Mobile Identity Management for Public Safety

Joshua Franklin
Computer Security Division

Yee-Yin Choong
Kristen Greene
Information Access Division

NIST

Cyber Innovation Forum
September 9 - 11, 2015

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.

Agenda

- Introduction
- NIST's identity management research efforts
- Relevant standards and guidance
- Credentials for first responders
- Applying this to public safety
  - Fire, EMS, Law enforcement
  - Usability
- Next Steps

Background

- The *Middle Class Tax Relief and Job Creation Act of 2012* created the First Responder Network Authority (FirstNet)
- Public Safety Communications Research (PSCR) Program (http://www.pscr.gov)
  - Joint NTIA/NIST research program based in Boulder, CO
  - Focusing on standards, network modeling/simulation, audio/video quality, and security
- Sponsored in part by DHS OIC (http://www.dhs.gov/st-oic)

FirstNet Operation

- FirstNet will run a cellular network for use by public safety:
  - EMS, Fire, Law enforcement, etc.
- Based on "4G" LTE technology
- Modern mobile devices will be used to access the network
- How do we ensure that the right people and the right devices get on the network?

Research Directions

- Need to understand how first responders authenticate now
- NIST working to provide guidance and analysis to public safety for:
  - Identity management
  - Federated identity and trust frameworks
  - Analysis of discipline-specific needs

NIST's Current Status

- NISTIR 8014 – *Considerations for Identity Management in Public Safety Networks*
  Status: **Complete**[PDF]
- *Usability and Security Considerations for Mobile Authentication in Public Safety*
  Status: **In-progress**

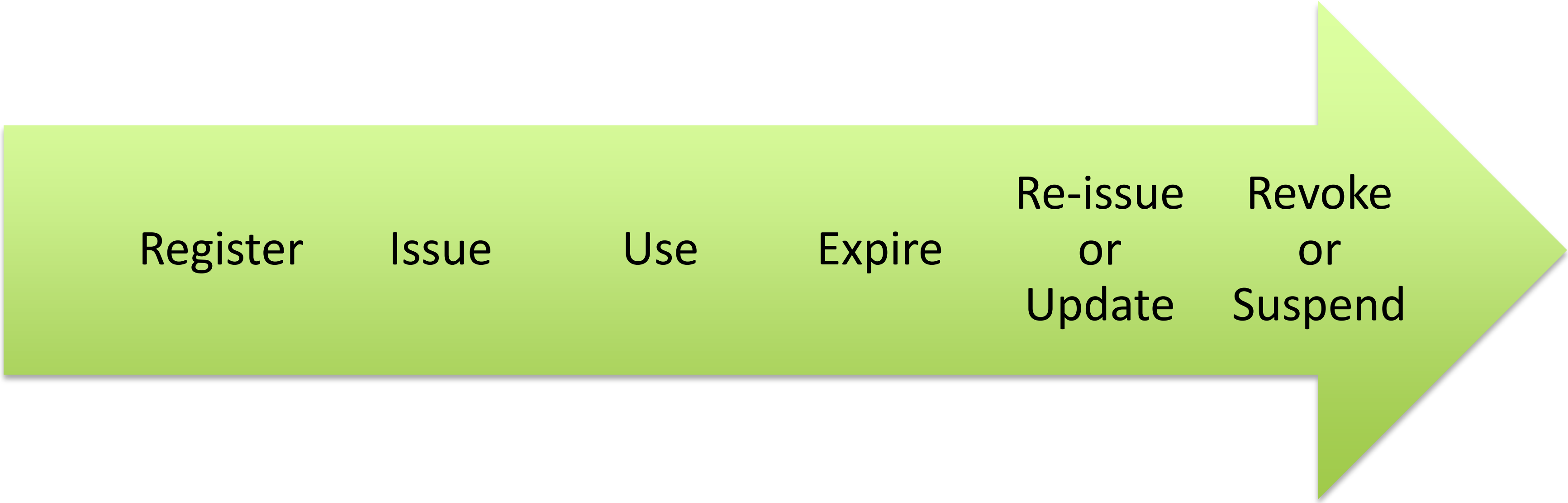
NISTIR 8014

- NIST first authored *Considerations for Identity Management in Public Safety Networks*
- Based on public safety's needs and requirements described by the National Public Safety Telecommunications Council (NPSTC)
- NISTIR 8014 covers:
  - Identity management basics
  - Guidance and Frameworks
  - Token registration and issuance
  - Mobile credentials and token selection
  - Authentication processes

