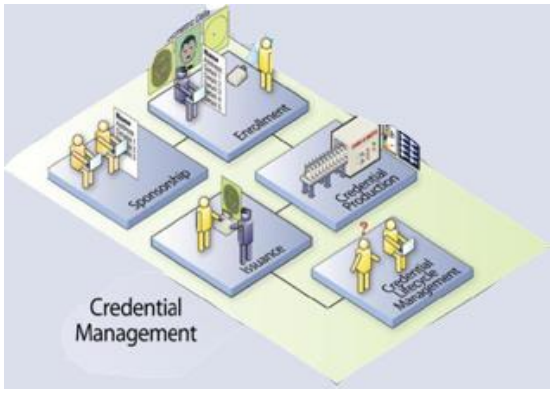
CREDENTIAL MANAGEMENT

Meeting the challenges of cyber and physical security threats is a necessity for the private and public sectors in the 21st Century. With continually changing threats to security, protecting sensitive data becomes ever more important. It is vitally important for any organization to reliably authenticate an individual's identity and to limit access to protected resources and information based on that identity. In the Federal Government, the initiative governing this effort is referred to as Identity, Credentialing, and Access Management (ICAM). ICAM comprises the programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals, organizations, and non-person entities (hereafter, the general term, 'entity' will be used); bind those identities to credentials that may serve as a proxy in access transactions; and leverage the credentials to provide authorized access to an agency's resources[1].

ICAM is made up of five core components: Identity Management, Credential Management, Access Management, ICAM Intersection, and Auditing and Reporting, and the activities performed in one ICAM area are leveraged in other ICAM areas to establish assurances and trust for improved security. A credential authoritatively binds an identity to a token possessed and controlled by an entity.[2] While the primary goal of identity management is to establish a trustworthy process for assigning attributes to a digital identity and to connect that identity to an entity,[3] Credential Management supports the life cycle of the credential itself, from the initial sponsorship through self-service.



OPERATIONAL ASPECTS OF CREDENTIAL MANAGEMENT[4]

In the Federal Government, examples of credentials include smart cards, private/public cryptographic keys, and digital certificates.[5] The Homeland Security Presidential Directive 12 (HSPD-12) mandate requires "a common, standardized identity credential that enables secure, interoperable online transactions[6]". Credentials not only establish identity, but also fulfill the 'something you have' component of a multifactor authentication requirement for access to resources or information.

---

[1]Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0. December 2, 2011 pg. 7

2 NIST Special Publication 800-63-2, Electronic Authentication Guideline, August 2013, p. 6

[3] Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0. December 2, 2011 pg. 9

4 Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0. December 2, 2011 pg. 7

5 Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0. December 2, 2011 pg. 10

6 Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0. December 2, 2011 pg. 2

The Requirements of Credential Management

Within the Federal Government, Federal ICAM initiatives must comply with the following laws and directives:

- OMB M-04-04 E-Authentication Guidance For Federal Agencies
- Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors
- Federal Public Key Infrastructure Initiatives, such as:
  - Federal Bridge Certificate Authority Certificate Policy
  - E-Governance Certificate Authority Certificate Policy
  - Federal PKI Common Policy Framework (FCPF) CA
- NIST SP 800-63, Electronic Authentication Guideline
- OMB, M-11-11, Continued Implementation Of HSPD-12 - Policy For A Common Identification Standard For Federal Employees And Contractors
- Federal Information Processing Standards Publication 201 (FIPS-201), Personal Identity Verification (PIV) of Federal Employees and Contractors

The Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0 provides implementation guidance and service models for complying with these laws and directives. It describes five required stages and one optional stage of credential management.

SERVICE COMPONENT	PROCESS DESCRIPTION
Sponsorship	Establishing the need for a card/credential by an authorized official.
Enrollment/Registration	Collecting and storing identity information for an entity.
Credential Production	Producing a credential.
Issuance	Passing possession of a credential to an entity.
Credential Lifecycle Management	Maintaining a credential and associated support over the life cycle, including renewal, reissuance, suspension, blocking and unblocking, and revocation.
Self-Service (optional)	Performing authorized credential management functions on the entity's own behalf.

