Identity as a Key Enabler for Cloud

A More Modern, Flexible Approach to Zero Trust

June 2022

VENABLE LLP

Introduction

Legacy identity and access management (IAM) is often considered a cumbersome, complex, and archaic monolith. In particular, legacy IAM often requires lengthy development time for updates and onboarding new applications, particularly cloud applications. Additionally, many security and technology professionals fear that changes made to an identity system will create havoc throughout their environment, especially with dependent downstream systems. All of this is leading many government agencies to look elsewhere to remedy their digital identity woes.

If legacy approaches to digital identity are inflexible and monolithic, modern identity solutions are agile and adaptable. Modern digital identity systems are flexible and lightweight and often come out of the box with pre-built integrations with a variety of applications and platforms. These new systems take an API-first approach to identity and are vendor-neutral, scalable, secure, and easy to use. Standard APIs for modern systems can be configured in days, if not hours; legacy systems can take weeks or months. The API approach also enables easier integration with cloud-based applications, while integrating legacy systems is often more complex.

As federal agencies contemplate switching to a modern digital identity system, they also need to account for new regulations. Executive Order 14028, "Improving the Nation's Cybersecurity," states that federal agencies must take a Zero Trust approach to access to online systems.[1] Identity is at the core of Zero Trust, and modern identity enables organizations to comply with this regulation. In addition, it allows organizations to bring partners to the table to help them comply with other Zero Trust requirements. Other regulations are driving change across the federal landscape, including at the U.S. Department of Defense (DoD), and are pushing federal entities toward scalable, flexible, and cloud-based solutions. These drivers are forcing agencies to look outside of the traditional Common Access Card (CAC) and Personal Identity Verification (PIV) credentials to other form factors, including those that are phishing resistant.

Policy and Regulatory Drivers

Cybersecurity has been top of mind for all recent administrations, with 2021's Executive Order 14028 laying out the priorities, and follow-on policies and regulations detailing more specifics. Modern, cloud-based digital identity is central to many of the initiatives, including:

- Zero Trust: Executive Order 14028 mandated that federal agencies must take a Zero Trust approach to access to online systems. Identity is a core pillar of Zero Trust, a point recognized by OMB implementing memo M-22-09 released in January 2022. The emphasis is not just multi-factor authentication (MFA), but rather taking a holistic, risk-based approach to digital identity and enabling continuous authentication and authorization that checks every interaction among device, data, and user. Classifying users and their access levels in the directory is critical, so that a modern digital identity system can enable appropriate access.
- DoD Identity Credential & Access Management (ICAM) Strategy: The DoD's Common Access Card (CAC) and the Personal Identity Verification (PIV) credentials used at other federal agencies have been in use for more than 15 years. While there is nothing wrong with the security provided by these smart cards, they provide operational challenges to an increasingly remote and mobile workforce—a challenge long faced by users in the Guard or Reserves. Moreover, authentication technologies have evolved, and other form factors have emerged. Particularly during the pandemic, other form factors have been used for access to federal systems because of the complexity of issuing the smart cards. Agencies want to explore "Bring Your Own Device" (BYOD) to enable other authenticators for soldiers, employees, and others—spouses and children—who may need secure access to DoD networks. Requiring only CAC or PIV for access to certain resources will make BYOD impossible. Agencies need a flexible identity system that can accept a range of commercial off-the-shelf (COTS) authenticators in addition to ones issued by federal agencies for access.

1 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

- Phishing-Resistant MFA: The White House Office of Management and Budget's Zero Trust strategy document calls for agency employees and contractors to use a phishing-resistant method to access agency-hosted accounts, including FIDO2 and mobile app-based push notification.[2] The option must also be made available to citizens accessing federal systems too.
- DoD Software Modernization Strategy: The strategy emphasizes the importance of commercial partnerships through the adoption of cloud-based technologies. There is also an emphasis on enterprise services that provide ready-to-use, composable functions, such as identity management and APIs, to support software modernization efforts. This enables the DoD to quickly adopt and use secure capabilities in support of mission requirements.
- Continuous Authority to Operate (CATO): With software modernization comes automation. This enables the DoD to reevaluate the Authority to Operate (ATO) process. The software modernization will shift the ATO process from a "box check" to continuous authorization that involves validating the quality and security of the software development platform, process, and platform team. It couples this validation with automation to produce real-time and continuous evidence, verifying the defensive posture of the platform and resulting in software in real time.
- CMMC 2.0: The certification aims to protect sensitive unclassified information that is shared by the DoD with its contractors and subcontractors.

Identity Management Life Cycle

Regardless of the policies and drivers, agencies all follow the same digital identity life cycle. This life cycle is the foundation of digital identity systems and enables agencies to know what to expect each step of the way.