Identity Management (IdM)

- IdM is the process of managing the identification, authentication, and authorization of entities
- **Identification**: making an identity claim
- **Authentication**: providing evidence for an identity claim
- **Authorization**: determining and enforcing access

Identity Management Lifecycle


Register

Issue

Use

Expire

Re-issue or Update

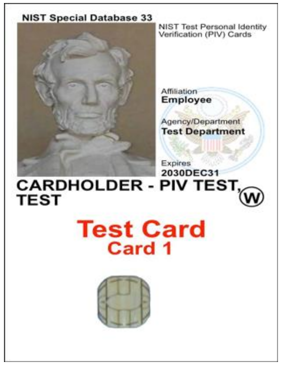
Revoke or Suspend

Token Issuance

- Credentials bind an identity to a token
- Tokens are used to authenticate
- How a token is created and issued as an impact on its overall *level of assurance*
  - Tokens can be distributed in-person or remotely

Examples of Tokens

One Time Password Generator


NIST Special Database 33

NIST Test Personal Identity Verification (PIV) Cards

Affiliation
Employee

Agency/Department
Test Department

Expires
2030DEC31

CARDHOLDER - PIV TEST, TEST

Test Card
Card 1

PIV Card

Fingerprint

p@$$w0rd

Password

Multifactor Authentication

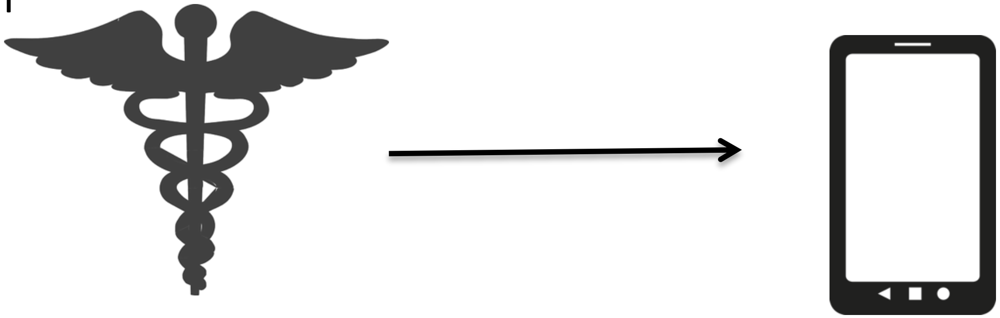
Something you know	Something you have	Something you are
Password	PIV Card	Fingerprint

Authentication Process

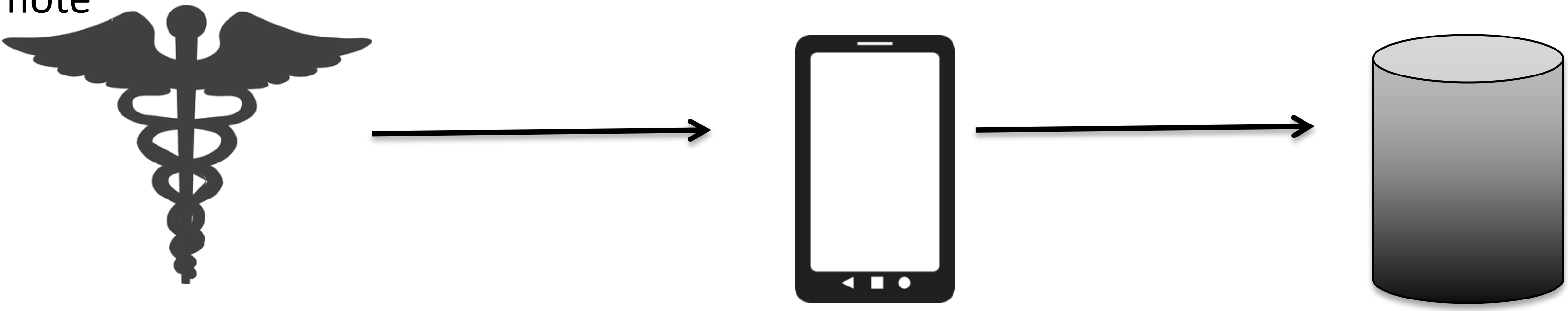
- Authentication protocols provide assurance in a secure manner
- User vs. device
  - Both may need to authenticate to other entities
- Determining the strength of authentication is difficult

