This **DRAFT** document (Draft NISTIR 8014, *Considerations for Identity Management in Public Safety Mobile Networks*) has been approved as final and is superseded by the following publication:

Publication Number: **NISTIR 8014**

Title: **Considerations for Identity Management in Public Safety Mobile Networks**

Publication Date: **March 2015**

- Final Publication:
  NIST Publications Portal
  http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8014.pdf
  DOI URL (note: The DOI actually redirects to the URL above):
  http://dx.doi.org/10.6028/NIST.IR.8014
- *Link to NISTIR 8014 can be found on the CSRC NISTIR webpage at:*
  http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-8014
- Information on other NIST Computer Security Division publications and programs can be found at: http://csrc.nist.gov/

The following announcement was posted about this documents release:

July 15, 2014

NIST IR 8014

DRAFT *Considerations for Identity Management in Public Safety Mobile Networks*

In cooperation with the Public Safety Communications Research (PSCR) Program, NIST announces the release of NIST Interagency Report (NISTIR) 8014, Considerations for Identity Management in Public Safety Mobile Networks. This document analyzes approaches to identity management for public safety networks in an effort to assist individuals developing technical and policy requirements for public safety use. These considerations are scoped into the context of their applicability to public safety communications networks with a particular focus on the nationwide public safety broadband network (NPSBN) based on the Long Term Evolution (LTE) family of standards. A short background on identity management is provided alongside a review of applicable federal and industry guidance. Considerations are provided for identity proofing, selecting tokens, and the authentication process.

The public comment period is from July 15, 2014 through August 22, 2014. Please send comments to nistir8014 @nist.gov using the public comment template that is provided - see link below (MS Excel).

DRAFT NISTIR 8014

Considerations for Identity Management in Public Safety Mobile Networks (DRAFT)

Nelson Hastings
Joshua Franklin

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

NISTIR 8014

Considerations for Identity Management in Public Safety Networks (DRAFT)

Nelson Hastings
Joshua Franklin
Computer Security Division
Information Technology Laboratory

July 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

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

National Institute of Standards and Technology Interagency or Internal Report 8014
43 pages (July 2014)

This publication is available free of charge

Public comment period: *July 15, 2014* through *August 22, 2014*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: nistir8014@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

This document analyzes approaches to identity management for public safety networks in an effort to assist individuals developing technical and policy requirements for public safety use. These considerations are scoped into the context of their applicability to public safety communications networks with a particular focus on the nationwide public safety broadband network (NPSBN) based on the Long Term Evolution (LTE) family of standards. A short background on identity management is provided alongside a review of applicable federal and industry guidance. Considerations are provided for identity proofing, selecting tokens, and the authentication process. While specific identity management technologies are analyzed, the document does not preclude other identity management technologies from being used in public safety communications networks.

Keywords

authentication; identity management; local authentication; Long Term Evolution; LTE; public safety; remote authentication

Acknowledgments

This publication was developed as part of the NTIA/NIST Public Safety Communication Research program with sponsorship from the Office for Interoperability and Compatibility (OIC) at the Department of Homeland Security (DHS). The authors wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content including William Burr, Paul Grassi, Ray Perlner, and Andrew Regenscheid of NIST; Alex Kreilein of DHS OEC; Kenneth Boley of The Interoperability Group; and Kevin Donaghy and John Mears of Lockheed Martin.

Notes to Reviewers

As this document does not cover the topic of authorization, the authors would welcome input on the usefulness of writing a companion document on the topic of authorization in public safety networks. Additionally, the authors would request input on the usefulness of the LTE authentication section located in Appendix F and of including a short section discussing various government identity management frameworks as additional background information in Section 3.

Audience

This document is intended for those wishing to understand possible approaches to identity management in next-generation public safety networks. Local public safety networks, private sector communities, and public safety applications leveraging identity management services (such as criminal justice information and records management systems) may also find the guidance useful.

Trademark Information

All product names are registered trademarks or trademarks of their respective companies.

Table of Contents

List of Appendices

List of Figures

1. Introduction

The Middle Class Tax Relief and Job Creation Act of 2012 created the First Responder Network Authority (FirstNet). FirstNet, an independent agency under the Department of Commerce's National Telecommunications & Information Administration (NTIA), has a mission to develop, build and operate the country's first nationwide public safety broadband network (NPSBN). Police, fire fighters, emergency medical services (EMS), and other emergency personnel[1] use public safety networks for coordination during emergency situations, disasters, and other incidents. States, counties, and other jurisdictions across the U.S. concurrently operate numerous independent public safety networks based on different communication technologies.

When public safety personnel from separate jurisdictions arrive at the same incident, interoperability problems often arise. This is due in part to jurisdictions using different communication technologies and non-standards based implementations. Personnel at the scene use land mobile radio devices, laptops, and other information technology designed by different manufacturers. Partly due to the fact that public safety devices are manufactured for a unique market, their price is often higher than their counterpart commercial off the shelf (COTS) devices with similar functionality. The NPSBN will be based on commercial standards, specifically the Long Term Evolution (LTE) family of standards, and to the extent practical use COTS mobile devices, which should decrease the cost of devices while increasing interoperability.

The move from current terrestrial radio to next-generation cellular technologies for public safety provides an opportunity to incorporate high bandwidth technology and services, assisting with information sharing and cross-jurisdictional support. The introduction of these technologies and services requires that current public safety identity management mechanisms be revisited. A robust approach to identity management will ensure only authorized users and devices seamlessly access the NPSBN and the services it provides. This type of access control requires an authentication framework extending beyond what is natively provided by LTE technology.[2]

1.1 Purpose and Scope

This document analyzes approaches to identity management for next generation public safety networks. A short background on identity management is provided alongside a review of applicable federal and industry guidance. Considerations are provided for identity proofing, selecting tokens, and the authentication process. All approaches and technologies are considered in the context of their applicability to public safety communications networks, particularly the NPSBN based on LTE technology. Local public safety networks, private sector communities, and public safety applications leveraging identity management services (such as criminal justice information and records management systems) may also find this guidance useful. While current and burgeoning identity management technologies are analyzed, the document does not preclude other identity management frameworks or technologies from being used in public safety communications networks.

This document helps to inform individuals developing technical and policy requirements for public safety communications networks. Areas are identified in which identity management policy decisions are required while refraining from suggesting particular policies for use. The particular policies used will depend highly on the network's architecture and security posture, in addition to the risk tolerance of the network's senior officials, administrators, users, and applications.

[1] National Preparedness Resource Library: http://www.fema.gov/national-preparedness-resource-library
[2] Appendix F provides a technical description of authentication in LTE.

In order to limit the length of this document, it does not provide guidance on the important topic of access control and authorization within public safety networks.[3] Sensitive information and services from many jurisdictions and organizations will be accessible solely by NPSBN users, but users will not be immediately granted access to all of the information and services by gaining access to the NPSBN. Users will need to prove their identity and then be provided access to information and services that are meant for them, and guidance for how to perform these functions is not within the scope of this document.

1.2 Document Structure

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

- **Identity Management & Authentication Background:** Describes the baseline set of identity management knowledge and nomenclature used throughout this document.
- **Identity Management Guidance and Frameworks:** Provides a description of existing Federal and industry guidance relating to identity management of users and devices authenticating to information systems.
- **Registration and Issuance:** Details the process of vetting an individual's or devices identity and binding a credential to an identity.
- **Token Selection:** Explores considerations for selecting tokens to be used as proof of identity to support the authentication process.
- **The Authentication Processes:** Describes how authentication protocols and assertions can be used to provide assurance in an individual's or device's identity.

The document also contains appendices with supporting material:

- Appendix A defines selected acronyms and abbreviations used in this specification,
- Appendix B contains a list of references used in the development of this document,
- Appendix C summarizes the NIST SP 800-63 registration and issuance requirements,
- Appendix D summarizes the NIST SP 800-63 requirements for token selection,
- Appendix E contains the National Public Safety Telecommunications Council (NPSTC) identity management requirements, and
- Appendix F provides a technical description of LTE authentication mechanisms.

1.3 Document Conventions

The following conventions are used throughout the Interagency Report:

- All references to NIST 800-63 are references to NIST 800-63 revision 2. [1]

[3]Authentication and authorization are related but separate processes, which provides a natural point for delineating the document's scope.

2. Identity Management & Authentication Background

Identity management may be described as the process of managing the identification, authentication, and authorization associated with individuals or entities (devices, processes, etc.). Identification is the process of making an identity claim. An identity is a set of attributes uniquely describing a person or entity within a given context. Authentication is the process of establishing confidence in a given identity. Authentication is performed by an individual or entity claiming an association with a specific identity and providing an authenticator or token (i.e. password, PIN, smartcard, biometric, etc.) as proof of that association. Finally, authorization is the act of determining and enforcing which information and systems an individual or non-person entity (such as devices) may access. The focus of this document is the identification and authentication of individuals and devices.

2.1 The Identity Management Lifecycle

Identities and tokens associated with individuals or entities are bound by an object or data structure called a credential. Tokens are possessed and controlled by a user to assert their identity, with passwords and cryptographic keys being common examples. It is helpful to describe the lifecycle of credentials in order to gain insight into the different aspects of the identity management process that influence the confidence, or level of assurance, that can be placed in a given credential. In general, the lifecycle of a credential has the following phases:

- **Registration:** An individual, entity, or their sponsor applies for a credential to be issued to the individual or entity. As part of this phase, information about the individual or entity is collected and verified to establish a level of assurance about their association to a claimed identity, often referred to as identity proofing.

- **Issuance:** A token and the claimed identity of the individual or entity are bound by a credential and issued to the individual, entity, or their sponsor. This phase may require the establishment or registration of the particular token used by the credential.

