PSCR 2021
THE DIGITAL EXPERIENCE
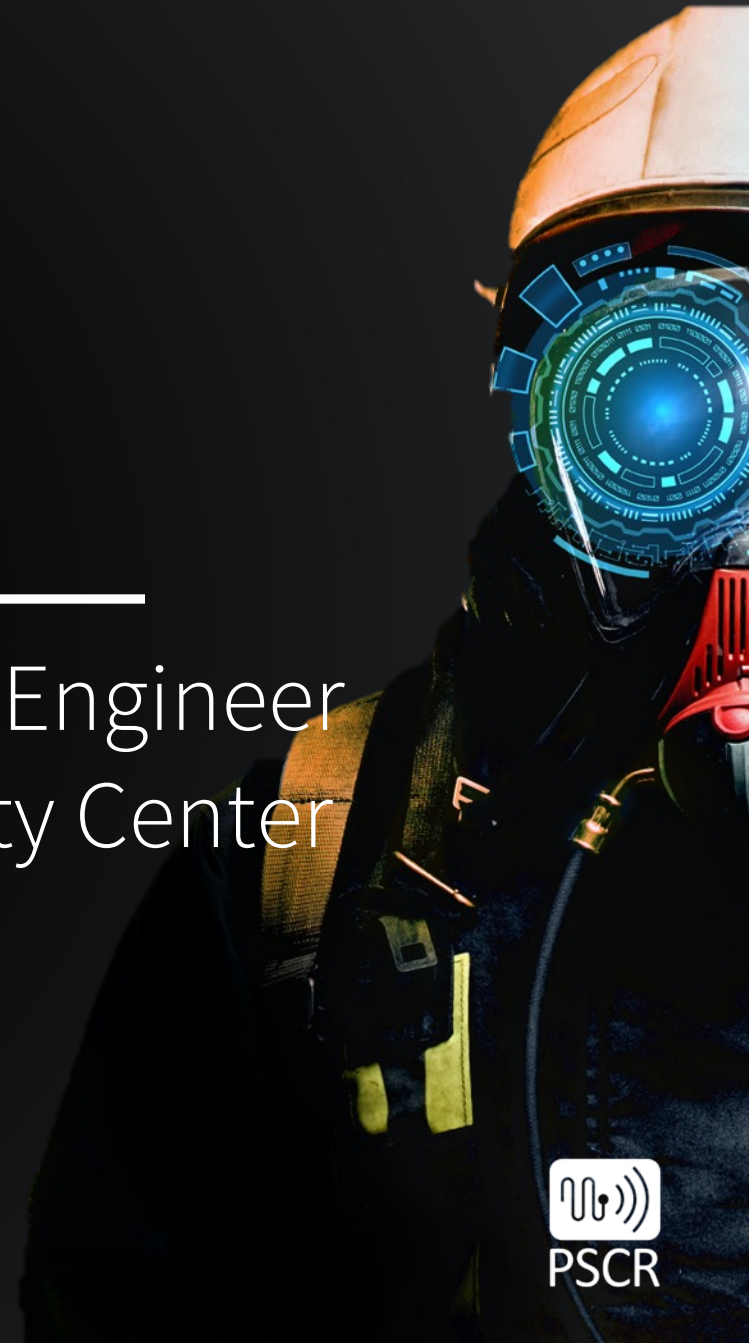#PSCR2021 • PSCR.GOV

NIST

1

PSCR

Public Safety
ICAM Update

Bill Fisher – Security Engineer

National Cybersecurity Center of Excellence

#PSCR2021

2

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately.

Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

* Please note, unless mentioned in reference to a NIST Publication, all information and data presented is preliminary/in-progress and subject to change

What is ICAM?

ICAM - Identity, Credential and Access Management

Getting the **right data** to the **right people** at the **right time** with the **right protections** and only if it's for the **proper reason** and in an **efficient manner**

What is Public Safety trying to accomplish?

"Who is accessing my information and what should they be authorized to access?"

Trustmarks

"How do I know your trustmarks and attributes align with my own security requirements?"

| Question One | Question Two | Question Three |

Information Sharing

ICAM
Authentication
Attributes
Federation
Authorization

"Which organizations can I trust to share information with?"

Compliance Alignment

PULLING THE FUTURE FORWARD

PSCR Security Team - Community Engagement

Where is NIST engaging to help?

