NISTIR 8080

Usability and Security Considerations for Public Safety Mobile Authentication

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

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8080

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

NISTIR 8080

Usability and Security Considerations for Public Safety Mobile Authentication

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 from:
http://dx.doi.org/10.6028/NIST.IR.8080

July 2016

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
39 pages (July 2016)

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8080

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Applied Cybersecurity 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 and security 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 the Fire Service, Emergency Medical Services (EMS), and Law Enforcement. This report describes the constraints presented by their personal protective equipment (PPE), specialized gear, and unique operating environments and how such constraints may interact with mobile authentication requirements. The overarching goal of this work is analyzing which authentication solutions are the most appropriate and usable for first responders using mobile devices in operational scenarios in the field.

Keywords

identity management; mobile authentication; public safety; 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. All authors contributed equally to this work.

Audience

This report is intended to support 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.

Executive Summary

In the near future, mobile devices used by first responders will access the forthcoming Nationwide Public Safety Broadband Network (NPSBN) [1] via long term evolution (LTE) technology. Although the NPSBN will offer first responders 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. This NIST Interagency Report (IR) explores mobile authentication technologies for public safety networks. The overarching goal of this work is analyzing which authentication solutions are the most appropriate and usable for first responders using mobile devices in operational scenarios in the field. In this document, we focus on smartphones due to their widespread usage. Although first responders work in a variety of disciplines, this report is focused on the Fire Service, Emergency Medical Services (EMS), and Law Enforcement.

In order to meet the objectives of the NPSBN, it is of utmost importance to conduct usability research to understand emergency response practitioners' needs, key characteristics, tasks, and environments. It is common to begin with qualitative research, which focuses on the rich and detailed information provided by smaller numbers of users [4]. Three NIST researchers met with six public safety subject matter experts (SMEs) in the areas of Fire, EMS, and Law Enforcement and gathered background information focused on public safety field operations. The usability analyses in this document are based on existing usability literature and the basic tenets of cognitive science, and were informed by our discussions with SMEs.

In this report, we present both the usability and technical considerations of a variety of mobile authentication methods and technologies, 17 in total.

- Knowledge-Based Authentication
- Password
- PIN
- Gesture
- One-Time Password Device
- Embedded Cryptographic Token
- Removable Hardware Cryptographic Token
- Smartcard with External Reader
- Near Field Communication (NFC) Enabled Smartcard
- Proximity Token
- Fingerprints
- Facial Recognition
- Iris Recognition
- Speaker Recognition
- Keystroke Dynamics
- On-Body Detection
- Location-Based Awareness

The usability considerations are further divided into memory, physical, and environmental considerations. Several themes emerged when looking across authentication methods:

- Challenges with text entry on mobile devices in the field,
- Difficulty memorizing information,
- Necessity of having access to a first responder's body for biometrics,
- Environmental issues that could negatively affect sensitive electronics (e.g., high heat, moisture), and
- Use of new mission-critical communication services should not introduce additional authentication barriers.

We assessed each of the 17 authentication methods from a usability perspective. Feasibility analyses are summarized below:

- Any authentication method requiring text entry, such as knowledge-based authentication (KBA) and passwords, will have critical usability issues.

- Personal Identification Numbers (PINs) may be slightly better than complex passwords since they require fewer keystrokes. However, even PINs will not work for gloved first responders.

- 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.

- For authentication methods that require a separate physical device (e.g., smartcard, wearable proximity token), first responders must remember to bring the device and have it readily accessible for authentication. If the device is used in conjunction with another authentication method (e.g., smartcard with PIN) the usability issues are magnified.

- Biometric authentication may be difficult for first responders in certain situations. 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 Self-Contained Breathing Apparatus (SCBA) in the field. Face and iris recognition may work for first responders from EMS or Law Enforcement if they are not wearing masks or protective eyewear. Speaker recognition will be difficult due to the noisy environments in which first responders operate. Keystroke dynamics authentication has the same critical usability issues described above for the other text entry methods (e.g., KBA, passwords, PINs).

- Our analysis concludes that there are three authentication methods that are currently more promising for first responders because they do not pose critical or significant usability issues. They are embedded cryptographic tokens, on-body detection, and location-based awareness. Depending upon the implementation, these methods should not require additional user interaction to authenticate with the mobile device when it is already unlocked. For example, embedded cryptographic tokens should be configured such that it does not require a user to select between multiple digital certificates. If first responders are sharing devices, it may be necessary for multiple user profiles to be enabled on the same device, to allow the correct certificates to be used for a given responder.