- **Usage:** The individual or entity provides their credential to applications or service providers to prove their identity in order to gain access to information and services. As part of this phase, an application or service provider may verify the credential is currently valid and has not been revoked, suspended, or expired via an authentication protocol before providing access to their information or services.

- **Expiration:** Credentials are often issued with a particular time frame for their use. This lifetime is based on the type of token used and the associated threats to the token and credential. Once a credential's lifetime has been met, the credential expires and is no longer valid and should not be accepted by applications and service providers.

- **Revocation:** A credential may need to be invalidated, or revoked, before its lifetime has expired, such as when the credential is lost or the token has been compromised. Once a credential is revoked it is no longer valid and should not be accepted by applications and service providers.

- **Suspension:** A credential may need to be made temporally invalid, or suspended, before its lifetime is reached. This may be necessary when an individual is on vacation or a device is out of service. Once a credential's suspension period is over, the credential can again be used by the individual or entity to authenticate.

- **Re-issuance/Updating:** Before the end of a credential's lifetime, a credential can be updated and/or reissued to reflect modifications in the identity and/or token bound to the credential. This modification may be due to a change in name, position, duties, responsibilities, or to simply keep the credential from expiring. Similarly, a token may need to be modified due to forgotten password or PIN, or a failure of hardware or software. In some cases, re-issuing or updating a credential is not permitted by the issuer's security policy and the old credential must be revoked and a new credential issued. It is often the case that credential re-issuance and updating is performed multiple times before the more rigorous and complete registration and issuance processes needs to occur.

The following sections provide background information on key aspects of the identity management lifecycle.

2.2 Registration & Issuance

Identity proofing is the process of providing sufficient information (e.g., identity history, credentials, documents) to a requesting verification entity when attempting to establish an identity. Registration and issuance activities can be performed remotely or in-person, but identity proofing for higher assurance often requires the requestor to be physically present and alongside a human sponsor. The manner in which a user requests an identity and how identities are vetted has important security implications throughout the identity management lifecycle.

Documents (e.g., U.S. passports, state issued driver's licenses, financial and utility statements, etc.) issued by commercial entities and/or local, state, or federal governments provide primary evidence of an individual's identity during the identity proofing process. Public safety organizations are most likely already familiar with these and other identity proofing concepts due to the ongoing need of vetting the identities of government employees and public safety personnel. A universally accepted standard for identity proofing does not exist, and the assurance offered by one jurisdiction's process is not necessarily equal to what is provided by another.

Once identity proofing is complete, the user is registered with their organization and the issuance process begins. In the simplest case, a credential must be created that binds the user's identity to a token, and this token must be distributed to the user. The manner in which a token is created and provided to the user influences the overall level of assurance. For example, can an individual or entity receive the credential remotely without physically picking it up from the issuer? Or, must the individual or the entity's sponsor appear in-person before an issuer to be verified and provided the credential? The answers to these types of questions carry significant implications for the security of the process and thus the confidence that there has been no error or impropriety in the process that might cause the credential to be issued to a person other than the person indicated on the credential.

2.3 Tokens & Credentials

In addition to the way registration and issuance processes are performed, the type of token used influences the level of assurance that can be placed in the credential. Tokens are categorized as follows:

- *Something you know:* A password or a PIN are common examples,
- *Something you have:* Such as an identification badge or a cryptographic key, and
- *Something you are:* For example, a fingerprint or other biometric data.

Typical types of tokens include:

- Memorized Secret Token – A secret shared between the user and the party issuing credentials. Memorized Secret Tokens are typically character strings (e.g., passwords and passphrases) or numerical strings (e.g., PINs.)

- Pre-registered Knowledge Token – A series of responses to a set of prompts or challenge questions resulting in a set of shared secrets. Typical challenge questions may include a user registering answers to questions such as “What was your mother’s maiden name?” and “Where did you go to high school?”

- Look-up Secret Token – A physical or electronic token that stores a set of secrets shared between the user and the party issuing credentials. For example, a user may be asked by the verifying entity to provide a specific subset of the numeric or character strings printed on a card in table format.

- Out of Band Token – A physical token that is uniquely addressable and can receive a one-time use secret from the verifying entity. The device is possessed and controlled by the user and supports private communication over a channel that is separate from the primary channel being used for authentication

- Single-factor (SF) One-Time Password (OTP) Device – a hardware device that performs cryptographic operations on input provided to the device.

- Single-factor (SF) Cryptographic Device – a hardware device that performs cryptographic operations on input provided to the device, often using embedded symmetric or asymmetric cryptographic keys.

- Multi-factor (MF) Software Cryptographic Token – A cryptographic key is stored on disk or some other “soft” media and requires activation through a second factor of authentication. Authentication is accomplished by proving possession and control of the key.

- Multi-factor (MF) One-Time Password (OTP) Device – A hardware device that generates one-time passwords for use in authentication and which requires activation through a second factor of authentication. The second factor of authentication may be achieved through some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port). The one-time password is typically displayed on the device and manually provided to the verifying entity as a password, although direct electronic input from the device to a computer is also allowed.

- Multi-factor (MF) Cryptographic Device – A hardware device that contains a protected cryptographic key that requires activation through a second authentication factor. Authentication is accomplished by proving possession of the device and control of the key.

The combination of multiple token categories is known as multi-factor authentication and provides greater assurance than using a single token. This does not imply that all tokens of the same type are equivalent in the assurance they provide, for instance - the length and complexity of password impacts the strength. External circumstances also affect assurance, such as storing credentials in protected hardware or firmware, which provide tamper detection and integrity protection. Additional circumstances include understanding the difficulty in forging or issuing a fraudulent credential and how resistant a credential or token is to tampering, disclosure, and guessing.

2.4 Authentication

The authentication process uses identities, credentials, and tokens to provide assurance in an entity's identity claims. Simple authentication schemes involve two parties: an entity asserting an identity claim (the claimant) and an entity verifying that the clam is accurate (the verifier). The manner in which this authentication process is conducted influences the assurance a verifier has in the veracity of an entity's identity claims. Authentication protocols are the mechanisms used to provide assurance to a verifier. These protocols exchange messages between two parties (often the verifier and claimant) and assist the verifier in arriving at an authentication decision. Additional management mechanisms can supplement the authentication protocol to provide enhanced assurance to a verifying party.

Authentication can be performed both locally and remotely. Local authentication often occurs when individuals are physically present, such as when an employee presents an identification badge or enters a PIN into the lockscreen of a mobile device. Remote authentication requires access to a network and is the primary method of authentication for the internet. NIST SP 800-63 defines remote authentication as "*An information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls.*"

Assessing the strength of an authentication scheme is a difficult task and, as previously stated, the use of multi-factor tokens can provide greater assurance. While tokens may support one, two, or three factors, it is possible that the chosen authentication scheme will not require all three factors at all times. There may be public safety scenarios in which the delay and complexity of using all of the supported factors may lead to life threatening or other dangerous situations. For instance, the same smartcard may be used as a multifactor cryptographic device to authenticate to an external application or as a single factor cryptographic device to gain access to a restricted area via a physical access control system. Identifying and implementing policies for these scenarios is a policy decision for organizations and agencies involved in public safety.

3. Identity Management Guidance and Frameworks

This section introduces the relevant identity management guidance from both public and private entities. Federal guidance includes OMB M-04-04 E-Authentication Guidance for Federal Agencies, NIST SP 800-63-2 Electronic Authentication Guideline, and HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors alongside its associated standards. Industry guidance includes information from the National Public Safety Telecommunications Council (NPSTC) and the Alliance for Telecommunications Industry Solutions (ATIS) guidance and frameworks.

3.1 OMB M-04-04: E-Authentication Guidance for Federal Agencies

OMB M-04-04 was issued to enable individuals to remotely access government services using the Internet and provide guidance to Federal agencies on identity verification and authentication [2]. OMB M-04-04 outlines a five-step process agencies should use to determine their identity verification and assurance needs:

1. Conduct a risk assessment of the government system.
2. Map identified risks to the appropriate assurance level.
3. Select technology based on e-authentication technical guidance.
4. Validate that the implemented system has met the required assurance level.
5. Periodically reassess the information system to determine technology refresh requirements.

Although all steps described are important for Federal agencies to follow when determining their identity verification and authentication level of assurance needs, this document focuses on the third step – selection of technology based on e-authentication technical guidance. Details about the relationship between steps 1, 2, 4, and 5 and how they can be performed is found in NIST SP 800-30 [3], NIST SP 800-37 [4], and NIST SP 800-53 [5].

OMB-04-04 provides a description of authentication errors and their potential impacts that can be used to help determine the level of assurance that needs to be associated with a credential based on the type of authentication errors that might result. The following authentication errors are described:

- Inconvenience, distress, or damage to standing or reputation,
- Financial loss,
- Harm to agency programs or public interests,
- Unauthorized release of sensitive information,
- Personal safety, and
- Civil or criminal violations.

Given these authentication errors, an impact level can be associated with the authentication errors. The potential impact levels (High, Moderate, Low) are defined in Federal Information Processing Standard (FIPS) 199, “Standards for Security Categorization of Federal Information and Information Systems.” [6]

OMB-04-04 defines four levels of assurance associated with the validity of the identity associated with a credential:

- Level 1: Little or no confidence in the validity of the identity associated with the credential.
- Level 2: Some confidence in the validity of the identity associated with the credential.
- Level 3: High confidence in the validity of the identity associated with the credential.
- Level 4: Very high confidence in validity of the identity associated with the credential.

Based on the authentication errors and their potential impacts, the level of assurance required for the credential can be determined. The following table from OMB M-04-04 provides a mapping between the authentication errors, their potential impact, and the credential's level of assurance.