Authentication Scenarios

Local



Remote



Guidance & Frameworks

- OMB M-04-04 – E-Authentication Guidance for Federal Agencies
- HSPD-12 – Common Identification Standard for Federal Employees and Contractors
- NIST 800-63 – Electronic authentication Guidelines
- NPSTC High-level Launch Requirements
- ATIS identity management framework

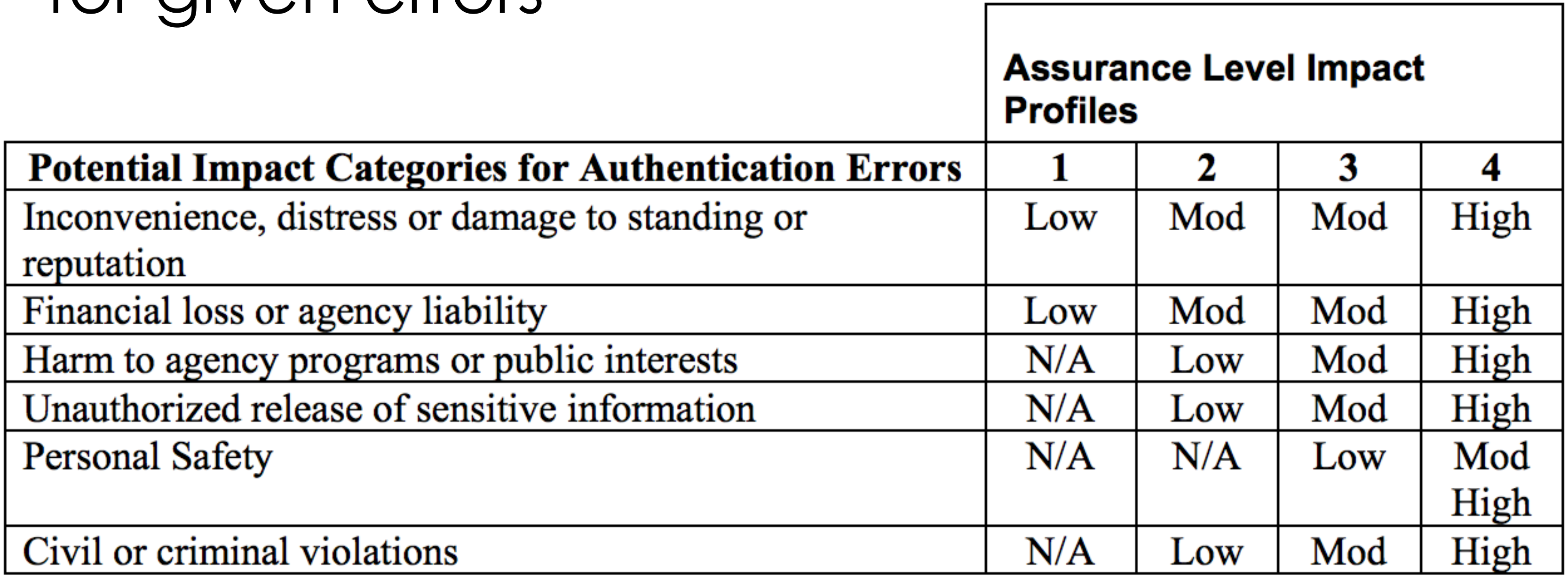
OMB M-04-04

- Outlines 5 step process for agencies to determine their assurance needs
  1. Conduct a risk assessment
  2. Map identified risks to the appropriate assurance level
  3. Select technology based on technical guidance
  4. Validate the implemented system
  5. Periodically reassess the system

