Enable Your Applications for CAC and PIV Smart Cards

Executive Summary
Since HSPD-12 was signed in 2004, government agencies have issued over 5 million identity badges. About 90% of government workers and contractors wear their identity around their neck. While most agencies are leveraging these for physical access, the challenge comes in trying to use them for logical access to systems. Today users still use multiple accounts and passwords to access systems. Ping Identity’s solutions allow end users to use their PIV cards for seamless access to on-premise, hosted and cloud-based applications. This paper describes how agencies can leverage the card that hangs around user necks to be the key all applications.
# Table of Contents

**Executive Summary** ................................................................. 1

**Deliver the Value of Smart Cards** .............................................. 3  
OMB M-11-11: Take HSPD-12 One Step Farther. ................................. 3  
Realizing the Promise of Smart Cards ............................................. 3

**CAC and PIV Integration Challenges** ......................................... 4  
Government Infrastructures Complicate Smart-Card Integration ............... 4  
Complex Behind-the-Scenes Functionality ........................................ 5

**Commercial Off-the-Shelf (COTS) Solutions** ............................ 5  
What to Look for in a COTS Solution ............................................. 5  
Why Choose PingFederate for Your COTS Solution ............................ 6

**Taking a Closer Look at PingFederate** ..................................... 7  
How PingFederate Works ............................................................... 7  
100% Adherence to Open Standards .............................................. 8  
How the X.509 Integration Kit Works ............................................. 8  

**How Service Provider Integration Works** ................................ 9  
Citrix XenApp Integration Kit ....................................................... 9  
CA SiteMinder Integration Kit ...................................................... 9  
SaaS Connectors ........................................................................ 10  
Identity-Enabled Web Services .................................................... 10

**Putting It All Together** ............................................................. 10  
Meeting OMB M-11-11—Today and Tomorrow ............................... 11

**About Ping Identity** ................................................................. 11
Deliver the Value of Smart Cards

OMB M-11-11: Take HSPD-12 One Step Farther

In 2011, the U.S. Government’s Office of Management and Budget (OMB) sent an explicit directive to all federal agencies: Now that most government workers and contractors possess an X.509 smart card (CAC, PIV or PIV-I), step up your efforts to enable its use for accessing facilities and IT resources or risk losing funding.

For government IT and security professionals, the stakes are high. The memorandum, known as OMB M-11-11, mandates that funding for the development and maintenance of systems and resources—new or existing—is contingent on smart-card integration.

With the stakes so high, now is the time to …

- Understand why enabling applications to be smart-card compliant doesn’t have to be difficult, expensive and time-consuming
- Learn how commercial off-the-shelf (COTS) solutions provide easy-to-implement, cost-effective ways to address OMB M-11-11 requirements
- Discover how PingFederate can help you meet the challenges of smart-card integration

Realizing the Promise of Smart Cards

The U.S. government’s investment in X.509 smart-card technology is longstanding and considerable. The Department of Defense first deployed Common Access Cards (CACs) a decade ago. In 2004, Personal Identity Verification (PIV) and PIV-Interoperable (PIV-I) cards became a government-wide regulation with Homeland Security Presidential Directive 12 (HSPD-12), which called for multifactor authentication, digital signatures, encryption capabilities and a standardized background check for every government employee and contractor.

Distributing PIV smart cards to employees and PIV-I smart cards to contractors across all federal agencies was the first step, but now attention has shifted to integrating applications into the PIV authentication infrastructure. With the huge variety of applications and architectures in use by government workers, creating agency-wide smart-card compatibility is a significant task. But to realize the promise of smart cards—greater security, convenience and cost-savings—enabling applications to accept PIV credentials is a necessity.
CAC and PIV Integration Challenges

Government Infrastructures Complicate Smart-Card Integration

The need to provide access to a diverse set of applications complicates smart-card integration for many federal agencies, including the DoD, intelligence community and civilian agencies.

It’s not unusual for a government worker to need access to...

