

## Notes from GSA's Identity Services Industry Day Briefings (November 5, 2008)

### Key Points:

- The President's Identity Management Task Force September report recommended the design of a "network of networks" affirming the direction of the GSA e-Auth initiative.
- GSA is recommending following the Liberty Alliance specifications citing the June 2008 "Identify Assurance Framework."
- GSA is depending upon natural affinity groups to provide credentials to citizens who use federal services. (RealID is not yet considered a complete solution).

On November 5, 2008 the U.S. General Services Administration held a briefing for the security industry. This meeting appeared to be a major effort to get industry support for broad implementation of identity services in the federal government. More than 200 industry, federal department and agency, and higher education representatives attended the five-hour briefing.<sup>1,2</sup>

Mike Brooks open the briefings with the point "there is no change." OMB Memorandum M-0404—that defined the four levels of assurance—will continue to be the defining directive.<sup>3</sup> Essentially he was saying this briefing would be authoritative—no changes—for the foreseeable future.

Mike Butler cited E-Authentication Program accomplishments including the 8 approved identity service providers and 13 interoperable SAML 1.0 and 2.0 products, and 80 applications with more than 1 million transactions per year. His point: The technology works and scales.

He said the E-Authentication Program functions have been realigned. The Office of Government Policy now is responsible for management of the Interoperability Lab, technical document, acceptance testing, Liberty Alliance Product Testing, credential assessments, and node management (Common Domain Cookie, EGCA certificates etc.) Within the Federal Acquisition Service, responsibility for agency logical access strategy, project and implementation planning, technical proposal evaluation support, and technical support for Agency project planning, deployment and testing. FAS is responsible for the GSA IT Schedules used by federal and state agencies for procurement. [Most agencies may procure independent of GSA]. These Schedule 70 procurements include consulting and support services, and hardware and software.

Judy Spencer began her presentation saying "E-Authentication is NOT going away." She cited OMB (Office of Management and Budget) Memorandum M-04-04, 16 December 2004 and the technical implementation NIST (National Institute of Standards and Technology) Special Publication 800-63 commenting that draft 800-63-1 has been made available for public review.

Implicitly she addressed some of the source of uncertainty. Of the 200 attendees only a few raised their hands saying they had read M-04-04, even fewer NIST 800-63 and only two (from Georgetown University) had read the President's National Science and Technology Council's "Identity Management Task Force Report 2008" published 22 September 2008.<sup>4</sup>

Spencer was suggesting the Task Force's report was affirming the direction of GSA's E-Auth Initiative begun in February 2002. She reported the HSPD-12 federal employee and contractor credentialing efforts are now the part of e-Auth focused on internal effectiveness and efficiency.

She said assertion-based solutions (e.g. SAML) would provide NIST Levels 1 and 2 assurance; cryptographic solutions and the Federal Bridge would provide Levels 3 and 4. Spencer also said GSA was "partnering" with the Liberty Alliance for assertion-based solutions and referred to Liberty Alliance's recently published "Liberty Identity Assurance Framework."<sup>5</sup>

The Task Force recommends IdM to support a "network of networks." Some comments:

The city planning model underlies the basic structure of internetworking. It describes how entities join together to form networks, how networks join together to conduct internetworking, and it lays out the fundamental infrastructure requirements needed to make these networks interoperate. FEA [Federal Enterprise Architecture], and specifically its Business Reference Model, takes a cross-cutting view of government services in terms of their business functions. It can be thought of as defining the government as a business sector in a model city. Government services are grouped together in a logical way in order to facilitate organizational efficiency and citizen access.

IdM is one of the infrastructural components that permits a network of networks to operate, providing a basic service that validates claims of identity so that individual business applications can determine what privileges are to be granted to that validated identity. The IdM architecture proposed here transcends the existing (but nascent) state of federated identity management. Within enterprise efforts have been ongoing, and several organizations are working on ways to articulate a standards-based approach to IdM.

The scope envisioned for the network is U.S.S federal government-wide. That is, services will be provided for all departments and agencies of the federal government and intended to support all federal missions. Thus, the scope includes providing services to citizens and other clients of federal systems, such as other agencies, non-citizens, other governments, and business. This will necessitate a clear distinction between the identity service the network provides and the application-specific services that user agencies develop and maintain.

Excerpts from the Task Force Report, pages 65-67

Spencer continued saying higher education's InCommon was the type of affinity group GSA was hoping would expand the "trusted credential community." She did not say what federal services were available using InCommon assertions, or what levels of assurance would be supported. Since she said all credentials and their use had to comply with Federal standards, implicit to her discussion was InCommon support by of the federal standards for levels of assurance, network

security, and interoperability, and subsequent validation through a FISMA audit.<sup>6</sup> She said GSA was interested in an affinity group of older Americans since they used more federal services.