  - Although embedded cryptographic tokens, on-body detection, and location-based awareness are more promising from a usability perspective, on-body detection and location-based awareness are less promising from a security perspective because they do not uniquely identify an individual unless they are bound via pre-enrollment or registration.

  - As long as they are invisible to the user, location-based awareness and on-body detection do not pose critical or significant usability issues. However, since neither are stand-alone authentication methods, they can only be used to support a multifactor authentication (MFA) solution and the usability of the MFA factors must be considered.

- There is one authentication method—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.

Usability issues with authentication methods that were identified as currently not feasible for public safety use in the field may be mitigated with careful planning and implementation. The goal is that authentication should not interrupt actively responding first responders, nor should it overburden them in any stage of response. For example, if authentication can be implemented such that first responders authenticate at the beginning of a shift through Single Sign-on (SSO), and stay authenticated throughout the shift, then many of the authentication methods discussed in this report would then become more feasible. To support such a scenario, other controls, such as remote lock and remote wipe, can be implemented to ensure a lost or stolen first responder device is not compromised.

This report is an initial exploration of the mobile authentication space for first responders. Authentication research should take a holistic view of the entire first responder technology landscape. Current and future public safety authentication technologies should keep in mind the following:

- Mobile authentication should be behind-the-scenes and invisible to the user to the greatest extent possible.
- User effort during authentication should be minimal.
- The number of authentication events required in the field should be minimized, especially due to the high-stress nature of first responders' working environments.

Future research is necessary in the following areas:

- 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.

- Research with first responders will be necessary to further define mission-critical communication services and critical features that should be exempt from authentication

in order to minimize disruptions to first responders' existing workflows. Similarly to the way in which first responders currently use land mobile radios (LMRs) without authentication for voice communication, they should not be required to authenticate in order to use mission-critical communication services on their next-generation mobile devices.

- In order to mitigate the usability issues identified, research should be prioritized by focusing on authentication methods rated as readily feasible, then by investigating other less feasible authentication methods.

- Research is needed on the associated enterprise policies guiding mobile authentication implementation and deployment. For example, research on timeout policies and SSO implementation is necessary. 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 or incident, especially since their mobile devices would remain on their person. SSO will allow first responders to authenticate one time and receive access to multiple applications, systems, and domains within a variety of authentication mechanisms [24].

Table of Contents

List of Appendices

List of Tables

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, deal with the consequences of natural disasters, 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 blood borne pathogens, and law enforcement officers (LEOs) 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 (e.g., smartphones and tablets) and mobile applications, first responders are able to leverage advanced 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 or the capabilities present in these devices. For instance, the first step in using a mobile device often involves authenticating to, or unlocking, 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, authenticators, and applications available to consumers 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 using mobile devices in operational scenarios in the field. In addition to typical mobile devices (e.g., smart phones and tablets), a diverse set of devices may be used in conjunction with the forthcoming NPSBN, including drones, sensors, wearables, and robots. In this document, we focus on smartphones due to their widespread usage. This work 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. The topics of privacy, device identity, device authentication, device authorization, and risk management are out of scope. Although first responders work in a variety of disciplines, this report is focused on Fire, Emergency Medical Services (EMS), and Law Enforcement.

Readers are highly encouraged to first read NISTIR 8014, *Considerations for Identity Management in Public Safety Mobile Networks* [2]. NISTIR 8014 analyzes approaches to identity management for public safety networks in an effort to assist individuals developing technical and policy requirements for public safety.

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 Fire, 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 under review within this analysis.
- 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, EMS, and Law Enforcement disciplines.
- Section 6, Discussion and Future Directions: Summarizes the analysis of authentication methods for Fire, EMS, and Law Enforcement. Rates each method as impractical, challenging, or feasible for public safety. Discusses overarching concepts, potential mitigations, and identifies directions for future research.

The report also contains appendices with supporting material:

- Appendix A defines 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 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 unique 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" [3]. 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.

