

**Prescription Monitoring Program Information Exchange**

**( PMIX )**

**Service Description   
Version 1.1  
  
July 2013**

**Sponsored by:**



**TABLE OF CONTENTS**

[1. Introduction 5](#_Toc334166235)

[2. Service Overview 8](#_Toc334166236)

[3. Document Purpose 9](#_Toc334166237)

[4. Service Scope 9](#_Toc334166238)

[5. Capabilities 9](#_Toc334166239)

[6. Real-World Effects 9](#_Toc334166240)

[7. Summary 9](#_Toc334166241)

[8. Description 10](#_Toc334166242)

[9. Security Classification 10](#_Toc334166243)

[10. Service Specification Package Version 10](#_Toc334166244)

[11. Business Scenario 11](#_Toc334166245)

[12. Primary Flow 11](#_Toc334166246)

[13. Alternative Flow 11](#_Toc334166247)

[14. Service Interoperability Requirements 12](#_Toc334166248)

[15. Service Assumptions 15](#_Toc334166249)

[16. Service Dependencies 15](#_Toc334166250)

[18. Execution Context 15](#_Toc334166251)

[19. Policies and Contracts 15](#_Toc334166252)

[20. Service Security 15](#_Toc334166253)

[21. Service Privacy 16](#_Toc334166254)

[22. Additional Requirements 16](#_Toc334166255)

[23. Service Model 17](#_Toc334166256)

[24. Information Model 17](#_Toc334166257)

[25. Data Inputs 18](#_Toc334166258)

[26. Data Outputs 19](#_Toc334166259)

[27. Data Provenance 19](#_Toc334166260)

[28. Behavior Model 20](#_Toc334166261)

[29. Action Model 21](#_Toc334166262)

[30. Process Model 22](#_Toc334166263)

[31. Appendix A — References 25](#_Toc334166264)

[32. Appendix B — Acronyms 25](#_Toc334166265)

[34. Appendix C — Document History 26](#_Toc334166266)

**TABLE OF FIGURES**

[Figure 1: State PMP Overview 6](#_Toc361384828)

[Figure 2: PMIX Post Office Analogy 8](#_Toc361384829)

[Figure 3: PMIX System Overview 10](#_Toc361384830)

[Figure 4: Primary Flow: Trusted Service Interface 11](#_Toc361384831)

[Figure 5: Alternative Flow: Hub Overview 12](#_Toc361384832)

[Figure 6: Alternative Flow: Secure Hub Connection 13](#_Toc361384833)

[Figure 7: Using the GRA and NIEM 14](#_Toc361384834)

[Figure 8: PMIX Flow Diagram 17](#_Toc361384835)

[Figure 9: Behavior Model of PMIX Exchanges 20](#_Toc361384836)

[Figure 10: PMIX Service Business Process Modeling Notation 23](#_Toc361384837)

[Figure 11: PMIX Sequence Diagram 24](#_Toc361384838)

**TABLES**

[Table 1: Service Interaction Requirements 14](#_Toc361384839)

[Table 2: Provide Prescription Drug History 21](#_Toc361384840)

**Acknowledgements**

This document was produced as part of the BJA-sponsored IJIS Institute project in support of the Prescription Monitoring Program Information Exchange. Major portions of this document were derived directly from the earlier PMIX Project documents and significant contributions were made by the following organizations:

Office of Justice Programs Bureau of Justice Assistance

Prescription Drug Monitoring Program Training and Technical Assistance Center (PDMP TTAC)

IJIS Institute Prescription Monitoring Program (PMP) Committee

Open Networks, Inc.

This project was supported by Grant No. 2009-PM-BX-K044 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

# Introduction

**Overview**

This document is a Service Description of the Prescription Monitoring Program Information Exchange (PMIX) Service.

In the context of a service-oriented architecture and, more specifically, the Global Reference Architecture (GRA), a service is the means by which one partner gains access to one or more capabilities offered by another partner. Capabilities generate real-world effects that can be as simple as sharing information or can involve performing a function or changing the state of some other processes. Organizations have numerous capabilities and partner organizations. There are significant benefits for these organizations to have access to each other's capabilities. Each state has its own governance, business needs, applications, hardware, and networks. Achieving interoperability within this environment, and with external partner organizations, calls for alignment of business and technical requirements and capabilities by specifying them consistently across organizational boundaries. The GRA was developed to facilitate interoperability and to assist in meeting other key requirements in an information sharing environment. In order to achieve this goal, there is a strong need to define a consistent approach to identifying and describing services and their interactions that can be implemented in many different technical environments, across multiple government lines of business, at all levels of government and with other partner organizations.

