Identity, Credential, and Access Management (ICAM)

Executive Primer

Science and Technology Directorate

Homeland Security

Science and Technology

Primary Authors

Christine Owen

Larry Kroll

Chris Price

Ryan Page

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) Executive Primer

February 2019

Version 2

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 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 an Executive Primer on ICAM principles for the Public Safety Community (Community). This document provides an ICAM educational guide for all levels of any organization (executive leadership, program managers and solution architects).

The Community's goal is to have the ability to appropriately share critical information among members of the Community. 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). 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.

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, particularly identity federations, 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 ensure the information is not compromised. This is where ICAM is essential for the Community. Identity proofing 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.

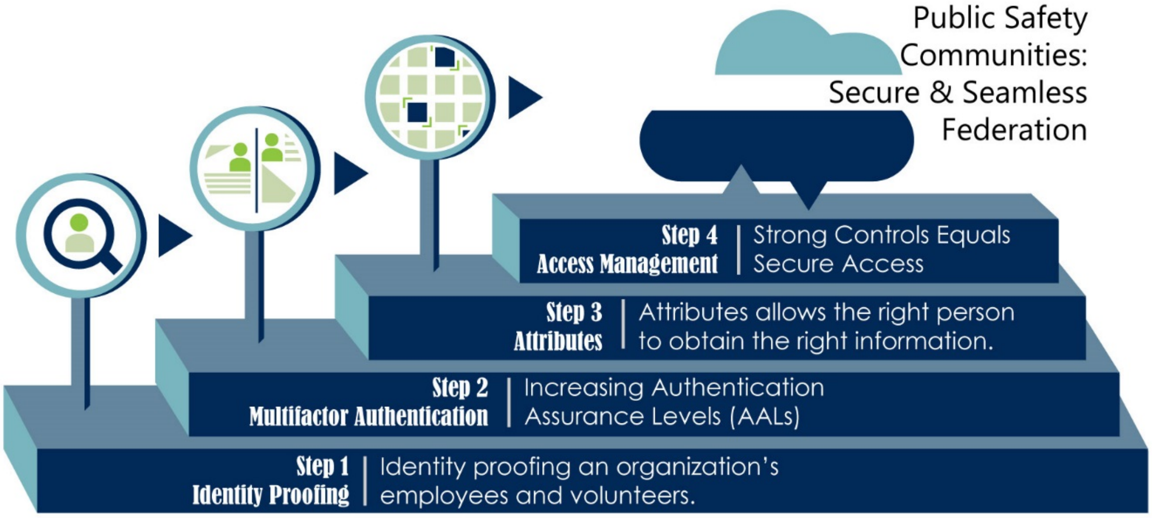

Public Safety Communities: Secure & Seamless Federation
Step 4 Access Management | Strong Controls Equals Secure Access
Step 3 Attributes | Attributes allows the right person to obtain the right information.
Step 2 Multifactor Authentication | Increasing Authentication Assurance Levels (AALs)
Step 1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

Figure 1 - Steps to secure and seamless information sharing (Federation)

This document is written to educate professionals, regardless of role or organization, about ICAM as a whole, and why ICAM principles will lead to more effective Community interoperability. It is not intended to recommend specific ICAM products. However, this document does encourage organizations to adopt a multifactor authentication solution of their choice as a first step to incorporating ICAM methodology. This document is paired with the ICAM Acquisition Guidance, ICAM Implementation Guides and ICAM Federation System Checklist.

Intended Audience

The document informs each of the following stakeholder groups[1] about ICAM, 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.	This document
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 solution 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 and standards that are required of an interoperable ICAM architecture solution.	This document, ICAM Acquisition Guidance & ICAM Federation System Checklist
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's companion documents (the ICAM Acquisition Guidance and ICAM Implementation Guides) provide structured technical guidance and reference artifacts to assist in achieving an ICAM-enabled system.	This document, ICAM Acquisition Guidance, ICAM Implementation Guides & ICAM Federation Checklist

[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 a source of high-level education of Identity, Credential, and Access Management (ICAM). The ICAM landscape is complex and there are many elements to consider. ICAM policies are important in enabling technology to share data across a wide variety of applications; these applications may include an organization's existing legacy systems and emerging nationwide initiatives, such as the Nationwide Public Safety Broadband Network (NPSBN), Next Generation 911 services, and the First Responder Network Authority (FirstNet).