In the context of public safety, poor usability of mission-critical technology can equal loss of lives. User acceptance is critical to the success of emerging technologies and procedures. In order to meet the objectives of the 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 [4] rather than the statistical analyses from larger numbers of users in quantitative research. 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, 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, technologies, 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. It is necessary to understand what users expect from an LMR perspective in order to support user expectations moving forward with next generation LTE devices. LMR 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 our discussions indicated they had not been provided with an enterprise-owned smartphone and had been using their personal smartphones in the field (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 schedules. 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 the 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 Fire, 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 the 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 the 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 fires.

Firefighters often carry additional equipment beyond the minimum PPE required by National Fire Protection Association (NFPA) standards [5]. 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 (1.8 m) pike pole, and/or a power saw, in addition to other items in their pockets. The total weight can be anywhere from approximately 34 kg to 45 kg (75 lbs. to 100 lbs.) or more of equipment [6]. 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 firefighters may respond to medical emergencies [7].

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" [8].

General responsibilities include:

- Emergency patient care, and
- 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 [8]. 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 respond to 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; and
- 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 approximately 7 kg to 18 kg (15 lbs. to 40 lbs.) 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).

Figure 3 – Example LEO Gear

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

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 [9]), 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 biometric database, such as the FBI's Next Generation Identification (NGI) system [10]. 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, 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 [11] and NISTIR 8014, *Considerations for Identity Management in Public Safety Mobile Networks*, [2]. 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 [2], the topics of local and remote authentication are sufficiently important to understand subject matter that is discussed 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 device. 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.

It is possible that some data and information systems do not require authentication to gain access. In addition, 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. In addition, this method is widely considered a weak form of authentication and is therefore not recommended.

- **Password and PIN:** NIST SP 800-63-2 [11] refers to these as memorized secret tokens. PINs are typically numeric and often system generated while passwords could allow a range of alphanumeric characters, special characters, lengths, to include spaces to support pass phrases.

- **Gesture:** A gesture is a pattern drawn on a touchscreen connecting a series of points or shapes. Although gestures are not explicitly reference within NIST SP 800-63-2 [11], they fit within the definition of memorized secret tokens. The gesture authentication mechanisms analyzed within this document do not include the more advanced behavioral measurements such as the speed, pressure, and trajectory of gesture entry.

- **One-Time Password Device**: One-time password (OTP) devices are physical devices used to generate a password with a short lifespan. Typically, OTP's are used in conjunction with a memorized secret token, like a password. Proof of possession of the device by presenting a valid OTP (what you have) and the password (what you know)

results in a multifactor solution. OTP devices are often key fobs that present passwords via a small electronic display, and these passwords change after some pre-specified period of time (e.g., one minute). The backend entity performing authentication also knows this password. A sub-classification for OTP devices is a *software-based OTP* (e.g., a mobile application continuously generating new OTPs).

- **Embedded Cryptographic Token**: Embedded cryptographic tokens are hardware and/or software components that contain a cryptographic key used to authenticate a user (or a device). Authentication is accomplished by using a cryptographic protocol to prove possession of that key. For the purposes of this document, this token is embedded in a mobile device, for example, as a specialized chip embedded in the phone, or as a software component running as part of the operating system (OS), or as a 3rd-party utility. While symmetric cryptography may be used, in most cases, cryptographic tokens use asymmetric cryptography; the token stores, protects and uses a private key that is kept secret, and the user possesses an associated public key that is bound to the user's identity, often, but not required, through the use of a digital certificate backed by a Public Key Infrastructure (PKI). Embedded cryptographic tokens would be considered a form of single-factor authentication if anyone in possession of the token is able to use it to authenticate to a system or service. However, in many cases, cryptographic tokens support multi-factor authentication by requiring the user to authenticate to the token (e.g., using a PIN or biometric) to unlock the secret or private key.

- **Removable Hardware Cryptographic Token:** Removable 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. Although some hardware cryptographic tokens are easily removable, others require more effort to remove such as the Universal Integrated Circuit Card (UICC), colloquially referred to as a Subscriber Identity Module (SIM) card that resides within a mobile device.

- **Smartcard with External Reader:** Multi-factor 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 800-63-2 [11] refers to smartcards used in this manner as multifactor 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.

- **Near Field Communication (NFC) Enabled Smartcard:** This approach achieves multifactor authentication (MFA) 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 as they enter the PIN protecting the credentials stored on the smartcard.

- **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 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 (Fast IDentity Online) Alliance [12]. 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 multifactor solution.