The GRA defines a service interface as "the means for interacting with a service.” It includes the specific protocols, commands, and information exchange by which actions are initiated on the service. A service interface is what a system designer or implementer (programmer) uses to design or build executable software that interacts with the service. That is, the service interface represents the “how” of the interaction. Since the service interface is the physical manifestation of the service, best practices call for a service interface which can be described in an open-standard format (that is, a format which could be automatically processed by a computer).

A Service Specification is a formal document describing the capabilities made available through the service; the service model that defines the semantics of the service by representing its behavioral model, information model, and interactions; the policies that constrain the use of the service, and the service interface that provides a means of interaction with the service. A Service Specification is analogous to the software documentation of an Application Programming Interface (API). It provides stakeholders with an understanding of the structure of the service and the applicability to its implementation interface rules. It gives the service consumers the information necessary for consuming a particular service, and service providers the information necessary for implementing the service in a consistent and interoperable way.

The main components of a Service Specification are the Service Description and one or more Service Interface Descriptions. A Service Description describes all aspects of a service that are not directly tied to the physical implementation or service interface. A Service Interface Description is a description of the physical implementation or service interface used in a specific implementation of a service.

**Background**

All states have laws and regulations that govern the distribution and handling of controlled substances and other pharmaceuticals. Diversion of, and addiction to, such substances are generally recognized as serious problems throughout the country. States have found that prescription monitoring programs (PMPs), which collect prescription-controlled-substance dispensing data from pharmacies and other authorized dispensers, can be effective tools for identifying and preventing these problems. (In the remainder of this document, the term “prescription” will refer to controlled-substance prescriptions.) These data are then reviewed and analyzed for medical, educational, public health and investigative purposes.

The figure below shows the key requesting stakeholders for PMP data.

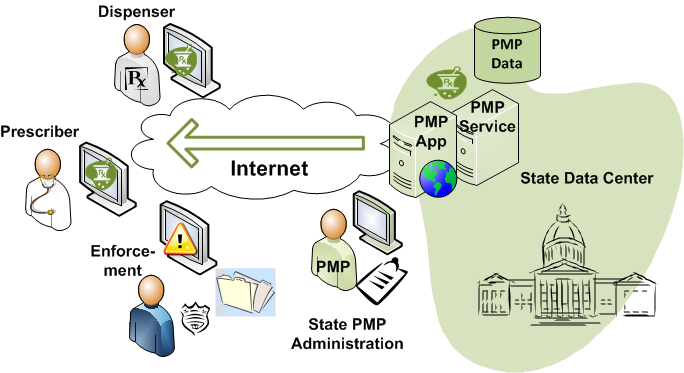


Figure : State PMP Overview

States implementing new PMP systems may find it desirable to conform closely to the PMIX Service Specification in order to help ensure consistency with potential interstate exchange partners in the future.

**PMIX Architecture**

The Prescription Drug Monitoring Program Training and Technical Assistance Center (PDMP TTAC) and other stakeholders have undertaken the development of a consensus, national PMIX Architecture to enable the interstate sharing of PMP data. The use of open, consensus standards promotes interoperability. The National Information Exchange Model (NIEM) and the Global Reference Architecture (GRA) are foundational standards of the PMIX Architecture.

The PMIX architecture requires 1) Compliance with Global Reference Architecture Reliable Secure Web Services Profile, 2) Common NIEM exchange data and metadata, 3) Hub connections (and hub to hub capability) and 4) End-to-end security (including encryption key management).

The architecture will result in a shared infrastructure to support certificate/key management capabilities and basic directory services, specifically the PMIX Directory Service. The PMIX Directory, also known as the PMIX LDAP Server, provided for X.509 certificate management and public key exchange as well as PMP contact and service requirement information.

The PMIX Service Specification Package was developed consistent with the GRA Service Specification Guideline (SSG). The GRA SSG provides a method for describing and documenting the scope of the service, including the functional and technical requirements of a service. The SSG documentation includes sufficient detail to allow service providers to develop interoperable service implementations by referring to the same specification.