Sponsorship is the stage where it is determined if an entity will need a credential. During this stage, basic personal identification information is entered into the identity management system. This step is particularly critical for the credential request and issuance of a non-person entity as it improves traceability, security, and control within an environment by establishing trusted applications, computers, peripherals, and devices.

Sponsorship is followed by the *Enrollment* stage, where additional information is collected to distinguish one entity from another. The entity is represented within a specific context and allows the entity to be distinguished from any other entity in the same context. Such unique identifiers often include additional biographic data, such as an individual's image and biometric data (i.e., fingerprints, retinal scans, or palm prints).

After enrollment, a credential is created. *Production* may be offered at multiple locations or at one central shared location. It can include printing an image, loading identifying data or

attributes on to a smart card or Personal Identity Verification credential, and/or assigning a cryptographic key to a specific entity. Deciding on production location is often determined based on cost and security requirements of an organization, such as if a location is secure enough to have a production facility onsite.

Issuance follows the production stage, when an entity is provided their credential. In this stage, the authority of the credential is passed on to the user or entity. They now have the ability to identify themselves to the system or facility with known information.

Credential Lifecycle Management is focused on the maintenance of the credential, allowing for regulation, ensuring users have accurate identities and attributes bound to their credentials, and eliminating former or suspended users from accessing the system using false or expired credentials. Lifecycle activities, including processes such as revocation, renewal and reissuance, expiration, and PIN reset, vary depending on the credential type and may include a self-service component. Often the policies governing a credential include a set length of time before the expiration of digital certificates on the credential or expiration of the credential itself. Since credentials serve as a tool for authentication as well as identification, revocation and termination of expired credentials are an important aspect to maintain trust within the Federal ICAM network.

The sixth, and only optional, stage of Credential Management is *Self-Service*. This stage allows authorized and already authenticated users' to make changes to or update their credentials without supervisory mediation. This can often allow for quicker resolution for basic administrative functions, like password reset or certificate updates. This can introduce significant efficiencies for large Federal agencies, but not all organizations choose to provide their users with this capability.

Challenges of Credential Management

Many of the risks encountered throughout credential management will be eased through the standardization of Identity, Credential and Access Management policy. In the past, without a single standard, users could often be issued multiple credentials based on specific projects and need for access to specific sites and locations. While this remains manageable for smaller groups or organizations the management and maintenance of multiple credentials increases both cost and vulnerability. As larger organizations have seen the benefit of credentials to improve security, managing increased numbers of unknown individuals without a common authoritative standard becomes unfeasible.

The distributed nature of Federal operations introduces unexpected complications for Credential Management. Consider the following scenarios:

- A Forest Ranger at a Federal park may not come within 100 miles of a Federal office building in the course of daily responsibilities.
- Interns are only on board for, maybe, two months, and the credential may not be issued until the individual is almost ready to return to school.
- A Federal office building may house several different agencies, each with different physical security policies and requirements.
- Some locations, such as a remote Coast Guard station, may have technical thresholds or environmental situations not common to a climate-controlled office building.

The Credential Management approach and solution to support these, and other, types of Federal employees requires careful planning to ensure a smooth, efficient, and secure experience. As Federal agencies weigh the costs and benefits of credentialing, they may

consider a shared service provider and a common credentialing standard to offset initial and long-term costs and reduce risk, but it is important to be aware of key risk challenges inherent in Credential Management.

