Ping Identity®

White Paper

Passing on Passwords

Five Ways that Identity Federation is Improving Online Security for Government Agencies

Abstract

Cloud computing, social networking and mobile devices are improving efficiency and collaboration in the public sector. But anytime, anywhere accessibility also increases the need to simplify, control and secure identities. In addition, the public sector must maintain a strong focus on reducing costs and delivering a positive user experience. This paper provides a brief overview of federated identity and reviews its roles within the identity management strategies of civilian agencies, the Department of Defense (DoD) and the intelligence community.

Table of Contents

Abstract 1

Introduction 3

Background 3

Quick Review: What is federated identity? 3

Federated Identity and the FICAM Roadmap 3

The ICAM Open Identity Initiative 4

Securing Cloud Migration 5

Information Sharing 5

Extending PKI Smart Card Authentication 6

1. Enabling Applications to Accept PIV Card Authentication 6

2. Backend Attribute Exchange 7

3. Intermediate Step Toward Full PKI Bridge-based Interoperability 8

National Strategy for Trusted Identities in Cyberspace 8

About Ping Identity | The Identity Security Company 9

Introduction

Cloud computing, social networking and mobile devices are having a profound effect on the public sector, driving government agencies to strengthen online security and allowing them to increase transparency. But cost-savings and a positive user experience are also top of mind. Federated identity technology allows identities that are established and managed in one security domain to be recognized and used in another. In November 2009, ICAM published Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance, a 200-page document detailing an identity management segment architecture. This white paper describes five ways that federated identity--a core element of this architecture--is being used by US federal government agencies:

- A basis for **ICAM Open Identity initiatives**
- Keeping federal government **cloud migration initiatives secure**
- **Information sharing** between intelligence and law enforcement agencies at all levels of government
- Extending **functionality of PKI** smart card-based authentication
- A foundational technology for the **National Strategy for Trusted Identities in Cyberspace (NSTIC)**

Background

Quick Review: What is federated identity?

Federated identity is a technology that allows identities established and managed by one organization or security domain to be recognized and used in another, providing secure and convenient online access anytime, anywhere to accommodate an increasingly mobile workforce. The most common use for federated identity is Single Sign-On (SSO), where a user authenticating at their "home" organization (such as their employer) can seamlessly access external applications (such as a SaaS provider) without multiple logins. However, federated identity's ability to move identity attributes plays a role in secure mobile access, securing SOAP and RESTful Web APIs and leveraging cloud identity providers to eliminate repetititive user accounts and logins.

To avoid proprietary implementations, federated identity requires a standards-based strategy. Standards such as Security Assertion Markup Language (SAML), OpenID, WS-Trust, OAuth and Simple Cloud Identity Management (SCIM) have emerged over the past decade and now form the foundation for Ping Identity's cloud identity management solutions.

Federated Identity and the FICAM Roadmap

In October 2008, the Federal CIO Council established the Information Security & Identity Management Committee (ISIMC) to oversee government-wide activities related to identity management and cybersecurity. The ISIMC then established the Identity, Credential & Access Management (ICAM) subcommittee to align government identity management initiatives.

The aforementioned **Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance** produced by ICAM in February 2009 detailed a comprehensive identity management segment architecture and its benefits, including increased security, better compliance, improved interoperability, enhanced customer service, and increased protection of personally identifiable information (PII).

As shown in Figure One, federated identity is one of five key FICAM roadmap architecture systems, along with credential management, identity management, access management and auditing and reporting.

From a business perspective, the FICAM roadmap identifies four eGovernment service sectors where federated identity adds business value:

Government to Citizen (G2C)	Aims to facilitate interaction between government and the American public
Government to Business (G2B)	Drives interaction between agencies and the private sector
Government to Government (G2G)	Fosters inter-agency relationships and information sharing across all levels of government (federal, state, local and tribal)mobile device, etc.) for enhanced security.
Internal Efficiency and Effectiveness (IEE)	Drives internal agency processes and activities to be more friendly, convenient, transparent and cost-effective

The FICAM Roadmap also recognizes government's broad range of security requirements, calling for government-wide adoption of an NIST-defined security model with four different "levels of assurance" (LOAs) for electronic transactions.

