PSCR 2020:

THE DIGITAL EXPERIENCE

NIST

#PSCR2020

PSCR

Public Safety ICAM – Critical Topics and New NIST Documents

Bill Fisher – NIST National Cybersecurity Center of Excellence

#PSCR2020

NIST

PSCR

DISCLAIMER

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

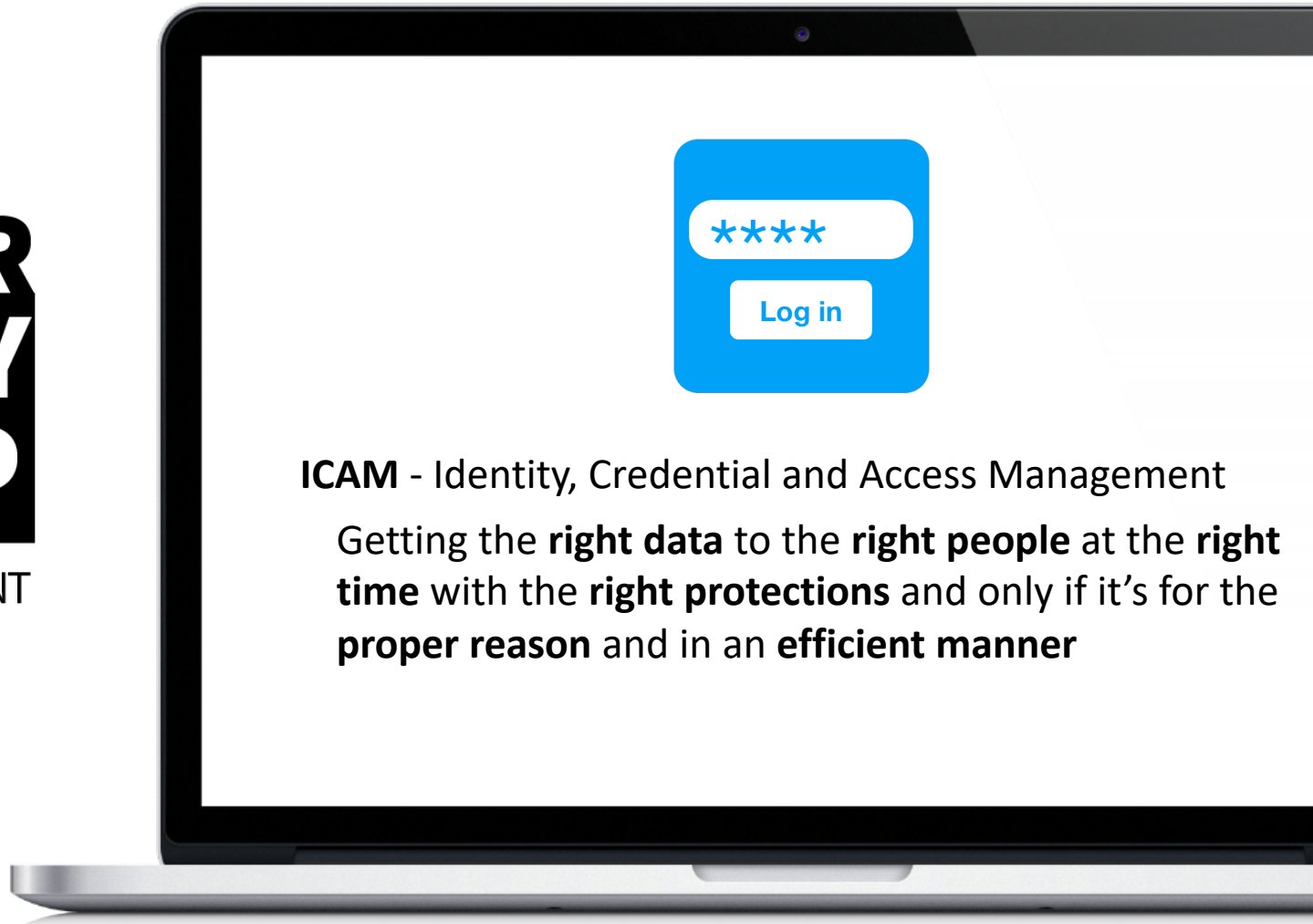
Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

*** 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?

NCCOE AND PSCR CYBERSECURITY WORKSHOP

IDENTITY, CREDENTIAL, & ACCESS MANAGEMENT
APRIL 16 – 17, 2019



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**

Why Should You Care?