Figure A – Maximum Potential Impacts for Each Assurance Level

Categories of Authentication Errors	Assurance Level			
	1	2	3	4
Inconvenience, distress, or damage to standing or reputation	**Low**	**Mod**	**Mod**	**High**
Financial loss	**Low**	**Mod**	**Mod**	**High**
Harm to agency programs or public interests	**N/A**	**Low**	**Mod**	**High**
Unauthorized release of sensitive information	**N/A**	**Low**	**Mod**	**High**
Personal safety	**N/A**	**N/A**	**Low**	**Mod to High**
Civil or criminal violations	**N/A**	**Low**	**Mod**	**High**

For example, a credential at assurance level 1 can be used when inconvenience or financial loss have a low impact but not when it involves release of sensitive information, personal safety, and civil or criminal violations. A level 2 credential (or higher) can be used when release of sensitive information and civil or criminal violations have a low impact but not when it involves personnel safety. At the other end of the spectrum, a level 4 credential must be used when the impact of an authentication error has high impact. If a user already has a level 4 credential, they are covered for all uses without need for another credential, even for lower-level applications. It is important to note that the authentication errors in the *personal safety* and *civil or criminal violations* categories may be applicable to public safety scenarios.

NIST SP 800-63 provides technical guidance on the types of technologies suitable to support the different level of assurance defined in OMB M-04-04 and is discussed in Section 4.

3.2 Homeland Security Presidential Directive 12

Homeland Security Presidential Directive 12 (HSPD-12) mandates a common identification standard to enhance security, promote interoperability and increase government efficiency [7]. To meet the goals outlined in HSPD-12, the PIV card and its supporting infrastrucure was designed to be interoperable across Federal government for both physical access to government facilities and logical access to federal information systems. The PIV card contains several identity credentials (i.e., digital certificates) supported by a Public Key Infrastructure (PKI) to provide strong identity assurance in an interoperable manner. To provide a high level of assurance in the credentials across the Federal enterprise, the PIV standard established common processes for identity proofing and credential issuance. The technical requirements for PIV cards are found in Federal Information Processing Standard (FIPS) 201-2 (PIV) Personal Identity Verification (PIV) of Federal Employees and Contractor [8].

With the successful issuance and deployment of PIV cards and PIV enabled systems, non-federal organizations expressed interest in issuing identity cards that provide an equivalent level of assurance as PIV cards and are able to interoperate not only among themselves, but also with PIV enabled systems. Since PIV cards are limited to the Federal government community, the Federal CIO Council recognized the need for a non-federal equivalent to the PIV card and developed the "Personal Identity Verification Interoperability For Non-Federal Issuers" (also referred to as PIV-I cards) to fill this gap [9]. Currently, PIV-I is the only PIV-compatible solution available to users outside the federal workforce. The majority of FirstNet users are likely to be non-federal thus PIV-I cards or credentials may be useful in this circumstance.

Using PIV and PIV-I cards as credentials for mobile devices can be achieved in several ways. A mobile device could have an integrated smart card reader as part of the device or a separate smart card reader could be attached to the device via a wired or wireless connection. In addition to the PIV and PIV-I card's wired interface, there is a wireless interface that a mobile device could leverage to directly communicate using Near Field Communication (NFC) technology. However, these solutions are probably not optimal for the mobile devices due to the form factor of the PIV card. To address the form factor issue, FIPS 201 permits the issuance of an additional Derived PIV credential in an alternative form factor to the PIV card. A derived PIV credential can be issued by demonstrating possession of a valid PIV card without repeating the PIV identity proofing and vetting process. The initial draft requirements for Derived PIV credentials being considered can be found in draft NIST Special Publication 800-157: Guidelines for Derived Personal Identity Verification (PIV) Credentials [10]. Finally, draft NIST Interagency Report 7981: Mobile, PIV, and Authentication provides guidance for using PIV credentials in conjunction with mobile devices [11].

3.3 NIST SP 800-63: Electronic Authentication Guideline

NIST 800-63 was designed to supplement OMB M-04-04 by providing guidelines for implementing the third step of OMB's process for agencies to meet their e-authentication assurance requirements - selecting a technology based on e-authentication technical guidance [1]. It is important to note that NIST 800-63 solely provides guidance for remote authentication - local authentication is not considered. This guidance defines technical requirements for the following five areas:

1. Identity proofing and registration of applicants,
2. Tokens (typically a cryptographic key or password) for authentication,
3. Token and credential management mechanisms used to establish and maintain token and credential information,
4. Protocols used to support the authentication mechanism between the claimant and the verifier, and
5. Assertion mechanisms used to communicate the results of a remote authentication if these results are sent to other parties.

The requirements help to assess the strength of an authentication solution and are grouped into four levels of assurance. To help demonstrate the interplay between the five areas and the assurance levels we will briefly explore a modified public safety scenario from the Criminal Justice Information Services Security Policy [12] requirements.[4] In this scenario, a detective has already been vetted and issued a PIV-I token by procedures in accordance with assurance level 4.

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued tablet device. The tablet device does not have a built-in smartcard reader, nor does the detective have an external card reader on hand. The detective contacts his agency, which remotely provisions a credential derived from his existing PIV-I credential, which is subsequently stored on his device. To gain access, the detective uses a tablet to establish a remote session via a secure virtual private network (VPN) tunnel. Upon connecting to the agency network, the detective is challenged for a username and possession of the newly provisioned credential. Before he can use the credential, the detective is required to authenticate to the token via a password-based mechanism. Once the detective's credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

According to the definitions from NIST SP 800-63, this scenario illustrates usage of a multifactor software cryptographic token. The token achieves multifactor status due to the use of *something you know* (a password) and *something you have* (a software token). The highest assurance level this type of token can obtain if it is used in a manner consistent with the requirements of NIST SP 800-63 is assurance level 3. A summary of requirements for tokens are provided in Appendix D and NIST SP 800-63 details the specific technical requirements.

To ascertain the overall assurance level for the authentication solution, one must look to the other four areas of NIST SP 800-63 and guidance from DRAFT SP 800-157. The only way this solution would provide assurance level 4 is if it obtained assurance level 4 in all five of the areas. For this scenario, the following levels of assurance achieved by this authentication solution are provided:

Figure B - Level of assurance achieved by CJIS scenario

	Level 1	Level 2	Level 3	Level 4
Registration & Identity Proofing	--	--	Achieved	--
Tokens	--	--	Achieved	--
Tokens and Credential Management	--	--	--	Achieved
Authentication Mechanisms	--	--	--	Achieved
Assertion Mechanisms	--	--	--	Achieved

Although the detective had been vetted and issued a PIV-I token by procedures in accordance with assurance level 4, because the token was remotely provisioned, the assurance level drops to level 3. Additionally, even though the original PIV-I smartcard provides assurance level 4, the derived credential's comparable OMB E-Authentication Level is assurance level 3 when remotely provisioned. It

[4] This use case has been modified from the original to provide additional context for the analysis of the scenario.

is possible to issue a derived credential at assurance level 4 if the guidance from NIST SP 800-157 is followed.[5] For an authentication solution to achieve one of the four assurance levels an equal or greater level of assurance must be obtained for all five areas. The overall level of assurance for an authentication solution is determined by the lowest level obtained by the solution in any of these five areas.

3.4 NPSTC Guidance

The National Public Safety Telecommunications Council (NPSTC) is an organization focusing on improving public safety communications and interoperability. NPSTC released a group of requirements "for an interoperable public safety broadband communications nationwide network to serve all local, tribal, state, and federal first responder communications" [13].

These requirements are intended for FirstNet and pertain to identity management for both the user and application, among other areas of interest such as provisioning.[6] The document assumes the existence of an identity management framework used to "simplify the life of the first responder, simplify management of their credentials on behalf of the user's administrative staff, and simplify application development by standardizing on the mechanics of user identity and user authentication" [13]. NPSTC states that this identity management framework is necessary in addition to the authentication provided by the LTE family of standards discussed in Appendix E.[7]

Although all of NPSTC's identity management requirements are presented in Appendix E of this document, the following provides a summary to assist the reader in understanding the types of requirements NPSTC recommends. NPTSC recommends a standards-based approach to identity management in which users and devices with identities can authenticate to both applications and services. Additionally, NPSTC recommends that local entities establish policies and procedures to govern the management of user identities and local entities should maintain these same identities. These policies must be capable of governing identities over the lifetime of their use and standard authentication interfaces for use in the NPBSN.

3.5 The ATIS Identity Management Framework

The Alliance for Telecommunications Industry Solutions (ATIS) is a standards development organization for the wireless industry. There are three ATIS documents relating to identity management:

- ATIS-1000035: Identity Management (IdM) Framework, [14]
- ATIS-1000044: Identity Management (IdM) Requirements and Use Cases Standard, [15] and
- ATIS-1000045: Identity Management (IdM) Mechanisms and Procedures Standard. [16]

ATIS-1000035: Identity Management (IdM) Framework provides a foundation for the concepts, components, and capabilities required to perform identity management in next generation wireless networks. ATIS-1000044: Identity Management (IdM) Requirements and Use Cases Standard prescribes requirements and provides use cases for identity management. ATIS-1000045: Identity Management

---

[5] DRAFT NIST SP 800-157, Page 23

[6] [12] Table 10: "FirstNet SHALL develop and maintain standard operating procedures at the local, tribal, state, and federal agency level that will define the process for provisioning users."

[7] [12] Page 49: "Because public safety is likely to have many situations where equipment will be shared amongst different users during different shifts or even during different incidents, an authentication framework that extends beyond LTE device authentication is required."

(IdM) Mechanisms and Procedures Standard provides ways in which an identity management solution can confirm to ATIS's identity management requirements.

4. Registration and Issuance

The registration and issuance phases are the first two phases in the identity management life cycle. These phases and their associated processes form the foundation for the level of assurance that should be placed in identities, credentials, and tokens. This section addresses the registration and issuance phases for both individuals and devices.

