WHITE PAPER

NetIQ - TriVir Federal

HSPD-12: Rapidly and Affordably Achieving Compliance

NetIQ and TriVir build on innovating federal agencies' successes, providing the fastest and most cost effective path to OMB and GAO compliance with the HSPD-12 mandates.

NetIQ | TriVir

NetIQ | TriVir

WHITE PAPER

Table of Contents

Executive Summary

Trailblazing federal agencies deploy innovative and production-proven solutions for achieving HSPD-12 compliance

Homeland Security Directive 12 (HSPD-12) was initially handed down in 2004. Since then, executives at federal agencies have faced an incredible challenge in achieving compliance. HSPD-12 is an unfunded mandate that employs a variety of emerging technologies rife with risk, complex integrations and high-stakes security requirements. Because of this, most agencies put off HSPD-12 compliance rather than attack it head on. As time passes, the following account has become a common refrain shared by many agency executives.

"I used to lay awake in bed at night frustrated; riffling through my various projects and their competing priorities. There just didn't seem to be a clear path toward HSPD-12 compliance within our current budget and staffing constraints. I always knew that we couldn't push it off forever. Each year the Office of Management (OMB) and Government Accountability Office (GAO) were applying more pressure. Over the years just putting it off has become a headache, writing POAMs and regularly explaining our lack of progress." – **Michael Chu**, *US Department of Veterans Affairs, HSPD-12 Program Management Office*

Today, agencies continue to receive aggressive pressure from OMB, GAO and the Office of the President to achieve HSPD-12 compliance. While data published in the White House Cross Agency Priorities (CAP) report indicates progress, for many agencies, it also clearly demonstrates the significant gap between current state and true HSPD-12 compliance. Throughout the federal agencies there is also a strong ongoing push to eliminate passwords and move to the Personal Identity Verification (PIV) credential for all access—logical, physical or mobile. It is clear that the priorities are not changing, with White House officials continuing to offer quotes like the following.

"I often say that one of my key goals in my job that I would really love to be able to do is to kill the password dead." – **Michael Daniel**, *White House Cyber-Security Coordinator*

What is changing, however, is that agencies are emerging that have seen significant success in achieving compliance. A few agencies can now issue PIV cards to all staff, utilizing the PIV cards for both logical and physical access, and in some cases, even supporting mobile access via PIV. These agencies fully automate the lifecycle of the cards and associated identities through integration with their existing identity management infrastructure. Agencies that began taking steps toward compliance feel dramatic relief from the pressure of constantly delaying.

"TriVir, using NetIQ technology, helped me to quickly generate a plan to achieve compliance without replacing any of our systems. They used a unique approach that I was able to see working at other agencies.

This immediately relieved pressure, helping me to satisfy my management and get OMB & GAO off my back. I was also quickly able to show a workable plan and was able to demonstrate improvements in security, reduction in costs and simplify our management of the Personal Identity Verification (PIV) credential." – **Sam Highsmith,** *Agency Lead, US Census Bureau HSPD-12 Program Management Office*

This recent wave of successes creates a unique opportunity to be one of the early HSPD-12 success stories without shouldering risk that comes with working on the bleeding edge of such a complex solution. By leveraging existing infrastructure and employing a pragmatic approach focused on delivering visible security value as quickly as possible, agencies can make significant progress towards full compliance without requiring drastic rip-and-replace deployments. Key components to successfully capitalizing on this opportunity may be partnering with a solutions service provider that guided these successes, and selecting technology platforms consistent with your unique requirements.

TriVir is a solutions service provider uniquely focused on helping clients attack high-complexity, high-risk projects involving challenging customizations. Their long history of delivering identity and security solutions to a broad range of federal agencies made them especially fit to work with clients to solve the myriad of unique challenges in the FICAM space. Clients choose TriVir for its unique focus on gathering the most talented staff, delivering each engagement with the discipline to ensure success and cultivating a culture committed to thrilling clients above everything else.

As a longtime partner of TriVir in delivering identity, security and access management solutions, NetIQ provides the industry's most complete and integrated solutions platform. With the ideal customer experience in mind, and in stark

contrast to their competitors' "acquire-and-cobble mentality," NetIQ creates a truly integrated platform that provides all of the underpinnings of a fully compliant HSPD-12 solution. The NetIQ product suite gives TriVir the tools to build a solution customized enough for each client and yet supportable through NetIQ as off-the-shelf software.

Immediately following this summary are detailed case stories from two successful clients: The US Census Bureau and the National Archives and Records Administration. Each faced challenges unique to their charters, environment and focuses. However, both were able to leverage their existing NetIQ infrastructure along with unique services from TriVir to guide them toward fully compliant solutions that continue to grow today. Like most federal agencies, these clients are excited to share details of their successes with other federal agencies, and whether you ultimately choose to leverage TriVir or NetIQ in your HSPD-12 solution, we would love to connect you with these and other successful agencies for information sharing activities.

Federal FICAM Success

Success with FICAM initiatives does not have to be a long multi-year project. Success can be attained as milestones of objectives in your timeframe, building upon one another, and can be addressed in an order of relevance and priority defined by the departments and agencies. The progression of success is not a single, linear progression.

TriVir and NetIQ have worked with several departments and agencies with a proven approach. The following represents two examples of federal departments and agencies where TriVir guided the teams in meeting their specific requirements and priorities with NetIQ technology.

Case Study: Census Bureau Conquers HSPD-12

The Challenge

The federal government operates in a constantly shifting threat environment with new technological risks emerging all the time. To address the risks of data breaches, identity theft and unauthorized access, Census was required to utilize their Personal Identity Verification (PIV) cards for computer and network access in addition to physical building access.

