Identity, Credential, and Access Management (ICAM) Federation System Checklist

Science and Technology Directorate

Homeland Security

Science and Technology

Primary Authors

Christine Owen

Chris Price

Nino Barranco

Rasheeda Berry

Contributing Organizations

Oasys International Corporation

Department of Homeland Security (DHS) Science and Technology Directorate

Partner Engagement-Information Sharing Environment (PE-ISE)

DHS Office of Emergency Communications (OEC)

First Responder Network Authority (FirstNet)

Federal Communication Commission (FCC)

National Institute for Science and Technology Public Safety Communications Research Division (NIST PSCR)

PUBLIC SAFETY COMMUNICATIONS

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

WORKING GROUP

Identity, Credential, and Access Management (ICAM) Federation System Checklist

February 2019

Version 1

Prepared for

Department of Homeland Security

Science and Technology Directorate

Dedicated to the memory of:

Tom Sorley
1965-2018

The Identity, Credential, and Access Management (ICAM) Executive Primer is dedicated to the memory of Tom Sorley. Tom was a member of the executive leadership of the Public Safety Communications ICAM Working Group, which sponsored this document. He was the Chief Information Officer and Deputy Director of the Information Technology Department for Public Safety for the City of Houston, Texas, and National Chair of the Public Safety Advisory Committee (PSAC). Tom was a thought leader in public safety communications and his vision is reflected in this ICAM Educational Series.

DISCLAIMER OF LIABILITY

The Identity, Credential, and Access Management (ICAM) Educational Series is provided by the Public Safety Communications ICAM Working Group (PSC ICAM WG) “as is” with no warranty of any kind, either expressed or implied, including, but not limited to, any warranty of merchantability or fitness for a particular purpose. This material is provided to support the efforts of public safety information sharing, situational awareness and key decision making. These documents are intended to guide users for making informed decisions on improving the security posture of their information systems by using ICAM principles.

The ICAM Educational Series is intended to provide guidance for implementing ICAM principles, and does not contain or infer any official requirements, policies or procedures, nor does it supersede any existing official emergency operations planning guidance or requirements documents. As a condition of the use of the series, the recipient agrees that in no event shall the United States government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected to the series or the use of information from the series for any purpose. It is recommended that organizations align their resources with tools that would best fit their infrastructure, as well as their own standards and requirements.

The PSC ICAM WG does not endorse any commercial product or service referenced in the ICAM Educational Series, either explicitly or implicitly. Any reference herein to any specific commercial product, process, or service by service mark, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the PSC ICAM WG. The views and opinions of authors expressed herein do not necessarily state or reflect those of the PSC ICAM WG, the Department of Homeland Security Science and Technology Directorate or other partners and shall not be used for advertising or product endorsement purposes.

Executive Summary

The Public Safety Communications (PSC) Identity, Credential, and Access Management (ICAM) Working Group (WG) created a Federation System checklist to provide tips on how to approach data management practices, interoperability techniques, and cybersecurity challenges for the Public Safety Community (Community).

The Community's goal is to have the ability to appropriately share critical information among members of the Community, which can aid in saving lives and protecting property. This critical information is at times highly sensitive and can include law enforcement information, as well as personally identifiable information (PII) and protected health information (PHI). It is important for Community members who are sharing information between different organizations to make sure the information is not compromised. Organizations have a responsibility to ensure the right person with the right credentials is accessing information at the right time. This is where ICAM comes in. It ensures that the right person with the right credentials is assessing information at the right time.

Federations align public safety communities around common identity and access management practices, and this document discusses best practices and their usefulness for program managers and solutions architects. When organizations agree to share information on an ICAM-enabled system, they must agree on terms and conditions that will determine how their federation will operate.

To support the Community with its mission-critical tasks, 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.

It is also important for Community members who are sharing information between different organizations to make sure the information is not compromised. ICAM principles provide identity proofing for an organization's employees and volunteers, providing strong credentials for system access, enabling the use of multifactor authentication, using attributes to provision resources and creating strong access management all help an organization ensure that the right person is accessing an organization's information through a secure and seamless federation.