The following four biometric authentication methods all require initial enrollment(s), where a user's biometric sample is stored in the authentication system, preferably within secure storage on the device (local) but sometimes in a central repository (remote). These biometric modalities are more commonly used for individual identification. Per NIST SP 800-63-2[2] [11], biometrics are not authorized for use as single or 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 800-63-2. 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 Fast Identity Online (FIDO) Alliance Universal Authentication Framework (UAF) address mobile authentication, including performance metadata, with various types of biometric modalities [12].

- **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 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.

[2] Guidelines regarding the use of biometrics for authentication may change with the release of NIST SP 800-63-3.

- **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 passively and continuously as users control the device. 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 continuous authentication methods are not meant to be used as a traditional authentication factor, but are instead to be used to supplement other authentication mechanisms:

- **Keystroke Dynamics:** By using the time intervals and pressure of keyboard presses, it is possible to authenticate an individual [13]. 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 Awareness:** A user's "location" is used to support authentication of an individual, which could be determined via a device's GPS (Global Positioning System) location, IP address, or proximity to a specific wireless network. Depending on how it's deployed, it could be invisible to the user and allows services to set policies that dictate access in or around certain vicinities or coordinates.

5 Usability and Technical Considerations of Authentication Methods

It is critical to examine the usability of authentication, since poor usability often results in user circumvention, which can ultimately degrade the intended security control. 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 user memory considerations, physical considerations, and environmental considerations. Several themes emerged when looking across authentication methods: usability issues with memorizing information, the difficulty of text entry on mobile devices, the necessity of having access to the biometric samples of a user, and the environmental issues that could negatively affect sensitive electronics. Although the analyses are focused on mobile authentication in the field, many of the same considerations would apply to systems used by public safety personnel at the office.

It is of note that specific security considerations are detailed within NISTIR 8014, *Considerations for Identity Management in Public Safety Mobile Networks* [2].

5.1 Knowledge-Based Authentication

Memory Considerations:

This method relies on users remembering their KBA answers. When KBA uses questions that are static to a user and/or their personal history (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, especially those that may be contextual or historically-based (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 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 [14]. 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). However, if KBA answers are spoken aloud in the company of others, then the answers would no longer be secret. 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 would need to enroll themselves into the backend authentication system by providing answers to pre-determined or user-defined questions such as “What was the name of your first pet?” Providing the correct responses to these questions will result in successful authentication. KBA is vulnerable to shoulder surfing attacks.

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. Number of passwords that users must manage both for work and for personal use has also been increasing. 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 [15].

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) [16].

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. 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 [14]. 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 the onscreen keyboard and enter passwords on the screen.

Technical Considerations:

Passwords 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 [11] and discussed in NISTIR 8014 [2]. 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. Furthermore, predictive text algorithms should be disabled for password entry fields, since such algorithms would incorrectly attempt to autocorrect passwords into words.

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., [11], [17], [18]), the field of computer security lacks a universally agreed upon measurement standard with sufficient evidence to prove the merit of the standard. 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) [16]. PINs may be masked so users cannot see what they have entered. 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 [14]. 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). However, if a PIN is spoken aloud in the company of others, then it would no longer be a secret. 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 the onscreen keyboard and enter PINs on the screen.

Technical Considerations:

PINs consist solely of numbers, are less complex, and are generated from a smaller character pool than passwords which usually contain letters, numbers and non-alphabetic characters, 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 800-63-2 [11] 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 [11]. This method of authentication is vulnerable to shoulder surfing and 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 [19].

5.4 Gesture

Memory Considerations:

This method relies on users remembering their patterns. More complex gestural patterns are 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 as described above for PINs.

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) [16].

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 [20]. 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. Furthermore, some MFA OTP devices require users to enter a PIN or supply a biometric before the OTP device will generate an OTP. The physical considerations for PINs and biometrics will also apply to an MFA OTP device.

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 [14]. 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). However, if an OTP is spoken aloud in the company of others, then it would no longer be a secret. 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.

When using 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 Embedded Cryptographic Tokens

Note: Embedded cryptographic tokens are commonly used in MFA situations alongside a PIN, password, or biometric, 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. The use of a PIN, password, or biometric to unlock a mobile device could be considered the first factor in an MFA scenario.