Compliance requirements for security tightened as the Office of Management and Budget (OMB) recently clamped down on the mandate to comply with the president's Homeland Security Presidential Directive-12 (HSPD-12). This directive requires the use of the PIV card for physical and logical (computing) access. Additionally, the Federal Information Security Management Act (FISMA) reporting requirements began to require more progress in the area of HSPD-12. Census needed to update their budget to close the compliance and security gaps for HSPD-12.

At the same time, the Federal CIO Council provided the Federal Identity, Credential and Access Management (FICAM) Roadmap for guidance on how to enable trust across organizational, operational, physical and network boundaries. However, it was difficult to see how existing agency IT systems and networks could incorporate the roadmap architecture to meet the common business use cases and facilitate automated enablement of HSPD-12.

The Solution

Census implemented a NetIQ identity and access management (IAM) solution with HSPD-12 PIV connectors and FICAM policies to enable PIV logical access to computer and IT resources and tie in the physical access systems. This solution improved the experience for Census workers and other federal employees who now access Census buildings and computing systems with their PIV card. The solution also enabled PIV-based single sign-on (SSO) to streamline the experience for users and relieve application owners from the responsibility of implementing PIV support directly into their applications.

Because the NetIQ IAM solution for HSPD-12 is platform agnostic, it was able to incorporate and PIV-enable Census applications and platforms such as Microsoft Active Directory, Oracle Internet Directory and Novell eDirectory. A myriad of applications was also connected through NetIQ, such as Lotus Notes, Remedy, Learning Management Systems, HR Connect/Commerce Business Systems (CBS), WebTA, cloud applications and others. Additionally, it linked in the Lenel Physical Access Control System (PACS) to provision users, PIV cards and synchronize terminated status as well as improve visibility of access for audit reports.

By automating the process of managing and synchronizing user identities and PIV certificates, the solution became scalable and maintainable for the entire Census enterprise environment to include users at headquarters and field offices. The solution was implemented as an enterprise platform to enable application and system owners to plug into the architecture using one of a number of standardized options. This enabled quick deployment of the enterprise solution with prioritized projects to follow, managed by their respective application owners.

TriVir, an HSPD-12 services provider and platinum NetIQ partner, worked with Census staff to deploy the NetIQ HSPD-12 solution in a development lab and customize the solution for Census business and security policy. After successful implementation, the team promoted the solution into a limited-scope production pilot. Once production system functionality was tested, the pilot was expanded to the rest of agency personnel. The implementation team and Census personnel identified bottlenecks in the rollout process to streamline and automate the process of gaining PIV credentials and enabling them to the physical and logical networks. Systems that were incorporated into the integration project that may be common for other agencies include:

- General Services Administration (GSA) Managed Service Offering (MSO) US Access (for automated PIV issuance and certificate synchronization)
- PIV derived credentials for mobile devices (in pilot)
- McAfee Endpoint Encryption for PIV access to the Full Disk Encryption system
- Multiple Active Directory instances
- Oracle (Oracle databases, Oracle Internet Directory and Oracle Identity Manager/Access Manager)
- Commerce Business Systems (CBS)
- Commerce Learning Management System (LMS)
- Kronos Web Time and Attendance system
- eDirectory (LDAP directory service)
- Lenel PACS
- BigIP F5 Load Balancers PIV-Enabled for Sharepoint and other external apps (lab, not yet in production)
- Lotus Notes
- Citrix (NetScaler and Web Interface) (lab, not yet in production)
- Cisco ASA VPN
- Remedy
- SharePoint
- SSO infrastructure for other application owners to integrate
- Workflows for external user registration and account lifecycle management
- PIV-enabled access to standard and elevated privileged accounts through the same card
- PIV-derived credentials (virtual PIV cards and certificates on mobile)

About Census

The Mission

The Census Bureau's mission is to serve as the leading source of quality data about the nation's people and economy. Census honors privacy, protects confidentiality, shares expertise globally and conducts work openly. Census is guided on this mission by scientific objectivity, a strong and capable workforce, devotion to research-based innovation, and abiding commitment to its customers.

Authority

The Census Bureau operates under Title 13 and Title 26 of the U.S. Code.

The Goal of the Census Bureau

The goal is to provide the best mix of timeliness, relevancy, quality and cost for the data that is collected and services provided.

Currently, Census is preparing to issue PIV-derived credentials (also known as PIV-D). This will allow smartcard-based PIV authentication from mobile devices without the need for the physical PIV card or a smartcard reader. Personnel will gain access to computing and physical resources through their mobile devices.

More details on the logical and physical access implementation built on top of this NetIQ technology platform are available upon request.

Case Study: National Archives and Records Administration

The Challenge

The National Archives and Records Administration (NARA) reported a plan to the Office of Management and Budget (OMB) to become compliant with HSPD-12 requirements, which mandate the use of the PIV card for physical and logical access. Without immediate budget to allow for full PIV-enablement, NARA needed to draft a phased implementation plan that demonstrated the path to progress along this mandate's requirements once funding became available. TriVir previously worked with NARA to install a NetIQ identity management solution to facilitate two-factor remote authentication to the agency's network. Initial efforts to prototype smartcard-based authentication through their complex and distributed network showed that it would be difficult to close technology gaps and resolve unanticipated challenges posed by the internal network architecture.

The Solution

TriVir worked with NARA to complete an assessment of key enterprise systems, identify integration points, and created a detailed plan for a complete NetIQ HSPD-12 identity and access management (IAM) solution. This deployment would automate the PIV lifecycle and bring the administration in line with HSPD-12 mandated requirements to enable personnel to access buildings and computing systems with their PIV card. This analysis resulted in an implementation plan, which aligns with the FICAM Roadmap and Implementation Guidance. This plan provided a phased approach with relatively small, high-visibility, high-value projects that would gradually move the administration into full compliance.

