Advancing the National Strategy for Trusted Identities in Cyberspace: Government as Early Adopter

Howard A. Schmidt
October 14, 2011
05:32 PM EDT

When I last discussed the need for better digital credentials in this blog, the President had just signed the National Strategy for Trusted Identities in Cyberspace (NSTIC) [http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf] to address two challenges that can affect economic growth online: (1) the insecurity and inconvenience of static passwords and (2) the cost of transactional risks that arise from the inability of individuals to prove their true identity online. The solution proposed by NSTIC is a user-centric "Identity Ecosystem" [http://www.nist.gov/nstic/identity-ecosystem.html] built on the foundation of private-sector identity providers.

Now the Administration has taken another key step towards realizing the vision of NSTIC. Our Federal Chief Information Officer (CIO), Steven VanRoekel, just issued a Memorandum for Chief Information Officers of Executive Departments and Agencies [http://www.cio.gov/Documents/OMBReqforAcceptingExternally_IssuedIdCred10-6-2011.pdf] detailing requirements for accepting externally-issued digital credentials. Going forward, Executive Departments and Agencies must accept approved externally-issued credentials when they are upgrading or developing Level 1 websites (as defined by OMB Memorandum 04-04 and NIST SP 800-63) that allow members of the public and business partners to register or log on. In addition, websites requiring credentials with higher levels of assurance (Levels 2, 3 and 4) should also be enabled to accept approved externally-issued credentials where appropriate. In basic terms, this means that solutions from firms like Equifax, Google, PayPal, Symantec and Wave Systems – all of whom have had their credentialing solutions certified to meet Federal security and privacy requirements – can be trusted identity providers for certain types of Federal applications.

This memorandum marks a new day for Federal efficiency: a citizen who is a veteran, a college student and a taxpayer ought not to have to obtain separate digital credentials at each agency website, but instead should be able to use ones he or she already has – a university-issued credential for example - across sites hosted by the Departments of Veterans Affairs, Education and Treasury. Doing so allows the Federal government to streamline the customer experience and recognize real cost savings just when we need to be tightening our belts. Moreover, by using accredited identity providers, Federal agencies see to it that Americans' information is treated with privacy and security online.

Yet the Federal government's role in facilitating the growth of the Identity Ecosystem is only half the story. To date, a handful of identity providers have undergone or are undergoing the Federal approval process. We are eager to see – particularly at the higher levels of credential assurance – a larger, vibrant pool of accredited identity providers to provide more choices for people and Federal agencies. The Federal government has developed a viable framework for using federated digital credentials, and with this memorandum, taken a significant step towards creating a more efficient government that can meet the needs of the American people in the 21st century. Now we look to the private sector to support our efforts and reap the collective benefits.

Learn more about the Federal approval process and the Open Identity Solutions for Open Government [http://www.idmanagement.gov/pages.cfm/page/IDManagement-open-identity-solutions-for-open-government] and Federal Public Key Infrastructure initiatives, or contact icam@gsa.gov.

Howard A. Schmidt is the Cybersecurity Coordinator and Special Assistant to the President

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

October 6, 2011

MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Steven VanRoekel
Federal Chief Information Officer

SUBJECT: Requirements for Accepting Externally-Issued Identity Credentials

As we work to achieve a more responsive and cost-effective government, it is essential that we identify opportunities to both improve services that deliver results for the American people, ensure their information is private and secure online and eliminate duplication. One such opportunity is in the area of identity management. Currently, members of the public and business partners maintain dozens of identity credentials to interact with the government online, and agencies maintain duplicative backend systems. To decrease the burden on users of our systems, and reduce costs associated with managing credentials, agencies are to begin leveraging externally-issued[1] credentials, in addition to continuing to offer federally-issued credentials.

The U.S. Department of Health and Human Services' National Institutes of Health (NIH) has successfully demonstrated the value of leveraging externally-issued credentials across its web sites, such as PubMed[2]. Since the initiative launch in June 2010, the number of users leveraging externally-issued credentials to access NIH sites has grown to more than 72 thousand. NIH estimates that its identity management initiative will result in cost avoidance of more than $2.98 million for fiscal years 2011 through 2015. These savings will result from not having to manage user IDs and passwords for external users across approximately 50 systems.

Effective 90 days following final approval of at least one Trust Framework Provider[3] (identified in Attachment A), agencies are to begin implementing the new requirement that will result in full implementation over the next three years by taking the following actions[4]:

- All new development of assurance Level 1[5] web sites that allow members of the public and business partners to register or log on must be enabled to accept externally-issued credentials in accordance with government-wide requirements.

---

[1] Externally-issued credentials are those that have been issued by an entity other than the federal government.
[2] "PubMed" is an NIH-managed website that comprises more than 20 million citations for biomedical literature from MEDLINE, life science journals, and online books.
[3] The General Services Administration, in collaboration with the Federal Chief Information Officers Council, approves the Trust Framework Providers and will publish the approval dates on http://www.idmanagement.gov.
[4] These requirements apply to E-authentication systems as defined in OMB Memorandum 10-15, "*FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.*"
[5] Identity Assurance Levels are described in OMB Memorandum 04-04, *E-authentication Guidance for Federal Agencies*, and NIST Special Publication 800-63, *Electronic Authentication Guidance*. For additional information refer to http://www.whitehouse.gov/omb/memoranda_2004 and http://csrc.nist.gov/publications/PubsSPs.html.