While this document is focused on helping state, local, tribal and territorial (SLTT) Public Safety Community (Community) entities improve the security posture of their systems so they can safely and securely share information with each other, it can be used by anyone wishing to obtain a base-level understanding of ICAM principles. 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 first of a series of ICAM educational tools, including the ICAM Acquisition Guidance, ICAM Implementation Guides and ICAM Federation System Checklist.

1.1 PURPOSE

The intended benefit of this document is to educate the Community and other organizations on ICAM principles, components and services, and to promote the increased adoption of multifactor authentication. Implementing ICAM policies in systems enables faster, more efficient and safer information sharing, especially during response to threats and disasters of all sizes. This documents also references appropriate standards for ICAM based on stakeholder system assessments.

1.2 BACKGROUND

The Public Safety Communications Identity, Credential, and Access Management Working Group (PSC ICAM WG) 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 members include the 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

Through outreach to various communities (including FirstNet Stakeholders, the Federal ICAM Subcommittee, DHS Cybersecurity and the Office of the Director of National Intelligence's Sensitive But Unclassified (SBU) Technical Advisory Committee (STAC)), the PSC ICAM WG gathered existing ICAM documents that would support its ICAM test environment (i.e., sandbox). The resultant ICAM-enabled systems created in the sandbox revealed several findings and lessons learned that have informed and educated PSC ICAM WG on federated identity environments.

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 vulnerable to hackers. Since passwords are easily obtained via email phishing, single factor credentials played a factor in 81percent 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 [PIN]). 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 organization 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

Approach this document as a high-level ICAM guide for both adopting ICAM-enabled multifactor authentication solutions and how those solutions and general ICAM concepts are applied in the real world. This document is the introduction to a progressive series that offers an initial overview of ICAM and its importance to executive leadership, program managers and solution architects. 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 also has Implementation Guides that provide step-by-step instructions on building several different ICAM-enabled systems configured with multifactor authentication. The series ends with an ICAM Federation System Checklist, which includes 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.

[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 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

This document was developed by the PSC ICAM WG; questions and comments can be sent to DHS S&T at: SandTFRG@hq.dhs.gov.

2 AN INTRODUCTION TO IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (ICAM)

ICAM is a framework of policies and technology that helps protect sensitive information stored on computer systems by providing an organization higher assurance that the right individual is accessing the right resource at the right time for the right reason. Perhaps unknowingly, we all encounter these principles by performing ICAM-analogous functions every day. Unlocking doors, checking email, and unlocking cell phones are all real-world examples. This section aims to expand the reader's knowledge of specific ICAM concepts.

When you deposit money in a bank, you expect your money to be safe and secure, no matter how you access it – in person with a teller, online or through an ATM. To keep your money safe, the bank wants to ensure that you are the right person accessing the right bank account at the right time. To accomplish that, you expect the bank to verify that you are the person on the account with a driver's license if you withdraw money in person. When you withdraw money through an ATM, you must insert your card (also known as a credential or something you have) and enter your PIN (something you know) to prove your identity. This is an example of both ICAM and multifactor authentication.

Much like a bank, many Community organizations have access to and keep law enforcement sensitive information, as well as sensitive personally identifiable information (PII) and protected health information (PHI), of the people they protect. Because copious amounts of sensitive information are stored on many of the Community members' systems and cloud-based applications, it is important for the Community to think of their technical infrastructure as a bank vault containing precious items. Accessing a system using only username and password (single factor authentication, which results in a weak credential) is akin to a bank giving money to a person who just presents their ATM card without using a PIN. While the bank would confirm that account was open with money at the institution, it does not actually know whether the person is an authorized user of the account without verifying their identity.

However, when the bank verifies the person's identity by use of an ATM card and PIN (multifactor authentication), the bank can be reasonably sure that person is the right person to access the right bank account at that time, because this is a much stronger credential. This practice helps to keep unauthorized users away from a person's money. Similarly, the Community's systems should be secured with credentials that help keep intruders from its systems via multifactor authentication – meaning users are not just using username/password, but rather authenticating with two of the following three categories: (1) something they have (credential), (2) something they are (biometric), and (3) something they know (PIN/password).

