BJA

Bureau of Justice Assistance
U.S. Department of Justice

Federated Identity and Privilege Management

Overview

Version 1.0

June 2012

Global
Information
Sharing Standard

Global Standards

Global's collection of normative standards has been versioned independently and assembled into a package of composable, interoperable solutions specifically supporting an information exchange. The package is known as the Global Standards Package (GSP). GSP solutions are generally technically focused but also may include associated guidelines and operating documents. GSP deliverables include artifacts associated with many of the Global product areas, including but not limited to:

- **Global Reference Architecture (GRA):** Offers guidance on the design, specification, and implementation of services (and related infrastructure) as part of a justice Service-Oriented Architecture (SOA).
- **Global Service Specification Packages (SSPs):** Reference services that serve as the means by which the information needs of a consumer are connected with the information capabilities of an information provider.
- **Global Federated Identity and Privilege Management (GFIPM):** Guidelines and standards for establishing, implementing, and governing federated identity management approaches.
- **Global Privacy Technology Framework:** A framework for automating access control (in particular, privacy) policy as part of information exchange.

For More Information

For more information on the GSP and the Global Standards Council (GSC)—the Global group responsible for developing, maintaining, and sustaining the same—please visit http://www.it.ojp.gov/gsc.

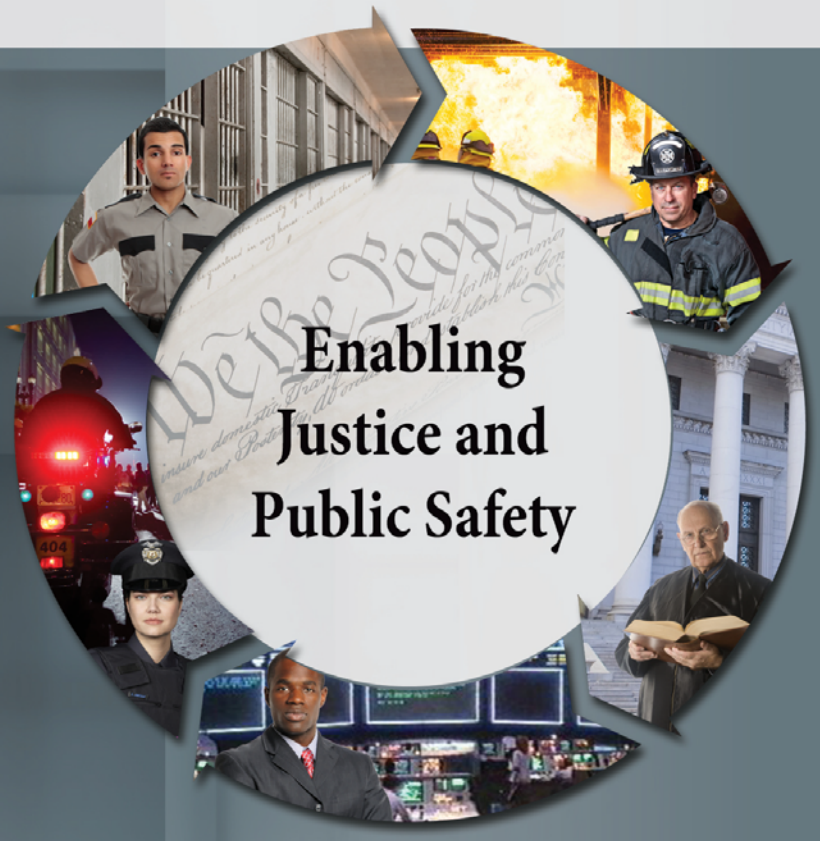

Table of Contents

Acknowledgements ii
1. Purpose of This Document 1
2. The Business Case for GFIPM 1
3. GFIPM Value Proposition 2
4. GFIPM Work Products 3
5. Federations Using GFIPM Work Products 5
    5.1 National Information Exchange Federation 5
    5.2 FBI CJIS Law Enforcement Online Enterprise Portal (LEO-EP) 6
    5.3 CONNECT Consortium 6
6. GFIPM Online Resources 7
7. GFIPM Points of Contact 8
Appendix A—Document History 9

Acknowledgements

The Global Federated Identity and Privilege Management (GFIPM) initiative was developed through a collaborative effort of the Global Justice Information Sharing Initiative (Global) membership; the U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA); and the U.S. Department of Homeland Security (DHS). The Global Standards Council (GSC) would like to express its appreciation to BJA and DHS for their continued guidance and support of this key initiative for secure and trusted information sharing among state, regional, local, tribal, and federal organizations. The GSC would also like to thank the GFIPM Delivery Team (DT), under the direction of Mr. John Ruegg, Los Angeles County Information Systems Advisory Body, for its dedication and commitment to developing this artifact and all other companion GFIPM artifacts. The creation of this document was guided by a volunteer effort of numerous contributors who participated by leveraging GFIPM standards within their state, regional, and federal organizations. Without their subject-matter expertise, ongoing experience, and feedback from lessons learned, the development of these guidelines would not have been possible.