Memory Considerations:

If authentication via digital certificates does not require another factor (beyond the initial unlocking of the mobile device) to "activate" the token to be presented, 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. Certificates are not typically set up and named by end users, and often do not have meaningful and descriptive names. In this case the term *name* is used to identify the certificate rather than referring to the user of that certificate. It is possible for multiple similarly and ambiguously named certificates to be stored on the same device. Therefore, users would have to recognize and recall which certificate to use for which authentication task. Some systems allow for a user-friendly certificate name to be established, helping the end user to distinguish among certificates. Overall, this task would be impacted by differences in the user interfaces (UIs) 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., encrypting emails, digitally signing documents), it may be difficult for users to learn and remember which procedures are required for which activities.

Physical Considerations:

If authentication via embedded cryptographic tokens happens automatically, then there would be few if any physical considerations for users. However, if users must select from a list of digital 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) [16]. In addition to variability in physical surface size, UIs also vary from device to device and browser to browser.

Environment Considerations:

If authentication via embedded cryptographic tokens 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 digital 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 embedded cryptographic tokens can be implemented on mobile devices. This method of authentication may be best suited for remote authentication, instead of local authentication to a mobile device's lockscreen. A PKI is often necessary to support the use of digital certificates, although this is not always the case. The certificate model used on the public internet could be used, although a private PKI system could also be constructed.

Protecting software tokens using software-based mechanisms potentially increases the risk that the credential could be stolen or subject to unauthorized use via malware – hardware-based storage is preferred to software-based mechanisms for credential storage.

5.7 Removable 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) [16]. 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 [14]. 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 already built-in and such capabilities 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 than passwords which usually contain letters, numbers and non-alphabetic characters, 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 [11]. NIST 800-157 recommends a 6-character password as a minimum to protect a derived PIV (Personal Identity Verification) credential [21]. 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.

5.8 Smartcard with External Reader

Memory Considerations:

This method relies on users remembering to bring their smartcard and external reader with them, although this could be ameliorated by tethering the external reader to the mobile device in some fashion, such as a device sleeve. 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) [16]. 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 or device sleeve 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 [14]. 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). However, if a PIN is spoken aloud in the company of others, then it would no longer be a secret. 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 MFA, 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.

5.9 NFC-Enabled Smartcard

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) [16]. 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 [14]. 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). However, if a PIN is spoken aloud in the company of others, then it would no longer be a secret. 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 containing multiple credentials, which is distributed to every US federal employee [22]. 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 (PIV-Interoperable) is working to define mechanisms to do so [23].

5.10 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, and 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 to 2 days, while low-power wearables may last much longer. Certain classes of proximity tokens do not require an embedded power source, and are passive in nature. These passive proximity tokens are powered when external devices request information via NFC.

5.11 Fingerprints

Memory Considerations:

Users must remember which finger(s) they initially enrolled with. Although users could try to authenticate with each of their fingers, a number of failed authentication attempts may have technical ramifications depending on lockout implementation.

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 fingers, temporarily injured fingers, or those individuals

with fingerprints that many fingerprint sensors have difficulty reading. The amount of moisture or dirt 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.

5.12 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 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 users to align their faces with the sensor properly in order 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 Iris Recognition

Memory Considerations:

There are no identified human memory considerations for iris recognition as long as both irises are initially enrolled. If single iris recognition is implemented, users must remember which iris they initially enrolled with.

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 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 even if using a mobile device's camera to capture an image of the iris. Iris recognition may not work in certain circumstances; for example, if people are enrolled prior to eye surgery, they may need to be re-enrolled post-surgery. In cases where iris recognition does not work, an alternative authentication method would need to be in place and functioning.

5.14 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.

5.15 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) [16]. 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 [14]. 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 desktop computer keyboard differ significantly from the way a user types the same text on a mobile touchscreen.

5.16 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 on its own but may be combined with other factors in an MFA scenario. However, 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.

5.17 Location-Based Awareness

Memory Considerations:

As long as users do not have to remember to turn on location-based services, there would not be any memory considerations. Since location-based awareness is not itself an authentication method, it can only be used to support an MFA solution. Therefore, memory considerations for the MFA factors would apply, as described above.

Physical Considerations:

As long as users do not have to turn on location-based services, there would not be any physical considerations. Since this supports an MFA solution, physical considerations for the MFA factors would apply, as described above.

Environment Considerations:

Location-based awareness could be impacted by any environmental conditions that negatively affect the accuracy of location-based services (e.g., being surrounded by tall buildings, being underground). Since location-based awareness supports an MFA solution, environmental considerations for the MFA factors would apply, as described above.