2.1 IDENTITY MANAGEMENT

Identity management allows an organization to establish, maintain and terminate identities. An *identity* is a set of characteristics that describe an individual within a given context, such as Army Reservist, volunteer firefighter or policeman. While identities can change (i.e., when a person moves from one organization to another) or be terminated (i.e., retire from the Army), identities never expire.

To create an identity, an organization must first *identity proof* a person by verifying that the person is who they say they are. There are three different Identity Assurance Levels (IALs)[4]:

[4] A deeper discussion of IALs can be found at NIST SP 800-63a.

- IAL1: anonymous (signing up for a social media account – the person's actual identity is not checked);
- IAL2: remote proofing (obtaining car insurance online – the person's identity is verified remotely through government documents (i.e., a driver's license number); or
- IAL3: in-person proofing (obtaining a license at the DMV – the person's identity is verified through official documents and in-person).

Note: Most of the Community will have already identity proofed their staff at an IAL3, which is the strongest possible.

Once an organization identity proofs a person, it will assign that person an *identifier*, which is a unique attribute that can be used to locate a specific identity within an organization. An example of an identifier is an employee number or a driver's license number.

2.2 CREDENTIAL MANAGEMENT

Credential management allows an organization to issue, track, update and revoke credentials for identities. A *credential* is authoritative evidence of an individual's identity within an organization. A credential could be anything from a driver's license to an ATM card, or an electronic item (such as a one-time password sent to your email).

Unlike identities, credentials generally expire. If a credential is lost or compromised before it expires, it can be revoked. With the use of a valid credential, an individual *authenticates* their identity for an organization.

Authentication is how you confirm who you are, generally with a credential. Authentication is a two step-process:

Step 1: Authenticate the credential itself –

- Was the credential issued by a trusted organization?
- Has the credential expired?
- Has the credential been revoked, voided or tampered?

Step 2: Ensure the individual the credential was issued to is the same individual presenting it –

- Does the photo and height/weight on the driver's license match the person who presented it?
- Does the person know the PIN for the ATM card that was used?

Authentication uses an identity (generally proven by a credential) that was established during the identity proofing process.

Credentials can incorporate something you know (a password or PIN), something you have (an ATM card) or something you are (your fingerprint). Some credentials incorporate more than one of those three things, which creates multifactor authentication.

