ICAM: A Foundation for Trusted Identities in Cyberspace

William Stallings, WilliamStallings.com

The US government’s Identity, Credential, and Access Management (ICAM) strategy aims to provide a secure, manageable, and user-friendly foundation for building a trustworthy identity ecosystem among government agencies, state and local partners, and the private sector.

In today’s online environment, a typical organization must provide access and maintain accounts for numerous users, including customers, personnel, government entities, and business partners. Typically, a large organization will have dozens of websites and databases, with individuals required to register and maintain usernames and passwords for each site they wish to access. This approach places a significant burden on the organization in managing numerous accounts and access environments. It’s also a burden to users, and encourages behavior such as the reuse of passwords that makes online fraud and identity theft easier.

To enhance security in a way that’s more manageable and user-friendly, both public- and private-sector organizations are moving toward integrated approaches that provide a high level of trust associated with identities in cyberspace. Ideally, a user will have a single unique digital identity, with associated credentials, that enables an organization to provide access to various services in various contexts based on the user’s identity and attributes.

In recognition of the rising cybersecurity risks as online transactions increase, the White House issued its National Strategy for Trusted Identities in Cyberspace (NSTIC). This initiative aims to work collaboratively with the private sector, advocacy groups, public-sector agencies, and other organizations to improve the privacy, security, and convenience of online transactions. The NSTIC has as its goal an identity ecosystem—an online environment in which individuals and organizations will be able to trust each other because they follow agreed-upon standards to obtain and authenticate their digital identities and those of devices. The identity ecosystem is
designed to securely support transactions ranging from anonymous to fully authenticated and from low to high value. Fundamental to the implementation of this strategy is the federal program known as Identity, Credential, and Access Management (ICAM).

This article introduces the elements that make up ICAM and discusses how ICAM fits in with an open trust framework for trustworthy identity and attribute exchange.

**ICAM Components**

ICAM is a comprehensive approach to managing and implementing digital identities (and associated attributes), credentials, and access control. It’s not only applicable to government agencies but can also be deployed by enterprises looking for a unified approach to access control. ICAM is designed to do the following:

- It creates trusted digital identity representations of subjects, which include individuals and nonperson entities (NPEs). The latter include processes, applications, and automated devices seeking access to a resource.
- It binds those identities to credentials that can serve as a proxy for the individual or NPE in access transactions. A credential is an object or data structure that authoritatively binds an identity and related attributes to a token possessed and controlled by a subscriber.
- It uses credentials to provide authorized access to an agency’s resources.

The next three sections examine each of these aspects in detail.

**Identity Management**

Identity management deals with assigning attributes to a digital identity and connecting that identity to an individual or NPE. Attributes are characteristics that define specific aspects of the subject, such as a subject’s identifier, name, organization, and job title. A subject’s role and access permissions can also be viewed as attributes.

The goal of identity management is to establish a trustworthy digital identity independent of a specific application or context. The traditional approach to access control for applications and programs is to create a digital representation of an identity for the application or program’s specific use. Maintenance and protection of the identity is treated as secondary to the mission associated with the application. There is considerable overlap in effort in establishing these application-specific identities.

In contrast, enterprise identity records are not tied to job title, job duties, location, or whether access is needed to a specific system. Those items might become attributes tied to an enterprise identity record and become part of what uniquely identifies an individual in a specific application. Access control decisions are based on the context and relevant attributes of a user—not solely his or her identity. The concept of an enterprise identity is that individuals will have a single digital representation of themselves that can be leveraged across departments and agencies for multiple purposes, including access control.

Figure 1 depicts the key functions involved in identity management. Establishment of a digital identity begins with collecting identity data as part of an on-boarding process. A digital identity consists of a set of attributes that uniquely identify a user within an enterprise. To establish trust in the individual represented by a particular identity, an agency can also conduct a background investigation. Attributes about an individual can be stored in various authoritative sources in an agency, and linked to form an enterprise view of the digital identity. This identity is then provisioned into applications to support physical and logical access and de-provisioned when access is no longer required.