- Virtualized client/server applications via a Web browser
- Web Access Management (WAM)—protected applications (e.g., CA SiteMinder, IBM Tivoli)
- Cloud-based applications (e.g., Google Concur, salesforce.com)
- Information-sharing applications that call identity-enabled Web services
- Other legacy government applications or systems

Developing custom code to ready even one application for smart-card authentication is no small feat. For most government agencies, the quantity of resources—people, time, money—needed to meet smart-card compliance seems staggering. Fortunately, a variety of commercial off-the-shelf (COTS) products and technologies are available to help agencies meet the requirements of OMB M-11-11. An agency needs to carefully weigh the costs and benefits of a COTS solution vs. custom development to determine which option best meets the needs of the agency.
Complex Behind-the-Scenes Functionality

To understand the challenges of enabling an application to accept smart-card credentials, consider the e-authentication model that NIST recommends in the *NIST Special Publication 800-63 Electronic Authentication Guideline*.

The left side of the diagram shows the steps required to set up smart-card authentication for a government worker. The worker registers (1) with a registration authority (RA). The RA vets the worker (2) and sends a registration confirmation (3) to a credential service provider (CSP). In turn, the CSP issues an identity token and credential (4) to be used for subsequent authentication events (e.g., accessing an application). The CSP maintains the credential; the worker maintains the smart card, which stores the token.

The right side of the diagram shows the steps that must occur when the worker uses the smart card for authentication. The worker proves to a verifier that he or she possesses and controls the token through an authentication protocol exchange (A). The verifier interacts with the CSP (B) to validate the token and credential associated with the worker. The verifier then issues an identity assertion about the worker to the relying party (e.g., an application—C). The relying party establishes an authenticated session with the worker (D).

The workhorse in the NIST model is the verifier. Deploying a COTS solution that can fulfill the role of the verifier for a broad spectrum of applications can help you rapidly enable your agency applications to accept PIV credentials.

Commercial Off-the-Shelf (COTS) Solutions

What to Look for in a COTS Solution

While the government does not require an agency to purchase a COTS solution or solution
suite, agencies that consider this option need to answer several questions before deciding to purchase:

- How successfully will the product help us meet our service goals?
- How will the product integrate with our existing infrastructure?
- Is software licensing (or other cost-saving options) available?
- Does the solution use proprietary technology or is it based on open standards?
- With an eye on future needs, how adaptable is the solution?
- Does the solution support government initiatives and policies?

Integrating an IT resource into the CAC and PIV authentication infrastructure can vary from simple to complex, depending on the type of resource, its age and ability to be updated, and the diversity of its user base. For example, transitioning some legacy applications might take months or more to complete and require extensive—and costly—custom development. So, it’s important to make sure any COTS solution that you consider is robust enough so that you can enable most (if not all) of your agency resources simply, rapidly and cost-effectively.

**Why Choose PingFederate for Your COTS Solution**

PingFederate provides secure single sign-on (SSO) access to multiple applications and application architectures—to all the types of applications a government worker typically uses.

Working behind the scenes in the role of the verifier, PingFederate can conduct CAC or PIV user authentication exchange, validate the certificate with the credential service provider and securely pass the necessary identity information to the desired application to establish an authenticated session with the user.
Built on open standards and security technologies such as HTTP, HTTPS, SSL, TLS, SAML, and PKI, PingFederate is designed specifically to help extend existing applications—and its robust. Commercial integration kits support all leading identity management vendors and applications to enable rapid deployment into your existing infrastructure. The solution offers an SDK so that you can create custom adapters for systems that do not have an integration kit. PingFederate works with more than 200 SaaS partners out of the box.

In addition to its core federated identity and SAML-based SSO capabilities, PingFederate also enables secure mobile access, automated cloud user provisioning and API security.

**Taking a Closer Look at PingFederate**

**How PingFederate Works**

PingFederate is standalone, enterprise software. It provides an administration console and management services, runtime services and extensive logging and monitoring capabilities. But the most significant PingFederate feature—and the reason WHY you can implement the software in days in most government environments—is the rich set of integration capabilities that comes with the product.

PingFederate provides turnkey integration kits for more than 30 identity and application infrastructures. For CAC and PIV smart card integration, you use the X.509 integration kit, but PingFederate provides integration kits for Microsoft AD, CA SiteMinder, LDAP and many other identity provider environments, as well as an SDK for agentless integration.