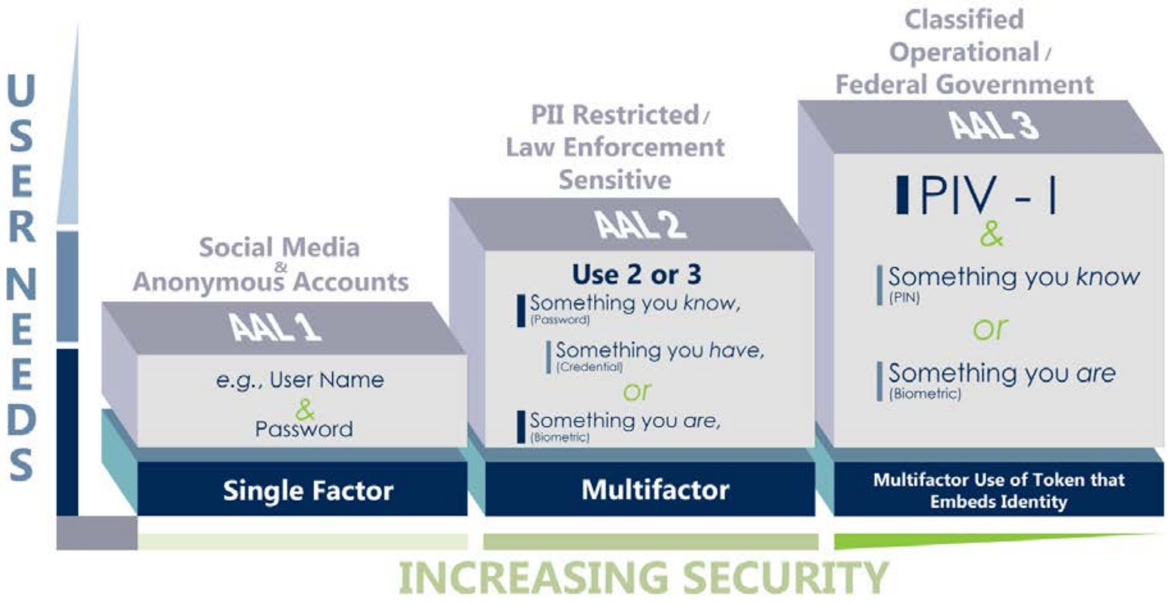

USER NEEDS
Social Media & Anonymous Accounts
AAL 1
e.g., User Name & Password
PII Restricted/ Law Enforcement Sensitive
AAL 2
Use 2 or 3
Something you know, (Password)
Something you have, (Credential)
or
Something you are, (Biometric)
Classified Operational/ Federal Government
AAL 3
PIV - I
&
Something you know (PIN)
or
Something you are (Biometric)
Single Factor
Multifactor
Multifactor Use of Token that Embeds Identity
INCREASING SECURITY

Figure 2 - Authentication Assurance Levels for multifactor authentication.

There are three different assurance levels for credentials (called Authentication Assurance Levels (AALs)[5]):

- AAL1: single factor, signing into your email by just using a password;
- AAL2: multifactor, signing into your bank account using a password (something you know) and a one-time password emailed to you (something you have)); or
- AAL3: multifactor with a hard-token credential that includes an electronic version of your identity, using your debit card with a chip in it (something you have), and a PIN (something you know).

Note: Since using a single factor, such as a username and password, to access a computer system is the weakest approach to protecting your system, every organization should consider implementing multifactor authentication on its systems to provide a stronger credential within its systems.

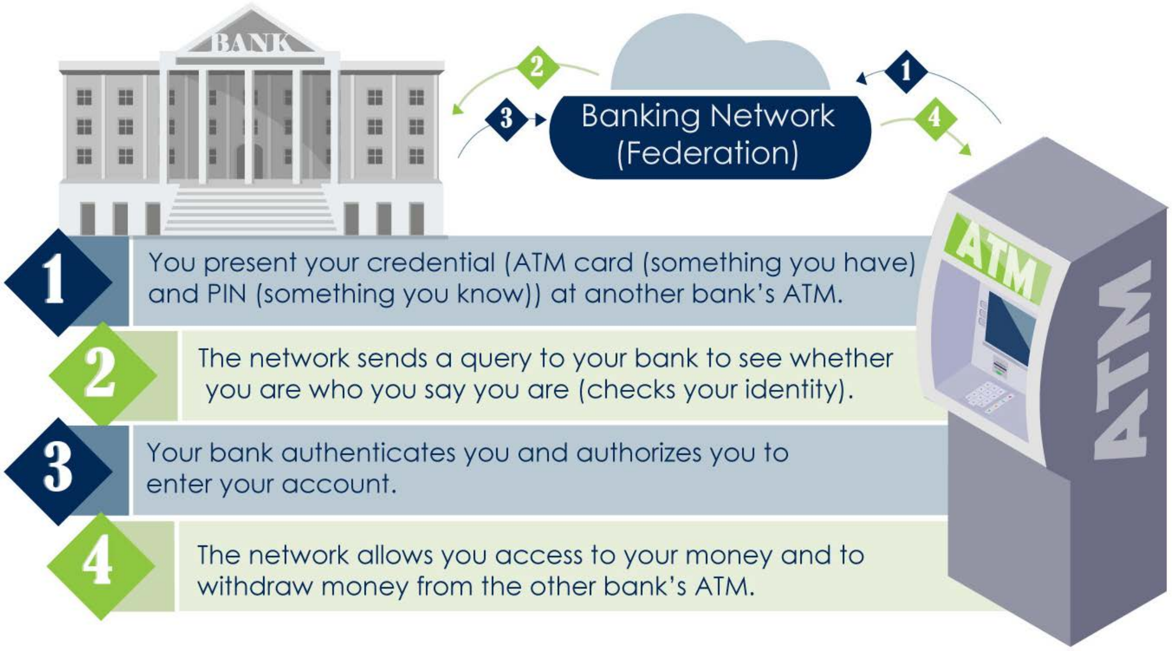
2.3 Access Management

Access management allows only certain individuals to access documents or applications within an organization's system. It is critical to be certain that the person to whom you are providing access is indeed the person you intend – that is why the assurance level of the identity (described above) is so important. Access management can be governed by laws and regulations, as in the case of a governmental organization, but are generally governed by the requirements and policies of an organization. For example, an organization might want only its human resources team to view personnel records or only medical personnel to have access to a medical database, and therefore it would provision access accordingly.