In addition to the drafting of the HSPD-12 implementation plan, NARA and TriVir staff completed a pilot of 50 users in production with successful PIV access. For the pilot, NARA's test and production authentication infrastructure was updated to support SmartCard authentication—including installation of smartcard support software, updating schema, installation of management tools, establishment of trust stores and updating firewall rules for Certificate Revocation List (CRL) checking. The production pilot supported PIV authentication of 50 employees, including workstation configuration via an automated desktop configuration package to facilitate large-scale production deployment.

TriVir's FICAM aligned plan for the implementation of HSPD-12 and resulting pilot components included PIV enablement and provisioning for the following systems and areas:

- GSA MSO US Access (for automated PIV issuance and certificate synchronization)
- eDirectory and Active Directory
- Interior Business Center Human Resources system (IBC HR)
- Internal and external web applications
- Cisco VPN
- Citrix (NetScalers and Web Interface)
- PIV-accessible federation with partner agencies and commercial institutions
- Consolidated Physical Access Control System (PACS) interface to link all PACS systems at each site to the IDMS
- Certificate validation infrastructure (internal)
- Single sign-on (SSO) infrastructure within the IDMS to indirectly PIV enable web applications
- Automated FISMA audit and reporting against HSPD-12 metrics and data calls
- Secure standard and elevated privileges with the PIV card

Currently, the agency is working to expand the pilot and incrementally turn on automation through NetIQ identity and access management connected systems, including those in the cloud.

About National Archives and Records Administration

The Mission

The mission of the National Archives is to provide public access to federal government records in their custody and control. Public access to government records strengthens democracy by allowing Americans to claim their rights of citizenship, hold their government accountable, and understand their history so they can participate more effectively in their government.

Authority

NARA is authorized to establish, maintain and operate records centers for federal agencies under 44 U.S.C. 2907 and to approve a records center that is maintained and operated by an agency under 44 U.S.C. 3103. NARA is also authorized to promulgate standards, procedures and guidelines to federal agencies with respect to the storage of their records in commercial records storage facilities under 44 U.S.C. 2104(a), 2904 and 3102. NARA is authorized to determine the disposition of federal records under 44 U.S.C. 2904.

The Goal of the National Archives and Records Administration

The vision of the National Archives is to transform the American public's relationship with their government, with archives as a relevant and vital resource. This vision harnesses the opportunities to collaborate with other federal agencies, the private sector, and the public to offer information—including records, data and context—when, where and how it is needed. NARA will lead the archival and information professions to ensure archives thrive in a digital world.

Background

In 2004, via the Homeland Security Presidential Directive 12 (HSPD-12) and later the OMB Memorandum 11-11 (M-11-11), the federal government began to mandate the issuance and usage of Personal Identity Verification (PIV) cards to all government employees and contractors. The directive mandated that PIV cards be used for access to all physical facilities as well as access to IT resources (commonly referred to as logical access). The umbrella term used to describe operations in support of the PIV credential and usage is Federal Identity, Credential, and Access Management (FICAM).

To help guide the implementation of the directive, the Federal CIO Council created a subcommittee known as the ICAM-SC. The subcommittee produces and maintains guidance, roadmaps and other material to assist agencies when implementing FICAM solutions. The lists of standards, solutions, technologies and options under the FICAM umbrella have grown to become a quite complex framework. Despite the complexity, the issuance of PIV cards to government employees and contractors is widespread across federal departments and agencies.

Even with progress and guidance, implementing a fully compliant FICAM solution is a large and complex project. According to a study done by the Standish Group, only 6.4% of projects from 2003 to 2012 were successful[1]. The Standish data showed that 52% of the large projects were "challenged," meaning they were over budget, behind schedule or did not meet user expectations. The remaining 41.4% were failures—they were either abandoned entirely or started anew from scratch.

[1] Of 3,555 projects that had labor costs of at least $10 million

Still, the potential benefits to every department/agency associated with the implementation of FICAM are clear and compelling—including the following:

- **Increased security,** which correlates directly to reduction in identity theft, data breaches and trust violations. Specifically, FICAM closes security gaps in the areas of user identification and authentication, authorization, encryption of sensitive data, and logging and auditing.
- **Improved user experience through the elimination of username and password.** With a single credential, users may access physical assets such as buildings and rooms as well as computers and applications. Additionally, single sign-on (SSO) may be incorporated into the PIV-enabled platform in an HSPD-12 compliant way so that applications may be accessed without bothersome regular prompts for authentication once a user has authenticated with a PIV card into the network.
- **Compliance** with laws, regulations, and standards as well as resolution of issues highlighted in GAO/FISMA reports of agency progress. These include the aforementioned HSPD-12 and M-11-11 plus directives included in OMB Circular A-130, OMB M-04-04, FIPS 201-2, FISMA and a number of NIST Special Publications.
- **Improved interoperability** between agencies using their PIV credentials along with partners carrying PIV-interoperable or third party credentials that meet the requirements of the federal trust framework. Additional benefits include minimizing the number of credentials requiring lifecycle management.
- **Enhanced customer service,** both within agencies and with their business partners and constituents. Facilitating secure, streamlined and user-friendly transactions—including information sharing and self-service—translates directly into improved customer service scores, lower help desk costs, and increased consumer confidence in agency services.
- **Elimination of redundancy,** both through agency consolidation of processes and workflow and the provision of government-wide services to support ICAM processes. This results in extensibility of the IT enterprise throughout the network and into the cloud and reduction in the overall cost of security infrastructure.
- **Increase in protection of Personally Identifiable Information (PII)** by consolidating and securing identity data. This is accomplished by consistently locating identity data, improving access controls, increasing use of encryption, and automating provisioning processes.
- **Mobile access, cloud (public and private) and virtualization,** which…

For agencies that have not deployed any systems following the FICAM guidance, implementations can be fraught with risks, liabilities and challenges. To address this, NetIQ developed a template-based approach for implementing FICAM compliant, HSPD-12 solutions. This approach can rapidly bring government agencies into compliance with the directives while leveraging existing systems and infrastructure. While template-based and rapidly deployable, the NetIQ framework is not a "quick and dirty" solution. Rather, it brings all of the benefits noted above, while avoiding the common pitfalls that put an HSDP-12 project into the "challenged" or "failure" buckets noted above.