NLETS TOC

National Law Enforcement Telecommunications Systems Technical Operating Committee

PSAC ICAM Working Group

Public Safety Advisory Committee ICAM Working Group

CJIS Security Policy Updates

Criminal Justice Information System security policy is currently being modernized. Expect continued alignment with NIST

How does PSCR's work align

ICAM

New NIST Documents

Trustmarks

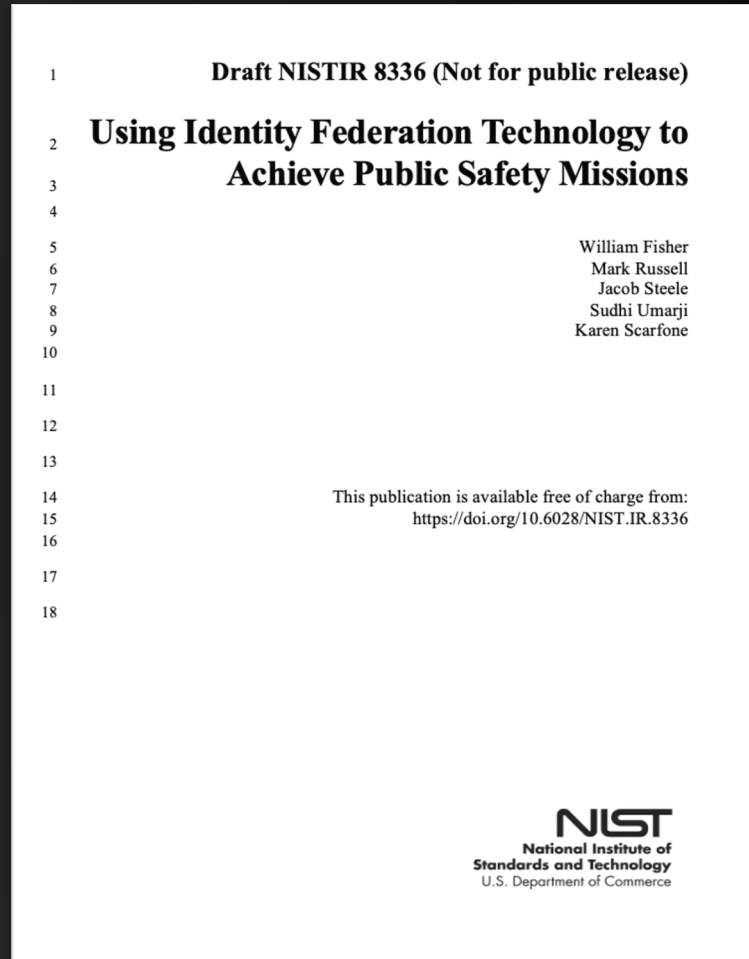Grant to GTRI to support development of trustmark work

Compliance Alignment

Advisement to CJIS on aligning security policy with NIST

New NIST Guidance

New NISTIR Using Identity Federation

Draft NISTIR 8336 (Not for public release)

Using Identity Federation Technology to Achieve Public Safety Missions

William Fisher
Mark Russell
Jacob Steele
Sudhi Umarji
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8336

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

What is federation?

- And how does it benefit public safety communities

What would a public safety federation look like?

- Defining entities in a PS federation, public safety relevant examples

What technology is needed to support a public safety federation?

- Defining possible public safety federation architectures

What about security?

- Explanation of key federation security components

New NISTIR Using IDaaS

Draft NISTIR 8335 (Not for public release)

Identity as a Service (IDaaS) for the Public Safety and First Responder Community

Christopher Brown
William Fisher
Mark Russell
Sudhi Umarji
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8335

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

What is IDaaS?

- Introduction to IdaaS & benefits
- Overview of different types of architectures
- Review of types of authenticators offered and how to think about each type from a risk perspective

Key considerations for IDaaS

- Methodology for understanding authenticator types
- Mapping to 800-63-3
- Impact or public safety relevant security requirements

New NISTIR Using Biometric Authentication

Draft NISTIR 8334 (Not for public release)

Using Mobile Device Biometrics for Authenticating First Responders

William Fisher
Don Faatz
Mark Russell
Christopher Brown
Sanjeev Sharma
Sudhi Umarji
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8334

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

Looking at biometrics from a risk perspective?