One component of identity management is life-cycle management, which includes the mechanisms, policies, and procedures for protecting personal identity information. Identity management also deals with controlling access to identity data, and techniques for sharing authoritative identity data with applications that need it.

**Credential Management**

A credential is an object or data structure that authoritatively binds an identity and associated attributes to a token possessed and controlled by a subscriber. Examples of credentials are smart cards, private and public cryptographic keys, and digital certificates. Credential management is the management of the credential’s life cycle. It encompasses the following five logical components.
First, an authorized individual sponsors an individual or entity for the credential. For example, a department supervisor sponsors a department employee. Next, the sponsored individual enrolls for the credential, a process that typically consists of identity proofing and the capture of biographic and biometric data. This step might also involve incorporating authoritative attribute data. Then, a credential is produced. Production might involve encryption, the use of a digital signature, the production of a smartcard, or other functions. Next, the credential is issued to the individual or NPE. Finally, a credential must be maintained over its life cycle, which might include revocation, reissuance or replacement, reenrollment, expiration, PIN reset, suspension, or reinstatement.

**Access Management**

The access management component deals with the management and control of how entities are granted access to both logical and physical resources. Access management ensures that the proper identity verification is made when an individual attempts to access security-sensitive buildings, computer systems, or data. The access control function uses credentials presented by those requesting access and the requestor’s digital identity. Three support elements are needed.

**Resource management** defines rules for a resource that requires access control. The rules include credential requirements and what user attributes, resource attributes, and environmental conditions
are required to access a given resource for a given function.

Privilege management establishes and maintains the entitlement or privilege attributes that comprise an individual’s access profile. These attributes represent features of an individual that can be used to determine access decisions to both physical and logical resources. Privileges are considered attributes that can be linked to a digital identity.

Policy management governs what is allowable in an access transaction. Given the identity and attributes of the requestor, the attributes of the resource or object, and environmental conditions, a policy specifies what actions this user can perform on this object.

Identity Federation
Identity federation addresses two questions: How do you trust the identities of individuals from external organizations that need access to your systems? And how do you vouch for the identities of individuals in your organization when they need to collaborate with external organizations?

Identity federation comprises the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization.

Trust Frameworks
The interrelated concepts of trust, identity, and attributes have become core concerns of Internet businesses, network service providers, and large enterprises. These concerns can clearly be seen in the e-commerce setting. For efficiency, privacy, and legal simplicity, parties to transactions generally apply the need-to-know principle: What do you need to know about someone in order to deal with them? The answer varies, and includes such attributes as professional registration or license number, organization and department, staff ID, security clearance, customer reference number, credit-card number, unique health identifier, blood type, Social Security number, address, citizenship status, and social networking handle. The attributes of an individual that must be known and verified to permit a transaction depend on context.

The same concern for attributes is increasingly important for all types of access control situations. For example, an enterprise might need to provide access to resources for customers, users, suppliers, and partners. Depending on context, access will be determined not just by identity but also by the attributes of the requestor and the resource.

Traditional Identity Exchange Approach
Online transactions involving parties from different organizations, or between an organization and a user such as an online customer, generally require the sharing of identity information. This information can include associated attributes in addition to a name or numerical identifier. Both the party disclosing the information and the party receiving it must have a level of trust about security and privacy issues related to that information.

Figure 2a shows the traditional technique for the exchange of identity information, which involves users developing arrangements with an identity service provider to procure digital identity and credentials, as well as arrangements with relying parties that provide user services and applications and that are willing to rely on the identity and credential information generated by the identity service provider.

This arrangement must meet several requirements. The relying party requires that the user be authenticated to some degree of assurance, that the attributes imputed to the user by the identity service provider are accurate, and that the provider is authoritative for those attributes. The identity service provider requires assurance that it has accurate information about the user and that, if it shares information, the relying party will use it in accordance with contractual terms and the law. The user requires assurance that the identity service provider and relying party can be entrusted with sensitive information and that they will abide by the user’s
preferences and respect his or her privacy. All parties require that the practices described by the other parties are those implemented by the parties, and must know how reliable those parties are.