Critical Capabilities

- Information sharing
- Authentication
- Interoperability

Industry Momentum

- New ICAM working group under the PSAC
- FirstNet rolling out ICAM capabilities

Gap Areas

- Governance
- Education on technology
- Risk-based decision making

Supports Future Tech

- Mobile
- Cloud
- Bring your own device
- Biometrics

NIST Focus - Critical Topics In ICAM

Identity Federation

"A process that allows the conveyance of identity and authentication information across a set of networked systems" Example: Using your Google identity at third party services

Biometric Authentication

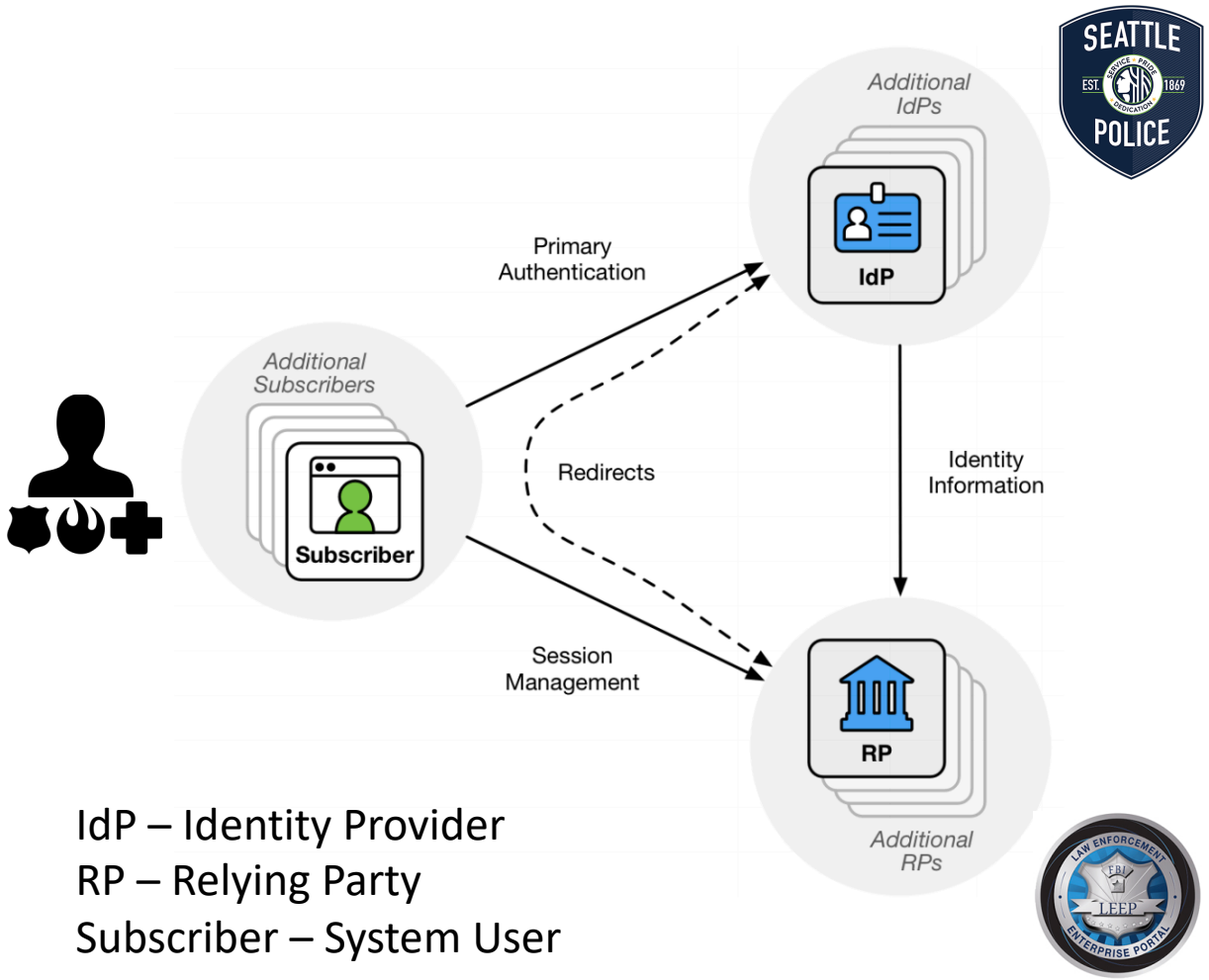
"Automated recognition of individuals based on their biological and behavioral characteristics" Example: FaceID & TouchID on mobile devices

Identity As A Service (IDaaS)

Identity Services delivered as cloud software as a service (SaaS) offering.