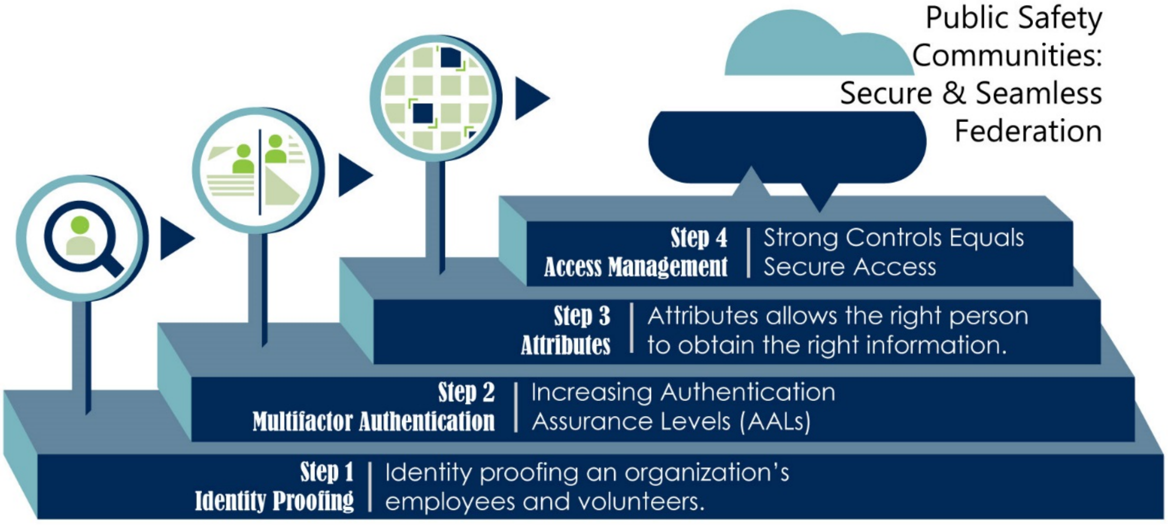
Public Safety Communities: Secure & Seamless Federation
Step 4 Access Management | Strong Controls Equals Secure Access
Step 3 Attributes | Attributes allows the right person to obtain the right information.
Step 2 Multifactor Authentication | Increasing Authentication Assurance Levels (AALs)
Step 1 Identity Proofing | Identity proofing an organization's employees and volunteers.

Figure 1 - Steps to Secure and Seamlessly Share Information (Federation)

The intent of this document is to highlight key system security requirements and best practices before sharing information and connecting with a federation. It is not intended to recommend specific ICAM products, but does strive to aid in the sharing of resources and encourage the adoption of multifactor authentication with a focus on the use of open source products. This document is paired with the ICAM Executive Primer, ICAM Acquisition Guide and ICAM Implementation Guides.

Intended Audience

The ICAM Federation Checklist is an amalgamation of lessons learned and best practices to consult before deciding to share information with outside organizations electronically. This document outlines five major principles that will help systems engineers and architects take prudent measures to build a secure ICAM-enabled federation. The document informs each of the following stakeholder groups[1] about multifactor authentication and ICAM solutions:

Stakeholder Group	**Responsibilities**	**Documents to Read**
Executive Leadership	…is the responsible authority for the department, state, or agency's fiscal and human resources for ICAM investments. This stakeholder group will use the document to understand the importance of ICAM investments, and to translate the value proposition of ICAM solutions to their mission needs.	ICAM Executive Primer
Program Managers	…are responsible for the operational implementation and oversight of ICAM capabilities to ensure they meet the functional mission requirements defined by the intended users. They must communicate to both the executive leadership and solutions architects to ensure understanding and expectations of the requirements for interoperable ICAM investments. Managers are required to quantify the benefit and resource impacts, including cost and integration savings, to executive leadership to ensure continued support and resource sustainment. This document provides program managers with a description of the key capabilities, processes, services, infrastructure, standards, and procurement language samples that are required of an interoperable ICAM architecture solution.	This document, ICAM Executive Primer & ICAM Acquisition Guidance
Solution Architects	…are responsible for acquisition requirements and the design/development/integration of ICAM solutions in accordance with their respective organization's enterprise architecture technical and management requirements. The solution architects will be required to compare and quantify the technical implementation options, alternatives, and cost constraints to the program managers. This document provides structured technical guidance and reference artifacts to assist in achieving an ICAM-enabled system.	This document, ICAM Executive Primer, ICAM Acquisition Guidance & ICAM Implementation Guides

[1] Each stakeholder's responsibilities were adopted from the Information Sharing Environment Geospatial Interoperability Reference Architecture (GIRA), available at https://www.dni.gov/files/ISE/documents/DocumentLibrary/GIRA.pdf.