Authorization is the adjudication of access requests; it determines whether the system's policies allow a user to perform a requested action and enforces the applicable policy. Examples of authorization include the ability of an individual to sign into an application or cross a perimeter at a rescue site. In many cases, it is necessary to authenticate an individual to authorize them, much like a bartender authenticates you by

[5] A deeper discussion of AALs can be found at NIST SP 800-63b.

checking your photo ID while authorizing you to ensure you are old enough to be served alcohol by checking your birth date.



1 You present your credential (ATM card (something you have) and PIN (something you know)) at another bank's ATM.

2 The network sends a query to your bank to see whether you are who you say you are (checks your identity).

3 Your bank authenticates you and authorizes you to enter your account.

4 The network allows you access to your money and to withdraw money from the other bank's ATM.

Figure 3 - The steps for secure banking all over the world.

Once an organization has baked ICAM principles into its systems, it has begun to mitigate the risk of system compromise. The organization can also enter into information sharing agreements and connect its systems with other organizations that have a similar security posture, which is called federation.

Federation is the ability of one organization to accept another organization's work (i.e., identity proofing, credentials and/or attributes) based on inter-organizational trust. An example of federation includes using your ATM card at another bank's ATM to withdraw money around the world. Federation is useful because it allows an individual to use one credential to access information in multiple systems at multiple organizations. It also facilitates the seamless and secure exchange of information.

An organization can automate its access management by placing *attribute-based access control (ABAC)* within its system. In an ABAC-enabled system, an organization assigns attributes to users, tags data within its system with attributes, and creates access control rules that allow or disallow the users to access data with matching attributes (called data tags) after the user has been authenticated into the system. An analogous example of an ABAC-enabled system is the Transportation Security Administration (TSA) lines at an airport. Each traveler can be automatically assigned an attribute, such as TSA PreCheck, or given no attribute based on a background check and risk assessment of the traveler. The traveler is then admitted to their assigned line after their driver's licensed is verified (i.e., the traveler is authenticated) and their level of screening is based on the attribute assigned to their ticket.

3 THE STEPS OF AN ICAM-ENABLED SYSTEM

Successfully implementing ICAM policies requires the use of reliable and expandable "core" elements.[6] Those elements include data assessment, risk evaluation, architecture design, an identity provider, a credential service provider and access management. Once an organization successfully implements these core elements, the organization can participate in federation (resource sharing with outside organizations) and/or create an attribute exchange.

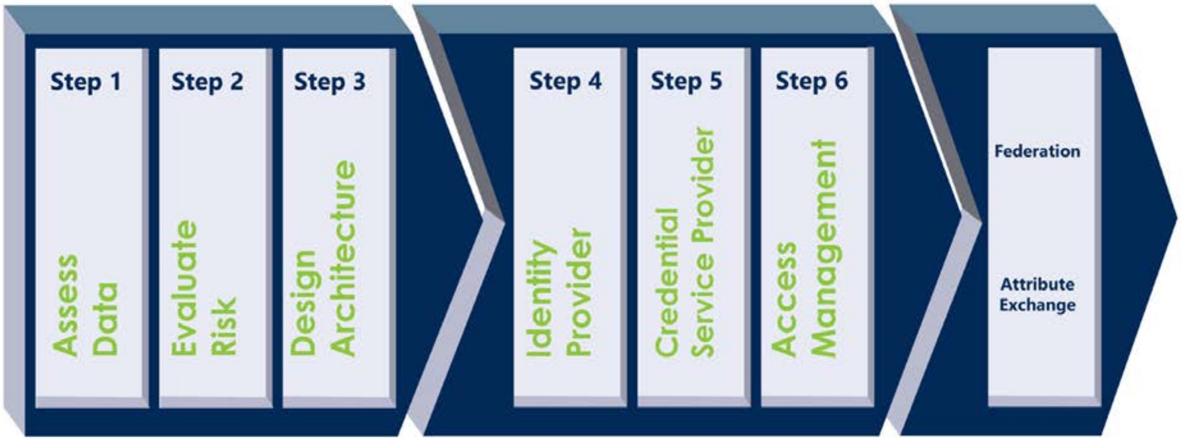


Figure 4 - The steps of an ICAM-enabled system.

