FCW

How To Achieve Secure ID Assurance

"Who are you?"

That is among the most important challenge-response questions an IT system can pose to individuals seeking physical or logical access to a federal building, base, ship yard, test range, plant, or data network.

Yet, nearly 10 years after establishment of the Federal Identity, Credential and Access Management (FICAM) program, most federal agencies have yet to complete a comprehensive approach to unifying physical and logical access using a single smart card or token. The technology exists to accomplish the goals set forth in a 2004 executive order and subsequent legislation and orders. Standards and guidance remain in draft form, but they are sufficiently mature that agency security and IT managers can act to meet the mandates – and improve cybersecurity – with personal identity verification (PIV) as the linchpin in digital access processes.

Moreover, the time to act is now. Here's why:

• Thanks to the sequester in March of 2013 and subsequent budget negotiations, agency spending ceilings are as tight as ever. Compliance with FICAM guidance can yield measurable cost savings.

• The Homeland Security Department recently boosted its emphasis on continuous monitoring of network security posture, and access activity ranks high among the factors on which to collect data. Legislation to update the Federal Information Security Management Act (FISMA) is slow in coming, but when it does eventually become enacted, it will codify executive branch policy for agencies to get with the program on continuous monitoring. After software and hardware inventories and update/patch information, a logical condition to monitor is user behavior, and the key to that will be centralized digital identification information.

• With physical access control mostly accomplished, hundreds of thousands of cards compliant with Homeland Security Presidential Directive 12 (HSPD-12) still aren't used for logical access to agency IT resources, despite it being mandated by OMB memorandum M-11-11. That's got to change for both cost and cybersecurity reasons.

• The sudden and steep rise in telework, use of mobile devices and cloud computing has added urgency, and a measure of complexity, to the challenges of PIV management. The better the tools, the better agency IT staffs can keep identity and access management under control without stifling users.

In this white paper, we'll review the key FICAM use cases and the approaches agencies can take to efficiently accomplish them. You'll learn best practices for the foundational use cases among the 11 identified in the FICAM Roadmap and Implementation Guidance, Version 2.0, released by the CIO Council in December 2011. We'll focus on the creation and maintenance of digital identity records for both internal and external users, provisioning and revoking access to specific applications for specific user accounts, and granting both physical and logical access.

Challenges of Digital IDs

Use Cases Numbers One and Two as detailed in the FICAM guidance sound simple enough – create and maintain digital ID records for internal (Use Case One) and external (Use Case Two) users. In practice it can get complicated.

That's because the digital representation of a person is the proxy for his or her real self, so the ID must embody all of the policies, including access rights, a person has to applications and data. Keep in mind, the digital identity doesn't exist solely to let the agency enforce policies and maintain security. It also enables

productivity and fast onboarding of users, essential though it may be to maintaining the cybersecurity posture and data integrity of the agency.

You can see the complexity develop when you consider all of the elements that potentially make up a digital identity. These include users' physical characteristics, biographical details in both the cyber and real worlds (e.g. e-mail address and home address or mail stops), what the FICAM calls "context-specific attributes" such as rank, salary and level of clearance. Plus a growing number of organizations implementing two-factor authentication also want a biometric marker such as facial image or fingerprint. This presumes presence of the first factor such as password or digital certificate.

To all this, system administrators add the specific roles and rights of each individual user.

Several issues come into play. One is the speed at which all this information is obtained, such that onboarding or changing the characteristics of a user don't become long, tedious processes.

A second issue is the difficulty of synchronizing all of this data across the multiple systems a user may need to touch. This is presuming the agency has even identified all of the systems that do require synchronizing. Incomplete data here and there works against efficient onboarding on the front end, and against thorough closeout of access when the user departs or changes status. As the FICAM guidance authors point out, federal Inspectors General regularly report on the security back doors left by incomplete de-provisioning.

A third issue is the need to maintain privacy of individuals' data. This become increasingly difficult as the number of servers in which data resides grows.

Moreover, with self-service becoming a normal operating mode for users to provision themselves and their devices – often multiple devices per person – transaction monitoring logs add to the data associated with an individual. Each user ID may consist of hundreds of individual data elements.

It all points to the need for a solution that scales easily to millions of objects. Agencies also need a fast solution – one that relies on a directory-driven architecture to provide the repository of data for all of the relevant systems, simplifying the otherwise complex synchronization schemes. These are often weaknesses of database-driven ID management approaches.

The directory or repository approach maintains that efficiency throughout the lifecycle of the ID. A digital ID is rarely a set-and-forget function in the dynamic, real world of working individuals. For these reasons, the FICAM guidance states, "In the case of core digital identity attributes, all systems should be automatically provisioned from the core identity repository."

External Users Need IDs Too

It's hardly news that federal agency users and contractor employees are heavily intertwined from a working standpoint. More so than in the private sector, contractor access to government IT assets also requires careful digital identification. A second class of external users consists of those visiting federal sites for any of a myriad of services, from student loans to Medicaid. Still another group consists of domain-similar government functionaries at non-federal levels of government. For example, local and state police departments interact with federal law enforcement. A fourth group might be federal users external to the agency that needs to register them. FICAM guidance spells these out in Use Case Number Two.

Clearly these various types of external users each require significantly different ID profiles, just as they will interact with different systems using different pathways. The challenge lies partly in the lack of standardization for what data elements constitute an ID, and partly in the lack of a uniform ID that an individual can use for all of his or her encounters with government. This use case shares with the internal users use case the need for privacy protection.

The four types of users in some sense could all be separate use cases; they have externality in common. But for many federal agencies, giving external users a trusted, interoperable digital identity is mission critical.