1. Purpose of This Document

This document provides a high-level executive overview of basic Federated Identity and Privilege Management (FIPM) concepts and also introduces the Global Federated Identity and Privilege Management (GFIPM) concept of information sharing based on FIPM. It also discusses the GFIPM value proposition and provides additional resources for those interested in learning more. Its primary audience is executive management desiring to understand the GFIPM's value proposition within the justice information-sharing environment.

2. The Business Case for GFIPM

Ensuring that the right people (and only the right people) have access to the right information is a daunting task for the justice community, for several reasons.

1. Justice information users are represented at all levels of government and are provisioned in many systems. Because of fragmented funding for justice and public safety systems, local, state, tribal, and federal government agencies have invested (and reinvested) in security solutions that are not interoperable and fail to take into account the changing needs of the justice community.

2. Traditionally, the end user in the justice information exchange transaction has to manage the different credentials, passwords, tokens, and secondary factors on a system-by-system basis. This administrative effort—which includes juggling the access requests and expirations for different system credentials and passwords—limits the time law enforcement and others have available to prevent and solve crimes and engage in other substantive work.

3. No single data source for justice users exists. The creation of a central user store is not practical, cost-effective, or easy to maintain because of high personnel turnover in the justice arena and the distributed nature of justice and public safety systems. Also, many justice systems require the use of private networks, which are often costly and burdened with administrative processes and lag time. In turn, justice users are burdened with additional overhead for obtaining access to disparate systems.

To solve these problems and enable cost-effective, interjurisdiction information sharing within the justice community, the Global Justice Information Sharing Initiative[1] has developed GFIPM.

[1] See http://it.ojp.gov/global.

3. GFIPM Value Proposition

GFIPM Advantages at a Glance

- ***Improves privacy and security***
- ***Significant cost savings***
- ***Reduces administrative burden***
- ***Fewer user credentials per user***
- ***Distributed and highly scalable***
- ***Reduces complexity of systems***

The conceptual foundation of the GFIPM project is the idea of secure, interoperable, cost-effective federated identity and privilege management (FIPM). FIPM is an extension of the more common concept of federated identity management, which allows for the separation of user identities from the systems and applications in which those identities are used. Within a federation, *identity providers* (IDPs) manage user identities, and *service providers* (SPs) manage applications and other resources. Federated identity management provides valuable benefits for information sharing, including greater usability due to identity reuse, as well as improved privacy and security. The FIPM concept seeks to extend federated identity management by addressing the issue of authorization—or *privilege management*—within systems and applications in a federated environment. Each system or application in a federation typically has its own set of business requirements and access control policies. FIPM provides a cost-effective framework that allows these systems to be made available to federated users while still respecting their native requirements.

The GFIPM concept has been designed and implemented based on a well-grounded knowledge of the needs of real-world law enforcement information sharing systems. GFIPM development began with a bottom-up analysis of the usage and access requirements of several prototypical information sharing systems at the state, local, and tribal law enforcement levels. The process also included extensive community involvement and feedback, similar to the process used in the development of the Global Justice XML Data Model (GJXDM)[2] and the National Information Exchange Model (NIEM)[3]. The end result is that GFIPM not only meets the needs of a large class of its target systems (state and local law enforcement information sharing applications), but also has achieved a broad level of acceptance within its target community.

The GFIPM concept recognizes and seeks to facilitate interoperability and scalability at all critical levels of a federation, including governance, policy and business rules, technology standards, implementation and onboarding of participants, and ongoing operations such as change management and user support. At the governance level, GFIPM is consensus-based, with all participating agencies represented in a federation governance structure. The core governance philosophy is to provide enough structure to enable the establishment of basic trust agreements and memoranda of understanding between participants, but also to respect the desire of participating agencies to remain autonomous and retain full control over their information resources. At the levels of policy and technology standards, GFIPM specifies a small set of well-defined requirements to provide a baseline for identity

[2] See http://it.ojp.gov/jxdm/.
[3] See http://www.niem.gov/.

interoperability while still giving participants a high degree of latitude in terms of local policy and implementation. In addition to the basic interoperability requirements, GFIPM provides documentation, tools, and other facilities to encourage rapid, low-cost, and independent participant onboarding in parallel with each other. GFIPM includes very little centralized infrastructure and has no mandatory centralized services within the critical path of information sharing transactions, so there is no single point of failure or bottleneck in the federation from a technical standpoint. This philosophy also carries over into the area of day-to-day operations management, as GFIPM seeks to reuse and leverage existing operations and user support infrastructure as much as possible. In every dimension, GFIPM's goal is to facilitate an interoperable identity solution that maximizes scalability by minimizing centralization and embracing the distributed, disparate nature of a federation.