NetIQ's HSPD-12 solutions are delivered through TriVir, a platinum NetIQ partner. TriVir has experience helping multiple departments and agencies reap the benefits of becoming FICAM compliant. TriVir has an exceptionally deep background in delivering identity and access management solutions, and an unparalleled understanding of the FICAM guidance. As an independent solution services provider, TriVir also brings a breadth of experience integrating third-party software into NetIQ based HSPD-12 solutions. This ensures that current investments continue to be leveraged even in a NetIQ based HSPD-12 architecture. Most importantly, TriVir is a uniquely focused service provider with a culture centered on thrilling clients, making them especially compatible with the NetIQ vision for the FICAM solution delivery experience. Capable of providing end-to-end support through the entire process: from program management assistance, project definition and requirements gathering through to the hands-on implementation and ongoing maintenance of the solution, TriVir represents the best NetIQ has to offer in the implementation of a FICAM compliant solution infrastructure.

The ICAMSC Guidance Visualization of the FICAM Solution Components

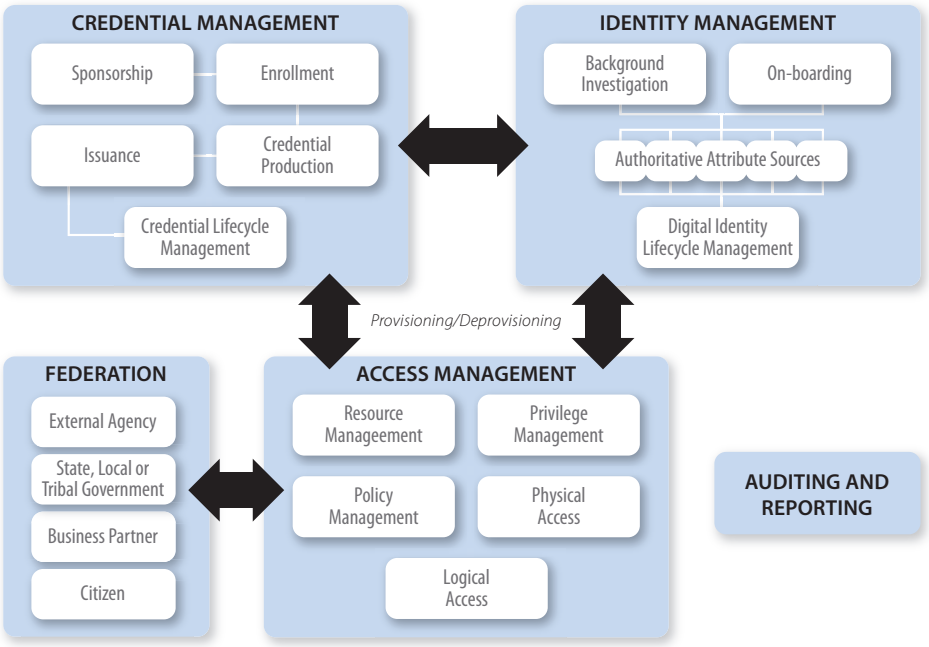

Figure 1

The ICAMSC Guidance Services Roadmap for FICAM Solutions

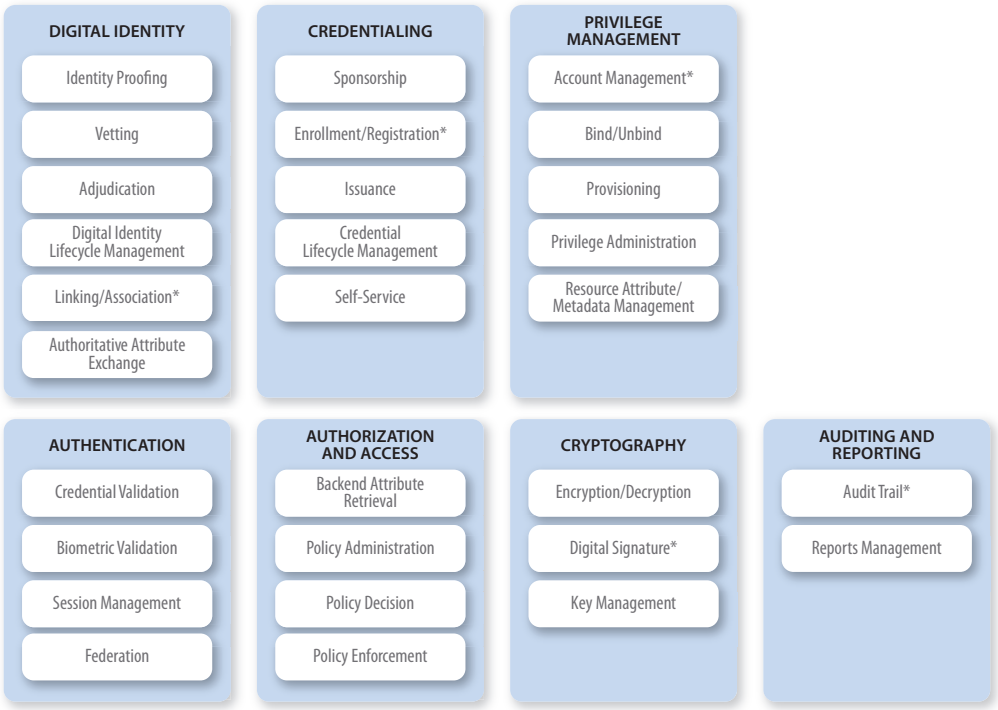

Figure 2

Products from NetIQ provide most of the services specified in the roadmap.