On the service provider side, PingFederate integrates with Java, .NET and PHP application environments; Web and application servers such as Apache or Microsoft IIS; WAM systems such as CA SiteMinder, Oracle OAM and IBM TAM; and commercial applications such as Citrix and Microsoft SharePoint.
PingFederate X.509
Certificate Integration Kit

Certification provides an identity provider (IdP) adapter that lets a PingFederate IdP server perform X.509 certificate authentication for SSO to service provider applications.

100% Adherence to Open Standards

PingFederate provides integrated support for all predominant open communications standards—SAML, OAuth, OpenID, WS-Trust and WS-Federation—to meet the needs of a wide range of government environments. SAML, an XML-based standard for communicating identity information between organizations, is the most accepted protocol for communicating identities across the Internet. Because of PingFederate’s SAML-based capabilities, more than 200 partners have teamed with Ping Identity to deliver Tier 1 SSO solutions.

How the X.509 Integration Kit Works

Consider a typical scenario in which a government worker logs on with a CAC or PIV smart card then requests an application through a Web portal. The X.509 integration kit, which installs with PingFederate, lets PingFederate acquire the user’s certificate directly from the Web browser via SSL (1)

Next, PingFederate authenticates and validates the certificate (2). Finally, PingFederate bundles up all the user attributes from the certificate and other sources (e.g., a directory) into a secure SAML assertion and sends it to the requested application, authenticating the user (3).
How Service Provider Integration Works

In the service provider role, PingFederate receives and decodes the security token. The various integration kits then enable the target application to consume the user information and use it to set up a valid session or other security context for the user.

**Citrix XenApp Integration Kit**

For example, consider what happens with the Citrix XenApp (a virtualized client/server application) integration kit.

Once the SAML assertion arrives, PingFederate uses an IIS server to generate an equivalent Kerberos ticket. XenApp uses the Kerberos ticket to authenticate the user and establish a user session.

**CA SiteMinder Integration Kit**

The PingFederate SiteMinder (a WAM-protected application) integration kit works differently. In this case, once the SAML assertion arrives (1), PingFederate instructs SiteMinder Policy Server to generate an SMSESSION cookie (2).

PingFederate then redirects the user to the application where the SiteMinder Web Agent extracts and validates the SMSESSION cookie (3).
SaaS Connectors

The connectors supporting Google and other SaaS applications take advantage of the fact that these applications support SAML natively. In this case, PingFederate is involved only on the identity provider side.

When a government worker logs on with a CAC or PIV card then clicks a link for Google Apps or Gmail in the Web portal, the link redirects the user to PingFederate (1), which validates the user identity (2). PingFederate sends a SAML assertion directly to the Google application, and the application completes the SAML processing, establishes a secure session with the user and redirects the user to the application.

Identity-Enabled Web Services

In the case of identity-enabled Web services, PingFederate supports both SOAP-based and REST-ful APIs. In the SOAP case, PingFederate receives the X.509 certificate from a Web service client and uses a security token service to translate the certificate into a SAML assertion that it places in the SOAP header. SAML is the protocol of choice because it’s designed to be portable and secure in hostile environments. When the Web service provider receives the SAML assertion, it can make a quick, complete determination about whether the request is authorized.

PingFederate also supports the OAuth 2 standard for REST-based Web services, which numerous government agencies are starting to use.
Putting It All Together

Meeting OMB M-11-11—Today and Tomorrow

The mandates of OMB M-11-11 have raised the bar for enabling the usefulness of CAC and PIV credentials in federal agencies. Agencies that have made significant progress issuing smart cards must leverage that investment today and going forward.

A multitude of ways exist for agencies to adapt their logical access control systems (LACS) infrastructure to accommodate CAC and PIV cards for authentication, including a variety of solution alternatives and implementation approaches. Analyzing the costs, benefits and timeliness of custom development, COTS solutions or some combination of both is a critical part of agency’s transition plan.

Taking a close look at the capabilities of Ping Identity’s PingFederate for CAC and PIV enablement can benefit many government agencies. We invite you to visit our website and contact us for more information.

About Ping Identity

Ping Identity provides cloud identity security solutions to the world’s foremost companies, government organizations and cloud businesses. For more information, dial U.S. toll-free 877.898.2905 or +1.303.468.2882, email sales@pingidentity.com or visit pingidentity.com/gov.