Identity, Credential, and Access Management: Public Safety Value Proposition Overview

BACKGROUND

This document is part of SAFECOM and National Council of Statewide Interoperability Coordinators' (NCSWIC) Identity, Credential, and Access Management (ICAM) Value Proposition Suite and provides an overview of ICAM and its potential value to public safety. Other documents in the suite explore ICAM use cases for drug, hurricane, active shooter, and bombing response operations and information sharing.

THE CHALLENGE – SECURE INFORMATION SHARING

Public safety organizations use a variety of systems to store and share information. To achieve their mission goals, organizations have a responsibility to ensure that *the right person with the right privileges can access the right information at the right time*. The challenge facing many federal, state, local, and tribal agencies and other public safety organizations is that they cannot easily or securely access and share information with each other in today's environment. In addition, these entities are often tasked with storing highly-sensitive critical information such as law enforcement information, personally identifiable information (PII), and protected health information (PHI), requiring an enhanced diligence in physical and cyber security.

POTENTIAL SOLUTION – FEDERATED IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

ICAM does not fix all information sharing problems, but it is a way to verify and control that it is *the right person with the right privileges accessing the right information at the right time*. A successful ICAM program provides tools, policies, and governance for individuals to safely, confidently, and quickly access resources across existing systems and emerging platforms (Figure 1). Elements of ICAM are often in use today, even if they are not referred to as "ICAM."

Figure 1. Elements of ICAM

Identity refers to the set of characteristics that describe an individual within a certain context. For example, name, social security number, address, and education are attributes associated with your unique job identity. **Identity Management** includes issuing, validating (proofing), maintaining, and terminating identities.

Credentials are pieces of evidence that confirm an individual's claimed identity. For example, a driver's license or an online ID and password tie the credential owner to his or her identity. **Credential Management** includes issuing, tracking, updating, and terminating credentials.

Access is the process of connecting verified users to potentially sensitive resources or information. Access management involves:

- Developing and enforcing **policies**
- **Authenticating** a user's identity as asserted by his or her credential(s) (e.g., ID and password). Strong authentication combines two or more factors, consisting of things that you know, have, or are.
- **Authorizing** access to resources or information through a decision process which ensures compliance with relevant security policies. Authorization occurs after authentication.

A **federated ICAM** solution allows one organization to accept another organization's identity processes and procedures (i.e. identity proofing, credentials, and attributes) based on inter-organizational trust; it allows an individual to use a single log-on method (i.e. authenticate once) to access information in multiple systems at multiple organizations. **This is referred to as single sign-on (SSO)**.

Banking institutions are an example of a federated set of organizations. An account holder can access funds using his or her bank card (something you physically have) and a personal identification number (PIN) (something you know) to obtain money from **any** banking institution's automated teller machine (ATM) across the country. The ATM, through a **federation** established by all participating banks, authenticates the individual's identity and dispenses funds belonging to the user's bank. The entire process takes a matter of seconds, but technologies, policies, and governance behind the scenes make this all possible. An ATM transaction is also an example of **multi-factor authentication** because it requires both a bank card and a PIN.

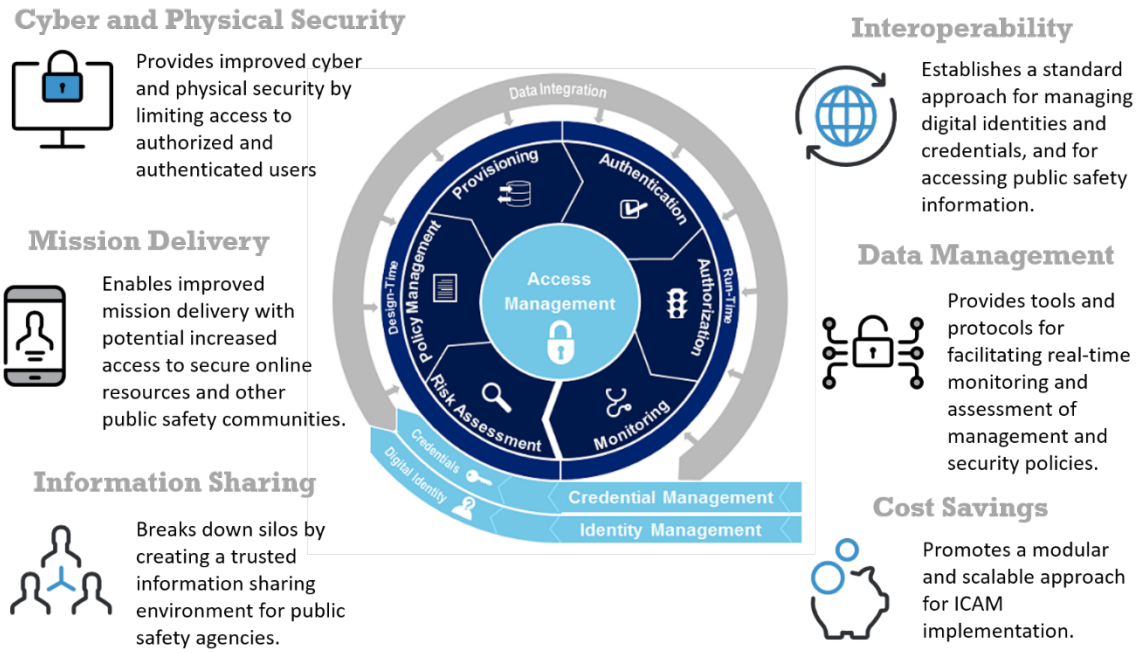

Figure 2. ICAM Benefits

VALUE PROPOSITION – REAL-WORLD USE CASES

SAFECOM and the NCSWIC developed resources to show how ICAM can support routine and emergency response operations in different public safety domains.[1] Real-world examples of how federated ICAM solutions can support public safety emergencies include:

Drug Crisis. In 2018, 67,367 deaths in the United States were the result of drug overdose.[2] A federated ICAM approach can allow previously siloed information from medical providers, emergency medical service (EMS) responders, and law enforcement to be easily shared and accessed between organizations. This provides stakeholders with a more complete view of the impacts of the opioid crisis in their communities, allowing them to develop a specific, comprehensive strategy to prevent and respond to opioid or other drug distribution, use, and overdoses.

[1] To find out more on how public safety uses ICAM solutions, visit https://www.cisa.gov/safecom/icam-resources or contact PublicSafetyComms@cisa.dhs.gov
[2] Drug Overdose Deaths. Centers for Disease Control and Prevention. Last reviewed March 29, 2020. https://www.cdc.gov/drugoverdose/data/statedeaths.html (accessed on July 1, 2020).

Active Shooters in Schools. According to the Federal Bureau of Investigation (FBI), there were 277 active shooter incidents in the United States from 2000 to 2018. In total, 884 individuals were killed and 1,546 were injured. Of these incidents, 57 (20.6 percent) occurred in educational environments.[3] As a result, many schools developed Action Response Plans (ARPs) that provide key information to help public safety organizations coordinate a response to shooting incidents. A federated ICAM approach could provide all first responders timely and easy access to the school's ARP and facilitate real-time information sharing between first responder organizations.

Federated ICAM solutions can also streamline public safety responses to natural disasters (e.g., hurricane), multi-jurisdictional criminal attacks (e.g., bombing). Other documents in the ICAM Value Proposition Suite provide more detailed descriptions of these four scenarios and their ICAM use cases.[4]

ADOPTION – STEPS TO GET STARTED WITH ICAM

A federated ICAM approach can mitigate security risks from unauthorized access, streamline access to critical information, and encourage discussions on organizational security posture and risk tolerance. Organizations looking to explore federated ICAM can take the following steps as a starting point:

- **Assess** organizational mission requirements to understand key information technology systems, data usage requirements, data categories[5] (i.e. how sensitive is the data?), and how those resources can be shared to advance mission and business objectives.
- **Identify** business and mission partners and use cases where shared resources can advance common mission requirements.
- **Evaluate** existing risks and determine how much risk the organization and its information sharing partners are willing to accept. Security policies, both internal and external (e.g., mission partners' policies), can help define security requirements for information sharing.
- **Engage** subject matter experts and business partners who can endorse various ICAM initiatives to advance organizational goals. Seek input from state and local agencies who have participated in federated ICAM initiatives or share similar missions and goals.[6]

Implement either a small-scale ICAM pilot to address key priorities or participate in ICAM initiatives from business partner(s) with similar missions and goals. Leverage existing technologies or shared partner knowledge to help minimize project risk and overall cost.

POLICY EXCHANGE – THE TRUSTMARK FRAMEWORK

In 2017, the SAFECOM and NCSWIC ICAM Working Group endorsed a position paper encouraging public safety agencies to adopt the Trustmark Framework[7] developed by the Georgia Tech Research Institute (GTRI).[8] The goal of the Trustmark Framework is to enable agile and scalable trust management by providing a template for: (1) data owners to outline their security policies; and (2) data users (requestors) to show conformance with those policies. These statements of conformance, known as Trustmarks, can be reused to achieve greater adaptability, interoperability, and potential cost savings.[9]

---

[3] *Quick Look: 277 Active Shooter Incidents in the United States From 2000 to 2018*. FBI. https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents-graphics (accessed November 12, 2019)
[4] The four ICAM Value Proposition use cases may be accessed at https://www.cisa.gov/safecom/icam-resources
[5] Documents, such as *National Institute of Standards and Technology (NIST) 800-63*, *Federal Information Processing Standards (FIPS) 199*, and *FIPS 200*, provide some guidance for identifying and categorizing data types.
[6] In addition to state, local, and commercial subject matter experts, the Cybersecurity and Infrastructure Security Agency (CISA) offers assistance to public safety agencies to: (1) implement consistent ICAM standards, policies, procedures; and (2) develop interoperability and implementation guidance for community-wide use.
[7] CISA "SAFECOM and NCSWIC Encourage Public Safety to Adopt Trustmark Framework," May 16, 2017.
[8] SAFECOM and National Council of Statewide Interoperability Coordinators (NCSWIC), "Position Paper: Endorsing the Trustmark Framework," last accessed on November 20, 2019.
[9] GTRI, "GTRI NSTIC Trustmark Pilot," last accessed on October 4, 2019.