Why Federation?

Federation Concepts



IdP – Identity Provider
RP – Relying Party
Subscriber – System User

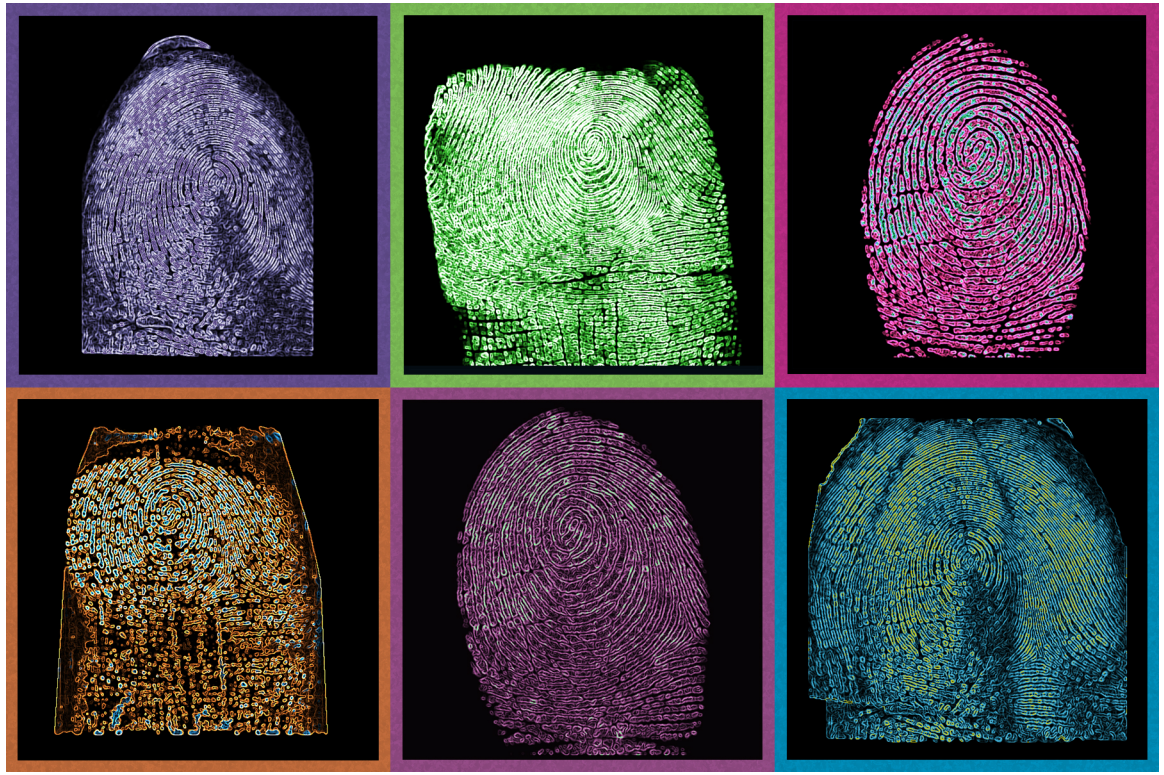
Federation Enables:

- Interoperability and information sharing
- Sharing identities across jurisdictions and to cloud services
- Sharing attributes and enabling Trustmarks
- Mobile and web Single Sign On (SSO)

Why Biometric Authentication?

Biometrics Challenges:

- Public Safety personnel want to use it for ease of use
- Need to understand the security implications/education around risks
- Implementation challenges such as shared devices



Why IDaaS?