For additional information, refer to the following: <http://it.ojp.gov/docdownloader.aspx?ddid=1215>

**Guiding Principles**

Several core principles have been utilized to guide the development of this document and other PMIX artifacts:

* **Distributed data sources:** assumes distributed, rather than centralized, information sources.
* **Maintenance of state-level controls:** PMIX implementation will not impact or modify a state’s control over the operation of the PMP and authorization to access prescription data.
* **End-to-end security:** Mechanisms must be utilized to assure the security of PMIX in-transit data between the sending and receiving endpoints.
* **Information traceability:** PMIX data flows will leave an audit trail, not to include protected health information (PHI), to enable reporting on demand to PMP administrators.
* **Standards-based information sharing:** PMIX standards will leverage open industry standards such as Extensible Markup Language (XML) and the National Information Exchange Model (NIEM) for encoding data to ensure maximal interoperability between future exchange partners.

# Service Overview

The figure below shows the PMIX service through a post office analogy. The PMIX service corresponds to the post box and the broader process of posting a letter.

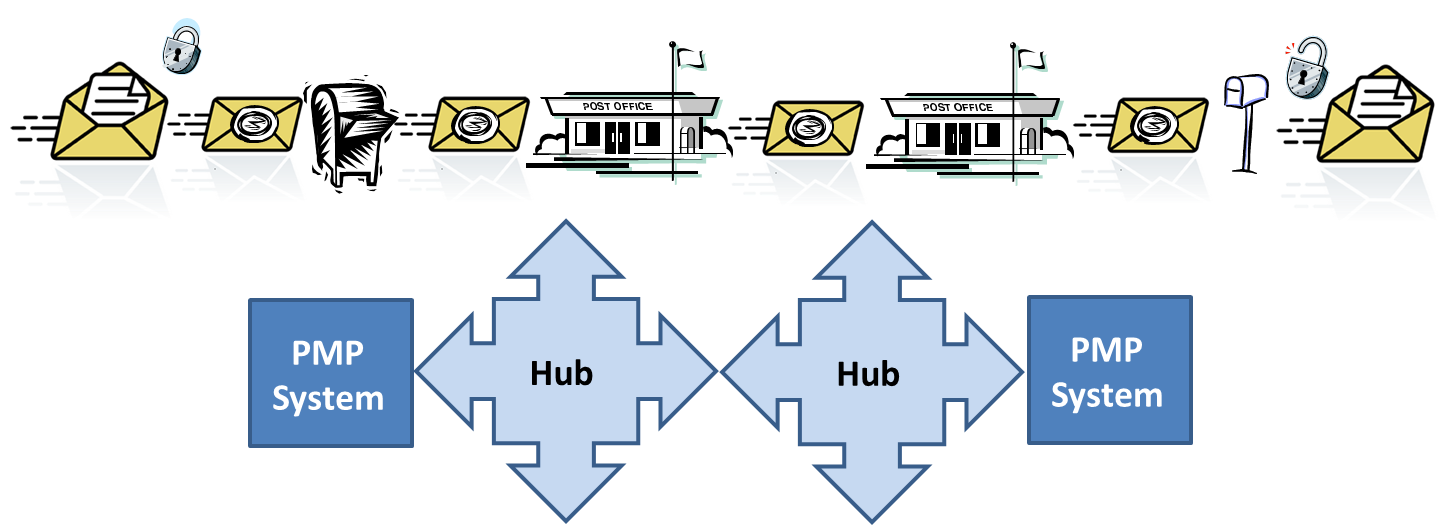


Figure : PMIX Post Office Analogy

# Document Purpose

The purpose of this service is to support the establishment and operation of automated Prescription Monitoring Information Exchange (PMIX) capabilities between states’ Prescription Monitoring Program (PMP) services. This document describes the basic functions comprising the information sharing process. This service specification has been created to assist PMP system stakeholders who wish to receive prescribing and dispensing data across state boundaries.

# Service Scope

The overall scope of the PMIX program includes electronic system-to-system exchange of dispensed prescription drug history information between states in support of a variety of usage scenarios. The scope assumed for this service is that of an end user (e.g., a prescriber) seeking the dispensed prescription drug history of a single patient. Enhancements such as prescriber or pharmacy requests, or requests for data from multiple patients, were considered to be beyond the scope of the current service. The components of the PMIX infrastructure described herein could very well be utilized to support these enhancements in the future.