4.1 User Registration and Credential Issuance

The registration and identity proofing processes ensure that (a) the individual being registered is in fact the individual who is entitled to the particular identity; (b) an individual exists with the claimed attributes and that the attributes are sufficient to uniquely identify an individual within a given context; and (c) documentation is in place to make it difficult for an individual to repudiate participation in the registration process and dispute authentications performed with their credential. As part of the registration process, an individual provides proof that they are entitled to the particular identity that they are claiming. Examples of documents that can help to provide acceptable proof include U.S. passports, state issued driver's licenses, and social security cards. Individuals may also be subject to background and credit history checks and requirements vary based on an organization's needs. The collected information is verified and the method of verification plays a large role in the resulting level of assurance.

Identity proofing can be performed remotely or by having the individual physically present. When an individual is physically present during the identity proofing process, it is referred to as in-person identity proofing. When in-person identity proofing is impractical, remote identity proofing can be performed at a lower level of assurance.

If the identity proofing process determines that an individual is entitled to a given identity, the issuance phase begins. The issuance process binds a particular identity to a specific token creating a new credential within the identity management system. Alternatively, a user may already have an existing token that will need to be registered into the existing identity management system. Similar to the registration process, the credential issuance can occur in-person or be provisioned remotely. When remote identity credential issuance takes place, care needs to be taken to ensure that the token's confidentiality and integrity are protected when transporting the token between the identity management system and individual. The type of credentials and tokens issued, alongside whether in-person or remote credential issuance takes place impacts the level of assurance provided by the credential.

Once a credential is established, an identity management system may allow a new derived credential to be issued based on an individual demonstrating possession of a valid established identity credential. A derived credential streamlines the registration process by leveraging the results of the identity proofing previously performed for the established identity credential.

The issuance of derived credentials can be in-person or remotely. When the token of a derived credential is remotely delivered, best practices for token activation dictates using proof of possession for both the derived and original credentials. To ensure that the original credential was not compromised at the time the derived credential was established, its status should be re-confirmed at a time after the derived credential was issued. In addition, the issuer of the derived credential may wish to regularly monitor the status of the original credential depending on how tightly their policies tie the status of the original and derived credentials together. When the derived credential is revoked, it is up to the issuing organization's policies whether or not to notify the issuer of the original credential used as the basis for the derived credential. Notification of the issuer of the original credential may result in the original credential being revoked.

NIST 800-63 provides more details and provides specific requirements related to registration, identity proofing, derived credentials, and credential issuance. A summary of the identity proofing and credential issuance for various levels of assurance can be found in Appendix C.

4.2 Device Registration and Issuance

This section discusses the registration and issuance phases of the identity management process for devices. Similar to individuals, the goal of device registration and issuance is to create a device credential containing an identity and token associated with the device. Mobile devices can have completely distinct user and device identities and there is a fundamental difference between establishing the identity of an individual versus the identity of a device. In the context of the NPSBN, device credentials would primarily be used to gain access to the network while user credentials would be used for gaining access to information and services such as criminal justice information and records management systems. Devices residing on the network such as firewalls, servers, and switches, may also need a device identity.

Various attributes are created and associated with individuals over time, such as date of birth, driver's license number, and credit ratings. At some point, the number and type of attributes associated with an individual provides sufficient evidence to satisfy an organization's policies for establishing and verifying identities. In contrast, devices generally do not accumulate the same type of attributes to establish a verifiable identity, thus limiting the effectiveness of the traditional identity proofing for devices. Instead of using the notion of identity proofing for devices, understanding how attributes can be assigned to uniquely identify a device, the stability of the assigned identity, and the assurance provided in the identity assignment process may be more appropriate.

Device identities can be assigned as part of a device's manufacturing process, configuration process, or dynamically while the device is in use. When assigned as part of the manufacturing process, device identities can be made fairly static by being placed into hardware or firmware components. Manufacturer created identities come from an authoritative source and have the greatest potential to be stable over a device's lifetime. Unique device identifiers are useful for a manufacturer's inventory control and quality assurance processes and therefore should be unique to each device. Device identities could be modified or spoofed during creation and how to prevent the modification of manufacturer components at the manufacturing facility and ensure the detection of counterfeit components is an open area of research. NIST provides guidance for addressing information and communications technology supply chain risk, which may be helpful in addressing counterfeit component detection and device identity modification and spoofing [17].

When device identities are assigned as part of the configuration process, they have the potential to remain relatively stable since they might only be configurable once or require the configuration process to be performed in order to change the previously assigned identity. Since device owners generally assign the device identities, the amount of assurance provided by these identities is less than what manufacturers offer. However, these identities may not be enough to uniquely identify a device, since there is no way to ensure different devices owners do not assign the same identity to other devices.

Assigning identities while a device is in use is typically the least stable and least authoritative means of identification and accordingly provides the least assurance in the device's identity. Multiple entities can potentially be concurrently assigning identities, but only for a limited timeframe or context. Therefore this type of device identity could change every time the device is used. Stable and authoritative identities are preferred. Insecure device credentials could be exfiltrated from mobile devices and used for malicious purposes, such as accessing the NPSBN in an effort to monitor unencrypted traffic or affect other systems during an emergency situation.

Once a device identity has been established, the issuance phase begins. As for individuals, the device issuance process binds a particular identity to a specific token creating a new credential within the identity management system. Alternatively, a device may already have an existing token generated by the device's manufacturer or owner that will need to be registered into the existing identity management system. Similar to the registration process, the credential issuance can occur in-person at the location where the device is manufactured or configured by its owner; or be provisioned remotely. When remote device credential issuance takes place, care needs to be taken to ensure that the token's confidentiality and integrity are protected when transporting the token between the identity management system and device. The type of credentials and tokens issued, alongside whether in-person or remote credential issuance takes place impacts the level of assurance provided by the credential.

There are many public safety scenarios that may require device identities. Device identities could help ensure that only authorized devices are able to access the NPSBN, leading to at least a partially closed network. Device identity plays an important role if mobile devices are to be shared between multiple users. Device sharing between users, regardless if it is within a single jurisdiction or loaned externally, may necessitate the use of asset tracking and management systems that could leverage device identities. This is especially true during Bring Your Own Device (BYOD) scenarios where volunteer personnel might use their personal mobile devices to access the NPSBN and other emergency services. Upon conclusion of an emergency scenario with shared devices, these mechanisms could help ensure that loaned devices are returned to the appropriate organization. When devices are shared between public safety personnel of the same organization there should already be an associated device credential provisioned by that organization. There would only be a need to provision devices with the identities of personnel of the upcoming shift. This concept extends to a public safety organization's cache of NPSBN-ready devices, as they already should have been provisioned with a strong device identity.

5. Token Selection in a Mobile Environment

The following provides guidance for selecting tokens in public safety scenarios and is divided into user authentication, remote user authentication, and remote device authentication. The type of authentication solution employed by an organization should be commensurate with the amount of risk posed to a particular information system. This solution should also be compatible with an organization's existing or developing IT infrastructure.

Public safety personnel work in a number of diverse disciplines, such as law enforcement, medical, fire safety. The specific type of environment someone is working in greatly impacts the authentication mechanism they can use. There may not be a single authentication solution that works for every discipline, even within a given jurisdiction. Some public safety scenarios require gloves or simultaneous access to multiple mobile information systems, while others require constant access to restricted public safety information. The feasibility of all authentication solutions should be assessed in accordance with public safety requirements and with the recognition that authentication technologies deployed in the near-term will need to adapt to the evolution of authentication technologies.

5.1 Local User Authentication

Local authentication occurs when a user inputs a PIN or uses a biometric reader (e.g., sensor for reading fingerprints, camera for iris scanning, microphone for voice authentication) to access their mobile device, typically granting access past a lockscreen. At this time, PINs, passwords, gestures, and fingerprint scanners are the most common form of local authentication and serve as the first line of defense against malicious attempts to access a mobile device's data and functionality. The authentication mechanisms described in the following sections are grouped into the *something you know*, *something you have*, and *something you are* categories.

5.1.1 PINs, Passwords, and Gestures

PINS, passwords, and gestures are all *something you know* and are sometimes referred to as memorized secret tokens. These tokens are the current de facto standard for local authentication on a mobile device, although this is slowly beginning to change due the influence of biometric technology. Many users have expressed dissatisfaction with using passwords on mobile devices, as they frequently make entry errors and must manually manage multiple passwords/PINs for a plethora of sites and portals [18]. In the case of public safety, operational requirements may either prohibit or constrain the ability of a first responder to authenticate to the device using a PIN, password, or gesture. During emergency circumstances, speed and ease of access may be the functional requirements of the user, which must be balanced with the security requirements of the network. For instance, the members of the fire service may find these authentication solutions disadvantageous due to their need for equipment designed to protect them from extreme temperatures and smoke inhalation.

These credentials are vulnerable to attacks, such as automated credential guessing attacks, offline credential guessing attacks, and shoulder surfing found in desktop computer systems. The default length of a PIN for many mobile platforms is 4 digits resulting in only 10,000 possible combinations.[8] Mobile device management systems can assist administrators by enforcing policies for longer and more complex PINs and passwords, resulting in a stronger, yet less usable authentication mechanism. To help alleviate a

[8] Larger numbers of combinations are associated with greater strength.

portion this problem, alternative password entry schemes like *fastwords* have been proposed to increase the usability and security of mobile password entry [19].[9]

Gesture-based memorized secret tokens take a variety of forms, such as the Android pattern lock, where users connect a series of dots on a lockscreen. Another type of gesture is to draw a simple image onscreen, such as a triangle within a circle, but this has not been widely implemented. Unique attacks exist for gestures, specifically the Android pattern lock, which is vulnerable to “smudge attacks.” These attacks use cameras under specific lighting to view the residue left by a user’s skin on the glass of the device to infer information about the gesture in order to bypass the lockscreen [20]. One weakness of the PINS, passwords, and gestures authentication model for public safety is the need for the user to interface with buttons or a touch-screen. The operational requirements of the fire service make this functionally improbable as they wear gloves and equipment designed to protect them from extreme temperatures and smoke inhalation. That equipment creates physical barriers between them and the device and makes manipulating an interface difficult, impractical, or impossible. To that end, a balance must be developed between their operational requirements and the need to authenticate users to the network.