Note: edited for brevity

OMB M-04-04 LOAs

- 4 levels of assurance are defined
- Specified minimum level of assurance (LOA) for given errors



	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	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 High
Civil or criminal violations	N/A	Low	Mod	High

HSPD-12

- Mandates common identification standard for federal government and contractors
- The PIV card contains several identity credentials
  - Technical specification: NIST SP 201-2
- Interoperable with other PIV enabled systems
  - PIV credentials can be used for mobile devices
- CIO council created PIV-I
  - Available to non-federal users
  - Should be compatible with PIV systems

NIST SP 800-63-2

- Supplements OMB M-04-04
- Provides technical guidance on selecting an authentication solution in 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,
  5. Assertion mechanisms used to communicate the results of a remote authentication if these results are sent to other parties.

Mobile Tokens

- PINs, passwords, and gestures
- Physical tokens
- Biometrics
- One-time password devices
- Attached smartcard readers
- NFC smartcards
- Software cryptographic tokens
- Hardware security modules
- Wearables

Needs of the Disciplines

First Responders

- Specialized training
- Operate in extreme environments
- Quick decisions under high stress
- A LOT of gear
  - – For example, firefighters carry between 75 to 100 pounds or more of equipment

First Responder: Fire Service

- – Air tank
- – Gloves
- – Helmet
- – Body suit
- – Rope
- – Pager
- – Radio

***Note**: This constitutes a preliminary list of equipment and is subject to change*

First Responder: EMS

- Gloves
- Mask
- Shears
- Stethoscope
- Ventilator
- EKG
- Radio

***Note**: This constitutes a preliminary list of equipment and is subject to change*

First Responder: Law Enforcement

- Handgun
- 2 mags
- Handcuffs
- CPR mask
- Flashlight
- Baton
- Radio

***Note**: This constitutes a preliminary list of equipment and is subject to change*

New LTE Devices

- Must work with existing gear
- Authentication must not compromise first responders' missions
- User acceptance is critical to realizing benefits of new technology

Usability

- ISO 9241-11: "Extent to which a product can be used by **specified users** to achieve **specified goals** with effectiveness, efficiency and satisfaction in a **specified context of use**"
  - Effectiveness: error rates
  - Efficiency: time on task
  - Satisfaction: subjective usability

Usability

- Must understand users' primary goals, users' characteristics, and the context in which they are operating (e.g., NPSBN)
- User-centered design (UCD) is a holistic approach that includes users in every element of the product development lifecycle
  - User requirements, design, development, and testing

Usability for Public Safety

- Common to begin with qualitative research
  - Understand first responders' characteristics, needs, tasks, and environments
- Crucial for domains with specialized personnel
  - Challenging operating environments
  - Interactions with unique tools, equipment, and technologies

Qualitative Research With SMEs

- NIST researchers met with SMEs in Fire Service, EMS, and Law Enforcement
- Qualitative data:
  - Communication is vital for coordinating emergency response operations in the field
  - Currently, such coordination relies heavily on voice communication via land mobile radio (LMR) technology
  - LMRs do not require authentication

Qualitative Data, Cont.

- Personal smartphones used to supplement LMR communications
- Coverage and signal penetration can be a problem in and around certain structures, especially in very rural areas or underground metropolitan transportation tunnels

Qualitative Data, Cont.