System owners will use the first three steps to evaluate what is in their system and what their system looks like, while the components (that are built or bought) of the middle steps will create a system. Creating an ICAM-enabled system can result in federation (resource sharing with other systems), as well as the ability to create an attribute exchange within a system. Each step also contains questions system owners need answered when protecting a system.

[6] These "core" elements were developed based on the SICAM Roadmap and NIST SP 800-63-3.

3.1 ASSESS SYSTEMS ENVIRONMENT

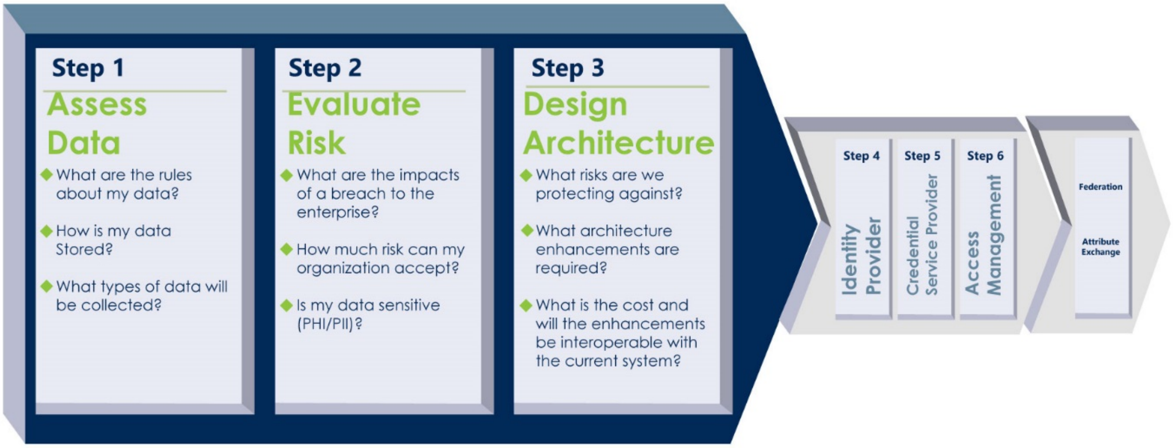

Step 1
Assess Data
What are the rules about my data?
How is my data Stored?
What types of data will be collected?
Step 2
Evaluate Risk
What are the impacts of a breach to the enterprise?
How much risk can my organization accept?
Is my data sensitive (PHI/PII)?
Step 3
Design Architecture
What risks are we protecting against?
What architecture enhancements are required?
What is the cost and will the enhancements be interoperable with the current system?
Step 4
Identity Provider
Step 5
Credential Service Provider
Step 6
Access Management
Federation
Attribute Exchange

Figure 5 - Questions for assessing a system.

To create an ICAM-enabled system, organizations should first evaluate their data by performing privacy and sensitivity assessments on the information they will keep in their system. A system that stores information containing PII, PHI and sensitive information (e.g., Law Enforcement Sensitive) would have a higher amount of risk associated with it, whereas another system might have less PII, PHI or sensitive information and would therefore carry less risk. Evaluating stored data helps organizations determine the amount of risk the organization can assume and what rules should be established to protect the system's data. After determining what type of data will be stored in the system, an organization must then evaluate the amount of risk it can carry for the system by evaluating the amount of money and damage a breach would cost, as well as ways to reduce the risk of a breach to the organization's system. At this point, an organization should decide at what assurance levels (xAL)[7] the system should be built.

The assurance levels and other requirements are the rules that inform the system architecture for the organization. Before drafting the system architecture, an organization should evaluate current system architecture, interoperability, product availability and costs to determine the best ICAM-enabled fit for the organization. It might be helpful to review the companion ICAM Implementation Guides for reference architecture.