- Secret vs Private information
- How they should be deployed in an authentication system
- Challenges using them with shared devices

Physical vs Behavioral biometrics

- Definitions and differences in use
- Challenges and unknowns
- Question for vendors selling these products

New NISTIR Format

New NISTIR Call Out Boxes

1.3 Report Conventions

This report uses callout boxes to highlight certain types of information, as depicted in Figure 1. Callout boxes may contain new material that is not covered elsewhere in the report. A **Caution** box provides a warning of a potential issue with doing or not doing something. A **Definition** box provides the definition of a key term. A **Note** box gives additional general information on a topic. A **Tip** box offers advice that may be beneficial to the reader.
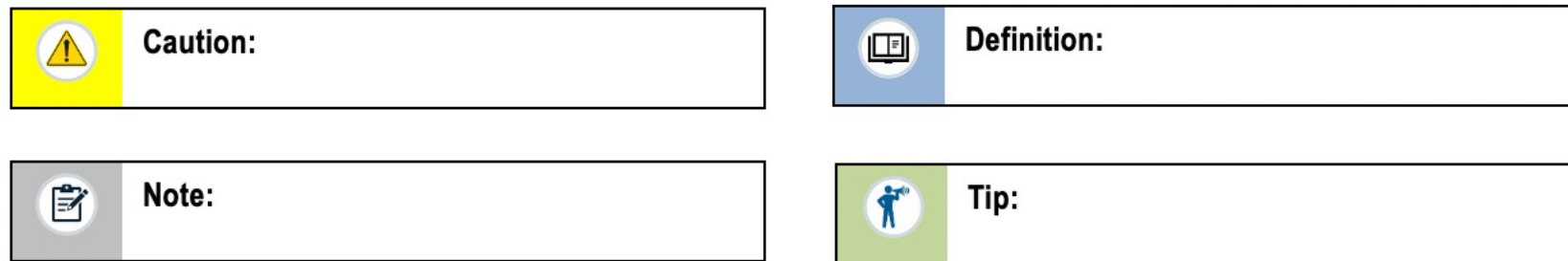
⚠	Caution:		📖	Definition:
📋	Note:		🧍	Tip:

Figure 1: Callout Box Formats

Call Out Boxes Example

Caution: Although presentation attack detection (PAD) technologies (e.g., liveness detection) can mitigate the risk of someone using a captured biometric, additional trust in the sensor or biometric processing is required to ensure that PAD is operating in accordance with the needs of the organization.

Definition: *Biometrics* is "the measurement and analysis of unique physical or behavioral characteristics […] especially as a means of verifying personal identity."[1]

Note: Apple has general support for multiple users of iPad tablets. Apple also provides a "Shared iPad" capability for schools,[6] where each account is synced from the cloud and user data may be purged across sessions, but this is not a practical solution for public safety.

Tip: The steps in Figure 2 can also be used to identify an unknown person. The template to be verified could be compared against all the enrollment templates, not just one. However, it is important to note that images used for verification may perform differently when used for identification purposes.

PSCR Lab Work

New Lab Tech ICAM and Message Switches

Update on IDaaS Lab work

- Completed a demo of several different authenticators and will be releasing a demo to accompany NISTIR 8335

New Lab work

- Currently have a public safety message switch implemented in the lab environment to test ICAM capabilities
- Working to get CAD/RMS capabilities as well
- Goal: test state level IDP architectures with directory services, federation, CAD/RMS and message switch infrastructure

Trustmarks

PSCR Grant Trustmarks

- Trustmarks - system for increasing trust & transparency between organizations
- Lots of open questions for the community:
  - Who will issue Trustmark definitions?
  - Who will be Trustmark providers?
  - How often are organizations audited and Trustmarks updated? Who is doing the audits?
  - Is there a need for real time checking of Trustmarks or is revocation check enough?
  - How many Trustmark definitions are really needed to meet security and privacy needs? (20? 600? 1000?)