Open Identity Trust Framework
Without some universal standard and framework, the arrangement depicted in Figure 2a must be replicated in multiple contexts. A preferable approach is to develop an open, standardized approach to...
trustworthy identity and attribute exchange. One such approach, the Open Identity Trust Framework, is gaining increasing acceptance.

This topic is burdened with numerous acronyms, so let’s first define the most important of these:

- **OpenID.** This open standard lets users be authenticated by cooperating sites (relying parties) using a third-party service, eliminating the need for webmasters to provide their own systems and allowing users to consolidate their digital identities. Users can create accounts with their preferred OpenID identity providers, and then use those accounts as the basis for signing on to any website that accepts OpenID authentication.

- **OIDF.** The OpenID Foundation is an international nonprofit organization of individuals and companies committed to enabling, promoting, and protecting OpenID technologies. OIDF assists the community by providing needed infrastructure and help in promoting and supporting expanded adoption of OpenID.

- **ICF.** The Information Card Foundation is a nonprofit community of companies and individuals working to evolve the information card ecosystem. Information cards are personal digital identities that people can use online, and the key component of identity metasystems.

- **OITF.** The Open Identity Trust Framework is a standardized, open specification of a trust framework for identity and attribute exchange, developed jointly by OIDF and ICF.

- **OIX.** The Open Identity Exchange Corporation is an independent, international provider of certification trust frameworks conforming to the OITF model.

- **AXN.** An attribute exchange network is an online, Internet-scale gateway for identity service attributes in high volumes at affordable costs.

System managers need to be able to trust that the attributes associated with a subject or object are authoritative and are exchanged securely. One approach to providing that trust in an organization is the ICAM model. Combined with an identity federation functionality that’s shared with other organizations, attributes can be exchanged in a trustworthy fashion, supporting secure access control.

The concept of identity federation and federated identity standards and protocols can serve as a foundation for developing an open attribute exchange capability that can be used across all digital business settings. The OITF specification provides such a capability by defining the elements needed for an AXN. The AXN is user-centric and privacy-enhancing in that it provides for user control of fine-grained and permissioned exchange of attributes and verification of those attributes. The intent is that private and public sector organizations can implement AXN infrastructure appropriate to their requirements, such that participating organizations (relying parties) can provide attribute information for the benefit of this information’s users.

In digital identity systems, a trust framework is a certification program that enables the relying party to trust the identity, security, and privacy policies of the party who issues the credential (the identity service provider) and vice versa. The OIX defines a trust framework as a set of verifiable commitments from each of the various parties in a transaction to their counterparts. These commitments include controls (including regulatory and contractual obligations) to help ensure that commitments are delivered, and remedies for failure to meet such commitments. A trust framework is developed by a community whose members have similar goals and perspectives. It defines the rights and responsibilities of the participants, specifies the policies and standards specific to the community, and defines the community-specific processes and procedures that provide assurance. Different trust frameworks can exist, and sets of participants can tailor trust frameworks to meet their particular needs.

Figure 2b shows the elements involved in the OITF. In any given organization or agency, the following roles are part of the overall framework. As discussed, relying parties, or service providers, are entities delivering services to users. Relying parties must have confidence in the identities or attributes of their intended users, and must rely on the various credentials presented. Subjects are users of a relying party’s services, including customers, employees, trading partners, and subscribers. **Attribute providers** are entities acknowledged by the community of interest as being able to verify given attributes as presented by subjects and that are equipped through the AXN to create conformant
attribute credentials according to the AXN’s rules and agreements. Some attribute providers will be sources of authority for certain information; more commonly, such providers will be brokers of derived attributes. Finally, as discussed, identity service providers authenticate user credentials and vouch for the names of subjects. They are equipped through the AXN or some other compatible identity and access management (IDAM) system to create digital identities that can be used to index user attributes.