Technical Considerations:

The technical considerations for any location-based awareness 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 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. If authentication is implemented in a usable way, then first responders will not be forced to resort to unintentionally insecure workarounds in order to accomplish their mission-critical tasks.

First responders should not be required to authenticate in order to use voice communication services on their next-generation mobile devices. This is similar to the way in which first responders currently use LMRs without authentication for voice communication. Furthermore, mission-critical communication services such as texting or video calling may not require authentication either. If first responders are required to authenticate even for basic communication, this may negatively affect their willingness to embrace new technology. Usability and user acceptance are 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 on the NPSBN, the mission-critical communication services that they are accustomed to must remain intact.

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 LMR devices are often affixed to them via a physical tether. First responders need to be able to access the same mission-critical communication services on their next-generation mobile device in a manner similar to the way they currently use their LMR devices. Allowing the use of certain functions without authentication is not without precedent, as many modern mobile operating systems allow users to access certain features without authenticating at the time of use. Common examples include accessing the camera, performing emergency calls, and viewing and interacting with 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 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.

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 as behind-the-scenes and invisible to the user as possible. 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, 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 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 users in the field, 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, many biometric modalities for 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 embedded cryptographic tokens, on-body detection, and location-based awareness. 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 embedded cryptographic tokens are securely stored, and that they do not require a user to select between multiple certificates. If first responders are sharing devices, it may be necessary for multiple user profiles to be enabled on the same device, to allow the correct certificates to be used for a given responder. Further research is required to understand the necessary functionality required to enable these capabilities.

As long as it is invisible to the user, location-based awareness alone does not pose critical or significant usability issues. However, since it supports an MFA scenario, the usability of the MFA factors must be considered. Although embedded cryptographic tokens, on-body detection, and location-based awareness are more promising from a usability perspective, on-body detection and location-based awareness 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—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. 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 ratings.

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 in the field.

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 in the field.

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 the field. In many cases feasibility depends upon the exact implementation of the technology at hand, as discussed in Section 6.1.

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.

The ratings listed in Table 1 are based on using currently available mobile devices, similar to touchscreen smartphones, used in the field. If future NPSBN devices differ significantly from touchscreen smartphones, then usability and technical considerations must be reassessed. For instance, it is currently impractical for a gloved firefighter to use a touchscreen smartphone while in the field. However, in the future their smartphone may act as a central hub connecting any number of wearables and sensors that are specific to the Fire Service.

Table 1 – Usability Analysis Summary of Public Safety Mobile Authentication Methods

Authentication Methods	Feasible	Challenging	Impractical
No Authentication[3]			
KBA			
Password			
PIN			
Gesture			
OTP Device			
Embedded Cryptographic Token			
Removable Hardware Cryptographic Token			
Smartcard with External Reader			
NFC-Enabled Smartcard			
Proximity Token			
Fingerprints			
Facial Recognition			
Iris Recognition			
Speaker Recognition			
Keystroke Dynamics			
On-Body Detection			
Location-Based Awareness			

[3] No authentication is currently the *de facto* authentication scenario.

6.1.1 Authentication Feasibility By Discipline

For the Fire Service, the most currently feasible authentication methods for in-field use are embedded cryptographic tokens, on-body detection, and location-based awareness. The remaining authentication methods are currently impractical for in-field Fire use, at least for gloved and masked firefighters; those authentication methods are KBA, password, PIN, gesture, OTP device, removable hardware cryptographic tokens, smartcard with external reader, NFC-enabled smartcard, proximity token, fingerprints, facial recognition, iris recognition, speaker recognition, and keystroke dynamics.

For EMS, the most currently feasible authentication methods for in-field use are embedded cryptographic tokens, proximity tokens, on-body detection, and location-based awareness. Challenging authentication methods for EMS are facial and iris recognition. Impractical methods for EMS are KBA, password, PIN, gesture, OTP device, removable hardware cryptographic tokens, smartcard with external reader, NFC-enabled smartcard, fingerprints, speaker recognition, and keystroke dynamics.

For Law Enforcement, the most currently feasible authentication methods for in-field use are embedded cryptographic tokens, proximity token, fingerprints, on-body detection, and location-based awareness. Challenging authentication methods for Law Enforcement are PIN, gesture, removable hardware cryptographic tokens, NFC-enabled smartcard, facial recognition, and iris recognition. Impractical methods for law enforcement are KBA, password, OTP device, smartcard with external reader, speaker recognition, and keystroke dynamics.