The ICAM Open Identity Initiative

The FICAM roadmap describes the underlying identity problem for G2C and G2B applications in the following way:

"Enabling the appropriate level of identity assurance for non-federal users. . . continues to be a challenge for the federal community. While solutions are available, the ability for the 100 million plus individuals and businesses that need to obtain re-usable credentials that are cost-effective has not been realized. In many cases agency application owners continue to establish userid/password relationships with their constituencies, thereby perpetuating the stove-piped approach to identity management, lacking high assurance of identity when such assurance may be necessary, and incurring high costs in password resets and maintenance."

As a follow up to the FICAM roadmap, ICAM announced an Open Identity Initiative in January 2009, which provided further details, including an architectural approach allowing users to authenticate at cloud identity providers such as Google and Facebook to access online government services, eliminating the need for additional usernames and passwords. The ICAM approach uses profiles, trust frameworks, industry-standard federated identity protocols, and the NIST LOA model to provide adequate government security as well as a convenient and private user experience.

In October 2011, Federal CIO Steven VanRoekel issued a memorandum (see Appendix A) mandating the acceptance of specific cloud identity provider credentials at all LOA1 websites. Ping Identity is currently working with a number of federal agencies to support this mandate.

To act as a service provider to these identity providers, government organizations must implement federated identity software with the same protocols and profiles as the targeted identity providers. Ping Identity provides this software as well as the support for a successful implementation.

Securing Cloud Migration

In addition to increasing security, convenience and cost-savings for public-facing websites, federated identity plays a key role in another major federal government IT initiative: the migration to cloud-based systems. In December 2010, Federal CIO Vivek Kundra published the **25 Point Plan to Reform Federal IT Management**. Point #3 called for a "cloud first" strategy, specifying that "When evaluating options for new IT deployments, the Office of Management and Budget (OMB) will require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists".

This plan also called upon NIST to define cloud security standards. NIST published an initial draft of **Guidelines on Security and Privacy in Public Cloud Computing** in January 2011, prominently highlighting the importance of identity management in cloud security and the key role SAML should play.

The Whitehouse CIO followed up in February 2011, publishing its **Federal Cloud Computing Strategy**, which highlighted the significant cost savings of moving to the Cloud. With tightening budgets, many agencies are now actively considering cloud migration projects.

Because users and applications are typically managed by different organizations, cloud computing is actually tailor-made for federation. Ping Identity has already worked with hundreds of companies and several government agencies on these deployments, including over 200 SaaS providers who have SAML-enabled their cloud-based products using Ping's technology.

It is important to note that new SaaS, PaaS or IaaS initiatives fall under OMB M-11-11, meaning they must be PIV-card compatible. By integrating federated identity software with their PIV authentication system, then establishing SAML connections with software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) providers, government agencies can PIV-enable cloud-based applications without requiring anything additional from cloud providers.

Information Sharing

While cloud computing represents a relatively new use of federated identity within government, information sharing has been a missing piece for over a decade. For example, in the aftermath of 9/11 and during the second Iraq war, both the 9/11 Commission and the Weapons of Mass Destruction Commission identified "siloed" intelligence data as a critical barrier preventing intelligence and law enforcement agency personnel from effective collaboration.

As a result, the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 called for a government-wide Information Sharing Environment to improve the flow of terrorism-related information between intelligence agencies and between state, local and federal law enforcement agencies. In October 2007, the **National Strategy for Information Sharing** implemented these provisions, including information sharing at federal, state, local and tribal law enforcement as well as sharing with the private sector and foreign partners.

This document was followed by the creation of a formal Information Sharing Environment (ISE) program office in 2010 that now drives information sharing projects government-wide.

ISE immediately recognized it faced two major technical hurdles. The first was a lack of standard formats for sharing intelligence data. The other was identity and access management. For data formats, ISE turned to National Information Exchange Model (NIEM), an XML-based information exchange framework, which is an outgrowth of the Department of Justice's Global Justice XML Data Model (GJXDM) project.

For identity and access management, ISE turned to the FICAM Roadmap, federated identity and single sign-on for the needed G2G and G2B usage scenarios. According to the 2011 Information Sharing Environment Report to Congress, "The ISE's efforts at promoting federated identity. . .is vital to the security of the United States."

