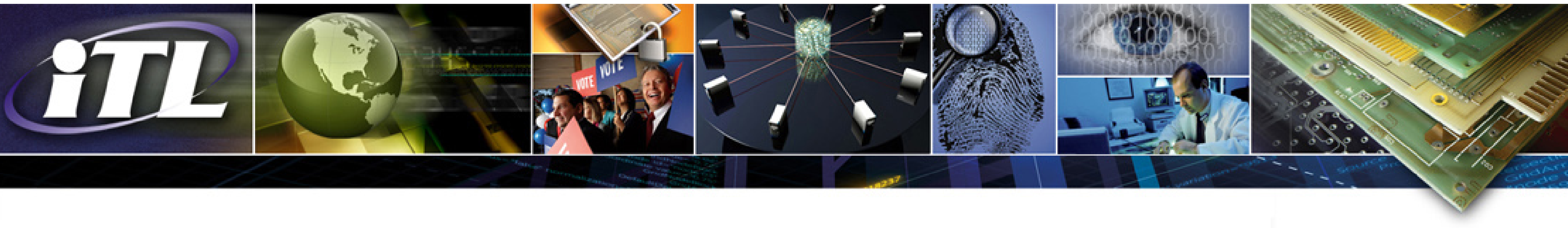


ITL BULLETIN FOR MAY 2015

AUTHENTICATION CONSIDERATIONS FOR PUBLIC SAFETY MOBILE NETWORKS

Nelson Hastings, Joshua Franklin, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

The First Responder Network Authority (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, firefighters, emergency medical services, and other emergency personnel use public safety networks for coordination during emergency situations, disasters, and other incidents.

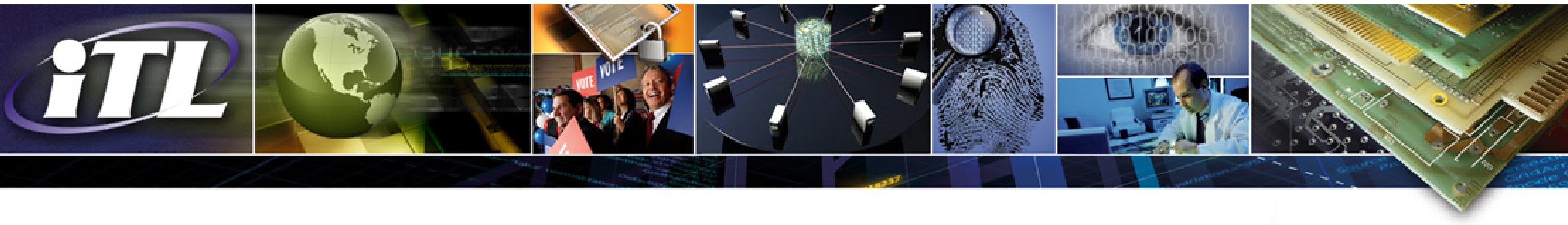
When public safety personnel from separate jurisdictions arrive at the same incident, interoperability problems with communications equipment often arise. The NPSBN will be based on commercial standards, specifically the Long Term Evolution (LTE) family of standards, which should increase interoperability between emergency personnel from distinct jurisdictions when responding to an incident.

A robust approach to identity management will ensure that only authorized users and devices 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.

Introduction

NIST recently released Interagency Report (NISTIR) 8014, *Considerations for Identity Management in Public Safety Mobile Networks*, which assists organizations that are looking to develop requirements for public safety use. The report analyzes approaches to identity management in relation to public safety communications networks with a particular focus on the NPSBN based on the LTE technology.

Although this report is intended to assist policy makers in their decision-making process, it does not suggest policies for use. The particular policies used will depend highly on the network's architecture and security posture.



Identity Management and Authentication

NISTIR 8014 provides background information on identity management and authentication of individuals and devices. It describes the life cycle of a credential, including the following phases:

- Registration
- Issuance
- Usage
- Expiration
- Revocation
- Suspension
- Re-issuance/Updating

In addition, the report describes typical types of tokens, including those used for multifactor authentication.