- False Credentialing: False credentials can be issued from the accidental or intentional entry of incorrect data into the ID Management System during the Sponsorship stage. The simple outcomes of this may include duplicate identity records, incorrectly distributed credentials, or improperly issued credentials, but the false credential may provide improper or unauthorized access, which would be a major security risk to a system or facility. Having strong and reliable policy enforcement during the stages of Enrollment and Lifecycle Management can mitigate the risk of improper access through false credentials. Enrollment often serves as a check point for incorrect data entry by requiring users to verify their personal information. If an incorrect credential is issued, it comes down to the Credential Lifecycle Management stage to preserve trust by suspending, terminating, or revoking a credential, such as those lost, stolen, or connected to an identity of a former or suspended employee.
- Interoperability: As Credential Management is just one aspect of ICAM, maintaining interoperability between each component is important to preserving a secure environment. Maintaining authoritative identity records and ensuring interoperability on a small scale is relatively straightforward, as direct relationships with users, authoritative identification records, and access requirements are simplified and any potential issues with identification of users are minimized. As larger organizations and governments stretching across multiple regions turn to credentialing, the complexity increases, along with the risks of an incomplete, poorly integrated, or ineffective solution. A standardized policy improves coordination between stakeholders and organizations responsible for implementing the individual ICAM components. Collaboration is critical to ensuring the technology securing information, systems, and facilities meet the required standard centered on a common credential.
- Slow Adoption: Delayed ICAM deployment and slow user adoption of credentials perpetuates insecure methods of log on and building access, resulting in increased security risks to the system or resources. While many organization may be unwilling to change or hesitant to replace a known approach, this can increase vulnerabilities as hackers, identity thieves, and other disreputable persons increase in skill and quantity. Often this reluctance is due to a lack of familiarity, which can be mitigated through adequate training and support structures.
- Changes in Standards/Requirements: With widespread adoption of credentials for protecting classified and sensitive data against the ever changing threats in cyber security, a change in policy, standards, or requirements can unintentionally introduce a risk to interoperability and continuity of operations. From the time that a change is considered, it is important to evaluate current operating procedures to ensure they remain relevant and compliant and that they maintain risk at an acceptable level. Even minor policy changes may alter the way a credential is issued or managed throughout its lifecycle, and if a change in policy or standard is left unaddressed, this could lead to security holes or compatibility problems, as users could be unknowingly "grandfathered" in with insecure credentials. A critical tool is an approved roadmap to guide your organization or agency through the change, identifying impacted information, systems, facilities, infrastructure, and people.

Guidance

Credentials serve as a critical tool in supporting the secure access to information, systems, infrastructure, and facilities. Whether a Federal agency or private enterprise, supporting the stages of Credential Management from identity enrollment through issuance and usage to revocation is essential in increasing security and minimizing risk. It is vital to have a proven, structured approach designed to reduce risk and bring an expertise to the management of credentials. There are three principles that are specifically designed to increase the likelihood of a successfully implemented Credential Management solution.

A **knowledgeable and experienced implementation team** is essential to ensure credibility and confidence from program definition through handover to operations. ICAM in general, and Credential Management specifically, is an emerging capability. It cannot be equated to an ERP or other enterprise deployment because of its highly invasive and broad reaching impact. The ICAM team must understand the policy and standards, be familiar with the technology and product landscape, have engineering and implementation experience, and have key relationships with a variety of stakeholders inside and outside of your organization.

Monitoring of the credentialing solution through **a roadmap-aligned master schedule and metrics tracking** should be maintained throughout all stages of the Credential Management deployment. This allows for tracking individual progress against internal milestones through the gathering and analysis of data for reporting against agreed to benchmarks. Timely steps can be taken to avoid or reduce impacts that may slow implementation or adoption of the credentialing solution, thereby ensuring continued progress through maturity.

Providing **authoritative and thorough training and support programs to users and role holders** reduces slow user adoption and operational errors, such as blocked cards, locked passwords, and out of date PINS. Training offers an opportunity to explain the process to new users, providing them with essential guidance on proper use of their credential. Continued support and management of users and credentials throughout the lifecycle preserves security and integrity during this component of the ICAM solution. Supplementing training and support with user guides, how-to guides, job aides, and standard operating procedures ensures proper assistance to any role.

In summary, a Credential Management solution that is supported from the initial design stages throughout its maturity and integrated with the overall ICAM solution serves as a critical component for authoritative identification and accessibility. With new and emerging physical and cyber threats occurring every day, it is important to have a knowledgeable and experienced team that can provide the services and support to keep your company or agency secure.