5.1.2 Physical Tokens

Physical tokens are *something you have* and are currently an uncommon form of local authentication for mobile devices. However, forthcoming proximity token technologies can leverage radio frequencies to support authentication between devices.

Proximity tokens could be used to unlock a mobile device when the token is within a very close range to a mobile device. These tokens, possibly using near field communication (NFC), radio-frequency identification (RFID), Bluetooth, or other wireless technologies, could be worn as rings, on sleeves, or elsewhere on a public safety user’s body. The specific location on the body or equipment these tokens would be placed is scenario dependent. Other factors, such as an organization’s policies, will dictate how long a device remains unlocked and how often it needs to communicate with the user’s proximity token. Depending on the needs of a jurisdiction, it may be useful to require a separate form of authentication such as a PIN, password, or gesture when first authenticating. This technology is not widely used but is gradually becoming feasible to implement.

Besides proximity tokens, it is possible to leverage the Universal Integrated Circuit Card (UICC) residing within many mobile devices to store software cryptographic tokens for authentication. The UICC is the next-generation Subscriber Identity Module (SIM) card contained in modern mobile devices running the Universal Subscriber Identity Module (USIM) application used for authentication in LTE cellular networks. Although not currently implemented, it is possible that a user could locally authenticate to a lockscreen via a PIN, which would in turn communicate with the USIM for verification. An alternative approach would be to insert and remove the UICC in a manner similar to a smartcard. Removing a USIM from a mobile device is generally difficult and could result in an untenable authentication situation for the user if it needs to be performed regularly. Therefore, the UICC password would best be used as an additional multifactor authentication mechanism, in a manner similar to a Basic Input/Output System (BIOS) password instead of the primary local authentication method.[10]

Although uncommon, physical tokens for generating one-time passwords and smartcards can also be used for local authentication to mobile devices. External smartcard readers can be connected to a mobile device

[9] Fastwords is an alternative to the traditional username/password paradigm leveraging error correcting mechanisms to facilitate password entry.

[10] The BIOS provides fundamental system firmware by initializing hardware upon boot and transferring control to the operating system. A BIOS password can be enabled to locally authenticate users immediately after a system powers on but before the operating system is loaded.

via an USB, Bluetooth, or an NFC interface to leverage existing smart cards. These concepts will be further explored within the remote authentication sections.

5.1.3 Biometrics

Biometric tokens are *something you are* and are gradually becoming a common form of local authentication for mobile devices. Many types of biological and physiological characteristics can be used for authentication, such the iris, face, voice, palm, and fingerprint but most are not commonly used in conjunction with mobile devices. In addition to physical characteristics, behavioral characteristics like how a user inputs text into a keyboard can be used for authentication. The gyroscopes, accelerometers and other sensors included within mobile deices allow for additional behavioral characteristics such as how a user walks, also known as their gait, to be used. Many first responders are required to wear gloves, masks, or other tactical gear that could infringe on the ability to accurately use biometric authentication systems.

The False Accept Rate (FAR) and False Rejection Rate (FRR) are measurements used to ascertain the correctness of biometric system. Biometric authentication systems are often bypassed via spoofing attacks in which fake biometric samples, such as a picture of a person, are presented to the authentication system. Liveness tests are the primary defense against spoofing attacks, in which an authentication system attempts to determine if a presented biometric is fake or genuine.

Fingerprint scanners are the most common biometric used in modern mobile devices due in part to the declining cost of fingerprint sensors over the past several years. There are multiple types of fingerprint sensors, such as optical and capacitance, each with unique ways of assessing characteristics of a sample. In general, fingerprint scanners on mobile devices have a smaller surface area than traditional scanners, affecting resolution, which may impact accuracy. Public safety organizations utilizing this technology should be aware of this limitation and vet the technology's ability to meet public safety requirements before implementation in live scenarios. Regardless of the type of fingerprint scanner, certain public safety personnel may find this as an untenable method of authentication. Firefighters, medical examiners, and other public safety personnel need to wear gloves while on duty, rendering their fingers inaccessible to the sensors. Flaws in the liveness tests used to detect spoofing are a common method of bypass, often performed with commercially available equipment and materials - making this a viable attack strategy.

Facial recognition used locally employs a mobile device's camera to take a picture of a user's face and compare it against a representation of that same user's facial characteristics. This authentication mechanism is offered natively by some mobile device platforms and the necessary hardware sensors are built into many mobile devices. In addition to the facial recognition capabilities of the mobile platform, applications can be developed using alternative recognition algorithms and implementations. Common bypass methods include presenting pictures, videos or a physical mask of the original individual to the camera to fool the authentication system. Liveness tests may require a user to perform an action such as blinking or moving their head.

Users are becoming accustomed to interacting with their mobile devices via voice due to the increased usage of voice-activated digital assistants and the rising accuracy of text-to-speech and speech-to-text. This technology can be extended to leveraging a user's voice for authentication purposes. Voice recognition takes a voice sample of user via the mobile device's microphone to identify 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. Voice recognition systems may be unsuitable for members of the fire service and other public safety personnel wearing masks or other headgear. Common methods of bypassing voice recognition systems include replaying an audio recording of a person's voice to the voice recognition system.

5.2 Remote User Authentication

Passwords, smartcards, and biometrics can be used for remote user authentication for mobile devices. Remote authentication differs from local authentication in that many untrustworthy entities exist between the user and the entity performing verification. It is common for remote authentication protocols to send information over an untrusted network. An example of remote authentication is the use case described in section 3.3 where a detective remotely accesses criminal justice information via a VPN.

5.2.1 PINs, Passwords, and Gestures

The considerations for PINs, passwords, and gestures for remote authentication are similar to those used for local authentication. NIST SP 800-63 classifies these tokens as memorized secret tokens. These tokens are only capable of attaining assurance level 1 or 2. PINs, passwords, and gestures are often used in conjunction with biometric data or cryptographic keys to reach higher levels of assurance. For instance, a password and a cryptographic key together form a multi-factor software cryptographic token.

5.2.2 Biometrics

The biometric authentication mechanisms available for remote authentication are in large part similar to those available for local authentication. One key difference is that when using multi-factor tokens with biometric information for local authentication, the verification process occurs without any information leaving the token, such as ‘on-the-card’ verification. When using remote authentication techniques, verification can occur on backend systems residing external to the mobile device. The increased computational ability provided by these backend systems can lead to greater accuracy, potentially providing a stronger form of authentication. NIST SP 800-63 does not consider a biometric as an acceptable token for remote authentication and requires that biometrics are used in conjunction with another factor as is the case when proving possession of a cryptographic key. Therefore, NIST SP 800-63 provides no guidance for determining the strength of single factor biometric authentication solutions.[11]

5.2.3 One-Time Password Devices

One-time password devices are physical devices used to generate a password with a short lifespan. NIST SP 800-63 classifies these devices as either single-factor or multi-factor one-time password tokens. In absence of an additional authentication factor, the user provides an acceptable one-time password from the token to another information system in a manner similar to password entry. OTP devices are commonly deployed alongside memorized secret tokens to result in a multifactor solution.

5.2.4 Attached Smartcard Reader

In compliance with Homeland Security Presidential Directive 12 (HSPD-12), smartcards were deployed throughout the federal government and other organizations. Smartcards can be used to store credentials and contain a processor capable of performing complex cryptographic operations. When used in conjunction with a PIN, these devices are referred to as multi-factor cryptographic tokens capable of reaching assurance level 4. 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. Smartcard readers can be connected to mobile devices via USB, Bluetooth, or other available interfaces to read credentials

[11] Specifically, NIST SP 800-63 states: Biometric characteristics do not constitute secrets suitable for use in the conventional remote authentication protocols addressed in this document either. In the local authentication case, where the Claimant is observed by an attendant and uses a capture device controlled by the Verifier, authentication does not require that biometrics be kept secret. This document supports the use of biometrics to “unlock” conventional authentication tokens, to prevent repudiation of registration, and to verify that the same individual participates in all phases of the registration process.

stored on smartcards. If large numbers of public safety personnel have already been issued a PIV or PIV-I related smartcard, there may not be a need to issue new tokens and credentials for those employees.

To authenticate with a smartcard, a user needs to insert their smartcard into the card reader, which must be connected to their mobile device. Although this may seem to be an attractive solution, this approach may introduce significant usability concerns. Active public safety personnel would be required to always carry an external card reader, which may have an undesirable form factor, with them and ensure that the reader stays connected to their mobile device in order to access critical external resources. Many public safety personnel already carry large amounts of equipment and may require immediate access to critical information during a life-threatening situation.

5.2.5 NFC Smartcard

NFC smartcard readers can address the usability concerns of using external smartcard readers with mobile devices. 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. This approach achieves multifactor authentication without the aforementioned bulky external card reader.

NFC technology has not been adopted by all mobile device manufacturers or mobile operating system developers. Therefore, organizations relying on NFC-capable devices will need to carefully select their mobile devices to ensure NFC-compatibility. Since jurisdictions may need to provide information and services to neighboring jurisdictions, it may be wise to have an additional authentication solution available for those without an NFC-capable device. Attacks on NFC technology have thus far focused on the NFC application stack, eavesdropping of the wireless information exchange, and presentation attacks via NFC tags [21] [22]. Sniffing NFC traffic has been accomplished using specialized equipment from ranges farther away than what is advertised by the NFC specification.