Contents

Table of Figures

1 INTRODUCTION

This document serves as an educational piece on how to assess and manage an organization's systems to prepare it for information sharing with outside organizations. The Identity, Credential, and Access Management (ICAM) landscape is complex and there are many elements to consider. ICAM policies are important to have in enabling technology to share data across a wide variety of applications; these applications may include an organization's existing legacy systems as well as emerging nationwide initiatives, such as the Nationwide Public Safety Broadband Network (NPSBN), Next Generation 911 services and the First Responder Network Authority (FirstNet).

This document is focused on helping state, local, tribal and territorial (SLTT) Public Safety Community (Community) entities in improving the security posture of their systems for safe and secure information sharing. Instead of considering both single and multifactor authentication, this document focuses on multifactor authentication. Adopting multifactor authentication when upgrading to an ICAM-enabled system is highly recommended for any organization, but it is especially recommended for the Community based on a risk assessment of the typical information stored in the Community's systems. This document is the second of a series of ICAM educational tools, including the ICAM Executive Primer, ICAM Implementation Guides and ICAM Acquisition Guide.

1.1 PURPOSE

The ICAM Federation Checklist advises organizations to establish their federation guidelines and conduct system analyses as they create an ability to seamlessly and securely share information across jurisdictions. This document seeks to leverage existing efforts to maximize the value of existing ICAM products, policies and solutions allowing organizations to pick "the best of breed" while avoiding duplication.

1.2 BACKGROUND

This document was commissioned by the Public Safety Communications Identity, Credential, and Access Management Working Group (PSC ICAM WG), which is a subsidiary group of the Information Sharing Council (ISC) with a Federal Advisory Committee Act (FACA) exempt status under Section 1016(g)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (as amended). Its member organizations include Department of Homeland Security (DHS) Science and Technology Directorate (S&T), Partner Engagement Information Sharing Environment (PE-ISE), DHS Office of Emergency Communications (OEC), First Responder Network Authority (FirstNet), Federal Communications Commission (FCC), as well as National Institute of Standards and Technology (NIST) Public Safety Communications Research Division (PSCR). The PSC ICAM WG supports the ISC in fulfilling the ISC's duties (with a focus on public safety) pertaining to the interchange of information between public safety agencies by addressing policy, governance, standards, technology and acquisition guidance on ICAM capabilities for the public safety community.

1.3 APPROACH

Instead of considering both single and multifactor authentication, this document focuses on multifactor authentication. Adopting multifactor authentication when upgrading to an ICAM-enabled system reduces the risk of a system intrusion and is highly recommended for any organization, but it is especially recommended for the Community based on a risk assessment of the typical information stored in the Community's systems.

1.4 Enabling Multifactor Authentication

ICAM concepts appear in everyday life. When leaving our homes or cars, most of us choose to lock our doors and restrict access only to those with a key.[2] Likewise, anyone who accesses the internet creates a username and password to access a computer system, email or social network, which are examples of *single factor authentication*.

Most people only use a username and password when accessing computer systems, likely due to a perceived notion of convenience. A username and password combination or pin number are examples of single factor authentication when they are used on their own. While single factor authentication is simple and easy to implement, the practice is akin to leaving a door unlocked for hackers. Since passwords are easily obtained via email phishing, single factor credentials played a factor in 81 percent of the systems that were hacked in 2016.[3]

Multifactor authentication uses a combination of credentials to provider higher assurance that the individual attempting to access a protected resource is that individual. To create this higher assurance, multifactor authentication requires the use of two of three "factors." The factors include something you have (an ATM card), something you are (a fingerprint or other biometric) or something you know (a password or personal identification number. Information breaches can be prevented using multifactor authentication. Implementing simple multifactor authentication methods can help organizations prevent costly, time-consuming attacks.

