entry, such as KBA and passwords, will have critical usability issues for fire service, EMS, and law enforcement. Password entry on mobile devices is an especially arduous task. PINs could be slightly better than complex passwords since they require fewer keystrokes and are composed of only numbers, which can mean users do not have to switch back and forth between different onscreen keyboards. However, even PINs will not work for fire service and EMS personnel when they are wearing gloves.

Any authentication method requiring that users recall information, such as KBA or memorized secret tokens (e.g., passwords, PINs, gestures) will have significant memory usability considerations. Memory issues may be exacerbated in stressful situations.

Authentication methods that require a separate physical device (e.g., smartcard, wearable proximity token) place additional burdens on the users, as they must remember to bring the device and have it readily accessible for authentication. If they are used in conjunction with another authentication method (e.g., smartcard with PIN) the usability issues are magnified.

In general, biometric authentication will be difficult for first responders. Fingerprints will only work for users who are not wearing gloves. Face and iris recognition will have significant usability issues for firefighters who are required to wear SCBA in the field. Face and iris recognition may work for EMS or LEOs if they are not wearing masks or protective eyewear. Keystroke dynamics authentication has the same critical usability issues described above for the other text entry methods (e.g., KBA, passwords, PINs). Speaker recognition will be difficult due to the noisy environments in which first responders operate.

There are three authentication methods that are more promising for first responders given the current state of COTS technology because they do not pose critical or significant usability issues. They are certificate-based authentication, on-body detection, and location-based authentication. Depending upon the implementation, these methods should not require additional user interaction to authenticate with the mobile device. For example, certificate-based authentication should be configured such that it does not require a user to select between multiple certificates. As long as it is invisible to the user, location-based authentication alone does not pose critical or significant usability issues. However, since it is often one factor in a multi-factor authentication scenario, the usability of the other factors must be considered. Although certificate-based authentication, on-body detection, and location-based authentication are more promising from a usability perspective, on-body detection and location-based authentication are less promising from a security perspective because they do not uniquely identify an individual unless they are bound via pre-enrollment or registration.

There is one authentication method—wearable proximity token—that is more promising for law enforcement and EMS than for fire. Since wearable proximity tokens are small electronic devices, they may be more difficult to ruggedize and harden to be resistant in fire environments.

In Table 1, authentication methods are rated as impractical, challenging, or feasible from a usability perspective[3]. These analyses are based on existing usability literature and the basic tenets of cognitive science, and were informed by our collegial discussions with SMEs. Testing devices with first responders is essential to validate the usability and technical ratings.

[3] Ratings were made assuming that devices for NPSBN may be similar to touchscreen smartphones. If future devices differ significantly from touchscreen smartphones, then usability and technical considerations must be reassessed.

Impractical: Methods rated as "impractical" have numerous critical usability issues that would need to be overcome before such methods would be feasible for use by first responders.

Challenging: Methods rated as "challenging" have several significant usability issues that would need to be overcome before such methods would be feasible for use by first responders.

Feasible: Methods rated as "feasible" do not have critical or significant usability issues and would likely be more acceptable for use by first responders. In many cases feasibility depends upon the exact implementation of the technology at hand, as discussed in Section 7.1.

In Table 1, the disciplines are denoted by the following symbols:  is used for fire,  is used for EMS, and  is used for law enforcement.

1173 **Table 1 - Analysis Summary of Authentication Methods for Fire Service, EMS, and Law Enforcement**

Authentication Methods	Feasible	Challenging	Impractical
No Authentication[4]			
KBA			
Password			
PIN			
OTP			
OTP Device			
Gesture			
Certificate-Based Authentication			
Hardware Cryptographic Token			
NFC Smartcard with Software token			
Smartcard with External Reader			
Wearable Proximity Token			
Facial Recognition			
Fingerprints			

1174

[4] No authentication is currently *de facto*.

6.2 Future Directions

This report is an initial exploration of the mobile authentication space for first responders. In order to mitigate the usability issues identified, research should be prioritized by focusing on authentication methods rated as “feasible,” then by investigating “challenging” authentication methods. It may be unwise to expend significant resources and efforts on authentication methods rated as “impractical,” since they pose significant or critical usability issues that would be difficult to overcome for public safety. Research with representative users in realistic contexts is necessary to validate the previously described analyses. Using the NPSBN, a realistic context should include appropriate tasks and mobile devices with authentication mechanisms implemented in order to evaluate both usability and security.

In addition to research on authentication methods, research is needed on the associated enterprise policies guiding the implementation and deployment. For example, many office systems force a user to re-authenticate after a period of inactivity (i.e., a timeout). For first responders in the field, the timeout policy would ideally be lifted, such that a single authentication event would suffice for an entire shift, especially since their mobile devices would remain on their person. The number of authentication events required in the field should be minimized, especially due to the high-stress nature of the first responders’ working environment.

For first responders in the field, it is vital to stay in constant communication. Today, voice communication via LMR push-to-talk (PTT) functionality does not require authentication. Therefore, new enterprise-issued mobile devices should not require authentication to make or receive voice calls. Other core mobile communication capabilities such as texting or video calling should not require authentication either. Research with first responders will be necessary to further define core mobile communication functions and critical features that should be exempt from authentication in order to minimize disruptions to first responders’ existing workflows. Some authentication methods would be more arduous and disruptive than others given the constraints of first responder operating environments.

It is important to remember that first responders must interact with many office systems that already require authentication. As indicated in Section 2.3, SMEs are already struggling with managing many passwords, with different password policies and change cycles. Authentication research should take a holistic view of the entire first responder technology landscape. Research conducted for mobile device authentication can help drive change for office system authentication as well.