Identity Management Guidance and Framework

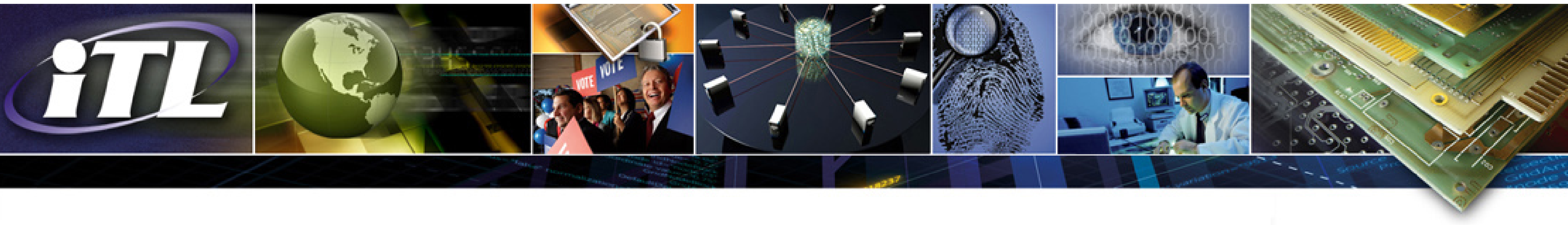
NISTIR 8014 provides a description of existing federal and industry identity management guidance that can inform and influence authentication considerations in public safety mobile networks. Federal guidance includes OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, NIST Special Publication (SP) 800-63-2, *Electronic Authentication Guideline*, and Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, alongside its associated standards and guidelines. Industry guidance includes information from the National Public Safety Telecommunications Council (NPSTC) and the Alliance for Telecommunications Industry Solutions (ATIS) guidance and frameworks.

Registration and Issuance

The report addresses the first two phases of the identity management life cycle. NISTIR 8014 describes the registration and issuance phases for both individuals and devices requiring access to public safety networks. These phases and their associated processes form the foundation for the level of assurance that should be placed in identities, credentials, and tokens, which will be leveraged by those interacting with emergency systems.

The registration and identity proofing processes ensure that:

- The individual being registered is in fact the individual who is entitled to the particular identity;



- An individual exists with the claimed attributes and that the attributes are sufficient to uniquely identify an individual within a given context; and
- 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.

Individuals also provide proof that they are entitled to the particular identity that they are claiming.

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. 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.

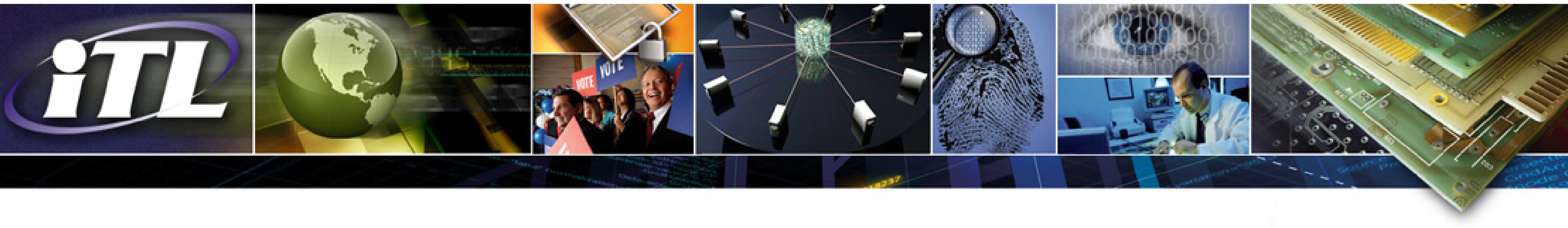
Each of these identities is especially important for sharing mobile devices between multiple users, as is commonplace with public safety personnel performing shift work.

Token Selection in a Mobile Environment

NISTIR 8014 provides guidance on how to select tokens in public safety scenarios, including user authentication, remote user authentication, and remote device authentication. An organization should select an authentication solution based on the amount of risk posed to a particular information system. This solution should also be compatible with an organization’s IT infrastructure.

The report describes the authentication mechanisms that are grouped into the *something you know*, *something you have*, and *something you are* categories. NISTIR 8014 provides a variety of credentials and describes common methods of bypass. It emphasizes that a balance must be developed between operational, functional, and security requirements to select an appropriate authentication technology.

For information purposes, NISTIR 8014 contains a summary of the identity proofing and credential issuance requirements and the token requirements for the different levels of assurance from NIST SP 800-63-2. The report also contains a summary of the NPSTC requirements on identity management provided in NPSTC’s Public Safety High-Level Launch Requirements.



Conclusion

NISTIR 8014 analyzes approaches to identity management to assist organizations developing requirements for use in the nationwide public safety network. In particular, this analysis covers a variety of technologies that allow public safety personnel and devices used to authenticate to systems used in response to disasters, to successfully complete their missions.

Currently, there is no immediately implementable authentication approach that can be recommended to all members of the public safety community. The requirements mandated by each public safety discipline will dictate if a given authentication technology is both usable and secure within a specific context.

New biometric capabilities and other, increasingly robust features in mobile devices necessitate additional research from a public safety perspective. Further research is needed to ensure that these technologies are accurate and that generally accepted methods of testing and/or verifying biometric technologies exist. Another general class of technologies requiring additional study is wearable technology. NISTIR 8014 only briefly explores the possibilities offered by wearable devices in a public safety context, but as the technology becomes more prevalent, new and novel applications may begin to surface, pushing today's boundaries.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.