[7] The three Assurance Levels, as explained in NIST 800-63-3, are Identity Assurance Level (IAL), Authentication Assurance Level (AAL) and Federation Assurance Level (FAL), or collectively xALs. There are three levels for each xAL – the higher each AL is, the more secure a system will be. See also section 2.1 and 2.2 above.

3.2 Connect Your Products or Services Together to Create an ICAM-enabled System

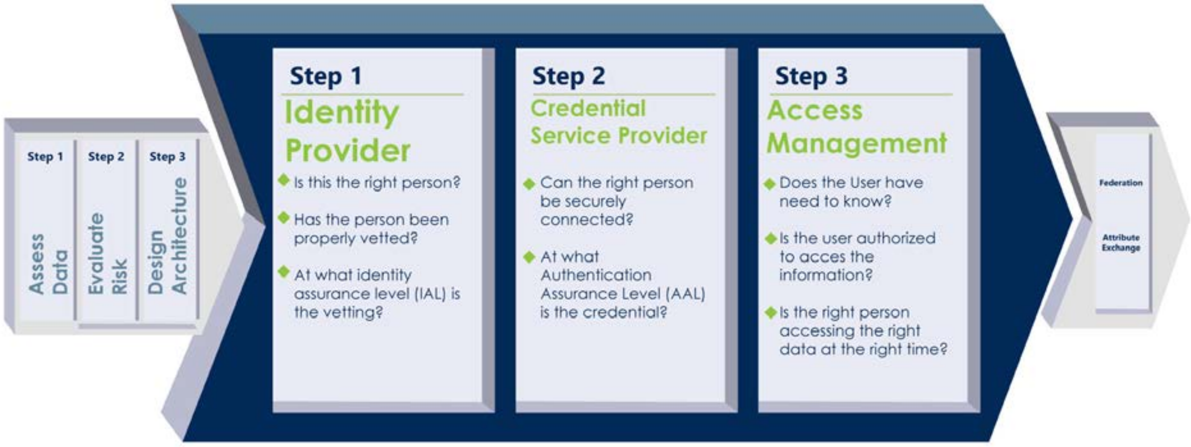

Step 1
Step 2
Step 3
Assess Data
Evaluate Risk
Design Architecture
Step 1
Identity Provider
Is this the right person?
Has the person been properly vetted?
At what identity assurance level (IAL) is the vetting?
Step 2
Credential Service Provider
Can the right person be securely connected?
At what Authentication Assurance Level (AAL) is the credential?
Step 3
Access Management
Does the User have need to know?
Is the user authorized to acces the information?
Is the right person accessing the right data at the right time?
Federation
Attribute Exchange

Figure 6 – ICAM answers key questions when you connect services together.

After determining a system's architecture, organizations can build and connect their identity provider, credential service provider and access management software.[8] An ICAM-enabled system configured for multifactor authentication facilitates secure information sharing with the right people when they need it.

The Community already performs identity proofing for their employees and volunteers,[9] and many communities secure their computer systems through a single factor – username/password. When SLTT Community members decide to implement more ICAM services, it is strongly recommended they include multifactor authentication in its systems upgrades, as those systems contain PII, PHI, law enforcement sensitive and other sensitive information.

Once AAL and IAL requirements are set into a system, an organization should also determine who should access which parts of the information available within each system. An ICAM-enabled system will determine whether a user is authorized to access information based on access management controls put in place by the system owners.

Additionally, these systems are combined over time, often from components not designed to operate neatly with each other. For example, one vendor might have created the system to create a user identity, whereas another might have set up a firewall perimeter. Because there is a large variety of products on the market, as well as a multitude of product combinations, each organization will have a different system configuration based on its own needs, recommendations from consultants, interoperability with current infrastructure and the technology available at the time of the build.

To conduct information sharing within and between organizations, the organizations will have to trust that each other's systems of assorted components are built to similar assurance levels. Protecting the systems with ICAM principles – including multifactor authentication – will help the organizations ensure that the wrong people are not accessing sensitive data that organizations want to keep protected.

[8] For more information on connecting an ICAM-enabled system together, see the companion Implementation Guides.

[9] A person's identity proofing may include a completed I-9 form, drug test, as well as credit and background checks.

