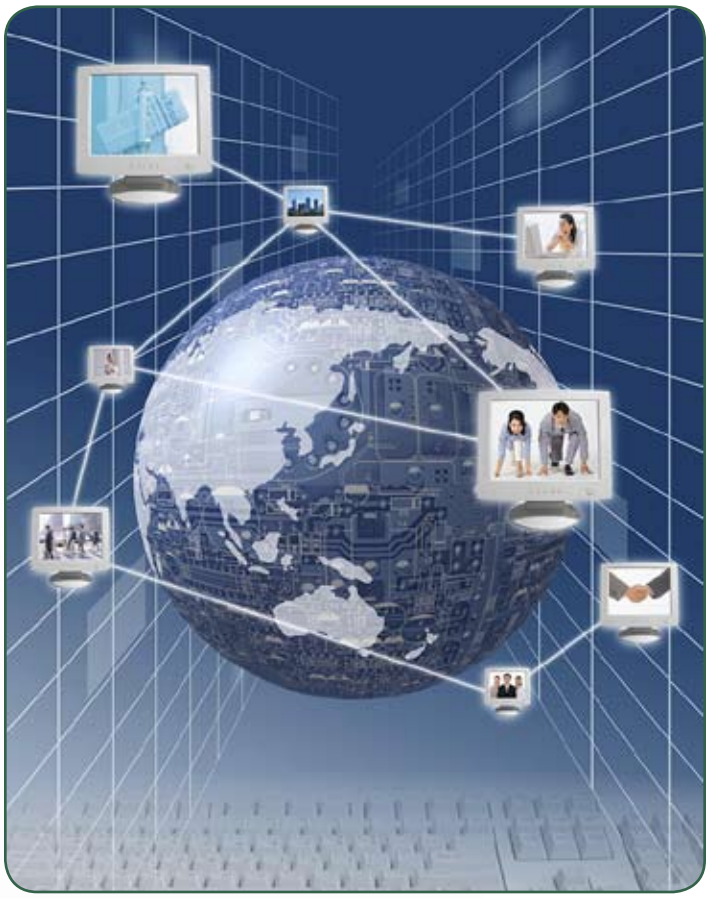
Global Federated Identity and Privilege Management (GFIPM)

United States Department of Justice

DRAFT

How can justice organizations share information with new partners while securely safeguarding data, maintaining privacy, reducing administrative burdens, and providing their users the ease of single sign on?

One recommended solution is GFIPM. It represents a strategic change and dramatic improvement in the way justice organizations establish the trust relationships needed to share information. GFIPM provides a standardized XML credential to be used by members and partners of the justice community. This credential will allow more information to be shared in new and automated ways—with reduced management burden and improved security and on a broader scale. GFIPM effectively breaks down the traditional barriers of stovepiped systems in order to better safeguard our nation.



GFIPM Framework

The **GFIPM** framework provides the justice community and partner organizations with a standards-based approach for implementing federated identity. Common use of these standards across federation systems is essential to their interoperability. Leveraging the Global Justice XML and National Information Exchange Models (NIEM), a standard set of XML-based elements and attributes (referred to collectively as GFIPM metadata) about a federation user's identities, privileges, and authentication can be universally communicated.

Security Benefits

Identification/Authentication
Who is the end user and how was their identity verified?

Privilege Management
What level of information access is appropriate for the user, as based on such criteria as certifications, security clearances, job functions, local privileges, and organizational affiliations?

Audit
What information is needed or required for the purposes of auditing systems, systems access and use, and legal compliance of data practices?

Building a Federation for Secure and Trusted Information Sharing

"Federation" is a fundamental concept in the GFIPM framework. The federation provides an agreed upon framework 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). 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.

Global Advisory Committee Recommendation

In the past several years, federated identity deployments have grown, matured, and expanded in depth and breadth across multiple industries. As the standards have matured, more organizations are becoming aware of the compelling business case for building federated communities. As such, a critical objective of the Global Justice Information Sharing Initiative Security Working Group (GSWG), which oversees the GFIPM project, is to ensure compatibility by collaborating with other key ongoing projects within Global as well as those that cross domain boundaries, such as NIEM, the Information Sharing Environment, and the Law Enforcement Information Sharing Program.

Federated identity is part of Global's vision for promoting secure nationwide information sharing. To this end, the Global Advisory Committee has made the following recommendations:

- Recognize GFIPM as the recommended approach for development of interoperable security functions for authentication and privilege management for information exchange among cross-domain justice information sharing systems, and
- Urge the members of the justice community to consider GFIPM as a potential building block to a layered security solution when authenticating users among cross-domain organizations.

Federation Benefits

User Convenience
Users can access multiple services using a common set of standardized security credentials, making it easier to sign on and access applications and to manage account information.

Interoperability
By specifying common security standards and framework, applications can adopt interoperable security specifications for authentication and authorization.

Cost Effective
GFIPM facilitates information sharing by using a standardized XML based credential that includes information about each users identity and privileges. This reduces the cost and complexity of identity administration required to access applications and vet users.

Privacy
GFIPM can reduce the propagation of personal identity information, reduce the redundant capture and storage of personal identity information, and depersonalize data exchanges across domains by use of privacy metadata.

Security
A federation model can improve the security of local identity information and data in applications by providing a standardized approach to online identities between agencies or applications.

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

For more information about Global efforts, including the GFIPM initiative and corresponding deliverables, please visit the Global Web site, **http://it.ojp.gov/GFIPM**.

BJA

This document was prepared under the leadership, guidance, and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.