# Capabilities

The PMIX service provides the capability to retrieve dispensed prescription drug history for a single person from one state to another.

# Real-World Effects

* End users (e.g., prescribers) will, via a requesting state’s PMP system, receive a prescription drug history, if any is available, in order to identify potential abuse or diversion in making their decisions (e.g., whether to prescribe).
* All PMIX transactions will be logged to allow for any necessary accounting.

# Summary

The PMIX service provides an individual’s prescription drug history from participating states given specific search criteria.

# Description

The PMIX service provides state PMP systems with the capability to retrieve interstate prescription drug history and display it to their in-state end users (requestor) to assist in the identification of potential abuse and diversion. The service can provide the requested drug history as a direct response to a request containing person identifiers. Multiple requests can be issued in sequence by a state PMP system to provide prescription drug histories from as many states as needed.

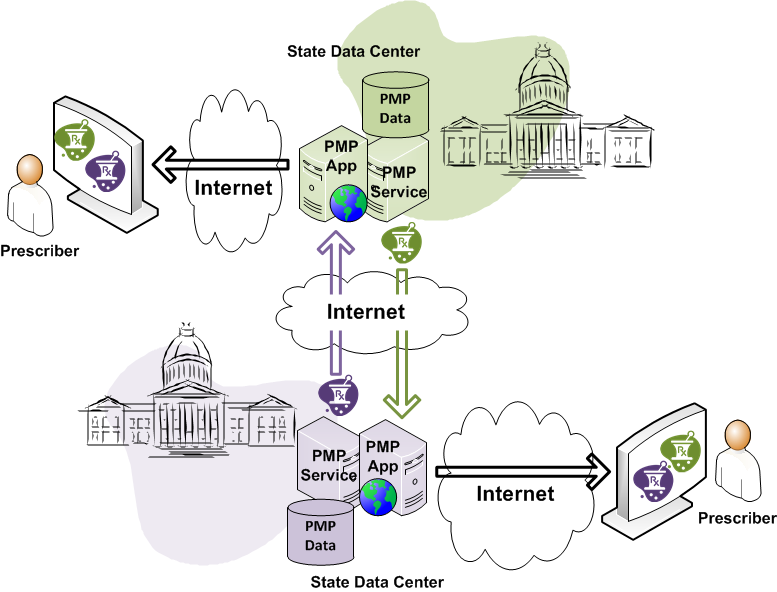


Figure : PMIX System Overview

# Security Classification

The patient health information exchanged by this service is assumed to be subject to strict privacy requirements (i.e., at least a strong as those required by the federal Health Insurance Portability and Accountability Act of 1996) in every participating jurisdiction.

# Service Specification Package Version

This specification is built based on version 1.0 of the GRA Service Specification Package.

# Business Scenario

Prescriptions for controlled substances are often dispensed in a different state from that of the patient’s residence or physician’s office. Many people have occasion to travel regularly to other states for work or leisure.

Prescriptions can be obtained fraudulently by individuals who have discovered that they can elude detection by crossing state borders to “shop” for unsuspecting prescribers or dispensers. These doctor shoppers often travel to multiple states to increase the quantities of controlled substances that can be diverted.

Since prescription information is reported to the PMP of the state in which the prescription is dispensed, authorized users of PMP systems in other states will have no access to this information without interstate data sharing.

Practitioners and law enforcement agencies are increasingly concerned about cross-border diversion of prescription controlled substances as the abuse involving these drugs continues to escalate. The President’s National Drug Control Strategy has also identified this as one of the nation’s highest priorities.

# Primary Flow

The primary flow is the sending of a PMIX request from the requesting state, followed immediately by a synchronous PMIX response. The request is routed through one or more hubs which act as intermediaries. A single Web Service is used to carry out all the sending and receiving of messages between the state PMP systems and the PMIX Hub. The diagram below depicts the flow within this web service.



Figure : Primary Flow: Trusted Service Interface

The Trusted Service Interface is described in the PMIX\_SIDD\_WS\_Trusted\_v\_1.1.0 artifact.