3.3 THE BENEFITS OF AN ICAM-ENABLED SYSTEM

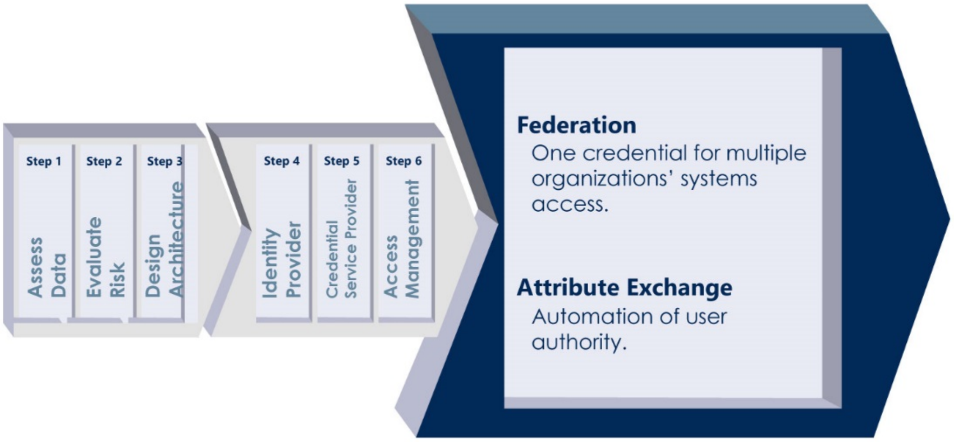


Figure 7 - ICAM-enabled systems can result in federation and/or an attribute exchange.

If a Community organization plans on sharing information with other organizations, that organization should consider securing its computer systems to higher assurance levels to protect its valuable information from intruders. It should also take into account the security posture of the other organization when assessing its overall risk of exposure, as a system is only as strong as its weakest link. It is important to always know precisely who is accessing information and what their attributes are, so only the right person will access the right information at the right time. To accomplish this, organizations' systems should be secured with credentials that facilitate multifactor authentication – meaning more than just username/password – requiring at least two of the following three categories: (1) something they have (credential), (2) something they are (biometric), and (3) something they know (PIN/password).

A federation connects more than one computer system together – this could be systems from the same organization or two different organizations. In many cases, a federation is created once an organization implements the requirements from a trust framework. These frameworks contain requirements to join a federation and allow for each organization to trust the other once authentication requirements are met.

A typical system draws on an access control list designated to different parts of a system to authenticate valid users into system resources. The system administrator is responsible for manually entering a determination of whether a particular user can access a system or piece of data. Such processes are onerous for IT departments and not suitable for rapid authorization determinations.

Once a "core" ICAM-enabled system is built, organizations can facilitate authorization determinations by automating access provisioning across a system using attribute exchange. Attributes are relevant user characteristics that trigger a positive or negative access decision – for example "EMT" for a medical record, "police officer" for a case file or "manager" for a personnel record.

When an organization is federated and has a strong credential that is bound to a well-vetted identity, such attributes can also be bound to the credential. In that case, a federated user can be asserted as attributes, e.g., "(1) a sworn police officer (2) in the jurisdiction of Pennsylvania (3) with arrest powers" rather than "Officer Bob Johnson." The system's access decision component can then automatically accept those three attributes from a trustworthy source outside the organization, so long as it is tied to a strong credential. This is much more efficient than having the user wait for an administrator to manually confirm Officer Bob Johnson's prerequisites.

Such a process presents a valuable reason to accept credentials from outside organizations for information sharing purposes through an identity federation. The above example is referred to as an ABAC system and can be used by an organization to automate policy controls within its system to control which people have access to certain data or resources.[10] ABAC is the automation of authorization within an organization system's cumbersome and delay-prone manual processes.

While automation can occur with federation and an ABAC system, you want to fully establish an ICAM-enabled system to ensure you know who is entering your system and accessing your data to ensure the information does not fall into the wrong person's hands. Using multifactor authentication along with an ABAC system allows you to better trust that the right person is accessing the right information at the right time for the right reason. With the addition of federation, such a system configuration allows for seamless and secure information sharing.

[10] For more information on ABAC, please see NIST SP 800-162 http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf and NIST's NCCoE ABAC Building Block at https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control.