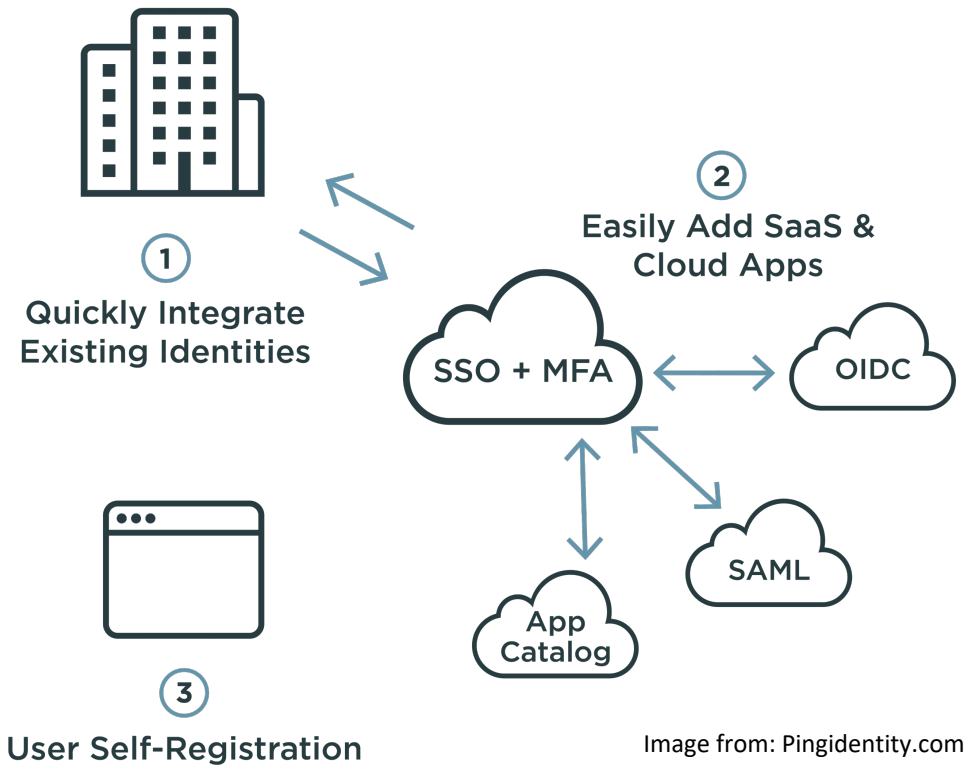


Image from: Pingidentity.com

IDaaS Considerations:

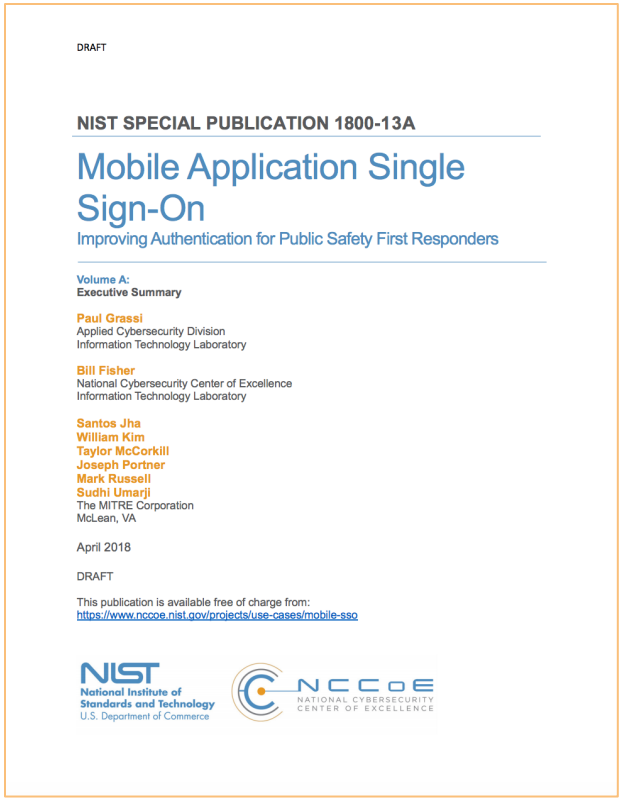
- Move toward cloud services – cost savings, ease of integration, diversity of authenticators, get other services like federation, lack of expertise in small organizations
- Confusion around MFA and different types of authenticators
- Confusion around CJIS compliance

Our Documentation

What to Expect?