Across disciplines, those authentication methods identified as currently feasible for in-field use should also be feasible for use at the station, since the in-field context presents the most difficult constraints. However, some methods that were identified as challenging and even impractical while responding may be feasible for use in the station context. For example, biometric authentication methods may be feasible for use in the station when first responders are not wearing their protective gear.

Usability issues with authentication methods that were identified as currently not feasible for use in the field may be mitigated with careful planning and implementation. The goal is that authentication should not interrupt actively responding first responders, nor should it overburden them in any stage of response. For example, if authentication can be implemented such that first responders authenticate at the beginning of a shift through SSO, and stay authenticated throughout the shift, then many of the authentication methods discussed above would then become more feasible.

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 effort 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 mobile authentication 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 or incident, 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 first responders' working environments. SSO may also alleviate the number of authentication events by allowing a user to authenticate one time, yet they will receive access to multiple applications, systems, and domains with a variety of authentication mechanisms [24].

For first responders in the field, it is vital to stay in constant communication. Today, first responders use voice communication via LMR push-to-talk (PTT) functionality, which does not require authentication. When first responders are in the field, they must be able to easily, quickly, and reliably access the mission-critical communication services they need. Therefore, new enterprise-issued mobile devices should not require authentication to make or receive voice calls. Other mission-critical communication services such as texting or video calling also may not require authentication each time an application or service is used. In contrast, more sophisticated and sensitive applications (e.g., enterprise email, public safety databases, document repositories) require protection such as a lockscreen with a PIN, passcode, gesture, or biometric to unlock. Other controls can be used as well, such as remote lock and remote wipe to ensure a lost or stolen first responder device is not compromised.

Research with first responders will be necessary to further define mission-critical communication services and critical features that should not require the user to regularly re-authenticate in order to minimize disruptions to first responders' existing workflows. This will require public safety discipline-specific research, as mission-critical communication services may vary by discipline. Some authentication methods would be more arduous and disruptive than others given the constraints of first responder operating environments. Furthermore, it will be necessary to conduct research to support credentials of varying levels for a variety of users, depending on the sensitivity of the public safety data or information system. Rather than a one size fits all model, authentication should be customized to address the unique requirements posed by public safety disciplines.

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
EMS	Emergency Medical Services
EMT	Emergency Medical Technician
FEMA	Federal Emergency Management Agency
FIDO	Fast IDentity Online
GPS	Global Positioning System
IAFIS	Integrated Automated Fingerprint Identification System
IR	Interagency Report
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
KBA	Knowledge-based authentication
LE	Low Energy
LEO	Law Enforcement Officer
LMR	Land Mobile Radio
LTE	Long Term Evolution
MDT	Mobile Data Terminal
MFA	Multifactor Authentication
NCIC	National Crime Information Center
NFC	Near Field Communication
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
NPSBN	Nationwide Public Safety Broadband Network
OS	Operating System
OTP	One-Time Password
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification-Interoperable
PKI	Public Key Infrastructure
PPE	Personal Protective Equipment
PTT	Push-To-Talk
RFID	Radio-Frequency Identification
SCBA	Self-Contained Breathing Apparatus
SIM	Subscriber Identity Module
SME	Subject Matter Expert
SP	Special Publication
SSO	Single Sign-on
TLS	Transport Layer Security
U2F	Universal 2nd Factor
UAF	Universal Authentication Framework
UCD	User-Centered Design

UI	User Interface
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*, Pub. L. 112–96, 126 Stat. 156, February 22, 2012. http://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf [accessed 07/25/2016].

[2] N. Hastings and J. Franklin, *Considerations for Identity Management in Public Safety Mobile Networks*, NIST Interagency Report (NISTIR) 8014, March 2015. http://dx.doi.org/10.6028/NIST.IR.8014.

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

[4] K. Charmaz, *Constructing grounded theory: A practical guide through qualitative analysis*, 2nd edition, Thousand Oaks, California: SAGE Publications, 2014.

[5] National Fire Protection Association, *Codes & Standards* [Web page], 2016. http://www.nfpa.org/codes-and-standards [accessed 07/25/2016].