Appendix A—Acronyms

Selected acronyms and abbreviations used in the guide are defined below.

BYOD	Bring Your Own Device
COTS	Commercial Off-The-Shelf
CPR	Cardiopulmonary Resuscitation
FAR	False Acceptance Rate
FEMA	Federal Emergency Management Agency
FRR	False Rejection Rate
IAFIS	Integrated Automated Fingerprint Identification System
IR	Interagency Report
LE	Low Energy
LEO	Law Enforcement Officer
LMR	Land Mobile Radio
LTE	Long Term Evolution
MF	Multifactor
NCIC	National Crime Information Center
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NPSBN	Nationwide Public Safety Broadband Network
OTP	One-Time Password
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PTT	Push-To-Talk
RFID	Radio-Frequency Identification
SCBA	Self-Contained Breathing Apparatus
SIM	Subscriber Identity Module
SME	Subject Matter Expert
SP	Special Publication
UCD	User-Centered Design
UICC	Universal Integrated Circuit Card
USB	Universal Serial Bus
USDA	United States Department of Agriculture

Appendix B—References

The list below provides references for this publication.

[1] Middle Class Tax Relief and Job Creation Act of 2012, *PUBLIC LAW 112–96*, February 22, 2012. http://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf [accessed 08/28/2015].

[2] International Organization for Standards. ISO 9241-11 Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on Usability, Geneva, Switzerland, (1998).

[3] Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Thousand Oaks, CA: SAGE.

[4] National Fire Protection Association, *Codes & Standards*, 2015. http://www.nfpa.org/codes-and-standards [accessed 08/28/2015].

[5] National Institute of Standards and Technology, *Special Publication (SP) 1191, Research Roadmap for Smart Fire Fighting*, 2015. http://dx.doi.org/10.6028/NIST.SP.1191 [accessed 08/28/2015].

[6] Federal Emergency Management Agency, *Emergency Support Function #4 – Firefighting Annex*, May 2013. http://www.fema.gov/media-library-data/20130726-1913-25045-7514/final_esf_4_firefighting_20130501.pdf[accessed 08/28/2015].

[7] Occupational Safety & Health Administration (OSHA), Best Practices for Protecting EMS Responders, 2009. https://www.osha.gov/Publications/OSHA3370-protecting-EMS-respondersSM.pdf [accessed 08/28/2015].

[8] Federal Bureau of Investigation, *National Crime Information Centerl Justice Information Services (CJIS) Security Policy*, 2015. https://www.fbi.gov/about-us/cjis/ncic [accessed 08/28/2015].

[9] Federal Bureau of Investigation, *Integrated Automated Fingerprint Identification System*, 2015. https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis [accessed 08/28/2015].

[10] National Institute of Standards and Technology, *Special Publication (SP) 800-63-2, Electronic Authentication Guideline*, 2013. http://dx.doi.org/10.6028/NIST.SP.800-63-2 [accessed 08/28/2015].

[11] National Institute of Standards and Technology, *NISTIR 8014, Considerations for Identity Management in Public Safety Mobile Networks*, 2014. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8014.pdf

[12] Nicolau, H., Jorge, J.: Touch typing using thumbs: understanding the effect of mobility and hand posture. In: Proceedings of the SIGCHI Conference on Human Factors in Computing System, pp. 2683-2686 (2012).

[13] National Institute of Standards and Technology Interagency Report NISTIR 7991. Choong, Y., Theofanos, M., Liu, H. K. United States Federal Employees' Password Management Behaviors – a Department of Commerce Case Study. 2014.

[14] Bi, X., Li, Y., Zhai, S.: FFitts Law: Modeling Finger Touch with Fitts' Law. In: Proceedings of the SIGCHI Conference on Human Factors in Computing System, pp. 1363-1372 (2013).

[15] National Institute of Standards and Technology, *NISTIR 7298 Revision 2, Glossary of Key Information Security Terms*, 2013. http://dx.doi.org/10.6028/NIST.IR.7298r2

[16] Greene, K. K., Gallagher, M. A., Stanton, B. C., Lee, P. Y.: I Can't Type That! P@$$w0rd Entry on Mobile Devices. In: Human Aspects of Information, Security, Privacy, and Trust. Lecture

Notes in Computer Science, Vol. 8533, pp 160-171. (2014)

[17] National Institute of Standards and Technology, *Special Publication (SP) 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials*, 2014. http://dx.doi.org/10.6028/NIST.SP.800-157 [accessed 08/28/2015].

[18] National Institute of Standards and Technology, *Federal Information Processing Standard (FIPS) 201-2*, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, 2013. http://dx.doi.org/10.6028/NIST.FIPS.201-2

[19] Federal CIO Council, *Personal Identity Verification Interoperability For Non-Federal Issuers*, July 2010. https://cio.gov/wp-content/uploads/downloads/2012/09/PIV_Interoperabillity_Non-Federal_Issuers_May-2009.pdf [accessed 08/28/15].

[20] Jun Chen, Guang Zhu, Jin Yang, Qingshen Jing, Peng Bai, Weiqing Yang, Xuewei Qi, Yuanjie Su, and Zhong Lin Wang, Personalized Keystroke Dynamics for Self-Powered Human–Machine Interfacing, American Chemical Society (ACS) Nano 2015 9 (1), 105-116. http://pubs.acs.org/doi/abs/10.1021/nn506832w [accessed 08/28/15].

[21] 3rd Generation Partnership Project, *TR 22.803 - Feasibility study for Proximity Services (ProSe)*, 2013. http://www.3gpp.org/DynaReport/22803.htm [accessed 03/20/15].