- White Papers & NIST Interagency Reports - allowing for quicker updates and more specific topics areas
- Not just controls, but aspects of technology that impact risk methodology and decision making
- Mappings into critical NIST documentation and Public Safety Resources

No 1800 series Practice Guides this year:



DRAFT

NIST SPECIAL PUBLICATION 1800-13A

Mobile Application Single Sign-On

Improving Authentication for Public Safety First Responders

Volume A:
Executive Summary

Paul Grassi
Applied Cybersecurity Division
Information Technology Laboratory

Bill Fisher
National Cybersecurity Center of Excellence
Information Technology Laboratory

Santos Jha
William Kim
Taylor McCorkill
Joseph Portner
Mark Russell
Sudhi Umarji
The MITRE Corporation
McLean, VA

April 2018

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/use-cases/mobile-sso

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

NCCoE National Cybersecurity Center of Excellence

Federation – What to Expect

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

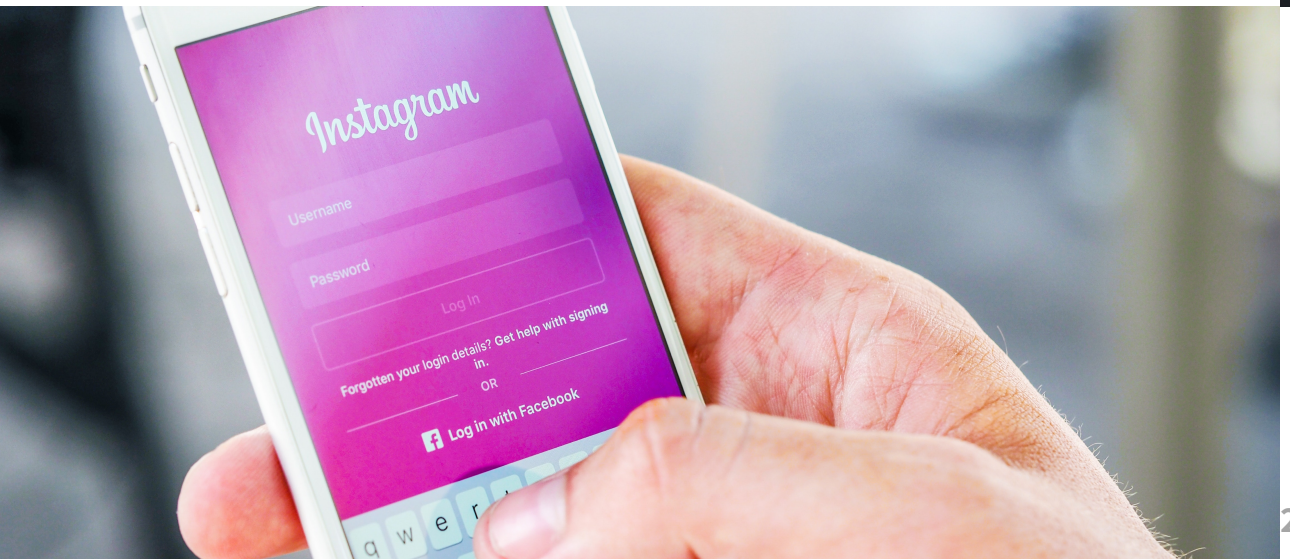
What about security?

- Explanation of key federation security components

Biometrics – What to Expect

Looking at biometrics from a risk perspective?