[6] C. Grant, A. Hamins, N. Bryner, A. Jones, and G. Koepke, *Research Roadmap for Smart Fire Fighting: Summary Report*, NIST Special Publication (SP) 1191, May 2015. http://dx.doi.org/10.6028/NIST.SP.1191.

[7] 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 07/25/2016].

[8] Occupational Safety & Health Administration (OSHA), *Best Practices for Protecting EMS Responders during Treatment and transport of Victims of Hazardous Substance Releases*, OSHA 3370-11 2009, 2009. https://www.osha.gov/Publications/OSHA3370-protecting-EMS-respondersSM.pdf [accessed 07/25/2016].

[9] Federal Bureau of Investigation, Criminal Justice Information Services Division, *Criminal Justice Information Services (CJIS) Security Policy*, CJISD-ITS-DOC-08140-5.5, June 1, 2016. https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center [accessed 07/25/2016].

[10] Federal Bureau of Investigation, *Next Generation Identification*, 2016. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi [accessed 07/26/2016].

[11] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbus, *Electronic Authentication Guideline*, NIST Special Publication (SP) 800-63-2, August 2013. http://dx.doi.org/10.6028/NIST.SP.800-63-2.

[12] FIDO Alliance, *Specifications Overview* [Web page], 2016. https://fidoalliance.org/specifications/overview [accessed 07/25/16].

[13] J. Chen, G. Zhu, J. Yang, Q. Jing, P. Bai, W. Yang, X. Qi, Y. Su, and Z. L. Wang, "Personalized Keystroke Dynamics for Self-Powered Human–Machine Interfacing," *ACS Nano* 9(1), January 27, 2015, pp. 105-116. http://dx.doi.org/10.1021/nn506832w.

[14] H. Nicolau and J. Jorge, "Touch typing using thumbs: understanding the effect of mobility and hand posture," in *Proceedings of the SIGCHI Conference on Human Factors in Computing System (CHI '12)*, New York: ACM, 2012, pp. 2683-2686. http://dx.doi.org/10.1145/2207676.2208661.

[15] Y. Choong, M. Theofanos, and H. K. Liu, *United States Federal Employees' Password Management Behaviors – a Department of Commerce Case Study*, NIST Internal Report (NISTIR) 7991, March 2014. http://dx.doi.org/10.6028/NIST.IR.7991.

[16] X. Bi, Y. Li, and S. Zhai, "FFitts Law: Modeling Finger Touch with Fitts' Law," in *Proceedings of the SIGCHI Conference on Human Factors in Computing System (CHI '13)*, New York: ACM, 2013, pp. 1363-1372. http://dx.doi.org/10.1145/2470654.2466180.

[17] M. Jakobsson and M. Dhiman, M, "The benefits of understanding passwords," in *Mobile Authentication: Problems and Solutions*, New York: Springer, August 2012, pp. 5-24. http://dx.doi.org/10.1007/978-1-4614-4878-5_2.

[18] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in *Proceedings of the 17th ACM Conference on Computer and Communications Security*, New York: ACM, 2010, pp. 162-175. http://dx.doi.org/10.1145/1866307.1866327.

[19] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge Attacks on Smartphone Touch Screens," *4th Usenix Workshop on Offensive Technologies (WOOT '10)*, Washington, DC, August 9, 2010, 7pp. https://www.usenix.org/legacy/event/woot10/tech/full_papers/Aviv.pdf [accessed 07/25/16].

[20] K. K. Greene, M. A. Gallagher, B. C. Stanton, and P. Y. Lee, "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 8533, 2014, pp 160-171. http://dx.doi.org/0.1007/978-3-319-07620-1_15.

[21] H. Ferraiolo, D. Cooper, S. Francomacaro, W. Burr, J. Mohler, and S. Gupta, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, NIST Special Publication (SP) 800-157, December 2014. http://dx.doi.org/10.6028/NIST.SP.800-157.

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

[23] Federal CIO Council, *Personal Identity Verification Interoperability For Non-Federal Issuers*, v 1.0.0, May 2009. https://cio.gov/wp-content/uploads/downloads/2012/09/PIV_Interoperabillity_Non-Federal_Issuers_May-2009.pdf [accessed 07/25/16].

[24] T. Grance, M. Stevens, and M. Myers, *Guide to Selecting Information Technology Security Products*, NIST Special Publication (SP) 800-36, October 2003. http://dx.doi.org/10.6028/NIST.SP.800-36.