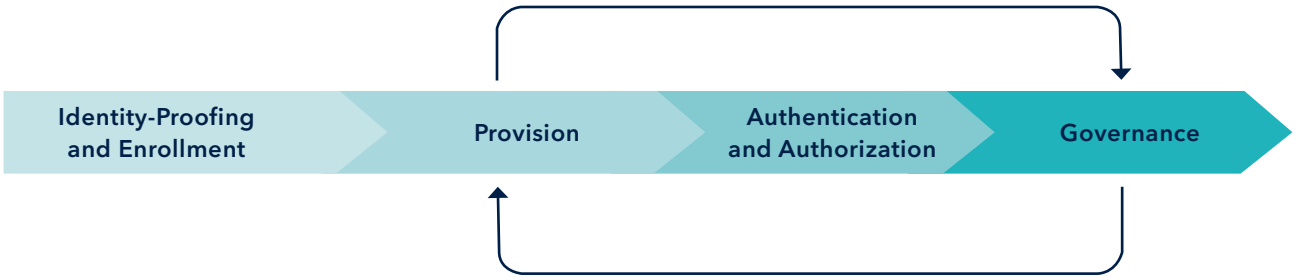

Figure 1: Identity Life Cycle

Table 1: Digital Identity Life Cycle

Step	Description
Identity-Proofing and Enrollment	Processes can differ widely, depending on the system that the individual is accessing. Federal employees must undergo a background check by the White House Office of Personnel and Management (OPM). Citizens creating accounts for access to various systems can simply supply an email or answer questions about their credential history or supply other Personally Identifiable Information (PII). If high-assurance identity-proofing is necessary, a third party typically provides this service, which is different from the digital identity provider.
Governance	Identity governance enables users to change their password and various other preferences within the system, get provisioned to necessary applications, and request additional access. Governance allows administrators to deprovision those who leave the organization. Governance also enables core cybersecurity tenants, such as rules for least privilege and separation of duties. Ideally, agencies should use automated solutions for life cycle management.
Authentication/Authorization	This is what is most commonly associated with digital identity: entering the username and password to access the system. This process now involves an additional step—entering a code from an app or inserting a token for MFA. However, not all MFA is created equal, and some digital identity systems are doing more—additionally checking Internet Protocol (IP) addresses and device and software information—to make sure the user is who they claim to be. While authentication enables initial access to a system, authorization is what allows access to a specific application or information within it. Authorization is based on roles or attributes stored with the user data in the directory. The commercial market is also taking steps toward passwordless authentication that relies on a variety of user attributes.

2 https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

This paper is focused primarily on authentication, authorization, and governance. Identity-proofing is traditionally done by third-party credential service providers that are consumed by the digital identity solution in a federated system, such as Login.Gov and the DoD's Defense Enrollment Eligibility Reporting System (DEERS).

How Modern Identity Enables Cloud

The life cycle described above is the same for legacy and modern systems; the primary difference is in how quickly and effectively organizations can move through the cycle. Legacy digital identity has been used with other legacy technologies, typically on-premises Government-off-the-Shelf (GOTS) applications with custom connectors that relay the information necessary for someone to access that application. Often, the integrations and the data sent are ad hoc, and there is little standardization across agencies, with each application integrating in a different way and with lines of legacy code to legacy directories.

Modern digital identity and cloud applications change this. Data is standardized and information is sent via a standard API so that new applications can be onboarded quickly, with little or no customization necessary. These systems are cloud-based and run as Software as a Service (SaaS). Cloud-based digital identity is much different from software running on the cloud as an application, like word processing and spreadsheet programs. Known as Identity as a Service (IDaaS), these modern digital identity systems reside on a DoD Impact Level or Federal Risk and Authorization Management Program (FedRAMP) certified system that connects with an agency's infrastructure. Directories that contain employee data can be stored on an agency's cloud if necessary.

These COTS modern digital identity products are different from the legacy systems that many federal agencies are still using. These modern systems are vendor agnostic and enable an agency to bring on new applications quickly via pre-built connectors or standard APIs, compared with the lengthy development time for legacy on-premises applications.

This highlights the difference between COTS and GOTS products. While progress has been made at some federal agencies, custom, legacy GOTS systems are still pervasive. These older systems are complex and expensive to maintain and can involve lengthy development time for updates. COTS systems enable faster integration and development, and agencies may be able to realize cost savings when moving to commercial solutions.

Finally, many of these COTS modern digital identity products come with ready-made integrations and partnerships with other cybersecurity providers that the DoD and other federal agencies can leverage as they build their Zero Trust architectures. While digital identity is a core pillar of Zero Trust, a vendor that has integration with others for network security, incident response, and penetration testing is critical. These partnerships with other companies mean tighter technology integrations and less development time for the agency.