- Authentication in the office
  - Using passwords
    - Training systems
    - Timekeeping systems
    - Incident reporting systems
  - Different password requirements
  - Different password expiration cycles
  - Resets often require technical support

Mobile Tokens

- PINs, passwords, and gestures
- Physical tokens
- Biometrics
- One-time password devices
- Attached smartcard readers
- NFC smartcards
- Software cryptographic tokens
- Hardware security modules
- Wearables

Mobile Tokens

- PINs, passwords, and gestures
- Physical tokens
- Biometrics
- One-time password devices
- Attached smartcard readers
- NFC smartcards
- Software cryptographic tokens
- Hardware security modules
- Wearables

Usability Considerations

- Mobile authentication should be behind-the-scenes and invisible to first responders
- First responder effort during authentication should be minimal
- When selecting mobile tokens, must consider a variety of factors:
  - Memory
  - Physical
  - Environment
  - Technical

Passwords

- **Memory**
  - Password recall difficult
  - More passwords, more memory interference
  - Expiration cycles burdensome
- **Physical**
  - Gloved first responders
  - Typing error prone, time consuming
  - Passwords are masked
  - Small touchscreen
- **Environmental**
  - Movement
  - Sun glare
- **Technical**
  - Password registration, reset, expiration
  - Shoulder surfing attacks

Biometrics

9:41 AM
100%
Complete
Touch ID is ready. Your print can be used for unlocking your iPhone.
Continue

Biometrics: Fingerprints

- **Memory**
  - Must remember which finger(s) they enrolled with
- **Physical**
  - Gloved first responders
  - Missing or injured fingers
- **Environmental**
  - Conditions affecting sensitivity of sensor
- **Technical**
  - Need alternative authentication in case of injured fingers
  - First responders with degraded fingerprints

Smartcard Readers

Smartcard Readers

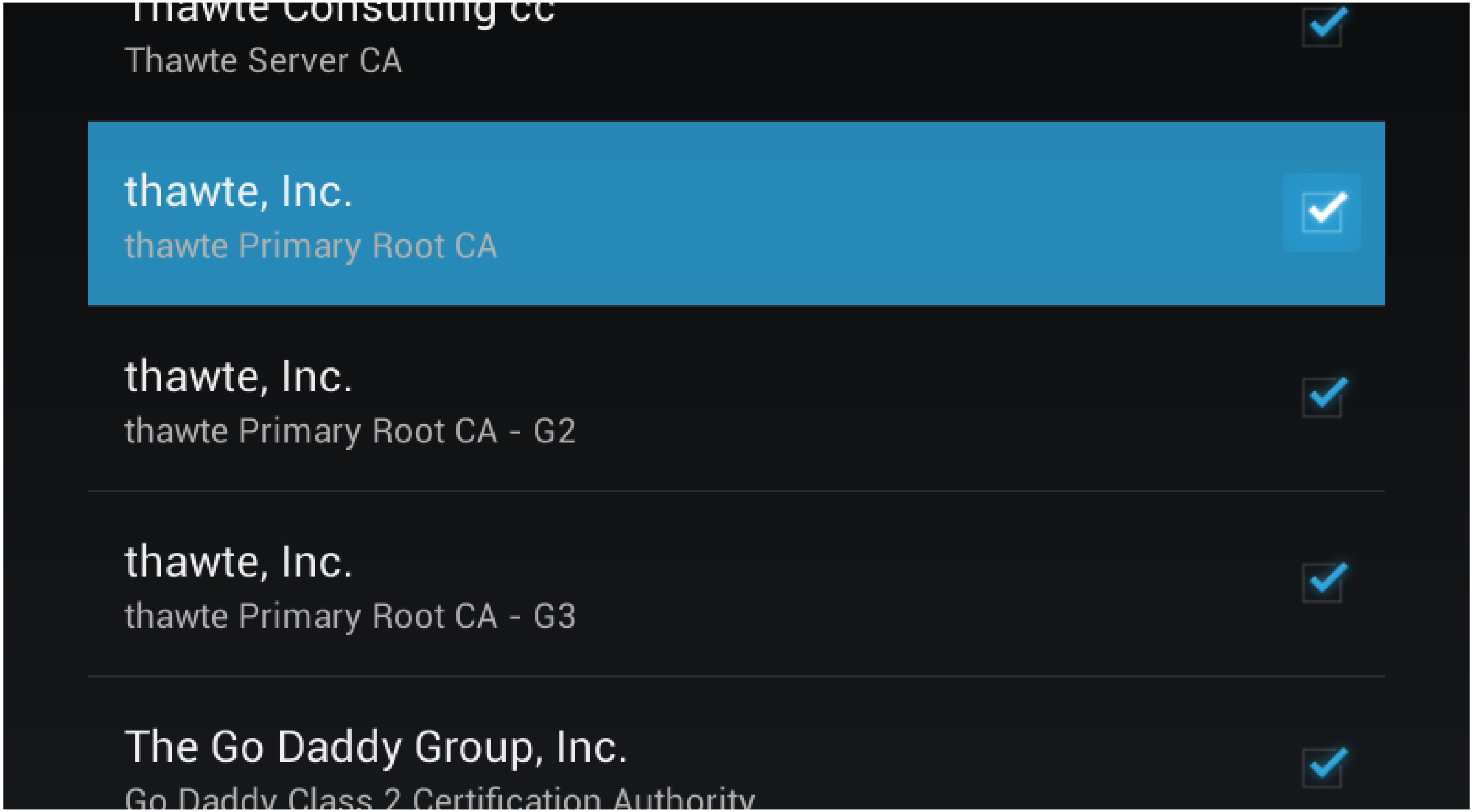
- **Memory**
  - Must remember smartcard, reader, PIN
- **Physical**
  - Two-handed usage scenario
  - Typing error-prone, time consuming
  - Gloved first responders
- **Environmental**
  - Movement
  - Sun glare
- **Technical**
  - Bulky readers
  - Power consumption