- **Workflow Management Solutions** – Many of these services, especially in the digital identity and credentialing areas, can be automated and enhanced via NetIQ workflow solutions, which reduce service time, reduce manual labor and cost, and provide consistent and repeatable services.
- **Identity Management Solutions** – NetIQ offers an integrated set of identity management solutions that are of particular importance in the credentialing, privilege management, and authentication service areas. These solutions impact all of the services listed in those service areas; particularly credential lifecycle management, self-service, account management, provisioning, privilege administration, resource attribute/ metadata management and federation. A key feature of the NetIQ solution is its ability to maintain real-time synchronization of attributes across multiple attribute repositories.
- **Access Management Solutions** – Both logical (LACS) and physical (PACS) access can be controlled with NetIQ access management solutions. These solutions are discussed in detail in subsequent sections of this document.
- **Auditing and Reporting Solutions** – NetIQ offers a log management solution which can collect and correlate log information from all FICAM-related systems, as well as a robust Security Information and Event Management (SIEM) solution that adds important reporting and forensic capability which support detection and mitigation of security violations in the FICAM deployment.

In addition to having all of its solutions in the upper right of Gartner Magic Quadrants, an independent study has shown that total cost of ownership (TCO) using NetIQ solutions average more than 20% less than solutions from competing vendors. This is primarily because NetIQ products are easier to configure, integrate and administer. Starting a large project like a FICAM implementation with solutions that offer such a large TCO benefit make success that much more likely.

TriVir and NetIQ also realize that not every agency is in a position to replace every component listed in the FICAM guidance roadmap. Agencies with significant investment in relevant technologies needn't worry about replacing an existing component. The NetIQ products are designed to be a flexible toolkit for implementing FICAM solutions. This forward thinking design ensures that there are many integration points, which can be leveraged to integrate third-party components into a complete HSPD-12 solution.

This remainder of this paper outlines NetIQ's approach to addressing the requirements of FICAM and the HSPD-12 mandate.

Logical Access Control Systems Modernization

A modern logical access control system (LACS) is based on an enterprise-wide identity management solution (IDMS). An IDMS provides the following services, which are the backbone of an LACS system:

- Strong authentication
- External credential support
- Automated workflow, provisioning, and de-provisioning
- Event monitoring, alerts and logging
- Auditing
- Directory services
- Self service
- Single/reduced sign on
- Authentication
- Authorization
- Access control policy management
- Federation

Implementing an enterprise-wide IDMS within an agency will bring the identities within each system, application, directory and database together into a single repository that can be referenced when needed. Identity assurance will be maintained all the way from the PIV issuer (for example GSA MSO, XTec, ORC or others) down into the agency systems. Correlation of identities across the agency is a key component of identity management, which is, in turn, a key component of PIV enablement. Once an identity has been correlated throughout the agency, that identity is known and can be verified and validated to ensure that person is who they claim to be.

Another important benefit of this is systems and applications are now able to validate identities as individuals request access to those applications and their data. PIV enablement becomes a simpler process as the applications already rely on the IDMS for identity verification and validation. PIV enabling the IDMS solution means one integration point and alleviates the need to enable each system and application. There is no longer a need for each application to provide its own identity validation, further reducing cost and complexity.

In addition to the IDMS, NetIQ® Access Manager™ completes the logical access picture for the modernized LACS infrastructure by bringing direct PIV-authentication capability to legacy applications. It also provides single sign-on (SSO) based on the PIV-authenticated connection. If the user logs into their workstation with their PIV card, they can access their applications without additional authentication prompts, instead relying on the workstation's PIV-authenticated connection.

OMB M-11-11 provides this as an option instead of direct PIV-enablement of an application: "System implementations protected by an Identity and Access Management solution that adheres to the principles... [defined in FIPS 201 and NIST SP 800-73]...are also considered PIV-enabled." Once a user is PIV authenticated to their workstation, or to the access management product, they can then access their SSO-enabled applications in a PIV-compliant fashion.

Federal Information Security Management Act (FISMA) reporting requirements now require more progress in the area logical authentication with a PIV card. This progress is being tracked for both standard users and elevated privilege users. NetIQ enables PIV access for both types of users from the same PIV card to allow the choice of network IDs (standard or admin) to be specified at login time.

Physical Access Control Systems Modernization

Traditionally, physical access control systems (PACS) are deployed and managed on stand-alone servers at each facility. These servers host the front-end application for the PACS and typically leverage a backend database for identity and credential storage for authentication. While they have adequately provided access to individuals, they also have shown their vulnerabilities. Often when a server goes down, identities (along with the policies and permissions that govern them) cannot be updated. Only cached identities that are stored locally on-site can go through door controllers and card readers. A gap in security could potentially occur if an individual is de-provisioned in the system after to the PACS failure. The server stands as a single point of failure and until it can be repaired, the de-provisioned user can still gain access to the facility. Each failure aggregates the cost for agencies due to not only the loss of productivity for individuals not able to gain access to the facility, but also for the security threat of unauthorized access. With recent exposures at the federal level, this threat needs to be addressed. The threats and vulnerabilities that continue to grow throughout the country elevated the need for agencies to consider modernization of their PACS system.

