GFIPM—A Passport for Information Sharing

Achieving information sharing objectives requires that partners establish wide-scale electronic trust among the caretakers of critical information and those who need and are authorized to use that information. The information is sensitive—inappropriate sharing is just as dangerous as lack of sharing. Enter the new and rapidly maturing technology called federated identity. Federated identity allows a user's roles, rights, and privileges to be communicated securely in the justice community and, in particular, to those who hold the information required to effectively safeguard our nation.

The Global Federated Identity and Privilege Management (GFIPM) framework provides the justice community and partner organizations with a standards-based approach for implementing federated identity. The concept of globally understood metadata across federation systems is essential to GFIPM interoperability. Just as a common Extensible Markup Language (XML) data model was the key to data interoperability, a standard set of XML elements and attributes about a federation user's identities, privileges, and authentication can be universally communicated. The GFIPM metadata and framework support the following three major interoperability areas of security in the federation:

- Identification/Authentication—Who are the end users and how were they authenticated?
- Privilege Management—What certifications, clearances, job functions, local privileges, and organizational affiliations are associated with end users that can serve as the basis for authorization decisions?
- Audit—What information is needed or required for the purposes of auditing systems, systems access and use, and legal compliance of data practices?

The GFIPM metadata specification is being used in a limited pilot capacity today. Lessons learned and feedback from this pilot were incorporated into the public release of the GFIPM metadata specification.

Building a Federation for Secure and Trusted Information Sharing

"Federation" is a fundamental concept in this framework. The federation provides a standardized means for allowing agencies to directly provide services for trusted users that they do not directly manage. A federation is defined as a "group of two or more trusted partners with business and technical agreements that allow a user from one federation partner (participating agency A) to seamlessly access information resources from another federation partner (participating agency B) in a secure and trustworthy manner." Major organizational participants in a federation vet and maintain information on the users they manage, and each federation partner retains control over the business rules for granting access to the sensitive information it owns. The federation partners establish the electronic trust needed to securely access information by sending standards-based electronic credentials to federation partner information service(s).

From: NIEM Newsletter, August 2009

The federation partner information service(s) evaluate the trusted electronic credential to determine whether to grant or deny access to the requested service or information.

A similar business model exists in passport processing. A federation of governmental agencies has agreed to vet and maintain information on its citizens as a prerequisite for issuing a passport. Border agents will grant or deny access to enter or leave the country based on evaluation of a passport—a trusted credential issued by a federation partner asserting identity and citizenship of a particular country. The country (federation partner) providing the service to enter or exit the country applies its own business rules based on the passport information and other attributes known at the time of the request.

GFIPM can be thought of as a method for generating a "passport" for information sharing—only those having the right passport can view data in the federated system, and all federated partners define what passports are necessary to view the data in their care.

Global Advisory Committee Recommendation

Over the last several years, federated identity deployments have grown, matured, and expanded in depth and breadth across multiple industries. As the standards have matured, more organizations have become aware of the compelling business case for building federated communities. As such, a critical objective of the Global Security Working Group (GSWG) for GFIPM is to ensure compatibility by collaborating with other key ongoing projects that cross domain boundaries, such as the National Information Exchange Model (NIEM), the Office of the Director of National Intelligence, and the Law Enforcement Information Sharing Program.

At the start of the GFIPM project, it was decided that the GFIPM metadata model would leverage the NIEM content and architectural framework. Given the work and success of the NIEM data modeling efforts, it is logical to leverage and reuse these specifications in describing the GFIPM metadata. The advantage of leveraging the NIEM specification is that it inherently makes the GFIPM metadata model immediately more applicable to other domains and systems, rather than focused only on criminal justice users and systems.

GFIPM metadata leverages the NIEM data modeling standard as the base vocabulary and naming and design rules in the data modeling effort for describing the conceptual model and building the associated schemas. However, neither GJXDM nor NIEM currently includes the concept of a federated user or a federated entity; therefore, these concepts must be defined here. It is expected that the GFIPM metadata defined as part of this effort will be reconciled and potentially added to NIEM in the future.

Federated identity is part of the GSWG's vision for promoting secure, nationwide information sharing. To this end, the Global Advisory Committee has adopted the following GSWG recommendations on behalf of the Attorney General's Global Justice Information Sharing Initiative:

- Recognize GFIPM as the recommended approach for development of interoperable security functions for authentication and privilege management for information access and exchange among cross-domain justice information sharing systems.
- Adopt the GFIPM: A Global Concept Activities and Progress Report as a recommended resource for next steps and activities to further the utility of GFIPM for the justice community.
- Urge the members of the justice community to consider GFIPM as a potential building block to a layered security solution when authenticating uses among cross-domain organizations.

GFIPM Initiative

The GFIPM initiative is supported through the Office of Justice Programs, Bureau of Justice Assistance (BJA); National Institute of Justice (NIJ); and the U.S. Department of Homeland Security (DHS). The GSWG provides oversight for this initiative. For more information about GFIPM, visit http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1179.