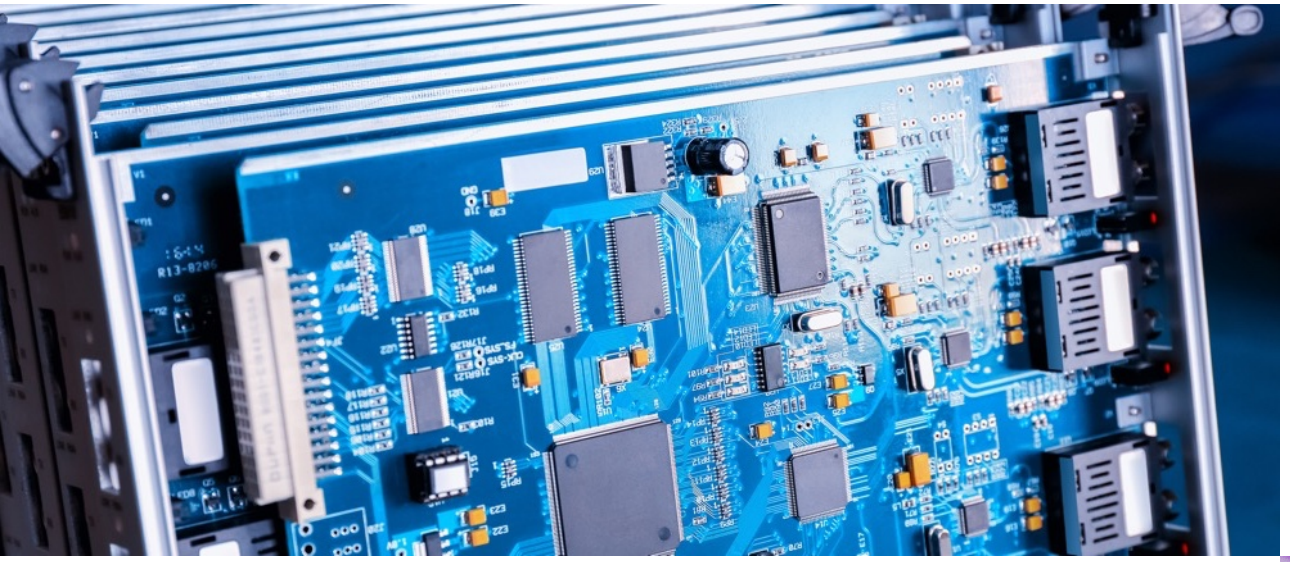
- Secret vs Private information
- How they should be deployed in an authentication system
- Challenges using them with shared devices



Physical vs Behavioral biometrics

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

IDaaS – What to Expect



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

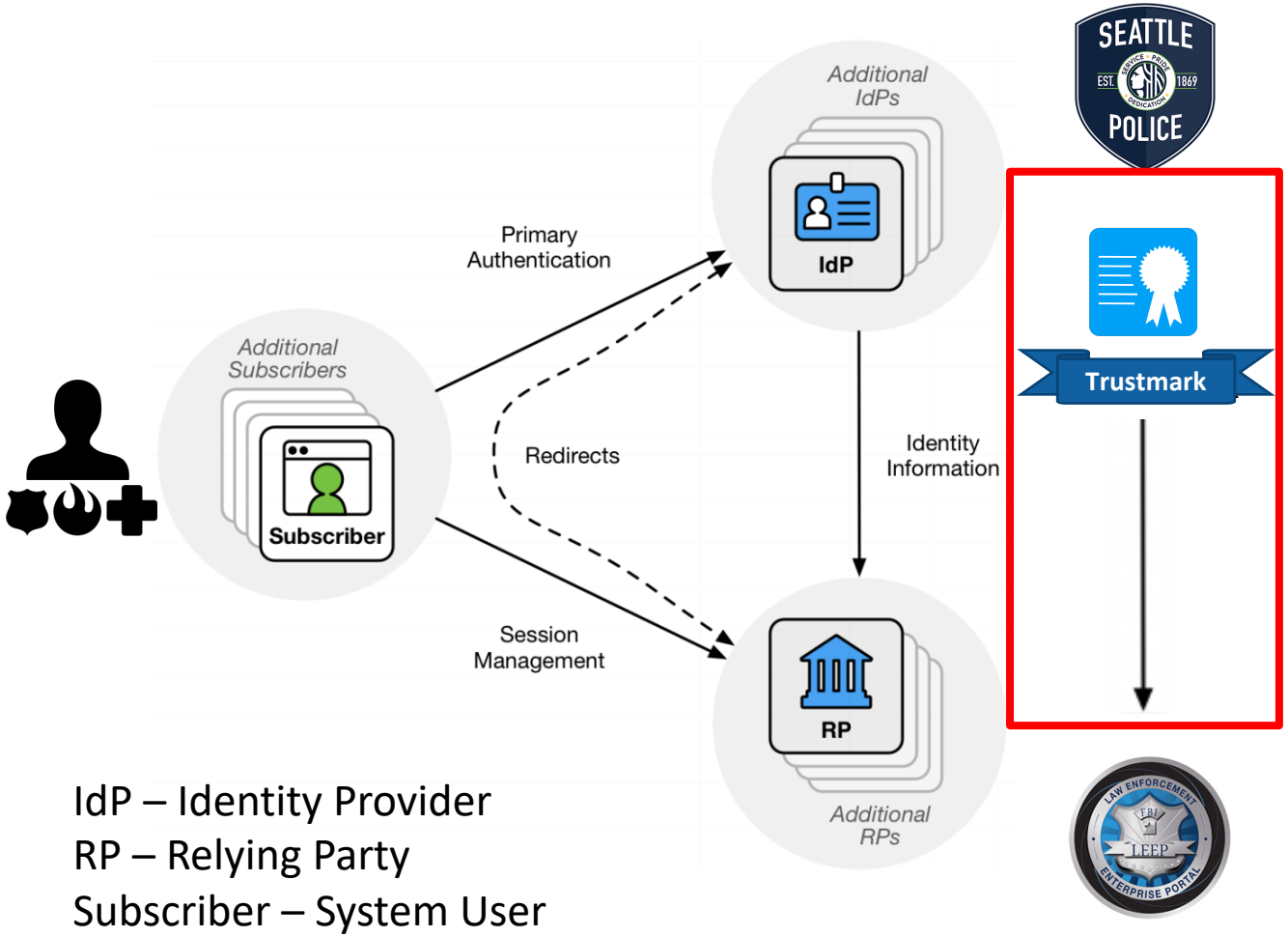
- Methodology for understanding authenticator types
- Mapping to 800-63-3
- Impact or public safety relevant security requirements

