



Advancing Identity Access Management (IdAM) with a Pilot Project in Pennsylvania

Posted by Michael E. Kennedy, PM-ISE Executive for Assured Interoperability on Thursday, April 12, 2012

In building responsible information sharing, Identity Management means that we can validate our users and that they have the proper credentials, or attributes, to access the right information. It's just like we follow a race car on the track full of competitors with its team name and number. Easy enough, right? Well not so fast, Mario Andretti!

Many finely tuned and fast-moving parts must come together perfectly for this to work. Proper Identity Management must assure all parties that the users accessing information are authorized, that they're seeing the right information, and that their privacy, civil rights, and civil liberties are appropriately protected. So, PM-ISE is co-sponsoring an exciting prototype!

Pilot Project with GSA

Earlier this month, we initiated a joint project with GSA to pilot a real-world test of a Backend Attribute Exchange. In the world of secure information sharing systems, "attributes" are the data points that systems use to validate a user has a legitimate need to access information. So a Backend Attribute Exchange allows this transfer of data to happen seamlessly as users login and research cases, intelligence, or any form of information owned and protected by another entity. The difference between a Backend Attribute Exchange and others is that it will accomplish this while adhering to important privacy and security policies. It will also be able to pull these attributes from multiple sources seamlessly as needed.

This initial test scenario will allow Pennsylvania law enforcement to access new information from external law enforcement portals like the [Regional Information Sharing System](#) ^[1] (RISS) (more about RISS on this blog [here](#) ^[2] and [here](#) ^[3]). In addition to other basic credentials, RISS requires a training certification in personal privacy information handling for access, so the Backend Attribute Exchange will direct it to the training provider's official records where it can see that the officer has the appropriate certification, and then grant access.

Beyond the Pilot Project

One of the keys to responsible information sharing that gets the right information to the right person at the right time is enabling systems to securely access various credentials that may originate from multiple authoritative sources. This is why the federal government has been working to develop a strong Backend Attribute Exchange capability.

Once this pilot test has proven successful, the GSA plans to offer a Backend Attribute Exchange Service for use by any federal system as part of an overall federal access control infrastructure that state, local,

and tribal partners could utilize. PM-ISE and GSA will also seek to make the Backend Attribute Exchange architecture a public voluntary standard, which may contribute to the development of the [Identity Ecosystem](#) [4] envisioned by the [National Strategy on Trusted Identities in Cyberspace](#) [5]. (Read more about the National Strategy in [this White House blog post](#) [6] by Howard Schmidt.)

Get ready!

We expect the return on investment in the Backend Attribute Exchange to be significant for collaboration and responsible information sharing across the government. It will require some investment by information sharing partners on both ends. While we develop and deliver the Backend Attribute Exchange, it will be up to the individual partners to normalize attributes to the Backend Attribute Exchange Standards throughout their organization and then to populate those attributes so they can be used by the Backend Attribute Exchange. A very small effort compared to the HUGE amount of payback for all of us and our nation.

What's next? Learn more about Backend Attribute Exchanges so you are ready to support and implement responsible information sharing at your agency:

- [IDManagement.gov: Latest Developments](#) [7]
- [BAE v2.0 Overview](#) [8]
- [BAE v2.0 Governance](#) [9]
- [SAML 2.0 Identifier and Protocol Profiles for BAE v2.0](#) [10]
- [SAML 2.0 Metadata Profile for BAE v2.0](#) [11]

Related Blog Posts:

[Building Information Interoperability](#) [12]

[Improving Oregon and South Dakota Law Enforcement's Access to Key Information](#) [13]

[Safeguarding Our Nation's Law Enforcement Officers](#) [14]

Tags:

[cybersecurity](#) [15]

[info sharing](#) [16]

[privacy & civil liberties](#) [17]

Source URL: <http://ise.gov/blog/michael-e-kennedy/advancing-identity-access-management-idam-pilot-project-pennsylvania>

Links:

[1] <http://www.riss.net/>

[2] <http://ise.gov/blog/george-march/improving-oregon-and-south-dakota-law-enforcement?s-access-key-information>

[3] <http://ise.gov/blog/george-march/safeguarding-our-nation?s-law-enforcement-officers>

[4] <http://www.nist.gov/nstic/identity-ecosystem.html>

[5] <http://www.nist.gov/nstic/>

[6] <http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace>

[7] <http://www.idmanagement.gov/pages.cfm/page/IDManagement-latest-developments>

[8] http://www.idmanagement.gov/documents/BAE_v2_Overview_Document_Final_v1.0.0.pdf

[9] http://www.idmanagement.gov/documents/BAE_v2_Governance_Document_Final_v1.0.0.pdf

[10] http://www.idmanagement.gov/documents/BAE_v2_SAML2_Profile_Final_v1.0.0.pdf

[11] http://www.idmanagement.gov/documents/BAE_v2_SAML2_Metadata_Profile_Final_v1.0.0.pdf

[12] <http://ise.gov/blog/kshemendra-paul/building-information-interoperability>

[13] <http://ise.gov/blog/george-march/improving-oregon-and-south-dakota-law-enforcement%E2%80%99s-access-key-information>

[14] <http://ise.gov/blog/george-march/safeguarding-our-nation%E2%80%99s-law-enforcement-officers>

[15] <http://ise.gov/category/free-tags/cybersecurity>

[16] <http://ise.gov/category/free-tags/info-sharing>

[17] <http://ise.gov/category/free-tags/privacy-civil-liberties>