Looking at it from another angle, providing external users digital identities enables e-services. The agency will want to provide users with single sign-on for multiple applications and systems. It may also require two-factor authentication for security. Effective management of this external use case requires central administration with links to various repositories that are typically beyond the direct control of the agency issuing the credential. Owners of those external repositories are more likely to cooperate if you can accomplish that administration without needing software agents on their systems.

Managing external repositories of user IDs should be coupled with an identity management system to control access and track changes that users may – and routinely do – make in their accounts. Plus a thorough event monitoring, alerting, logging and reporting capability will ensure security, compliance with regulations on access and data protection. You can configure such a solution to work across local and cloud systems.

Flexibility is also essential to the external user use case. You achieve this by decoupling provisioning data, or what the FICAM calls application-specific credentials, from the basic ID of the user. And because external users fall into various classes or communities of interest, the system will need to accept varying formats for digital identities. Often these will borrow elements from those communities' pre-existing systems.

Provisioning and De-provisioning Users

Use Case Seven – Provision and De-provision User Account for an Application – is at the center of FICAM compliance in more ways than one. It recognizes the dynamic nature of users and the work they do. It brings together the need for efficient delivery of resources, keeping both external and internal users productive, and the cybersecurity imperative. Plus, it ties together the digital identity, physical and logical access, and any other privileges related to IT assets.

As with other use cases, this one calls for an architectural framework approach. Within that framework the agency should devise a workflow that quickly gets people provisioned and eventually de-provisioned when their roles change or when they separate from the agency.

Too often, agency IT staff perform the provisioning / de-provisioning tasks manually upon receipt of a phone call or service ticket. This process is slow and doesn't scale for when the agency needs large numbers of changes simultaneously.

Other Use Cases Benefit From Strong ID an Access Management Tools

In this white paper, we've been describing how directory-powered, enterprise identity management and access management systems are foundational for the crucial use cases under the Federal Identity, Credential and Access Management (FICAM) program.

But these categories of middleware, while not central to other use cases, nevertheless can help an agency comply with other important use cases:

- Use Case Four – Creating, Issue, and Maintain PIV [personal identity verification] Card
- Use Case Six – Creating, Issuing and Maintaining Password Tokens
- Use Case Eight – Grant Physical Access to Employee or Contractor.

Card creation is serious business, governed in part by a Federal Information Processing Standard (FIPS) 201. FIPS-201 covers both the logical and physical characteristics of a PIV card, and in particular a Homeland Security Presidential Directive-12 (HSPD-12) cards.

Immediately you can see how this use case, as well as Use Case Eight, extends out from the basic ID issuances outlines in Use Cases One and Two. The data in the card itself, which contains a memory chip, will eventually include the digital ID. Beyond issuance and into the day-to-day access, provisioning and de-provisioning via a PIV or Common Access Card (CAC), core products like NetIQ's will complement use of tokens, passwords and biometric identifiers by providing the key element of policy enforcement from a central repository.

Use Case Six, management of tokens, also takes advantage of this capability. De-provisioning and, more importantly, de-activation or revocation of credentials, and therefore access, require a more thorough process than merely invalidating a token on the card. The central repository with links to applications and other resources across the enterprise will help IT make sure user privilege changes up to and including full termination, will leave no potential logical back doors.

Manual methodologies also introduce security risks. A technician may not be aware of all of the privileges and restrictions on each user. It may leave open a back door to access when someone should have been de-provisioned. Plus it is prone to leaving gaps in records of access - how and when applications were used, and by whom. Such records must be complete and auditable for purposes such as e-discovery or compliance with the Federal Information Security Management Act (FISMA).

Speed-up alone of the provisioning application itself certainly brings advantages in terms of service. But speed must be coupled with access to authoritative data about each user. So the directory approach described above in the ID creation use case also comes into play here. With the right framework and tools, IT gains the ability to orchestrate the provisioning / de-provisioning process.

In a growing number of organizations, users provision themselves, often from a private app download site or even a walled-off section of a public app store. This is fueled partly by growth in use of mobile devices as enterprise end points, and partly by the cost-savings it yields. IT staff become free to do other things.

Moreover, these same agencies are moving user e-mail accounts and applications to cloud facilities potentially lowering the organization's cost of administration.

So an alternate source of authoritative user policy and access data is required. What better source than a robust identity management engine? In fact, if identity and access management software is cloud co-located with virtual application machines, the vicissitudes of network topology become less important – an advantage in speed and storage costs.

Leverage That Piece of Plastic, Maybe

As with FICAM, a decade has passed since establishment of HSPD-12 in the aftermath of 9/11. Even today, very few federal agencies dual-use HSPD-12 cards for both physical and logical access. At this point, the card itself is becoming less relevant as smart mobile devices gain "senses" with cameras, microphones, directional and motion awareness, and multiple radio frequencies.

FICAM Use Case 10 describes the granting of logical access. Like physical access, it should be linked to the basic identity credentialing for insiders and outsiders described in use cases one and two.

To be sure, FICAM guidance calls for other technologies such as one-time password generators, biometrics, a trusted smart card (still the bulk of access devices) and public-key infrastructure (PKI) software. These technologies have been around a long time, yet they remain difficult to integrate. But a basic driver is the identity and access management engine enabling the integration of the other pieces. In fact that engine enables the logical access process to be agnostic about the authentication technology used.

Ironically, it lets organizations push card-physical access integration with card-logical access into the future. The FICAM guidance presumes that the infrastructure of card readers for logical access will take a while, if it ever comes. In fact, the opposite is equally likely, perhaps even more likely. That is, the logical access tokens – USB devices or smart phones – will double as the physical access media.

Regardless, a strong identity and access management plan lets an organization fulfill the real goal of FICAM compliance and improved cybersecurity, namely getting past user passwords, that increasingly brittle and vulnerable methodology for single-factor logon. And it integrates physical and logical access, by whatever medium.