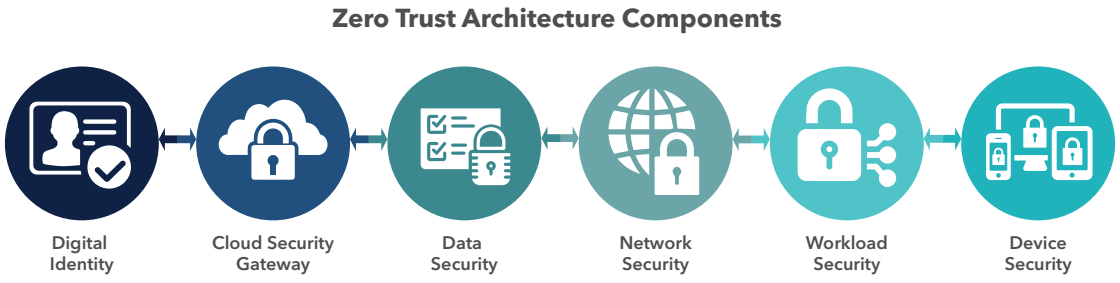

Figure 2: Architectural components of zero trust

Modern digital identity systems can also handle access for workforce apps — employees needing access to do their day-to-day work — and community apps — citizens or others needing access for a variety of purposes. These newer systems can be used across enterprises and external use cases and scaled to millions of users, whereas legacy systems have had difficulty achieving this.

Requirements for Cloud-Based Systems

Despite the clear advantages of a COTS solution, there are specific requirements that vendors must meet to qualify for DoD procurement eligibility. FedRAMP began in 2011 to ensure the security of cloud services used by U.S. government agencies. In the early days of cloud computing, security was a prime reason not to use it, and FedRAMP was designed to use the government's existing security practices and operationalize them for cloud environments. While changes to FedRAMP are in the offing, this is table stakes for any cloud provider wanting to serve the public sector market.

The DoD has other security requirements for cloud providers in addition to FedRAMP. Cloud providers must also be certified to process and store information based on the different Impact Levels. Additional information on the Impact Levels can be found in Table 2.

Table 2: DOD Impact Levels

Impact Level	Description
IL2	DoD information that has been approved for public release
IL4	DoD Controlled Unclassified Information (CUI)
IL5	DoD CUI and National Security Systems
IL6	DoD Classified information up to Secret

Systems are certified to specific impact levels based on various requirements. With digital identity systems, however, systems certified for IL4 can also be used to access IL5 systems if both systems are architected correctly, and the proper attributes and roles are provisioned to users in the directory. The digital identity system would be used to connect individuals to the IL5 applications but will not contain national security data. Additionally, users could be asked to re-authenticate or use a different authenticator when moving between an IL4 or IL5 system.

Think of it this way: The IL4 digital identity provider is the security guard outside of a building. They check to make sure that the individuals wanting to get into the building have the right token to get in, but they have no idea what is going on in the building or what information is stored there. The security guard doesn't need to be IL5, because they never touch the data or applications that have that designation; they just verify that those who want access are allowed.

Last, organizations must undergo Cybersecurity Maturity Model Certification (CMMC).[3] The certification is intended to protect sensitive unclassified information that is shared by the DoD with its contractors and subcontractors. The program incorporates a set of cybersecurity requirements into acquisition programs and provides the Department with increased assurance that contractors and subcontractors are meeting these requirements. CMMC 2.0 was released in November 2021, but compliance is unlikely to be required until sometime in 2023 at the earliest.

Table 3: CMMC 2.0

Level	Model	Assessment
Level 1	17 Practices	Annual self-assessment
Level 2	110 Practices aligned with NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)	Triennial third-party assessment for critical national security information; annual self-assessment for select programs
Level 3	110+ Practices based on NIST 800-172 (Enhanced Security Requirements for Protecting Controlled Unclassified Information)	Triennial government-led assessments

3 https://www.acq.osd.mil/cmmc/index.html

After meeting all of the requirements outlined in the various compliance regimes (e.g., FedRAMP, Impact Levels, CMMC), a company can start providing systems and services to the DoD. To comply with the different certifications and regulations, companies need to make serious investments of capital, human resources, and infrastructure. Organizations that provide services to federal agencies have to segregate the federal systems from other environments, and even assigned staff must focus solely on government work. That way, if anything happens with a provider's other systems, the one serving federal systems is separate and won't be affected.