- Existing assurance Level 1 web sites that allow members of the public and business partners to register or log on must include the requirement to accept externally-issued credentials in accordance with government-wide requirements when those sites are enhanced or upgraded.

Additionally, where appropriate and as resources permit, Levels 2, 3 and 4 websites that allow members of the public and business partners to register or log on should be enabled to accept externally-issued credentials at higher levels of identity assurance in accordance with government-wide requirements.[6]

To ensure federal privacy and security requirements are addressed, agencies are required to follow Office of Management and Budget (OMB) policy and may only accept externally-issued credentials that are issued in accordance with National Institute of Standards and Technology guidelines and Federal Chief Information Officers Council processes.[7] Refer to Attachment A for the current list of approved providers. For existing web sites accepting non-approved externally-issued credentials, the agency must have an OMB/agency agreed-upon plan for complying with the requirement to use approved providers and schemes. Plans must be submitted to the Federal Chief Information Officer. Additionally, OMB and the General Services Administration (GSA) will meet with agencies to provide additional information regarding this memorandum and to share best practices. Attachment B includes the schedule of initial meetings.

I appreciate your leadership and commitment as we work to reduce costs in the area of Information Technology, while improving services. If you have questions, please contact Carol Bales at 202-395-9915 or eauth@omb.eop.gov, or Deborah Gallagher at 202-219-1627 or ICAM@gsa.gov.

Attachments

[6] In accordance with HSPD-12 policy, federal employees and contractors accessing federal systems for work purposes are expected to use Personal Identity Verification Credentials where assurance of identity is required.
[7] It is expected that agencies will continue to offer federally-issued credentials to accommodate members of the public and business partners without externally-issued credentials.

Attachment A: Approved Providers and Schemes

It is essential that credentialing processes and schemes are reliable, sustainable, and interoperable; therefore, the federal government requires a mechanism to evaluate the identity management processes and schemes against applicable federal requirements, policies, and laws. The *Trust Framework Provider Adoption Process* and *Scheme Adoption Process*[8] outline the process to evaluate organizations that assess external (i.e. non-federal) identity providers. To date, three trust framework providers are provisionally approved and three identity schemes (listed below) have been approved. The current listing of approved identity providers, for Levels 1, 2, and non-Public Key Infrastructure (PKI) 3, is listed below.[9]

Trust Framework Providers:
InCommon Federation – Level of Assurance 1 *(provisionally approved)*
Kantara Initiative – Level of Assurance 1, 2, and non-PKI 3 *(provisionally approved)*
Open Identity Exchange – Level of Assurance 1 *(provisionally approved)*

Identity Schemes (Levels 1, 2 and non-PKI 3):
Identity Metasystem Interoperability (IMI) 1.0 Profile
OpenID 2.0 Profile
Security Assertion Markup Language 2.0 Web Browser Single Sign-On Profile

Identity Providers (Levels 1, 2, and non-PKI 3):
Equifax - IMI 1.0 Profile, Level of Assurance 1 [http://equifax.com]
Google - OpenID 2.0 Profile, Level of Assurance 1 [http://google.com]
PayPal - OpenID 2.0 Profile, Level of Assurance 1 [http://paypal.com]
PayPal - IMI 1.0 Profile, Level of Assurance 1 [http://paypal.com]
VeriSign - OpenID 2.0 Profile, Level of Assurance 1 [http://pip.verisignlabs.com]
Wave Systems - OpenID 2.0 Profile, Level of Assurance 1 [http://wave.com]

In accordance with OMB M-04-04, "*E-authentication Guidance for Federal Agencies*" and NIST Special Publication 800-63, "*Electronic Authentication Guidance*", identity assurance levels are as follows:

Level 1	Level 2	Level 3	Level 4
Little or no confidence in asserted identity	Some confidence in asserted identity	High confidence in asserted identity	Very high confidence in asserted identity
No identity proofing required, and some confidence the same claimant is accessing the protected transaction or data	Provides single factor remote authentication using a wide range of available authentication technologies	Provides multi-factor remote authentication using "soft" cryptographic tokens, "hard" cryptographic tokens, and one-time password tokens	Provides multi-factor remote authentication using "hard" cryptographic tokens

For additional information, including a current list of approved identity providers and schemes, visit Open Identity Solutions for Open Government[10] at http://www.idmanagement.gov.

[8] The *Trust Framework Providers Adoption Process* and *Scheme Adoption Process* focuses on Levels 1, 2, and non-PKI 3.
[9] When accepting Level 3 cryptographic and Level 4 credentials, agencies must follow Federal Public Key Infrastructure requirements. For additional information, refer to "The Federal Public Key Infrastructure" at http://www.idmanagement.gov.
[10] A how-to guide for accepting Levels 1, 2 and non-PKI 3 credentials from certified identity providers will be available on http://www.idmanagement.gov in November 2011.

Attachment B: Meeting Schedule

October 24-28: Department of Agriculture, Department of Commerce, Department of Defense, and Department of Education

October 31-November 4: Department of Energy, Department of Health and Human Services, Department of Homeland Security, and Department of Housing and Urban Development

November 14-18: Department of Interior, Department of Justice, Department of Labor, and Department of State

November 28-December 2: Department of the Treasury, Department of Transportation, Department of Veterans Affairs, and Environmental Protection Agency

December 5-9: General Services Administration, National Aeronautics and Space Administration, National Archives and Records Administration, and National Science Foundation

December 12-16: Nuclear Regulatory Commission, Office of Personnel Management, and Small Business Administration

December 19-23: Social Security Administration and United States Agency for International Development