



A Detailed Test Scenario for our Law Enforcement Backend Attribute Exchange Pilot

Posted by Michael E. Kennedy, PM-ISE Executive for Assured Interoperability on Tuesday, August 28, 2012

Earlier this year, [I wrote in this blog](#) ^[1] about our project to plan a Backend Attribute Exchange (BAE) pilot, and I also explained some of the more technical concepts. Recently, our partners in this project at GSA wrote about it on their IDManagement.gov blog in a post, [Shared Services and Government as Attribute Service Provider](#) ^[2].

Our plan for this test pilot is to grant Pennsylvania law enforcement access to an important law enforcement database, the [Regional Information Sharing System](#) ^[3], or better known as RISS or RISS-Net (the network system that RISS offers). Read more about RISS's work in [federated search](#) ^[4] or [simplified sign-on](#) ^[5].

As we discussed more broadly in April, RISS requires a training certification in personal privacy information handling (28CFRpart23) for access, so the plan for the Backend Attribute Exchange is to direct it to the training provider's official records, where it can verify an officer's certification, and then grant access.

We're happy to report on our progress ? an initial test pilot scenario has been agreed upon by all necessary parties, and we plan to move forward with discussions at the technical level over the next few weeks so that we can deploy the test pilot solution. The following details that test pilot scenario:

A law enforcement officer in Pennsylvania has an account on the Pennsylvania J-Net network, which supports many public safety, law enforcement, and state government agencies and mission communities. To obtain the J-Net account, the officer's identity and status were vetted and various facts about identity, assignment, and qualifications were captured and maintained in the J-Net user database.

In the course of an investigation, the officer needs to access data on the RISS-Net system. Because both J-Net and RISS-Net are members of the National Information Exchange Federation (NIEF), RISS-Net can accept electronic credentials from J-Net once the officer logs into a J-Net account and is authenticated. The officer does not have to have a separate user account with RISS-Net.

In accordance with NIEF procedures, RISS-Net has defined a policy for access to their information resources, which is expressed in terms of specific characteristics (?attributes?) of authenticated users. The RISS-Net policy requires that a user is certified as a ?Law Enforcement Officer?, and has the necessary 28CFRPart 23 training. The information needed by the Pennsylvania officer requires both certifications (attributes).

The officer's J-Net records shows qualification as a law enforcement officer, and using the

standards defined by NIEF, J-Net is able to assert this status to RISS-Net as part of the credentials it provides.

However, although the officer was trained on 28CFRPart23 in a course offered online by the Bureau of Justice Assistance (BJA), this fact is not part of the officer's J-Net's record (28CFRPart23 training status is not one of the facts gathered in their vetting process). Thus J-Net cannot provide all the credentials required by RISS-Net for access to the needed data.

The BAE service helps meet this mission requirement by allowing user attributes (credentials/certifications) to be obtained from more than one attribute provider. In this scenario, the user's identity was vetted by J-Net, which issued and maintains his IT account, and which authenticates him when he logs on to J-Net. J-Net also vetted and certifies the fact that this user qualifies as a "Law Enforcement Officer." When the user navigates to the RISS Portal, the RISS Portal accepts the J-Net credentials and will provide access to information requiring only an authenticated login via a NIEF Member identity provider (i.e., J-Net) plus certification of "Law Enforcement Officer" status.

However, when the user requests information that under RISS policy also requires certification that he is "28CFRpart23_trained," the additional attribute (certification) is needed. The RISS Portal requests the additional information, which is obtained via BAE from IIR who is the BJA contractor for 28 CFR Part 23 training and technical assistance, which is able to provide the "28CFRpart23_trained" certification, and the information request is granted.

This is actually just one example of how a Backend Attribute Exchange can provide a valuable solution to information sharing and exchange challenges. After this pilot, we hope to replicate this kind of solution appropriately as a federal enterprise service for state, local, and tribal partners.

Related Blog Posts:

[Advancing Identity Access Management \(IdAM\) with a Pilot Project in Pennsylvania](#) ^[1]

[Building Federated Search Capabilities for Homeland Security and Law Enforcement Partners](#) ^[4]

[Building Information Interoperability](#) ^[6]

Tags:

[info sharing](#) ^[7]

[law enforcement](#) ^[8]

[mission partners](#) ^[9]

[public safety](#) ^[10]

[state & local gov](#) ^[11]

Source URL: <http://ise.gov/blog/michael-e-kennedy/detailed-test-scenario-our-law-enforcement-backend-attribute-exchange-pilot>

Links:

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

[2] <http://blog.idmanagement.gov/2012/04/shared-services-and-government-as.html>

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

[4] <http://ise.gov/blog/george-march/building-federated-search-capabilities-homeland-security-and-law-enforcement>

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

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

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

[8] <http://ise.gov/category/free-tags/law-enforcement>

[9] <http://ise.gov/category/free-tags/mission-partners>

[10] <http://ise.gov/category/free-tags/public-safety>

[11] <http://ise.gov/category/free-tags/state-local-gov>