DoD officials need to check these boxes for digital identity providers and discuss a product's capabilities and service levels with the vendor. It is critical that the DoD find a partner that is willing to work with it to accomplish the goals laid out in the cybersecurity executive order around Zero Trust and digital identity. In choosing a trusted partner to work with to accomplish these goals, the best course of action is to open an honest, frank discussion.

The Case of Cloud Identity in the DoD

The DoD, like most organizations, has embraced commercial cloud capabilities to provide convenient, on-demand, and secure solutions. The DoD has an opportunity to increase efficiencies and reduce costs by implementing these cloud-based, modern digital identity systems for access to sensitive data. An additional benefit is that the identity management system does not contain the sensitive information being protected. Instead, it can be designed to contain IL4 information about what accesses a particular user should be granted. This provides the opportunity for a single IL4 cloud identity system to authorize access to IL4 or IL5 cloud services. With proper governance to ensure individuals are provisioned correctly with the correct roles and attributes, DoD would be able to take advantage of the flexibility of best-of-breed cloud-based digital identity. Below is a potential use case:

> *A DoD employee logs into NIPRNet in the morning, using their CAC card and PIN for authentication. Later that morning, the employee needs to access an IL4 certified cloud system to view some CUI information. From their NIPRNET machine, the employee navigates to the cloud system to access the CUI information. The cloud system contacts the IL4 Authentication agent to verify the accesses for the employee. The agent verifies the accesses of the employee using authentication data that is protected by IL4 controls and allows the employee to access the system. That afternoon the employee needs to access an IL5 cloud service. Since the employee's access information is considered IL4 information, the IL5 cloud service contacts the IL4 Authentication agent to verify the employee's token for access to the IL5 system. The IL4 agent verifies the token and attributes of the employee and grants them access to the IL5 cloud service system.*

Future of Authentication for DoD

The CAC is the forebear of strong authenticators and changed the way the industry looked at digital identity. While still a strong authenticator, the form factor hasn't held up quite as well over the years, and the DoD is exploring other technologies. Additionally, in the wake of the pandemic, in-person interactions to receive a credential have been challenging. The DoD needs a way to issue other types of authenticators, including BYOD, that enable access to some systems. These other authenticators can be used to access systems that have been identified as low risk.

The DoD's ICAM Strategy document states that the CAC remains the primary authentication credential; however, systems should also accept other credentials based on a risk framework.[4] These other credentials may include passwords, biometrics, one-time passwords, and other authenticators and may be issued by a variety of providers, including the DoD, other federal agencies, commercial entities, and non-U.S. government partners. But before these other credentials can be allowed for access, the DoD also needs to modernize its application for modern identity protocols, such as SAML 2.0, OAuth 2.0, and OpenID Connect.

4 https://dodcio.defense.gov/Portals/0/Documents/Cyber/ICAM_Strategy.pdf

Critical to this risk-based approach to digital identity is governance. Proper governance is foundational to digital identity and will enable DoD to provision access to applications and data based on the correct roles and attributes. Without a holistic governance program, agencies will have difficulty provisioning access, knowing who is accessing various systems, and knowing when access needs to change, just to name a few of the tasks governance encompasses. Laying this governance foundation will enable agencies to build a successful digital identity program and to provide secure access to systems.

The DoD also needs a digital identity system that is flexible enough to accept this range of credentials. CAC and PIV may be prevalent now, but as more credential service providers emerge, these new credentials will have to be evaluated and accepted into the new system. Legacy systems may have some difficulty integrating with a range of different credentials, whereas modern digital identity systems have greater flexibility to accept such a range. The DoD should prioritize updating its apps and infrastructure to accept modern identity protocols.

Digital identity is changing for federal agencies. What was once a series of siloed, monolithic identity systems is being broken down. As access is expanded to more users, a PIV or CAC may not always be necessary or cost effective, so agencies would be better off enabling individuals to BYOD. Underpinning all of this is a modern, agile, adaptable digital identity system that can enable access for those who need it while keeping others out.

Recommendations:

As federal agencies move away from monolithic, archaic, legacy digital identity systems, we offer three recommendations:

- Cloud first – Cloud native digital identity enables agencies to deploy a zero trust architecture that provides flexibility and pre-built integration with other components.
- Phishing-resistant MFA – Not all MFA is created equal, and as hackers have become savvier, so have federal agencies. Phishing-resistant MFA, based on public/private key cryptography, reduces the attacker's ability to intercept and replay access codes, as there are no shared codes. Additionally, the authentication action can occur only between the user's device and the site they are visiting.
- Automated life cycle management – Digital identity governance is often an afterthought, but agencies need to consider systems that automate the identity life cycle process. Automated life cycle management can automatically provision, de-provision, and change the rules of employees as they move around or leave an organization.

VENABLE LLP