# Alternative Flow

Similar to the primary flow, a PMIX request/response message transaction set can be routed from the requesting state through various intermediate hubs to the disclosing state. The PMIX intermediary hub-to-hub interaction utilizes standards-based web services to facilitate communication with disparate endpoint systems. The web service interfaces are protected by a combination of secure socket layer, which provides transport level encryption and service authentication and message level encryption, which ensure message privacy and integrity.

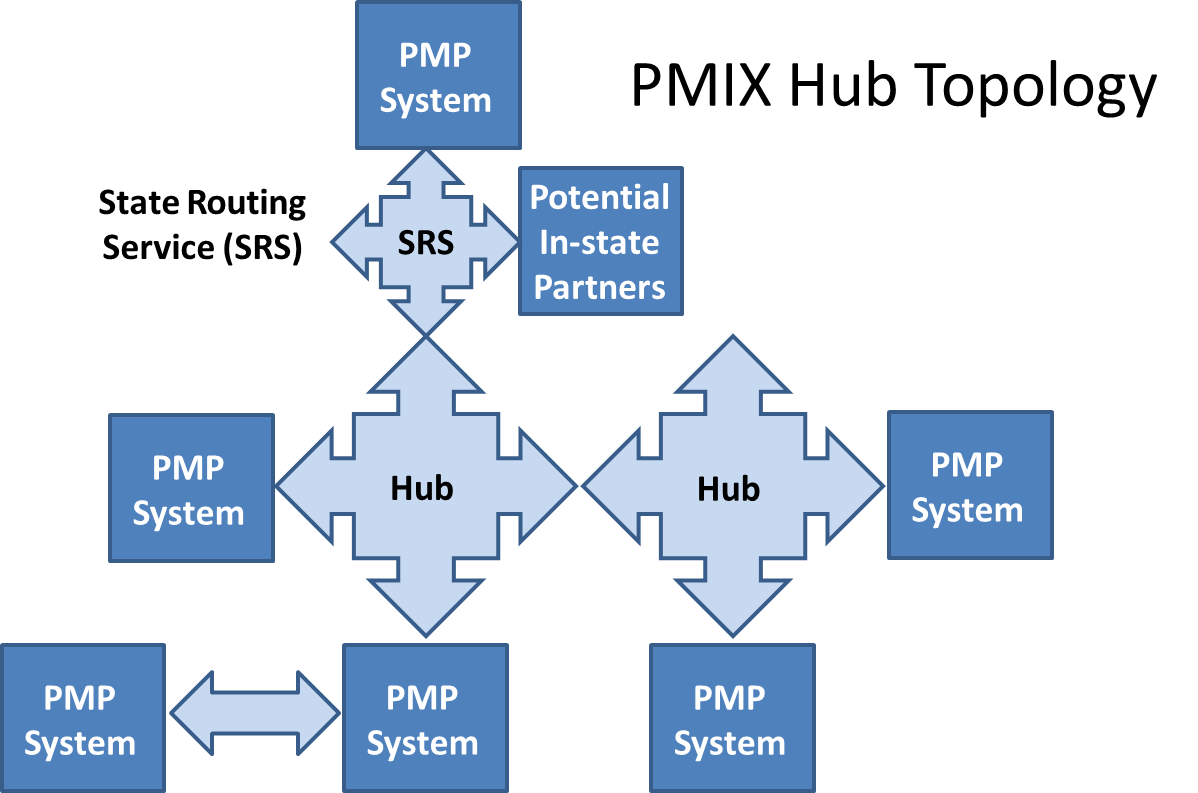


Figure : Alternative Flow: Hub Overview

A hub provides secure routing services to direct information exchanges as required. The hub approach limits the need to provide multiple State network security configurations. In addition, hubs can exchange data through other hubs. Hubs, referred to more technically in the GRA as intermediaries, support the same standards for transport, routing, addressing and security. It is also possible to implement PMIX compliant connections without the use of any hub, although the GRA recommends the use of intermediaries as outlined in the GRA Execution Context Guidelines document.

The PMIX Architecture requires any hub-to-hub connections to be compliant with the Global Reference Architecture Reliable Secure Web Services Profile, to use common NIEM exchange data and metadata and ensure end-to-end security. In particular, a hub must be able to route messages using the WS-Addressing standard and must be able to forward encrypted content without intervention using WS-Security.