NCCoE Lab Work - IDaaS

- Goal: Worked **examples** of **commercial technology** to **supplement** our guidance
- Starting with **IDaaS** technology and various **authenticator types**. Why? Because we see public safety **adopting** these technologies in the **near term**
- Have other ideas? Want to collaborate? Want to see a different example? **Let us know!**

New PSCR Grant – GTRI Trustmarks

- What? A system for **increasing trust & transparency** and **reducing costs** between identity providers and relying parties
- Why? Supports **identity federation** and **information sharing**



IdP – Identity Provider
RP – Relying Party
Subscriber – System User

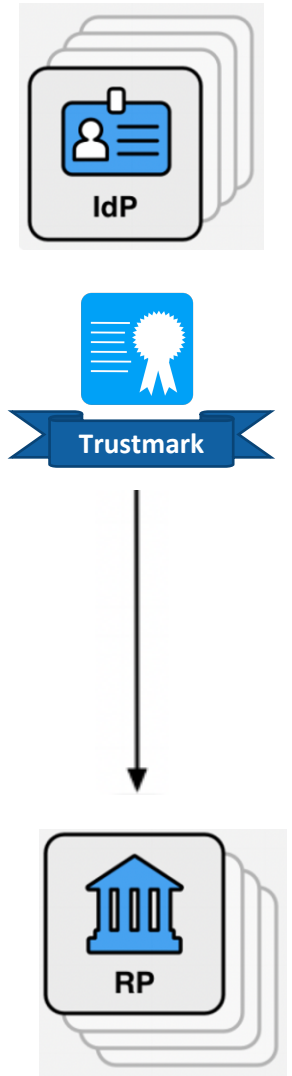
New PSCR Grant – GTRI Trustmarks

The **identity provider** needs to know:

- Is the relying party a **legitimate, bona fide agency**?
- Is the **data accurate**?
- What are the data **access control requirements**?
- Does the relying party implement **appropriate policies** (security, privacy, etc.)?

The **relying party** needs to know:

- Is the identity provider a **legitimate, bona fide agency**?
- What **users** at the identity provider are **accessing the data**?
- Do these users have appropriate **credentials, trainings, certifications**, etc.?
- Are the users aware of the **data handling** obligations for this data?
- Does the Data Consumer implement **appropriate policies** (security, privacy etc.)?



Future Work – Cloud Security

- Why? **Growing** area of **need** in the Public Safety community
- Goal: Not to recreate the wheel, **bridge gap** between **cloud security best practices** and current cloud security practices within public safety
- Initial outcome: **NIST whitepaper/guidance**, but not till 2021
- Topics: protecting various cloud architectures, **shared security** model, encryption **key management**, etc…

THANK YOU

#PSCR2020

NIST

PSCR