5.2.6 Software Cryptographic Tokens

In the absence of specialized equipment to incorporate smartcards and other physical tokens, multifactor software cryptographic tokens could be utilized. These tokens would be protected by a memorized secret token and stored within a mobile device's non-removable internal storage or other trusted storage location (e.g., host card emulation [23]). Protecting software tokens using software-based mechanisms potentially increases the risk that the credential could be stolen – hardware-based storage is preferred to software-based mechanisms for credential storage. Authentication would be accomplished via the mobile operating system or some other external application. All major mobile platforms provide interfaces for storing and using software-based digital certificates.

As discussed in section 3.1, new credentials can be derived from existing PIV credentials and issued to users with mobile devices. These credentials could be remotely provisioned to users who successfully authenticate with their PIV card, although this reduces their overall assurance level, whereas derived credentials provisioned in-person and meeting the requirements of NIST SP 800-157 could maintain level of assurance 4. Security and interoperability testing would likely be required for widespread use.

5.2.7 Removable Hardware Security Modules

Hardware security modules are physical devices providing trusted storage and other cryptographic operations such as encryption/decryption and digital signatures. USB and MicroSD security tokens are a common example of these types of tokens, and can contain a processor providing capabilities similar to that of a smartcard. These removable hardware tokens can be used to store software cryptographic credentials and other sensitive information while providing tamper resistance. Another example is the UICC residing within a mobile device, which can technically be removed from a device with some effort. USB and MicroSD tokens can be more easily be inserted and removed from a mobile device as needed – provided that a mobile device has the correct physical interface for the token. Currently, there is no single hardwired data interface across all commercial phones, with the possible exception of the auxiliary audio port, which is only capable of low data transfer rates but it is possible that this transfer rate may be sufficient for authentication.

5.2.8 Embedded Hardware Security Modules

Embedded hardware security modules are similar to removable hardware security modules, except that they cannot be removed from a mobile device. It is becoming increasingly common for mobile devices to have embedded hardware security modules, which are often distinct chips built into a mobile device. These modules provide authentication capabilities without the need for external hardware. Like removable hardware security modules, they typically have the ability to securely store cryptographic keys and perform cryptographic operations in hardware. This approach potentially provides unique security features not supported by other approaches, as small, trusted hardware is often presumed to provide a greater level of assurance in their operation. Many modern mobile devices provide some form of embedded hardware token but mobile operating system vendors and hardware manufacturers often restrict access by third-party developers. Therefore, specific approaches will depend on whatever hardware, firmware, and software support is ultimately provided by these parties.

5.3 Remote Device Authentication

Remote device authentication will be the method of authentication mobile devices use to gain access to the NPSBN. Software and hardware tokens can be leveraged for remote device authentication and used in a manner similar to remote user authentication. After provisioning, these devices could then prove its identity to a verifier by proving knowledge of a credential. This approach may require the establishment and management of a public key infrastructure (PKI) and for this, the existing Federal PKI could be leveraged. A greater level of assurance would be achieved if credentials were stored in hardware protected storage locations. A major difference would be the lack of user interaction in providing a password or PIN to unlock a credential for use.

It is possible that during an emergency, the NPSBN will not function as intended, possibly due to the NPSBN directly being attacked (e.g., jamming) or some other reason (e.g., flood, terrorist attack). In the instance of the network ceasing to function, devices may still be able to operate by communicating via the cellular tower, without the use of the core network. Alternatively, devices could communicate directly to each other completely bypassing the cellular towers. Devices would still need to authenticate to each other during these scenarios, possibly leveraging cached digital certificates and certificate status information. Another example of device to device authentication is two servers running public safety services mutually authenticating each other before sharing information.

6. The Authentication Process

During the usage phase of the identity management lifecycle, individuals and devices use their credentials to gain access to information and services provided by applications and service providers. To ensure that an individual or device gains access only to the information and services they are entitled to, applications and service providers need to establish confidence in a claimed identity.

6.1 Authentication Protocols

Authentication protocols establish confidence in the claimed identity. Authentication protocols use a set of messages to ensure an individual or device has control of a specific valid token. Determining whether or not a credential is still valid and has not been revoked, suspended, or expired is key to the authentication process. Protocols can also assist communicating parities to know who or what they are communication with. The level of assurance that can be placed in the claimed identity will be influenced by the authentication processes and protocols used.

An authentication protocol is one part of the overall authentication process and the strength of an authentication protocol depends heavily on the types of threats a protocol is designed to resist. NIST 800-63 derives level of assurance for protocols based on these threats. Examples of threats an authentication protocol may protect against are eavesdropping, replay attacks, and man-in-the-middle attacks. Attacks such as phishing, pharming, denial of service attacks, and malicious code may be outside of the scope of a protocol's ability to defend against. However, the threats that an authentication protocol cannot protect against may be mitigated by other parts of the authentication process. Protocols are situation specific and those used for device authentication likely do not need to defend against the same set of threats that protocols used for user authentication would, as phishing and social engineering are not possible in this scenario.

6.2 Assertions

Once the authentication process and protocols have been completed, the entity (application, service provider, or third party verifier) will either be satisfied or not (a successful or unsuccessful authentication, respectively) about the confidence that can be placed in the claimed identity. If the authentication process has been successful, the entity may issue statements about the claimed identity referred to as assertions. Assertions can be issued by entities, such as third party verifiers, directly to the individual or device, which presents the assertion to the application or service provider. Alternatively, the application or service provider can receive the assertion directly from the entity issuing the assertion. In this case, either an assertion reference[12] is provided to the individual or device that is then presented to the application or service provider; or the verifier acts as a proxy between the individual or device and the application or service provider. Advantages of the entity acting as proxy include providing access to multiple applications and services providers at one time, enabling network monitoring and filtering, and enhancing web caching. Based on the assertions received, the applications and service providers determine the appropriate privileges or access to information and services that they should provide to the particular individual or device.

Assertions can be expressed using various technologies such as cookies, Security Assertion Markup Language (SAML), and Kerberos tickets. SAML is an XML-based framework for creating and exchanging authentication and attribute information. Kerberos tickets provide strong authentication for

[12] A data object, created in conjunction with an assertion, which identifies the Verifier and includes a pointer to the full assertion held by the Verifier. NISTIR 7298 Revision 2: Glossary of Key Information Security Terms, May 2013. 24. NIST, *NISTIR 7298 Revision 2: Glossary of Key Information Security Terms.*

client/server applications using symmetric-key cryptography. Cookies can be used as an assertion to enable single-sign-on or re-authenticate to a server. Cookies are information (often a string of text) supplied by a web server to be stored temporarily on a visitor's computer that is returned to the server on subsequent visits. Cookies assist web servers in remembering information about a user, essentially keeping state after the closing of the previous connection. The assertion mechanisms included here are only examples as other assertion technologies exist and could be used as part of the authentication process.

Since assertions are a mechanism that enables access to information and services, they are a potential target for attackers so need to be protected against various threats – inappropriate creation, modification, substitution, disclosure, reuse, and repudiation. NIST 800-63 provides more details and specific requirements related to the authentication process, authentication protocols, and assertions.

Appendix A—Acronyms

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

3GPP	3rd Generation Partnership Project
AKA	Authentication and Key Agreement
ATIS	Alliance for Telecommunications Industry Solutions
AuC	Authentication Center
AUTN	Authentication token
BIOS	Basic Input/Output System
DHS	Department of Homeland Security
DOJ	Department of Justice
eNB	eNodeB, Evolved Node B
eNodeB	Evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FAR	False Acceptance Rate
FRR	False Rejection Rate
HSM	Hardware Security Module
HSPD	Homeland Security Presidential Directive
HW	Hardware
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscriber Identity
LTE	Long Term Evolution
LOA	Level of Assurance
ME	Mobile Equipment
MF	Multifactor
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NPSTC	National Public Safety Telecommunications Council
NTIA	National Telecommunications and Information Administration
OMB	Office of Management and Budget
OIC	Office for Interoperability and Compatibility
OS	Operating System
OTP	One Time Password
P-GW	Packet Gateway
PKI	Public Key Infrastructure
PSCR	Public Safety Communications Research
PSTN	Public Switched Telephone Network
RAND	Random
RES	Response
SAML	Security Assertion Markup Language
SIM	Subscriber Identity Module
SF	Single factor
SoC	System on a Chip
SQL	Structured Query Language
SSL	Secure Sockets Layer
S-GW	Serving Gateway
UE	User Equipment
UICC	Universal Integrated Circuit Card

USB	Universal Serial Bus
USIM	UMTS Subscriber Identity Module
VPN	Virtual Private Network
XML	Extensible Markup Language
XRES	Expected response

Appendix B—References

Selected acronyms and abbreviations used in this interagency report are defined below.