Figure : Alternative Flow: Secure Hub Connection

In addition to the security provided by WS-Security message level encryption, the secure service interface also provides two optional “double” encryption options; open standard XML Encryption and proprietary PMPi Encryption.

The Secure Service Interface is described in the PMIX\_SIDD\_WS\_Secure\_v\_1.1.0 artifact.

# Service Interoperability Requirements

In order to ensure PMP interoperability, the PMIX Architecture will provide the framework necessary to make PMIX information exchanges interoperable while reducing the risk and cost of implementation. The foundational data standard is the National Information Exchange Model and the foundational exchange/interaction standard is the Global Reference Architecture Reliable Secure Web Services Profile.

The GRA was developed to facilitate interoperability and to assist in meeting other key requirements in an information sharing environment. In order to achieve this goal, there is a strong need to define a consistent approach to identifying and describing services and their interactions that can be implemented in many different technical environments, across multiple government lines of business, at all levels of government and with other partner organizations.

The GRA Reliable Secure Web Services Service Interaction Profile (RS WS-SIP) specifies standards from the W3C and OASIS, including a standard service interface and WS-Security (plus transport security). The PMIX Architecture specifies the use of the GRA profile[[1]](#footnote-1), which defines the set of GRA non-functional requirements and specifies the standards for conformance.



Figure : Using the GRA and NIEM

The table below outlines the service interaction requirements and the associated standards that are being used to support this service interface.

|  |  |
| --- | --- |
| GRA Service Requirement | PMIX Architecture Standard |
| Simple Message | * XML (NIEM) * SOAP |
| Message Exchange Pattern | * Request-Response |
| Interface Description | * Web Service Description Language (WSDL) 1.1 |
| Message Confidentiality | * Transport Layer Security * OASIS Security Profile 1.1  w/XML Encryption, XML Signature |
| Message Addressing | * WS-Addressing |
| Service Consumer Authorization | * Specific role based “rules” |
| Message Reliability | * Implicitly provide by response |

Table 1: Service Interaction Requirements

# Service Assumptions

* All message headers (exchange information) are stored in a log file for auditing purposes. No private patient or drug history report data is logged (it is not in the clear anyway). All that is logged is the occurrence of a request and response.
* All messages exchanged require an acknowledgement or response.

# Service Dependencies

The PMIX services operate using a transport and message level security established using centralized key/certificate management (refer to the PMIX Execution Context Document).

# Execution Context

The PMIX Execution Context Document provides greater detail on the PMIX exchange model, centralized coordination and management of PMIX security. Please refer to the PMIX Execution Context located in the .\various artifacts\execution context\ directory of the Service Specification Package (SSP).

# Policies and Contracts

The presumption made throughout this document is that individual state legislation and particular state-to-state agreement(s) will address any issues of privacy and security beyond the transport and message-level security described below.

# Service Security

Message exchanges between states are protected using message level security from state to state. Secure conversations can be established between states through the hubs with the request/response contents (message body) encrypted.

Independent transport security sessions using Secure HTTP are established between the requesting state and the hub and between the hub and the receiving state. Transport security is being used to ensure that the message headers are encrypted during transfers but visible to the hub(s) for routing and logging purposes.

PMIX message metadata is included in the unencrypted (but signed) message header to permit logging.

# Service Privacy

PMIX requests and responses routed through a hub are securely transmitted using message level security and federally approved data encryption standards. This encryption of the Protected Health Information (PHI) will effectively prevent this data from being visible to the PMIX Hub or from any other intermediate network node. The message level encryption occurs between partner states, and as a result, the implementation of the encryption service is a responsibility of the partner states.

The details of the transaction encryption service are detailed below.

* **Routing information is separate from personal information**—Transactions are structured to separate sensitive PHI from basic transaction routing information such as destination state or request type. This separation allows the sensitive data to be encrypted for the destination state, while allowing the hub to retain visibility into the non-sensitive routing data. Since the sensitive information is encrypted only for the receiving state and for no other entity, the hub is unable to view this part of the transaction.
* **Encryption is used to secure the sensitive portion of the transaction**—The asymmetric encryption is accomplished by using Public Key Infrastructure (PKI) technology for asymmetric encryption key management. In this scheme, each participating state is responsible for procuring a PKI digital certificate (conforming to the X.509 v3 standard) and a corresponding pair of private and public keys.