By using GFIPM technology, organizations can realize two major benefits. First, they can provide more data to their existing user bases. Second, they can make their existing data more widely available to users in other organizations. GFIPM provides the requisite technology and policy infrastructure to permit these information sharing transactions to occur in a manner that is secure and also compliant with laws and other policy-level requirements.

In addition to benefitting organizations, GFIPM can provide valuable benefits to end users in the form of reduced complexity, increased convenience, and increased privacy when they access data sources. These benefits to users are the result of GFIPM's single sign-on (SSO) technology, as well as a well-defined taxonomy of information attributes about users. Their use results in fewer security forms to fill out, fewer log-ins and other security credentials to manage, and tighter control over the personal information about users that is often required by data providers.

4. GFIPM Work Products

The Global Federated Identity and Privilege Management (GFIPM) program began in 2005 as the GFIPM Security Interoperability Demonstration Project.[4] This project was initiated by the Global Security Working Group (GSWG)[5] in response to various technical challenges highlighted in the National Criminal Intelligence Sharing Plan (NCISP).[6] Since the conclusion of the original GFIPM demonstration project in 2007, the GFIPM program has continued to evolve under the guidance of the Global Security Working Group and the GFIPM Delivery Team. Together, these groups have developed a full suite of GFIPM work products with the goal of providing a mature, well-vetted framework for cross-jurisdictional identity management in support of business-level information sharing. This product suite

[4] http://it.ojp.gov/documents/GFIPM_Security_Interoperability_Demonstration_Project_Report_2007-08-30.pdf

[5] The Global Security Working Group is one of several technical committees that exist as part of the Global Justice Information Sharing Initiative ("Global"). For more information, please see the U.S. Department of Justice's Office of Justice Programs (OJP) page for Global at http://it.ojp.gov/default.aspx?area=globalJustice.

[6] http://www.iir.com/global/products/NCISP_Plan.pdf

addresses a multiplicity of challenges, from governance and policy to technical interoperability to implementation support. These work products are available at http://gfipm.net/.

After more than five years of development, the GFIPM concept has matured into a full suite of solutions, from interagency governance and policy guidance to technical specifications and sample implementations. Figure 1 depicts the current set of GFIPM deliverables.