Given the large number of organizations that need to share data, their disparate authentication and application architectures, and the fact that they have existing working relationships, SAML-based federated identity is an ideal solution for providing needed access.

In fact, ISE has already had success with SAML in the Global Federated Identity and Privilege Management (GFIPM) project, which built a SAML proof-of-concept several years ago. GFIPM has gone into production as the National Information Exchange Federation, a project that currently links the Criminal Information Sharing Alliance (CISA), Pennsylvania Justice Network (JNET), the Regional Information Sharing Systems (RISS), the U.S. Department of Homeland Security, Los Angeles County and the FBI.

Extending PKI Smart Card Authentication

Federated identity can help extend the reach of PKI, the basis of smart card authentication for many intelligence and law enforcement agencies.

The US federal government has a long and deep history in PKI. The military was the first to deploy PKI-based smart cards with their Common Access Cards (CAC). PKI smart cards then became a government-wide requirement with President Bush's HSPD-12 directive in 2004, which called for multi-factor authentication, digital signatures, encryption capabilities and a standardized background check for every government employee and contractor.

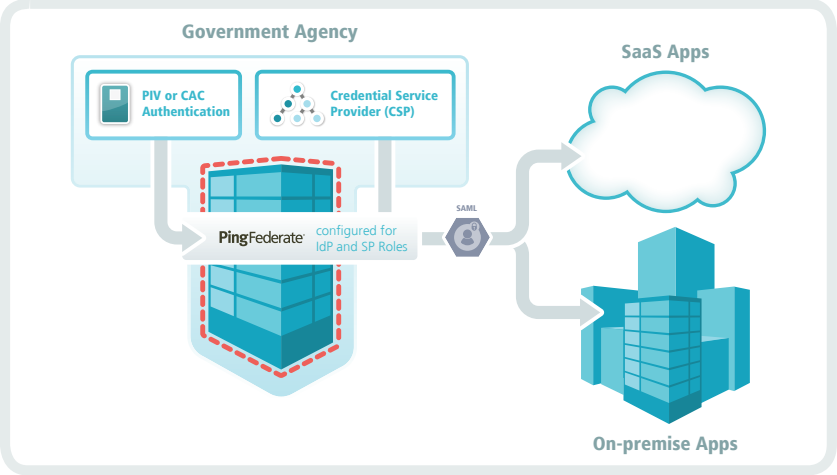
Standards for these Personal Identity Verification (PIV) and PIV-Interoperable (PIV-I) cards were subsequently published by NIST in 2005 as FIPS 201 and were then implemented. ICAM estimates that as of September 1, 2011, over five million HSPD-12 credentials have been issued to federal employees and contractors, representing 89% of the total federal workforce.

At this point, whether it be CAC cards in the DoD and Intelligence community, or PIV and PIV-I cards in the civilian agencies, federated identity is extending PKI infrastructures in three ways.

1. Enabling Applications to Accept PIV Card Authentication

PIV card distribution was the first step, but attention has now shifted to integrating applications into the PIV authentication infrastructure. This effort received significant visibility recently with the publication of M-11-11 by the White House, OMB and Department of Homeland Security (DHS) in February 2011, mandating that effective immediately, all new systems must accept PIV credentials.

With the huge variety of applications architectures in use by government employees, creating agency wide PIV-compatibility is a significant task. Fortunately, some federated identity software offers a shortcut. Products provided by independent vendors such as Ping Identity are usually designed to rapidly and easily integrate with an identity provider's current identity management and the service provider's existing application environment.



A single federation server can rapidly and securely integrate PIV authentication with numerous applications. The federation server can use attributes from the PIV card as well as additional attributes pulled from other sources.

In this scenario, a government agency that authenticates its own users and operates its own browser-based applications would act as both a SAML Identity Provider (IdP) and a SAML Service Provider (SP). Assuming their federated identity software can support both IdP and SP roles simultaneously, they can install a single federated identity server, integrate it with their PIV authentication mechanism, integrate it with their target applications, and then implement an internal SAML connection between the two. Using SAML as an intermediary can dramatically reduce the time and money needed to PIV card-enable existing applications.