At the enterprise level, PACS modernization will help your agency to realize greater cost savings and efficiency while maintaining your local access control decisions. An integral function in PACS modernization is the ability to provide routine access for PIV cardholders into your federally controlled facility, in accordance with HSPD-12. To update all readers to be PIV-compliant could cost millions. Identity management (IDM) and credential management will help to facilitate strong authentication and communication between the PIV and PACS, as outlined by the CIO Council for ICAM. With an IDM solution in place, PACS user accounts can be provisioned from authoritative sources as a part of the overall identity lifecycle management process. After being provisioned into PACS, users can leverage their PIV cards to routinely authenticate themselves into federal facilities they need to access. While modernized PACS will be able to electronically validate employees and visitors, IDM will help to provide the authoritative source to successfully authenticate users.

Leveraging an integrated IDM solution can provide real-time access controls to govern user access into each facility by integrating with your existing PACS. By doing so, your agency will be armed with stronger centralized management of your user community and ensure that the right people have the right access to the right resources at all times. When onboarding an individual to the agency, IDM can leverage roles, rules and workflow to provide the individual with the proper access to all necessary resources, including the PACS. When changes to the individual are needed, the IDM solution can record those changes in a centralized, authoritative data store. The changes are also distributed and synchronized in real time across all physical and virtual resources. Now, in the event that a user is provisioned or de-provisioned from the centralized system, the IDM solution should communicate the changes to your PACS to ensure secure real-time controls are in place to access the facility. To facilitate easier communication with your existing PACS, the IDM solution should have the necessary connectors to tie an identity to the PACS and ensure appropriate real-time access controls are in place.

Benefits of PACS Modernization

PACS modernization provides several key benefits:

- **Increased Security and Privacy at Your Facility** – Leveraging IDM solutions can help provide stronger technology to validate cardholders. Electronic verification can provide more reliable information to assist security teams in making sound access decisions.
- **Reduced Cost and Increased Efficiency** – Leveraging an agency-wide IDM solution can eliminate redundant processes and investments, which typically happen at the departmental level. Integration across the enterprise can help to reduce the manual efforts involved in the current state.
- **Promotion of Trust and Interoperability** – IDM solutions can help facilitate integration of PIV, PIV-I, and other trusted credentials for physical and logical authentication for your agency. Because of the growing need to achieve interoperability with other agencies, we can help to extend privileges to be shared across agency locations and trusted external sites.
- **Improved Overall Support for ICAM** – IDM solutions should not only provide access control and governance of your users, but also facilitate stronger capabilities to securely monitor and dynamically report on all resources within your enterprise.

Additional Solution Considerations

PIV-Enablement of Active Directory with NetIQ Identity Manager

NetIQ IDM solutions can help with PIV-enablement of Active Directory (AD) by providing synchronization of PIV certificate data from the credential provider to AD to make AD automatically "trust" a PIV card for authentication. To support the use of a single PIV card to access multiple accounts in AD, such as a standard account in addition to elevated privilege accounts, NetIQ IDM can leverage the capability to match a person's PIV authentication certificate with one or more accounts in AD. In addition to the ability to provision user credentials for enterprise resources, NetIQ IDM can also provide provisioning and trust of certificates from external credential issuers as well as internal certificate authorities. To address some of the reporting capabilities needed with PIV-enablement efforts, NetIQ® Sentinel™ with NetIQ IDM can be leveraged to inject identity data into AD logging to see which PIV-enabled users are using their PIV cards, which are using non-PIV tokens, and those that are still using passwords (OMB FISMA reporting).

Automated Integration

Consider how agency systems, applications, directories and databases are integrated with an IDMS to PIV-enable authentication. To reduce complexity, implementation time, and ultimately cost, NetIQ IDM provides a large number of "pre-built" or out-of-the-box connectors to ease integration with agency systems.

NetIQ IDM also provides automated integration with the PIV/PIV-I/CAC credential issuing service, also known as the Credential Management Server (CMS) to include capabilities for PIV/PIV-I/CAC Issuers:

- GSA MSO US Access
- XTec
- Operation Research Center (ORC)
- Others

By providing auto-enrollment of HR information into the CMS, NetIQ can provide greater efficiency. As an example, security officers can look up existing identities and capture their picture and fingerprints, rather than having to key in all initial identity information. NetIQ can provide automation around the process of importing certificate data from the CMS for activated PIV cards into the local identity and access management (IAM) system for logical access into information systems. When changes to an identity occur, the capability to synchronize those changes to the CMS can be leveraged. Some sample changes to an identity could be:

- Adjudication status
- Background check status
- Eligibility status
- Agency affiliation

NetIQ can assist with automating the process flow for the PIV credentialing process. After inviting users to receive a PIV credential, the NetIQ solution can track and report on the lifecycle progress (first PIV authentication, and so on) and even leveraging group policies to force PIV usage.

PIV-Enablement of Full Disk Encryption

NetIQ IDM provides synchronization of PIV certificate data to McAfee Endpoint Encryption/ePolicy Administrator. Configuration of McAfee policies can be done to consume synchronized certificates and distribute them to machines associated with each user to configure authentication with a PIV card. Enablement of SSO from McAfee ensures that no additional Windows authentication prompts are seen after PIV card and PIN authentication. Support is also available for Virtual Smartcard (VSC) authentication to Microsoft BitLocker.