1. NIST, *Special Publication (SP) 800-63-2: Electronic Authentication Guideline*. 2013.
2. OMB, *OMB M-04-04: E-Authentication Guidance for Federal Agencies.* 2003.
3. NIST, *SP 800-30 Revision 1 Guide for Conducting Risk Assessments*. 2012, National Institute of Standards and Technology.
4. NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems.* 2010.
5. NIST, *Special Publication (SP) 800-53-4 Security and Privacy Controls for Federal Information Systems and Organizations.* 2013.
6. NIST, *FIPS Pub 199 Standards for Security Categorization of Federal Information and Information Systems* 2004, National Institute of Standards and Technology.
7. *Homeland Security Presidential Directive 12*. 2004.
8. NIST, *Federal Information Processing Standard (FIPS) 201-2 (PIV) Personal Identity Verification (PIV) of Federal Employees and Contractors.* 2013.
9. Federal CIO Council, *Personal Identity Verification Interoperability For Non-Federal Issuers*. July 2010.
10. NIST, *Special Publication (SP) 800-157: Guidelines for Derived Personal Identity Verification (PIV) Credentials.* 2014.
11. NIST, *DRAFT NISTIR 7981: Mobile, PIV, and Authentication.* 2014.
12. Federal Bureau of Investigation, *Criminal Justice Information Services (CJIS) Security Policy*. 2013.
13. Communications, N.P.S., *Public Safety Broadband High-Level Launch Requirements Statement of Requirements for FirstNet Consideration*. 2012.
14. ATIS, *ATIS-1000035.2009: Next Generation Framework (NGN) Identity Management (IDM) Framework.*
15. ATIS, *ATIS-1000044.2011: ATIS Identity Management: Requirement and Use Cases Standard.*
16. ATIS, *ATIS-1000045.2012: ATIS Identity Management: Mechanisms and Procedures Standard.*
17. NIST, *(Second Draft) NIST Special Publication 800-161*. 2014.
18. Jakobsson, M., et al., *Implicit Authentication for Mobile Devices*, in *Usenix*. 2009.
19. Jakobsson, M. and R. Akavipat, *Rethinking Passwords to Adapt to Constrained Keyboards.* 2011.
20. Adam J. Aviv, K.G., Evan Mossop, Matt Blaze, and Jonathan M. Smith, *Smudge Attacks on Smartphone Touch Screens.* Usenix Workshop on Offensive Technologies, 2010.
21. Miller, C., *Don’t stand so close to me: An analysis of the NFC attack surface*, in *Blackhat* 2012.
22. Haselsteiner, E. and K. Breitfuß, *Security in Near Field Communication (NFC): Strengths and Weaknesses*, in *Workshop on RFID security*. 2006.
23. Google. *Host-based Card Emulation*. [cited 2014; Available from: http://developer.android.com/guide/topics/connectivity/nfc/hce.html.
24. NIST, *NISTIR 7298 Revision 2: Glossary of Key Information Security Terms.*

Appendix C—Summary of Identity Proofing and Credential Issuance Requirements

This appendix contains a summary of the identity proofing and credential issuance requirements for the different level of assurance from the requirements found in NIST 800-63. For more specific details, or to resolve ambiguities, about the requirements found in this appendix, the identity proofing and credential issuance requirements found in NIST 800-63 are authoritative and take precedence. The identity proofing and credential issuance requirements for each level of assurance are presented separate tables within this appendix.

The following table provides an example of how the identity proofing and credential issuance requirements are presented for a given level of assurance.

<table>
<tr><th colspan="4">Level of Assurance X Identity Proofing and Credential Issuance Requirements</th></tr>
<tr><td rowspan="2">In-person</td><td>Requirement A</td><td>Requirement B</td><td>Requirement C</td></tr>
<tr><td colspan="3">Requirement D</td></tr>
<tr><td rowspan="3">Remote</td><td rowspan="2">Requirement E</td><td colspan="2">Requirement F</td></tr>
<tr><td colspan="2">Requirement G</td></tr>
<tr><td colspan="3">Requirement H</td></tr>
</table>

In-person and Remote identity proofing can be used to meet the given level of assurance.

In-person identity proofing and credential issuance has to satisfy either requirement A OR requirement B OR requirement C. In addition, In-person identity proofing and credential issuance has to satisfy requirement D.

Remote identity proofing and credential issuance has to satisfy either requirement E OR [requirements F AND G]. In addition, Remote identity proofing and credential issuance has to satisfy requirement H.

Level of Assurance 1 Identity Proofing and Credential Issuance Requirements	
In-person	No specific requirements
	No specific requirements
	No specific requirements
Remote	No specific requirements
	No specific requirements
	No specific requirements

<table>
<tr><th colspan="7">Level of Assurance 2 Identity Proofing and Credential Issuance Requirements</th></tr>
<tr><td rowspan="6">In-person</td><td colspan="6">Possession of a valid current primary government picture ID</td></tr>
<tr><td colspan="6">Inspection of the photo-ID. Confirms that: name, date of birth, address and other personal information in record are consistent with the application. Compares picture to Applicant and records ID number</td></tr>
<tr><td colspan="2">Verifies photo-ID via the issuing government agency</td><td colspan="2">Verifies photo-ID through credit bureaus</td><td colspan="2">Verifies photo-ID through similar databases</td></tr>
<tr><td rowspan="2">When the photo-ID address and address of record is confirmed, credentials can be issued and notification sent to the address of record.</td><td colspan="5">Credentials are issued in a manner that confirms:</td></tr>
<tr><td colspan="2">The claimed address by the Applicant</td><td colspan="2">The ability of the Applicant to receive email messages at the email address of record</td><td>The ability of the Applicant to receive telephone communications or text message at telephone number of record</td></tr>
<tr><td rowspan="4">Remote</td><td colspan="6">Possession of a valid current primary government picture ID</td></tr>
<tr><td colspan="3">Possession of a financial account number</td><td colspan="3">Possession of a utility account number</td></tr>
<tr><td colspan="6">Inspects both ID number and account number. Confirms that: name, date of birth, address and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual</td></tr>
<tr><td colspan="3">Verifies primary government picture ID number through record checks either with the applicable agency or institution or through credit bureaus or similar</td><td colspan="3">Verifies account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases</td></tr>
</table>

<table>
<tr><td rowspan="4"></td><td>databases</td><td colspan="3">For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity</td></tr>
<tr><td rowspan="2">Credentials are issued in a manner that sends notification to an address of record confirmed by the records check</td><td colspan="3">Credentials are issued in a manner that confirms the ability of the Applicant to receive:</td></tr>
<tr><td>Mail at the physical address of record</td><td>Email messages at the email address of record</td><td>Text message at telephone number of record</td></tr>
<tr><td colspan="4">Any secret sent over an unprotected session shall be reset upon first use and shall be valid for a maximum lifetime of seven days.</td></tr>
</table>

<table>
<tr><th colspan="5">Level of Assurance 3 Identity Proofing and Credential Issuance Requirements</th></tr>
<tr><td rowspan="4">In-person</td><td colspan="4">Possession of a valid current primary government picture ID</td></tr>
<tr><td colspan="4">Inspection of the photo-ID. Confirms that: name, date of birth, address and other personal information in record are consistent with the application. Compares picture to Applicant and records ID number</td></tr>
<tr><td>Verifies photo-ID via the issuing government agency</td><td>Verifies photo-ID through credit bureaus</td><td colspan="2">Verifies photo-ID through similar databases</td></tr>
<tr><td>Credentials are issued in a manner that confirms the claimed address by the Applicant when the credential is issued</td><td>Credential are issued in a manner that sends notification to address of record when the credential is issued</td><td colspan="2">Credential are issued in a manner that confirms the Applicants ability to receive telephone communications at the telephone number of record while recording the Applicants voice or using alternate means that establishes an equivalent level of non-repudiation</td></tr>
<tr><td rowspan="6">Remote</td><td colspan="4">Possession of a valid current primary government picture ID</td></tr>
<tr><td colspan="2">Possession of a financial account number</td><td colspan="2">Possession of a utility account number</td></tr>
<tr><td colspan="4">Verifies the primary government picture ID information provided and confirms that: name, date of birth, address and other personal information in records are consistent with the application and sufficient to identify a unique individual</td></tr>
<tr><td>Verifies the primary government picture ID number through record checks with the applicable agency</td><td>Verifies the primary government picture ID number through record checks with the applicable institution</td><td>Verifies the primary government picture ID number through record checks with credit bureaus</td><td>Verifies the primary government picture ID number through record checks with similar databases</td></tr>
<tr><td colspan="4">At a minimum, the records check for the primary government picture ID number confirms the name and address of the Applicant</td></tr>
<tr><td colspan="2">Verifies the financial account number information provided and confirms that: name, date of birth, address and other personal information in records are</td><td colspan="2">Verifies the utility account number information provided and confirms that: name, date of birth, address and other personal information in records are</td></tr>
</table>

	consistent with the application and sufficient to identify a unique individual	consistent with the application and sufficient to identify a unique individual
	Verifies the financial account information through record checks either with the applicable agency or institution or through credit bureaus or similar databases	Verifies the utility account information through record checks either with the applicable agency or institution or through credit bureaus or similar databases
		For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity
	At a minimum, the records check for the financial account number should confirm the name and address of the Applicant.	At a minimum, the records check for the utility account number should confirm the name and address of the Applicant.
	Credentials are issued in a manner that confirms the ability of the Applicant to receive:	
	Mail at the physical address of record	Messages (SMS, voice, or email) sent to an electronic address that is linked to physical address with the Applicant's name when the electronic address and physical address is consistent with the information provided by the Applicant
	Any secret sent over an unprotected session shall be reset upon first use and shall be valid for a maximum lifetime of seven days	

Level of Assurance 4 Identity Proofing and Credential Issuance Requirements				
In-person	Possession of a valid current primary government picture ID			
	Possession of a second independent Government ID document	Possession of financial account number that can be confirmed		
	Inspects the primary government picture ID. Confirms that: name, date of birth, address, and other personal information in record are consistent with the application. Compares picture to Applicant and records ID number.			
	Verifies the primary government picture ID via issuing government agency	Verifies the primary government picture ID through credit bureaus	Verifies the primary government picture ID through similar databases	
	Verifies the second independent Government ID document. Confirms that the	Verifies the financial account number through record checks	Verifies the financial account number through credit bureaus	Verifies the financial account number through similar databases

	identifying information is consistent with the primary government picture ID.	Confirms that: name, date of birth, address, and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual
	Address of record shall be confirmed through validation of the primary ID	Address of record shall be confirmed through validation of the secondary ID
	Credentials are issued in a manner that confirms the address of record.	
	A current biometric (e.g., photograph or fingerprints) is recorded to ensure that Applicant cannot repudiate application	
Remote Not Admissible	Not applicable	
	Not applicable	
	Not applicable	

1105

Appendix D—Summary of Token Requirements

This appendix contains a summary of the token requirements for the different level of assurance from the requirements found in NIST 800-63. For more specific details, or to resolve ambiguities, about the requirements presented in this appendix, the token requirements found in NIST 800-63 are authoritative and take precedence. The token requirements for each level of assurance are presented separate tables within this appendix.