IdP – Identity Provider
RP – Relying Party
Subscriber – System User
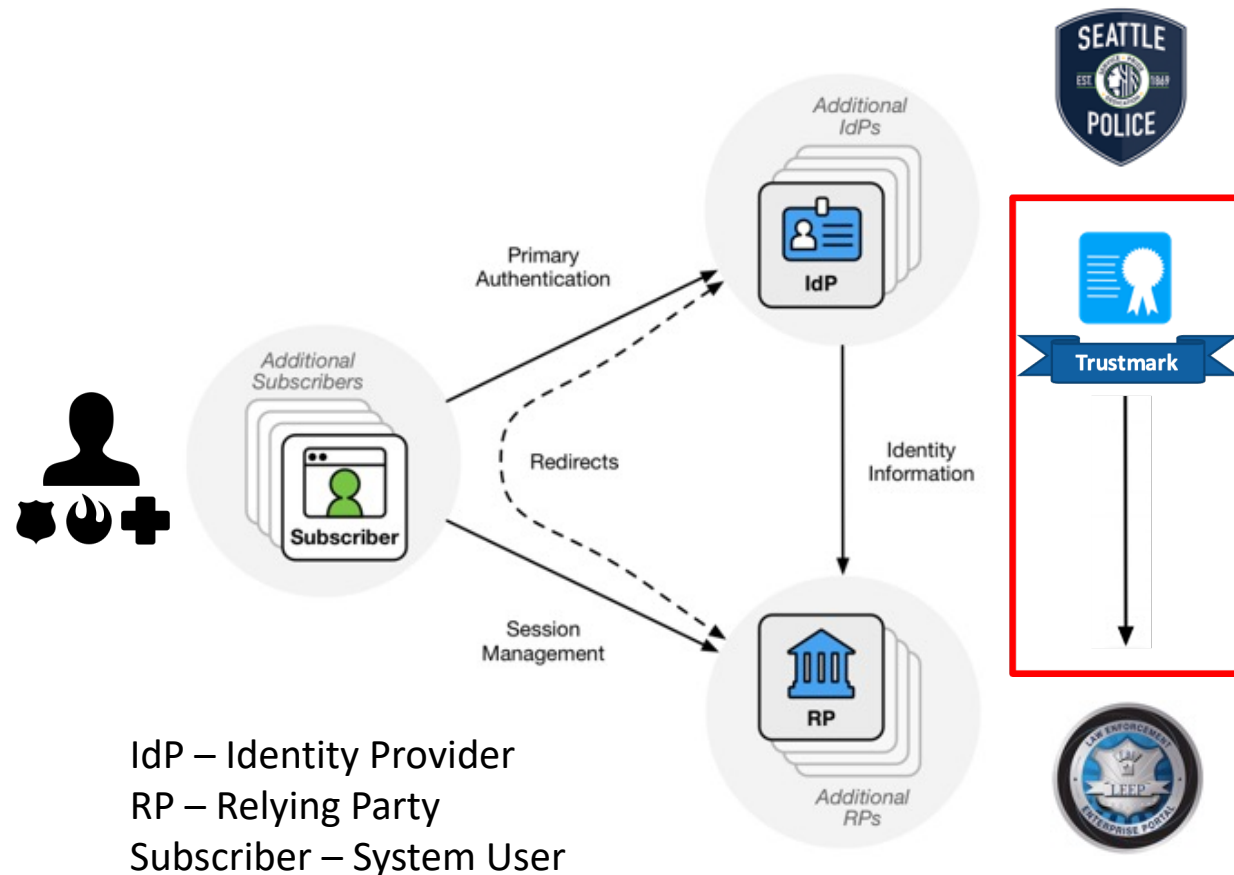
Future Work?

Other Areas of Interest in Public Safety Security

Cloud Security
- Last year we held a 3-hour virtual workshop and put together a white paper
- Currently waiting for public safety to tell us where they want to go in this space

Ransomware Security?
- Topic has come up several times recently
- Some Ransomware attacks have already happened in public safety communities

If you are interested in either of these, reach out to us!

There is no cloud
it's just someone else's computer

GET CONNECTED

✉ PSFR-NCCoE@nist.gov

🌐 https://www.nist.gov/ctl/pscr/research-portfolios/security

THANK YOU

#PSCR2021 • PSCR.GOV

Acronym List

- CAD - Computer Aided Dispatch
- CJIS – Criminal Justice Information System
- IDaaS – Identity as a service
- IDP – Identity Provider
- NIST – National Institute of Standards and Technology
- NISTIR – NIST interagency report
- RMS – Record Management System