Alternative Logon Methods

NetIQ IDM approval workflow allows users to request temporary alternative access to the network if a PIV card is lost, broken or stolen. Automation of policy constraints can deal with the PIV card's physical status (to disable and revoke certificates in the CMS if a card has been lost for more than 17 hours, for example). An auto-registration kiosk for PIV, PIV-I and CAC allows externally credentialed personnel to present their card at the kiosk to authenticate and gain policy-based access to local agency logical and physical resources on a temporary basis (may include approval flows).

Support for remote access with a PIV card from outside the network can be supported through configuration of the NetIQ IDM solution. Examples of such supported configurations range from PIV-enablement of Cisco ASA VPN devices to Citrix (NetScaler, Citrix Web Interface, Virtual Desktops and applications, and so on).

Physical Access Control Systems Considerations

Bringing the PACS systems into the larger FICAM solution can be a considerable challenge. Often PACS systems exist in isolation and are frequently managed by an entirely separate portion of the organization. However, the benefits of integrating the PACS system are significant, and the HSPD-12 mandate includes PACS integration as a key component. With an integrated PACS system, relevant data such as the PIV-I picture, identity, and status can be synchronized with the CMS.

Once connected, the unified systems allow for the implementation of simplified and improved business processes. For example, an agency might choose to immediately load a new identity into the PACS environment, but initially in a disabled state. The agency could then require a security officer to approve the access, ideally through the IDM integrated workflow system, before actually allowing the new user into the facilities. Of course, reverse scenarios also become possible, where a user loses physical access to facilities immediately if their PIV authentication certificate is revoked.

A simple but important strong point of NetIQ FICAM solutions platform is the number of connectors available to various systems—over 100 target resources today. This strength continues in the PACS specific connectors, where NetIQ federal identity solutions already have connectors to many of the major PACS vendors' platforms. This will continue to be a strong point as solution teams at NetIQ and TriVir work constantly to develop new connectors and maintain the existing connectors.

Authoritative Identity Sources

Authoritative identity source is the source of the data that flows to the IDM system. Typically, identity sources are either a directory or a database that contains identity details about individuals tied to your agency (such as employee ID, first name, last name, email, phone, department and so on). Most authoritative sources stem from corporate sources such as; HR databases, corporate email, payroll systems and so on.

One of the challenges to successfully implement an IDM solution is to determine what the authoritative source truly is. When considering implementation efforts around IDM, it is important to evaluate your current identity source and ensure that it is flexible and scalable enough to align with your IDM needs. Your agency might prioritize the need to scale identity management around the enterprise, which may include employees and non-employees. Will your current identity source be able to handle the forecasted user population? Another key element to consider is ensuring that the IDM solution you select is able to work within your heterogeneous environment—from application, to database, to identity source.

You don't have to replace your existing systems. NetIQ federal identity solutions integrate out-of-the-box with several leading identity stores including eDirectory, Active Directory and Sun One, HR systems, as well as any standard HTTP application.

Single Sign-On

When considering PIV enablement, your agency should consider single sign-on (SSO). Traditionally, agencies have attempted to PIV-enable their applications by re-writing the applications or leveraging native PIV software to accomplish SSO. Agencies spend a lot of money and effort managing passwords, which is one of the most common helpdesk requests. Password-related issues can create unacceptable risks and costs for your organization, because relying on your employees to remember long lists of user names and passwords can create severe consequences.

By integrating your PIV with IDM to enable SSO, password management becomes much simpler because your users only have to remember one login routine for access to all authorized applications. This not only makes your environment more secure, but also makes your users more productive and lowers support costs.

Leveraging an IDM solution to enable SSO provides centralized administration and more advanced security capabilities, while streamlining access to a wide range of applications and websites. SSO helps eliminate the need for username and password management in anything you build. From an end user perspective, SSO reduces the time spent re-entering passwords for the same identity.

How much are password-related calls costing your agency? Reducing the number of password-related calls to the help desk reduces IT costs. This can be achieved by providing self-service capabilities for the end user to reset their passwords or unlock their account without calling the help desk. And because NetIQ federal identity solutions distribute password updates in real time across all your physical and virtual resources, your entire environment is password maintenance free.

From a security perspective, NetIQ federal identity solutions not only provide SSO, but also fine-grain access controls over your application environment. And it is all done without requiring application modifications.

As agencies start considering PIV-enablement of their applications, they should also consider SSO by evaluating the number of applications that exist in the enterprise that need to be PIV-enabled along with identifying which applications are mission-critical and which will require a high degree of identity assurance. To further assist with this

process, NetIQ federal identity solutions leverage role information, which can be supplemented by additional queries of the user's identity to determine whether the user is authorized to access the requested resource.

IDM Co-Existence

As your agency begins formulating plans for PIV integration via NetIQ IDM, it is important to consider the technical architecture of the existing footprint along with the future footprint.

If your agency currently leverages an existing identity management solution, it is important to consider how your agency plans to weave in the integration plans with your existing architecture.

Most agencies have heterogeneous environments consisting of applications, databases and identity management products. Ensuring all of these pieces work together, while meeting your requirements for LACS and/or PACS integration, is critical.

NetIQ federal identity solutions have customer proof points that co-exist with other vendor identity management components. This is important because most agencies do not want to rip and replace their existing identity components.

Identity Tracking & Attestation

As your agency begins formulating PIV enablement plans, consider your cybersecurity posture. Can you leverage your known (and unknown) identities to monitor activities in your environment and match that activity to a specific identity? NetIQ access governance solutions ensure that for each PIV, automated reports can be generated to identify who is accessing what and how they were granted that privilege. Managers can regularly attest to whether or not existing access should remain for their users so PIV access that is no longer needed is automatically removed.