Wearables

Wearables

- **Memory**
  - Must remember to bring and affix token
- **Physical**
  - Small devices easily lost, damaged
- **Environmental**
  - Conditions affecting functionality of token
- **Technical**
  - Feature-rich wearables must be recharged every 1-2 days

Certificate-Based Authentication



Thawte Consulting cc
Thawte Server CA ☑

thawte, Inc.
thawte Primary Root CA ☑

thawte, Inc.
thawte Primary Root CA - G2 ☑

thawte, Inc.
thawte Primary Root CA - G3 ☑

The Go Daddy Group, Inc.
Go Daddy Class 2 Certification Authority ☑

Certificate-Based Authentication

- **Memory**
  - Must recognize and recall which certificate to use
- **Physical**
  - Gloved first responders
- **Environmental**
  - Movement
  - Sun glare
- **Technical**
  - PKI necessary

Recap: Communication is Key

- Authentication is uncommon for current public safety radios (LMRs)
- First responders need immediate use of voice services
  - Push-to-talk
  - Next generation push-to-talk is Proximity Services (ProSe) and Mission Critical Push to Talk (MCPTT)
  - Panic button
- May be unwise to introduce new authentication for critical functionality
  - Authentication still necessary to protect enterprise services (e.g., mail, messaging)

Recap: Usability is Critical

- Affects willingness to embrace new technology
  - User acceptance is essential
  - Shifting from personal to enterprise devices should be a seamless user experience
- New devices must support first responder missions
  - Work with existing gear
  - Not disrupt existing workflows
  - Core communication functionality must remain intact
- Must not overburden first responders with new authentication

Conclusions

- Public safety is a unique and challenging use case for identity management
- Usability is essential
- NISTIRs
  - – Published NISTIR 8014, *Considerations for Identity Management in Public Safety Mobile Networks*
  - – Coming soon: NISTIR, *Usability and Security Considerations for Public Safety Mobile Authentication*

Questions?

Joshua M Franklin
joshua.franklin@nist.gov
csrc.nist.gov

Dr. Kristen K Greene
kristen.greene@nist.gov
nist.gov/itl/iad

Dr. Yee-Yin Choong
yee-yin.choong@nist.gov
nist.gov/itl/iad