ICAM 101 Briefing for Public Safety Officials

Background

ICAM stands for identity, credential, and access management. The term refers to a comprehensive approach for dealing with digital identities (and associated attributes), credentials, and access control. ICAM helps to address the growing data management, interoperability, and cybersecurity challenges facing public safety today. ICAM solutions, especially federated ones, align public safety communities around common identity and access management practices.

ICAM concepts are not new to public safety agencies. In most public safety communications systems, radio sites, public safety facilities, data centers, and radios are physically secured against internal and external threats. Additionally, Information technology (IT) networks are routinely hardened and secured to prevent compromise or loss of personally identifiable information and law enforcement sensitive data. However, as federal, state, local, and tribal public safety organizations increasingly collaborate and share information over the internet, the challenges of safeguarding technology and information now extends to cyberspace. A holistic solution such as federated ICAM provides many tools and processes for enhancing both physical and cyber security.

Federated ICAM solutions build trust by aligning all participants to an agreed-upon set of policies, technical standards, and best practices. While Identity Management, Credential Management, and Access Management are closely interrelated, it is important to understand the each individual ICAM facet.
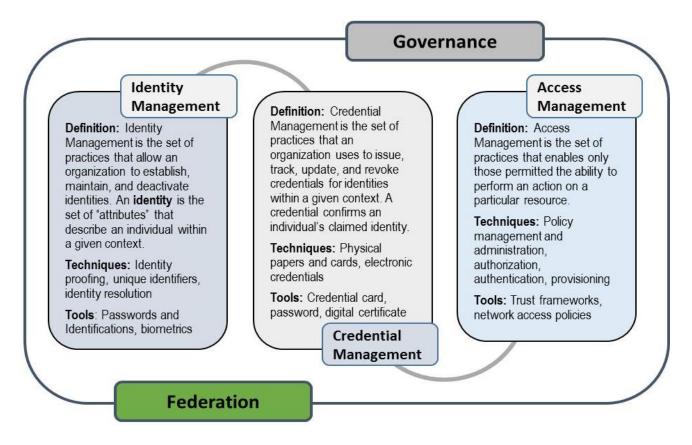

Governance

Identity Management

Definition: Identity Management is the set of practices that allow an organization to establish, maintain, and deactivate identities. An **identity** is the set of "attributes" that describe an individual within a given context.

Techniques: Identity proofing, unique identifiers, identity resolution

Tools: Passwords and Identifications, biometrics

Definition: Credential Management is the set of practices that an organization uses to issue, track, update, and revoke credentials for identities within a given context. A credential confirms an individual's claimed identity.

Techniques: Physical papers and cards, electronic credentials

Tools: Credential card, password, digital certificate

Credential Management

Access Management

Definition: Access Management is the set of practices that enables only those permitted the ability to perform an action on a particular resource.

Techniques: Policy management and administration, authorization, authentication, provisioning

Tools: Trust frameworks, network access policies

Federation

FIGURE 1 - DEFINITION OF IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

Federated ICAM for Public Safety

Immediate access to critical information will provide public safety personnel with the ability to make informed decisions and better protect themselves and the public. Collectively, the public safety community lacks a nationwide interoperable information sharing system designed to coordinate across all public safety disciplines (e.g., law enforcement, fire, emergency medical services [EMS], 911 dispatch centers, emergency management, and public health). As a result, information is stored in disparate systems; making it difficult for federal, state, local, and tribal agencies to access and share information.

A federated approach promotes mutual trust and interoperability between public safety agencies and communities of interest (COIs). Federated organizations have the autonomy to set agreed-upon rules for establishing trust and conditions for sharing information. Currently, there are many trust frameworks in place to support various ICAM needs and identity federations. Figure 2 depicts the possible benefits of adopting an established federated ICAM solution.

FIGURE 2 – POTENTIAL BENEFITS OF FEDERATED ICAM

Physical and Cyber Security

Provides improved physical and cyber security by limiting access to authorized and authenticated users
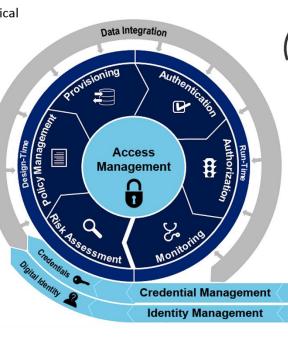
Mission Delivery

Enables improved mission delivery with potential increased access to secure online resources and other public safety communities.

Information Sharing

Breaks down silos by creating a trusted information sharing environment for public safety agencies.

Interoperability

Establishes a standard approach for managing digital identities and credentials, and for accessing public safety information.

Data Management

Provides tools and protocols for facilitating real-time monitoring and assessment of management and security policies.

Cost Savings

Promotes a modular and scalable approach for ICAM implementation.

SAFECOM and NCSWIC and committed to working with ICAM providers to communicate public safety needs and establish a nationwide ICAM solution.

For more information on ICAM, please visit https://www.dhs.gov/safecom/icam-resources