Legacy Application Integration (including mainframe)

A major "application" that is usually overlooked for PIV enablement is the mainframe. The agency mainframe often holds a large amount of sensitive agency data. This sensitive data needs a higher level of authentication and identity verification. PIV enablement of mainframe authentication meets the requirements to secure sensitive data.

How can older, legacy applications be secured? NetIQ's identity management solution can PIV-enable many legacy applications without coding changes to the application itself. This allows agencies to meet federal government cybersecurity regulations, as well as reduces costs.

Other Related Services Available

- Workstation configuration (certificates, software, BIOS/hardware, USB ports, and so on) through NetIQ® Identity Manager synchronization into the target destktop management platform (such as Microsoft SCCM or Novell ZENworks Configuration Management)
- Configuration of FIPS-201-2 Near Field Communication (ISO 14443) for PIV with workstations and mobile
- Configuration and management of Online Certificate Status Protocol (OCSP) servers based on the Windows platform or other vendors to streamline and control certificate validation within the firewall for LACS and PACS
- Ability to tie down and control privileged user access on Windows and UNIX through NetIQ® Privileged User Manager and Identity Manager
- Card behavior configuration (card removal, PIN management, and so on)
- Documentation (policy, HR, agency communications, helpdesk, hardware team, end user)
- Tier 2 support (issues identified and unresolved by the agency may be escalated to NetIQ/TriVir for resolution)
- Enablement of mobile devices for PIV related authentication through the provisioning and linkage of derived credentials on each device, tied to the user's eligibility status and possession of an active PIV card
- Monitoring/reporting of FISMA metrics progress in regards to PIV enablement and use within each user audience; standard, elevated access and remote
- Program Management Office (PMO) assistance and implementation services for HSPD-12 programs through NetIQ/TriVir partnered ICAM services (GSA IT Schedule 70, Contract Number GS-35F-0603X ***http://www.gsa.gov/portal/content/104506?utm_source=FAS&utm_medium=print-radio&utm_term=schedule70&utm_campaign=shortcuts)***

Solution Differentiator Summary

The NetIQ federal identity solution is the only solution in the marketplace that manages the PIV-enablement process at all levels, such as:

- Invitation to enroll and receive a PIV card
- Provisioning of the user into the CMS for issuance and activation of the badge
- Synchronization of PIV certificates into the local network for use at workstations and in applications
- PIV-enabled access to workstations, laptops, mobile devices and web applications (internal/external)
- Interoperability allowing externally issued credentials by other agencies to be trusted for internal access through Attribute Based Access Control (ABAC) and manually approved processes implemented in approval flows
- Incorporation into the full disk encryption of each machine used by the user to enable access with their PIV card
- Alternative logon mechanisms to allow graceful handling of lost, stolen or forgotten PIV cards

Several key takeaways should factor into your evaluation and decisions regarding your PIV enablement strategy:

- The NetIQ federal identity management solution leads the industry with the first fully functional commercial-off-the-shelf (COTS) integration with the General Services Administration (GSA) Managed Service Offering (MSO) US Access PIV credential management system.
- The NetIQ federal identity management solution is the only COTS solution that can synchronize identity and certificate information between the PIV issuer to Active Directory, PIV-enabling network access and applications without writing a single line of code through human-readable digital policy.
- The NetIQ federal identity management FICAM implementation is the only COTS FICAM implementation that can be tested automatically to simplify solution extensions and maintenance.

The NetIQ federal identity management solution is the glue that ties all platforms together for managed identity that can be accessed through a PIV context regardless of vendor, thus avoiding vendor lock-in and providing the greatest solution flexibility for the lowest cost.

Sylvia Gonzales
Federal Account Manager, NetIQ
8609 Westwood Center Drive
Vienna, VA 22182 USA
713.418.5393
Sylvia.Gonzales@netiq.com

Larry Mooney
Business Development Manager, TriVir LLC
13890 Braddock Road; Suite 310
Centreville, VA 20121
301.869.3214
LMooney@trivir.com

About

TriVir

TriVir is a professional services company founded in 2003 focused on providing software solutions to help organizations solve their business challenges. TriVir concentrates on complex situations where having an experienced advisor can save time and money. This includes HSPD-12, identity and access management, single sign-on, compliance monitoring and reporting and systems development. TriVir is recognized as a consulting leader in the identity management space and is NetIQ's premier consulting services partner at a Platinum level. We have a diverse array of clients who come from both the public and private sectors. By focusing on three key cultural pillars of talent, discipline and commitment, TriVir has carefully cultivated a culture dedicated to delivering unmitigated success to every project for every client.

To learn more at **www.trivir.com**.

Headquarters
13890 Braddock Road
Suite 310
Centreville, Virginia 20121
Phone: 703.266.1353

NetIQ

NetIQ is a global, IT enterprise software company with relentless focus on customer success. Customers and partners choose NetIQ to cost-effectively tackle information protection challenges and manage the complexity of dynamic, highly-distributed business applications.

Our portfolio includes scalable, automated solutions for Identity, Security and Governance, and IT Operations Management that help organizations securely deliver, measure, and manage computing services across physical, virtual, and cloud computing environments. These solutions and our practical, customer-focused approach to solving persistent IT challenges ensure organizations are able to reduce cost, complexity and risk.

To learn more about our industry-acclaimed software solutions, visit **www.netiq.com**.

Worldwide Headquarters
515 Post Oak Blvd., Suite 1200
Houston, Texas 77027 USA
Worldwide: +713.548.1700
U.S. / Canada Toll Free: 888.323.6768
info@netiq.com
www.netiq.com

www.netiq.com/communities

For a complete list of our offices
In North America, Europe, the Middle East
Africa, Asia-Pacific and Latin America,
please visit **www.netiq.com/contacts**.