“Looking Forward” Spencer said “OGP will spearhead the integration of the three current IDM activities.” GSA will better align with industry parts, focus on communities of interest (based on natural affinity groups), and open up the architecture. She explained “open up” by saying SAML 2 would be supported and they would review the OASIS WS-\* standards for possible use. In response to a question, she said WS-Trust had not yet been considered.<sup>7</sup>

In response to a question about RealID—specifications to be followed by states in issuing driver’s licenses—Spencer said this was not yet a solution. She didn’t comment further on that evaluation.

Bill Sill followed focusing on the needs of the federal agencies and urging suppliers to “invest in GSA.” He did point out that 80% of the federal applications require Levels 1 or 2 assurance; not Levels 3 or 4. It appears most applications used by higher education—veteran’s benefits, student aid, e-Research, and Department of Labor employment programs—would be level 2.

Stephanie Turner described the procedures for vendors to become GSA Schedule 70 suppliers. Most of the subsequent questions were about this process and the extent to which federal agencies would be using services and equipment.

The cost of identity proofing continues to be the major cost associated with improved identity management. Analysis of the GSA strategy suggests using affinity groups that already have performed adequate identify proofing—employees and many students—or have other benefits from identify proofing—such as AARP (though never mentioned by GSA) that require identify proofing to provide medical insurance and other services. Spencer mentioned the financial community that, because of federal regulation, have identity proofing processes that approximate Level 2 and provide a credential—the ATM card—and remote authorization.

The message: Now is the time to complete the infrastructure required to implement e-authentication and e-authorization. An observation many in higher education have made.

The IAEG defines four levels of assurance. The four IAEG ALs are based on the four levels of assurance posited by the U.S. Federal Government and described in OMB M-04-04 [M-04-04] and NIST Special Publication 800-63 [NIST800-63] for use by Federal agencies. The IAEG ALs enable subscribers and relying parties to select appropriate electronic identity trust services. IAEG uses the ALs to define the service assessment criteria to be applied to electronic identity trust service providers when they are demonstrating compliance through the IAEG assessment process. Relying parties should use the assurance level descriptions to map risk and determine the type of credential issuance and authentication services they require. Credential service providers (CSPs) should use the levels to determine what types of credentialing electronic identity trust services they are capable of providing currently and/or aspire to provide in future service offerings.

From the Liberty Identity Assurance Framework, page 7.

---

<sup>1</sup> The event was sponsored by the Integrated Technology Services of the Federal Acquisition Service. The Office of Government Policy, reporting directly to the Administrator, is responsible for policy; it includes the Office of Technology Strategy now headed by Peter Alterman. The organization of OTS has not yet been published. The former e-Auth initiative is now within OTS.

<sup>2</sup> Meeting documents and slides are available from [www.cio.gov/eauthentication](http://www.cio.gov/eauthentication). A consolidated PDF version is also available at [www.immagic.com/eLibrary/ARCHIVES/GENERAL/US\\_GSA/G081105I.pdf](http://www.immagic.com/eLibrary/ARCHIVES/GENERAL/US_GSA/G081105I.pdf).

<sup>3</sup> Later Judy Spencer commented the four levels were “borrowed from the U.K.” She could have been referring to the three levels described in “HMG’s Minimum Requirements for the Verification of the Identity of Individuals” first published in 2000 by the e-Envoy. Dr. Nig Zhang in the final report of the JISC Project “E-Infrastructure Security: Levels of Assurance,” 5 November 2007, suggested use of the NIST Levels of Assurance by U.K. universities. He referenced the U.K. origin of the levels of assurance.

<sup>4</sup> See Subcommittee of Biometrics and Identity Management, National Science and Technology Council, “Identity Management Task Force Report 2008,” Executive Office of the President, Washington, DC, 22 September 2008.

<sup>5</sup> See Russ Cutler ed., Identity Assurance Experts Group, “Liberty Identity Assurance Framework,” Version 1.1 20 Liberty Alliance Project, June 2008.

<sup>6</sup> At the October 7, 2008 meeting of PESC’s EA2 Electronic Authentication and Authorization Task Force, there was discussion about asking AACRAO (American Association of Collegiate Registrars and Admissions Officers) to update their FERPA (Federal Education Rights and Privacy Act) guidance provided to colleges and universities in the late 1990s.

<sup>7</sup> David Chadwick, University of Kent, on 11 June 2008 wrote: “WS-Trust [WSTRUST] is a proposal from Microsoft, IBM and others that enables security token interoperability by defining a request/response SOAP protocol whereby clients can request from some trusted authority that a particular security token be exchanged for another one.” See “Use of WS-TRUST and SAML to access a CVS,” Open Grid Forum.