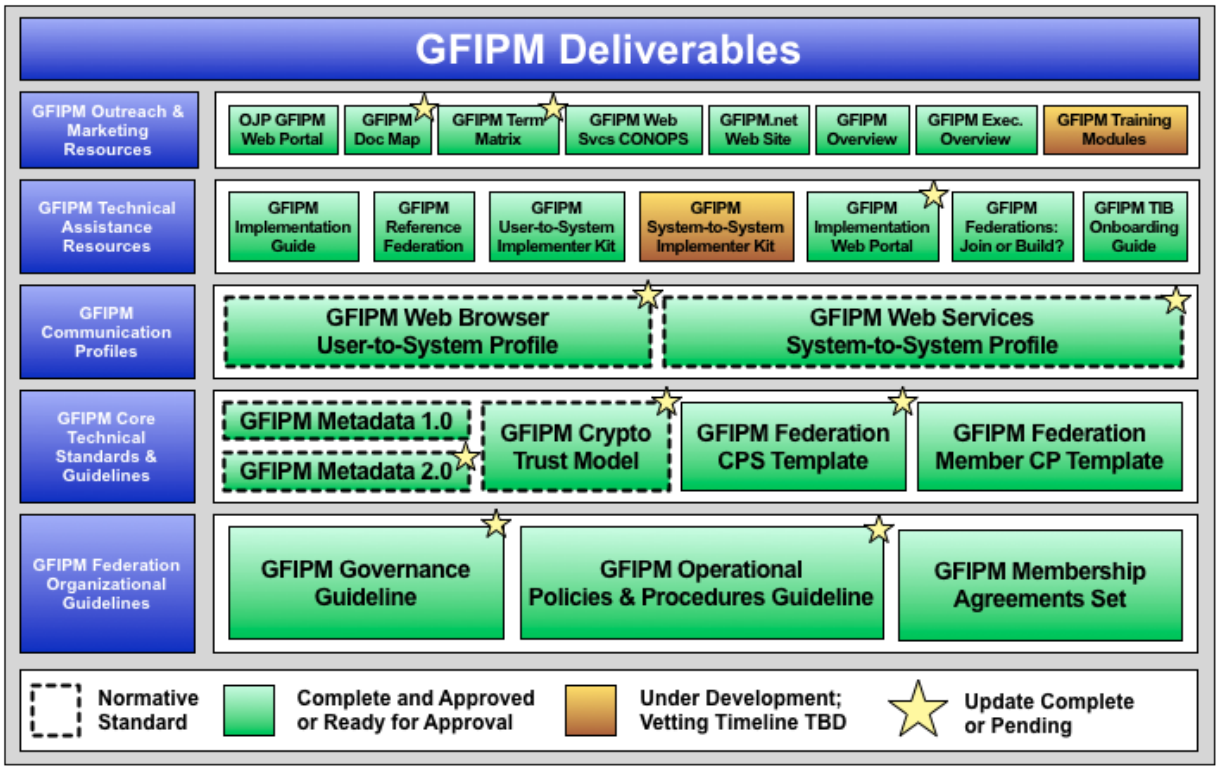

Figure 1: GFIPM Deliverables

GFIPM deliverables fall into five broad categories.

1. **GFIPM Federation Organizational Guidelines—**Interagency trust in an information sharing federation must be built on a well-defined federation governance structure, operational policies and procedures, and trusted membership documentation. Toward that objective, GFIPM provides a set of organizational guidelines for establishing and operating a federation. Without the mutual interagency trust created by these guidelines, it would not be possible to establish trust at the technical level of cryptographic standards and protocols.

2. **GFIPM Core Technical Standards and Guidelines—**Building on the interagency trust established through the GFIPM Federation Organizational Guidelines, GFIPM defines a set of core technical standards and guidelines

to enable interagency communications that are both cryptographically trusted and well-understood by all parties involved.

3. **GFIPM Communication Profiles—**Building on the GFIPM Core Technical Standards and Guidelines and the GFIPM Federation Organizational Guidelines, GFIPM defines a suite of normative communication profiles that allow specific types of transactions and other communications to occur between federation participants.

4. **GFIPM Technical Assistance Resources—**GFIPM provides a full suite of technical assistance resources to provide member organizations with technical assistance throughout the process of joining a GFIPM federation and implementing services within it.

5. **GFIPM Outreach and Marketing Resources—**GFIPM stakeholders have identified and developed a variety of resources that serve as tools for disseminating information about GFIPM to interested parties and educating the justice community about the value of the GFIPM concept.

5. Federations Using GFIPM Work Products

GFIPM work products are used within several federations, by multiple agencies at the federal, state, and local levels. The following subsections describe several federations that currently rely on GFIPM.

5.1 National Information Exchange Federation

The National Information Exchange Federation (NIEF) is a collection of agencies in the United States that have come together to share sensitive law enforcement information. It was created in 2008 as a direct outgrowth of the GFIPM program. NIEF maintains a close, symbiotic relationship with GFIPM, as it leverages existing GFIPM work products and also serves as a source of real-world feedback to drive the development of new GFIPM work products. Additional information about NIEF is available at https://nief.gfipm.net/.

Participating Agencies:

- Federal Bureau of Investigation (FBI)
- Regional Information Sharing Systems (RISS)
- U.S. Department of Homeland Security
- Criminal Information Sharing Alliance (CISA)
- Pennsylvania Justice Network (JNET)
- Los Angeles County Sheriff's Department

Point of Contact:

Mr. John Wandelt
Georgia Tech Research Institute
john.wandelt@gtri.gatech.edu

5.2 FBI CJIS Law Enforcement Online Enterprise Portal (LEO-EP)

The LEO-EP is a Federated Identity Management system developed by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division. The goal of the LEO-EP is to provide access to resources beneficial to the law enforcement, intelligence, and emergency management communities via its Federation Portal page. The LEO-EP was built based on the Global Federated Identity and Privilege Management (GFIPM) standard and uses a trusted broker concept to provide single sign-on access to the services on its Federation Portal. In addition to being a federation in its own right, the LEO-EP is connected to NIEF in an interfederation arrangement.