When organizations connect their systems with others within their community of interest, the organizations will need to know who is accessing which pieces of information at what times to ensure only authorized users are within the system. Multifactor authentication becomes useful in information sharing scenarios. After performing a risk assessment based on the type of information held in the SLTT Community's systems, it was determined that multifactor authentication would reduce the risk of a system intrusion. As a result, this document, as well as the implementation and procurement guides, are all tailored towards ICAM systems with multifactor authentication.

1.5 How to Use

This document is the final piece of a progressive series that begins with the ICAM Executive Primer, a high-level, educational dive into ICAM through ICAM concepts and real-world scenarios for executive leadership and others. It dives deeper in the ICAM Acquisition Guidance to give program managers an overview of what to look for while acquiring ICAM products. It advises solution architects on the lessons learned from building an ICAM-enabled sandbox with multifactor authentication. The series continues with Implementation Guides that provide a deeper view into an ICAM-enabled federation configured with multifactor authentication for solutions architects. This document explores five steps that should be addressed by a system owner before federating a system. This series also contains several helpful sections and appendices, including reference architecture, implementation guidance and procurement language.

This document was developed by the DHS-established Public Safety Communication (PSC) Identity, Credential, and Access Management (ICAM) Working Group (WG); questions and comments can be sent to DHS S&T at: SandTFRG@hq.dhs.gov

[2] Most public safety communications systems, radio sites, public safety facilities, data centers and radios are physically secured against internal and external threats.

[3] Verizon Enterprise Solutions, 2017 Data Breach Investigations Report, which can be found at https://enterprise.verizon.com/resources/reports/2017_dbir.pdf.

2 STEPS TO MATURING THE SECURITY POSTURE

As the Public Safety Community (Community) moves towards seamlessly and securely sharing information between organizations, its members are beginning to update their systems to enable federation. In an effort to show the Community what steps are needed to mature its existing systems to accomplish this goal, this document provides a special focus on information sharing and federations.

Over the past two years, S&T has implemented a variety of systems with Identity, Credential, and Access Management (ICAM) capabilities in an S&T sandbox. The implementations focused on identifying challenges and their potential solutions when designing systems for information sharing and federation. This document describes steps an organization should take to prepare itself before joining a federation. It serves as a quick guide for the Community, based on lessons learned from two years of S&T's research and implementation of a variety of ICAM solutions that conform to NIST standards.

This document identifies five steps that organizations should consider as they prepare to share information with another organization:

1. Conduct a data assessment that includes where your data is stored.
2. Implement multifactor authentication.
3. Identify ICAM products necessary for federation.
4. Choose additional ICAM products for advanced access control.
5. Determine which data is sharable with which organizations.

Additional information on procuring ICAM products can be found in *Section 2.2 Evaluation Criteria* in the ICAM Acquisition Guidance.

2.1 CONDUCT A DATA ASSESSMENT THAT INCLUDES WHERE YOUR DATA IS STORED.

Before an organization determines how to protect its systems, it needs to assess the sensitivity of its data. The organization should determine the types of information in each system and classify the stored data as personally identifiable information (PII), personal health information (PHI), or sensitive information (e.g., Law Enforcement Sensitive). This assessment is particularly important because the sensitivity of the data creates a higher level of risk within a system. More information about assessing the level of risk in a system can be found in the ICAM Executive Primer.

By conducting a risk assessment of its infrastructure, organizations determine what rules should be established to protect each component system's information. Data assessments help organizations identify which types of data each user should be accessing. Once implemented, ICAM principles aid organizations by identifying the users within their systems and painting a clear picture of who is accessing what data.

Additionally, organizations should know where each type of data is stored – whether it be in a cloud-based application, a custom application, or an application housed on the organization's premises. An organization should educate itself on the security measures taken to protect its data, then assess whether additional measures should be implemented.

If the organization uses any commercial applications or services (such as cloud storage), it should ensure (through contracts) that it owns the rights to any data and can easily take measures to completely remove said data from the commercial application, if needed. Additionally, many commercial applications only authenticate users and cannot accept additional authorization measures an organization may want to implement (such as attribute-based access control). Organizations should assess whether the capabilities and limitations of each application enhance or hinder the roadmap for their system architecture.