2. Backend Attribute Exchange

The second way federated identity can extend PKI smart card authentication is a capability described in the FICAM Roadmap as "backend attribute exchange" or BAE. BAE is designed to give service providers or relying parties a means of obtaining attributes about a user beyond those available on the user's smart card.

According to a recent Burton Group report on Federal Government Authentication, "DHS, DOJ, FEMA, and other agencies have important authorization requirements for information sharing and emergency response. These agencies, together with DoD, have led the Back End Attribute Exchange specification using SAML and Service Provisioning Markup Language (SPML) to support authorization functions. DoD is promoting Net-Centric Enterprise Services (NCES) enabled by PKI, CAC, and software tokens for machine-to-machine services. Other agencies examining authorization issues should acquaint themselves with this work and consider assertion-based attribute and authorization solutions."

In addition to using SAML for BAE, Ping Identity is working with government agencies who are using a WS-Trust Security Token Service (STS) and OAuth to extend PKI-based systems to secure SOAP and RESTful Web Service APIs. Whether SAML, an STS or OAuth is being used for BAE, the deployment architecture is similar: both the relying party and the identity provider would implement federated identity software, then establish a connection between each other to securely exchange attribute queries and responses.

The IdP's federation software would integrate with attribute sources, while the relying party's federation server would integrate with either the target application or an authorization system. In cases where a single organization is acting as both the identity provider and the relying party they can implement both roles on a single federation server, assuming the server has the capability to play both roles simultaneously.

3. Intermediate Step Toward Full PKI Bridge-based Interoperability

OMB-11-11 also reconfirms an original HSPD-12 mandate that agencies must "accept and electronically verify PIV credentials issued by other federal agencies." Unfortunately, implementing PKI interoperability at this scale is a challenge and this project is still in progress.

In these situations, federated identity offers a short-term alternative. If Agency A (users) implements a federated identity server, and Agency B (application) does the same, they can establish a SAML connection to provide Agency A's PIV-authenticated users with SSO access to Agency B's applications.

Once the PKI bridge infrastructure is fully deployed and Agency B's applications become fully enabled, the federated identity infrastructure could theoretically be decommissioned and redeployed elsewhere. However, as the two previous sections highlighted, federated identity can provide additional benefits beyond PIV interoperability.

National Strategy for Trusted Identities in Cyberspace

In addition to current government initiatives, the National Strategy for Trusted Identities in Cyberspace (NSTIC) has a vision to make the Internet more secure for governments, private sector and individual citizens by replacing insecure password-based authentication with an "identity ecosystem". This "identity ecosystem" would deliver strong-authentication-protected digital identities, supplied by the private sector—not the federal government, as some critics have claimed—which would work anywhere, anytime.

The origins of NSTIC go back to a Cyberspace Policy Review published in 2009 by Howard Schmidt, President Obama's cyberspace coordinator. Schmidt called for a ten point near-term action plan, one of which was to "build a cybersecurity-based identity management vision and strategy, which addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the nation". The White House and Department of Commerce officially announced NSTIC in June 2010. A NSTIC program manager came on board in January 2011, and he published a formal NSTIC strategy document in April 2011.

While the NSTIC envisions a future where a single identity can be recognized "everywhere" and federated identity envisions a single identity managed in one place, yet recognized and honored in many places, the two ideas are strikingly similar. It is clear that federated identity technology and standards such as SAML, OpenID and OAuth can play essential roles in making the NSTIC vision a future reality.

© 2013 Ping Identity Corporation. All rights reserved. Ping Identity, PingFederate, PingOne, PingEnable, the Ping Identity logo, and Cloud Identity Summit are registered trademarks, or servicemarks of Ping Identity Corporation. All other product and service names mentioned are the trademarks of their respective companies.

2/13.1

About Ping Identity | The Identity Security Company

Ping Identity believes secure professional and personal identities underlie human progress in a connected world. Our identity and access management platform gives enterprise customers and employees one-click access to any application from any device. Over 900 companies, including 45 of the Fortune 100, rely on our award-winning products to make the digital world a better experience for hundreds of millions of people. For more information, dial U.S. toll-free 877.898.2905 or +1.303.468.2882, email sales@pingidentity.com or visit pingidentity.com.