Participating Agencies:

- Federal Bureau of Investigation (FBI)
- Regional Information Sharing Systems (RISS)
- Chicago Police Department (CPD)
- Texas Department of Public Safety (TDPS)
- U.S. National Central Bureau of Interpol (USNCB)
- Law Enforcement Online (LEO)
- Department of Justice (DOJ)
- Director of National Intelligence (DNI)

Point of Contact:

Law Enforcement Online Operations Unit
FBI Criminal Justice Information Services Division
leoportal@leo.gov

5.3 CONNECT Consortium

The CONNECT Consortium is a group of U.S. states dedicated to working closely together to better solve specific information sharing challenges facing the criminal justice community. CONNECT provides a meaningful way for members to work together, pool limited resources, coordinate the creation and deployment of standards-based information sharing tools, and promote the sharing of information across jurisdictional borders to better solve and prevent crimes in their home communities. The Consortium consists of a structured way for each state's criminal justice information sharing organization to collaborate with its peers to solve specific information sharing challenges by leveraging the Global Justice

Information Sharing Initiative ("Global") standards. The first version developed by CONNECT provides a federated search of driver's license information from the four member states of Alabama, Kansas, Nebraska, and Wyoming. The CONNECT federated security model helped define the Global Federated Identity and Privilege Management (GFIPM) system-to-system profile. The current version of CONNECT has been expanded to implement both the system-to-system profile and the user-to-system profile of GFIPM. Single sign-on from the federation member states to the CONNECT Portal provides a federated query for searching driver's license data, court data, and corrections data, as well as N-DEx data. Utilizing the GFIPM standards, as well as many other Global standards, the CONNECT project is able to provide secure federated access to these resources to users within the CONNECT member states. Additional information about the CONNECT Consortium is available at http://www.connectconsortium.org/.

Participating Agencies:

- Alabama Criminal Justice Information Center
- Kansas Bureau of Investigation
- Nebraska Commission on Law Enforcement and Criminal Justice
- Wyoming Division of Criminal Investigations

Point of Contact:

Maury Mitchell
Director, Alabama Criminal Justice Information Center
maury.mitchell@alacop.gov

6. GFIPM Online Resources

The following GFIPM resources are available online.

1. **OJP GFIPM Portal—**http://it.ojp.gov/gfipm

   Operated by the U.S. Department of Justice (DOJ) Office of Justice Programming (OJP), the OJP GFIPM Portal contains basic background information about the GFIPM program, as well as all formal publications (technical specifications, non-normative policy guidance, and white papers) developed through the GFIPM program.

2. **GFIPM.net—**http://gfipm.net/

   GFIPM.net provides additional information about the GFIPM program and GFIPM concept.

3. **GFIPM Implementation Portal—**https://impl.gfipm.net/

   The GFIPM Implementation Portal contains a GFIPM Implementer Wiki with community-contributed articles about implementing information sharing solutions based on GFIPM standards. It also hosts a GFIPM Implementer Mailing List.

4. **GFIPM Reference Federation—**http://ref.gfipm.net/

   Operated by the Georgia Tech Research Institute (GTRI), the GFIPM Reference Federation is a collection of online systems that serve as an interoperability test bed for the GFIPM implementer community.

7. GFIPM Points of Contact

Global Standards Council

Thomas M. Clarke, Ph.D.
National Center for State Courts
tclarke@ncsc.org

GFIPM Delivery Team

Mr. John Ruegg
Los Angeles County Information Systems Advisory Body
jruegg@isab.lacounty.gov

Mr. James Dyche
Pennsylvania Justice Network
jdyche@state.pa.us

Appendix A—Document History

Date	Version	Editor	Change
04/12/2012	1.0	Global Standards Council (GSC), Global Federated Identity and Privilege Management Delivery Team (GFIPM DT)	Approved

About Global

www.it.ojp.gov/global

The 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 on Global and its products, including those referenced in this document, call (850) 385-0600 or visit http://www.it.ojp.gov/GIST.

About GSC

www.it.ojp.gov/gsc

In accordance with the founding principle of Global, the Global Standards Council (GSC) directly supports the broadscale exchange of pertinent justice and public safety information by promoting standards-based electronic information exchanges for the justice community as a whole. Specifically, the GSC develops, maintains, and sustains the standards—including this particular standard—associated with these aforementioned information exchanges. To further foster community participation and reuse, the GSC also receives, evaluates, and recommends to Global for adoption proposed standards submitted by Global consumers and stakeholders. In turn, the GSC employs an enterprise architecture approach for developing and maintaining the cohesive body of Global standards as one Global Standards Package (GSP), which can be accessed at http://www.it.ojp.gov/gsp.

http://www.it.ojp.gov/gsp

This project was supported by Grant No. 2009-DB-BX-K105 awarded by the Bureau of Justice Assistance, Office of Justice Programs, 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 publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.