2.2 Implement multifactor authentication.

As explained in the ICAM Executive Primer, multifactor authentication is recommended when a system contains any type of sensitive information. Many federal information sharing platforms require multifactor authentication, but most systems in the Community are only using a single factor – username/password – to authenticate. While it is not a silver bullet to prevent a system attack, multifactor authentication is a relatively easy and low-cost way to create a more-secure, first line of defense to protect against an information breach for some of an organization's most valuable information.

Many commercial applications have an option to implement multifactor authentication for all users. If an organization has a domain controller, but no identity provider (IdP), and uses the domain controller to provision users into on-premise applications, it may need to install additional software to implement multifactor authentication; more information can be found in the ICAM Implementation Guides.

2.3 Identify ICAM products necessary for federation.

If an organization does not have an IdP or domain controller, it cannot federate with another organization's system. Because federation involves one organization exchanging information about its users in a standard, agreed-upon format, an organization must have some sort of centralized identity store (to which its users authenticate) that can communicate a user's identity and assertions about their characteristics to external services or other organizations' identity hubs.

To federate and share information between systems, an organization requires a domain controller with additional software or an IdP. While some ICAM products are free, the downside is there is not always easily understandable documentation to review, or a help desk to call when support is needed. Wikis and open forums can be available and helpful, but they are not always a given. As a result, an organization might determine to purchase a product (or a product support contract) after a thorough review of available documentation and technical support because the product aligns with the organization's level of experience. Many fee-based products contain comprehensive documentation and are well-maintained; many products, regardless of price, offer expert fee-based support if needed.

Examples of no and low-cost ICAM solutions and products as well as steps for integration into a federation can be found in the ICAM Implementation Guides.

2.4 Choose additional ICAM products for advanced access control.

Organizations may want to control authorization to certain data based on time or other attributes. Many products that implement ICAM principles are specialized to perform one task exceptionally well – such as identity proofing, authentication, or attribute-based access control.

Some open source products can perform multiple functions but do not always possess the full capabilities out of the box. In such cases, an organization may want to consider hiring skilled engineers on staff or as consultants to configure and implement any desired additional capabilities within the product. If the organization has never created an ICAM-enabled system before, it might be best to have multiple engineers assigned to the project so they can help each other throughout the process of configuring the ICAM system. It could also benefit the organization to contract for a subject matter expert in ICAM principles and system requirements to help guide the engineers in overarching security concepts specific to the build.

The ICAM Acquisition Guidance includes questions that could be helpful when choosing ICAM products and consultants.

2.5 Determine which data is sharable with which organizations and how to share the data.

Once an organization's system is secured to the level the organization finds appropriate and has the necessary products for federation, the organization should return to its data assessment to determine what information it would like to share with other organizations. This information should be re-assessed to discern where it resides, and the level of risk associated with inter-organizational sharing. Then, the organization should decide the highest level of risk it can accept for an outside organization accessing its data. This determination will help organizations decide whether another organization's security posture and their ability to mitigate risk is strong enough to obtain access into their system. If not, organizations will have to decide whether they can accept the increased risk posed by another organization or deny another organization's access to their data.

Once the decision has been made to share information between organizations, an additional element for information sharing is required – the need to establish trust agreements between partners to safely and securely share information with users from other jurisdictions. Through information sharing agreements, partners acknowledge their trust that each partner operates their respective systems at the minimum security controls required, exercises adequate processes to vet every user's identity and utilizes a standard set of attributes for their users' identities. They also establish the intended use of the data, its protection and expiration of the data to users. This helps to protect the privacy of the data, with consideration to civil rights and civil liberties.

Joining a federation minimizes the number of bilateral agreements an organization must negotiate and monitor to share information. More information on federations and trust frameworks can be found in the ICAM Executive Primer.

3 CONCLUSION

To participate in information sharing between organizations, some members of the Community will need to follow one or more of the steps within this Checklist. The ICAM Educational Series was designed to help the Community seamlessly and securely share information with each other.