The following table provides an example of how token requirements are presented for a given level of assurance.

Level of Assurance X Type Tokens			
Token Description	**Requirements**		
Token A Description	Requirement A	Requirement B	Requirement C
	Requirement D		
Token B Description	Requirement E	Requirement F	
		Requirement G	
	Requirement H		

Token A and Token B can be used to meet the given level of assurance.

Token A has to satisfy either requirement A OR requirement B OR requirement C. In addition, Token A has to satisfy requirement D.

Token B has to satisfy either requirement E OR [requirements F AND G]. In addition, Token B has to satisfy requirement H.

Level of Assurance 1 Type Tokens			
Token Description	**Requirements**		
Memorized Secret Token (Something you know)	User chosen string of 6 or more characters from a 90 or more character alphabet	4 or more digit PIN generated randomly	a secret with equivalent strength[13]
	Failed authentication attempts limited to 100 or fewer in any 30-day period		
)Pre-Registered Knowledge Token (Something you know)	The secret provides at least 14 bits of entropy	The entropy in the secret cannot be directly calculated (e.g. user chosen or personnel knowledge questions)	
		No empty answers allowed	
		If the questions are not supplied by the user, the user	

[13] *NIST SP 800-63 Appendix A: Estimating Entropy and Strength* provides guidance on estimating the strength of randomly and user-generated passwords.

		shall select prompts from a set of at least 5 questions
	Failed authentication attempts limited to 100 or fewer in any 30-day period	

Level of Assurance 2 Type Tokens			
Token Description	**Requirements**		
Memorized Secret Token (Something you know)	User chosen string of 8 or more characters from a 90 or more character alphabet	6 or more digit PIN generated randomly	a secret with equivalent strength
	Failed authentication attempts limited to 100 or fewer in any 30-day period		
Pre-Registered Knowledge Token (Something you know)	The secret provides at least 20 bits of entropy	The entropy in the secret cannot be directly calculated (e.g. user chosen or personnel knowledge questions)	
		No empty answers allowed	
		If the questions are not supplied by the user, the user shall select prompts from a set of at least 7 questions	
	Failed authentication attempts limited to 100 or fewer in any 30-day period		
Look-up Secret Token (Something you have)	Token authenticator has 64 bits of entropy	Token authenticator has 20 bits of entropy	
		Failed authentication attempts limited to 100 or fewer in any 30-day period	
Out of Band Token (Something you have)	Token is uniquely addressable and supports communication over a channel that is separate from the primary authentication channel		
	Generated secret has at least 64 bits of entropy	Generated secret has at least 20 bits of entropy	
		Failed authentication attempts limited to 100 or fewer in any 30-day period	
Single Factor One-Time Password Device (Something you have)	One-time password generated by a NIST-approved block cipher or hash function[14]		
	One-time password lifetime limited on the order of minutes		
	FIPS 140-2 Level 1 or higher for the verification function		
Single Factor Cryptographic Device (Something you have)	FIPS 140-2 Level 1 or higher		
	Token generated output (e.g. a nonce or challenge) has at least 64 bits of entropy		

Level of Assurance 3 Type Tokens	
Token Description	**Requirements**
Multi-factor Software Cryptographic Token (Something you have AND Something you know)	FIPS 140-2 Level 1 or higher
	Password or other activation data to activate
	Erasure of unencrypted copy of the authentication key after each authentication
	Token generated output (e.g. a nonce or challenge) has at least 64 bits of entropy

[14] See *NIST FIPS 140-2 Security Requirements for Cryptographic Modules* for further information

Level of Assurance 4 Type Tokens	
Token Description	**Requirements**
Multi-factor One Time Password (OTP) Hardware Token (Something you have AND Something you know)	FIPS 140-2 Level 2 or higher with physical security at Level 3 or higher
	One-time password generated by using an Approved block cipher or hash function
	One-time password lifetime limited to less than 2 minutes
	Password or other activation data entered for each one-time password generated
Multi-factor Hardware Cryptographic Token (Something you have) AND [(Something you are) OR Something you know)]	FIPS 140-2 Level 2 or higher with physical security at Level 3 or higher
	Password, PIN, or biometric to activate
	No authentication key export capabilities
	Token generated output (e.g. a nonce or challenge) has at least 64 bits of entropy

Appendix E—NPSTC Identity Management Requirements

The following are the NPSTC requirements relating to identity management.

Identity Framework Network Service Requirements	
Technology	1. The identity management framework SHALL enable applications and services to securely verify the identity of users.
Technology	2. The identity management framework SHALL be standards based.
Technology	3. Identity assertions SHALL be cryptographically protected when being transmitted from one entity to another in the network.
Technology	4. The identity management framework SHALL issue identities to non-person entities on the network.
Technology	5. The identity management framework SHALL enable non-person entities to authenticate to applications and services where authorized.
Policy	6. The NPSBN SHALL define the process and procedures necessary for organizations (local, tribal, state, and federal) to gain approval to join the trust framework.
Identity Management Framework Requirements	
Policy	1. Governance of individual digital user identities SHALL be maintained by the local, tribal, state, or federal organization from which the user is affiliated.
Policy	2. FirstNet SHALL require that local, tribal, state, or federal organizations establish policies and procedures to govern the digital user identities of users within their respective organizations.
Device Identity Management	
Technology	1. NPSBN devices SHOULD be capable of being shared amongst different authorized human users.
Authentication Services Requirements	
Policy	1. A NPSBN governance framework SHALL be established that identifies a set of security policies for agencies to participate in the identity management framework and to remain included in the framework over time.
Technology	2. The NPSBN SHALL have access to the identity management framework for purposes of user activity monitoring, security monitoring, and application delivery.
Technology	3. The NPSBN identity management framework SHALL enable both NPSBN- and PSE-based applications and services to verify the identities of users irrespective of authorized administrator (both FirstNet and PSEN) management of the user's authentication credentials.
Technology	4. The NPSBN authentication services SHALL support industry standard authentication interfaces for mobile and fixed infrastructure components.
Authorization Services Requirements	
Technology	1. The identity management framework SHALL manage privileges for person and non-person entities.
Technology	2. Services and applications SHALL authorize access to information based on the identity of users, their roles, and other attributes based on policies for the services and applications.

Appendix F—Description of LTE Authentication & Key Agreement

Since the NPSBN will be based on LTE technology, it is important to understand the type of authentication mechanisms provided within that technology. The authentication provided by LTE does not authenticate the user or a mobile device to the network, as only the UICC/USIM is authenticated to the network, which is removable.

At a high level, an LTE network consists of a mobile device, a radio access network consisting of cellular towers, and the core network (i.e. S-GW, P-GW, AuC/HSS, and the IMS) controlled by the network operator. The primary LTE network components are the mobile device and the core network. The mobile device, notated as user equipment (UE), includes a UICC token running the USIM Java application. The USIM contains a secret key *K* that is pre-shared with the network operator. The network operator houses *K* within the Home Subscriber Server (HSS) running the authentication center (AuC), all residing within the core network. The HSS is the master database with subscriber data and the AuC assists in the mapping from an IMSI to the secret key *K*.

The radio network of cellular towers is referred to as the E-UTRAN. UEs connect to the E-UTRAN to send data to the core network. UEs receive control signals through eNodeBs via the MME (Mobility Management Entity). No user traffic is sent through the MME. The MME performs a large number of functions including managing and storing UE contexts, creating temporary IDs, paging, controlling authentication functions, and selecting the Serving and Packet Gateways (S-GW and P-GW, respectively). The S-GW anchors the UEs for intra-eNB handoffs and routes information between the P-GW and the E-UTRAN. The P-GW is the default router for the UE, making transfers between 3GPP and non-3GPP services, and allocating IP addresses to UEs.

In the context of public safety, LTE authenticates the USIM to the network. Each UE contains an IMEI number to identify the mobile device to the network and in newer model phones, this may be stored on the mobile device's internal flash and/or the USIM. Alternatively, the IMSI is used to identify a USIM to the cellular network and is stored within the USIM.

Authentication between the UE and the cellular network is accomplished via the AKA (Authentication and Key Agreement) procedure, more formally known as EPS AKA. The AKA cryptographically proves that both parties have knowledge of the secret key *K*. The AKA procedure is begun once a UE attaches to a network, after which a UE provides its identity to the requesting MME. (The identity may be a temporary or permanent.) The MME then obtains the IMSI associated with the temporary identity, and provides this information, along with additional security parameters to the HSS/AuC to generate an authentication vector.

To compute the authentication vector the HSS/AuC needs to choose a random number (RAND) and use RAND, the secret key K, and the Sequence Number as inputs to a cryptographic function. This function produces two cryptographic keys alongside the expected result (XRES) and authentication token (AUTN). This authentication vector is passed back to the MME for storage and partial transport to the UE.

The MME then provides the AUTN and RAND to the UE, which is then passed to the USIM application. The USIM sends AUTN, RAND, the secret key K, and its SQN through the same cryptographic function used by the HSS/AuC. The result is labeled as RES, which is sent back to the MME. If XRES is equal to RES, then the MME authenticates the UE to the network.