The following support elements are an important part of an AXN:

- **Assessors** evaluate identity service providers and relying parties and certify that they are capable of following the OITF provider’s blueprint.
- **Auditors** might be called on to check that parties’ practices have been in line with what was agreed on for the OITF.
- **Dispute resolvers** provide arbitration and dispute resolution under OIX guidelines.
- **Trust framework providers** translate the requirements of policymakers into a blueprint for a trust framework that they then proceed to build, doing so in a way that is consistent with the minimum requirements set out in the OITF specification.

Figure 3. Tiered ICAM architecture. The architecture consists of five layers and is designed to meet the needs of patients, insurers, and healthcare providers.

The solid arrows in Figure 2b indicate agreements with the trust framework provider for implementing technical, operations, and legal requirements. The dashed arrows indicate other agreements potentially affected by these requirements. In general terms, the model illustrated in Figure 2b operates as follows. Responsible people in participating organizations determine the technical, operational, and legal requirements for exchanges of identity information that fall under their authority. They then select OITF providers to implement these requirements. These providers translate the requirements into a blueprint for a trust framework that might include additional conditions of the OITF provider. This provider vets identity service providers and relying parties and contracts with them to follow its trust framework requirements when conducting identity information exchanges. The contracts carry provisions relating to dispute resolvers and auditors for contract interpretation and enforcement.

**Federal ICAM Applicability**

Although ICAM is designed to meet the needs of federal agencies, it is a useful model for other public- and private-sector organizations worldwide. Because the federal government is dictating the implementation and use of ICAM elements,
private sector companies that are providers of ICAM components to the government, as well as private sector companies under government contract, are gaining valuable experience in the design and implementation of ICAM and its constituent functions. This expertise readily carries over to other environments.

One prominent example is the adoption of the ICAM approach at the state level in the US. The National Association of State Chief Information Officers has developed a state-level version of ICAM, known as the State Identity, Credential, and Management (SICAM) architecture. The SICAM document uses the same architecture as the federal ICAM model and provides guidance on developing interoperable state-level ICAM systems.

In the private sector, a likely candidate for early implementation of the ICAM model is the healthcare industry. Healthcare providers, insurers, and patients operate in an increasingly digitized and online environment in which issues related to privacy, government regulation, the need for cooperation among providers, and cost are all paramount. A recent white paper by consulting firm the Triage Group outlines a viable approach for securing personal health information and making it easily accessible through health information technology (HITECH) applications, based on the ICAM model.

Figure 3 illustrates a tiered ICAM architecture designed to meet the needs of patients, insurers, and healthcare providers. The ICAM architecture consists of five layers, or tiers. The presentation tier facilitates authentication and access to services across PCs, phones, PDAs, tablets, and other user devices. The ICAM application tier includes core ICAM services to enable system and facility access. The integration tier provides various enterprise integration services. The data tier supports a wide variety of directories and other data repositories. The core technology tier assimilates with an enterprise’s existing core technology stack.

This architecture, properly implemented, will enable all of the concerned entities (healthcare providers, insurers, and patients) to interact efficiently and securely. For the patient, the system provides easy and secure access to personal health records. For all concerned entities, an ICAM system provides a way to define access privileges on the basis of identity, attributes, and privileges. With the proper user interfaces, an ICAM system achieves a comprehensive approach to secure access.

The interconnected, Internet-based global economy relies increasingly on digital identity management and use. The design and implementation of ICAM is a significant step in the direction of a secure, trusted, and manageable identity ecosystem.

References

William Stallings is a consultant, lecturer, and author of numerous computer science textbooks on cryptography, computer organization, operating systems, and computer networking. He created and maintains the Computer Science Student Resource Site at ComputerScienceStudent.com, which provides documents and links on a variety of subjects of general interest to computer science students and professionals. Stallings is a member of the editorial board of Cryptologia, a scholarly journal devoted to all aspects of cryptography. His latest book, with Laurie Brown, is Computer Security (Pearson, 2015). Contact him at ws@shore.net.

Selected CS articles and columns are available for free at http://ComputingNow.computer.org.