# Additional Requirements

* Header information (not private, protected payload data) for all PMIX requests and responses must be recorded.

# Service Model

The service model flow is shown in the diagram below.

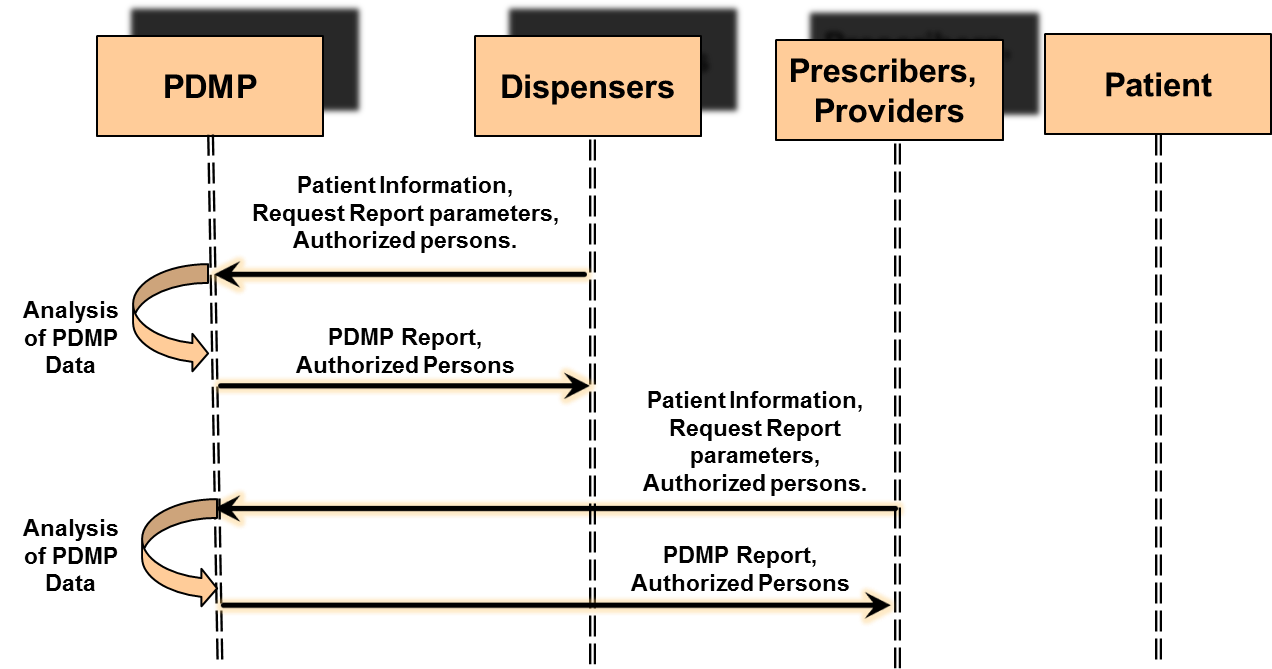


Figure : PMIX Flow Diagram

# Information Model

The information exchanged by the service consists of information regarding the patient and the patient’s prescription drug history. The PMIX Information Exchange Package Documentation (IEPD) provides the information model of this service.

As states desire to participate in PMIX exchanges, they can choose to use any of the elements located within the IEPD schemas that are suited to their technical and legal requirements. However, while there are no constraints on what any particular pair of states may choose to negotiate in their exchange, it is hoped that common exchange definitions will make it easier for states to enter into exchange transactions and increase reuse among the national community of state PMPs.

Authoritative references to the XML elements and instances suggested below can be found by accessing the enclosed version of the PMIX IEPD.

# Data Inputs

An instance of the PMIX\_NIEM\_2.0\_Request\_Schema should be used by a requesting state to formulate a request to be forwarded to a disclosing state.

The particular recommendations below were based upon an agreement between the Ohio OARRS and Kentucky KASPER PMP programs. After each element is a description of whether each state, in its role as disclosing state, requires the element, considers it optional (in which case it could be used to narrow the results of a database query), or will ignore it if present. Items in Camel-case (contiguous, capitalized words) represent schema element names.

These items are offered here only as an example. Please consult the IEPD (included with the SSP), along with the MOU or other agreement between exchange partners, for an authoritative listing of required and optional data elements for any particular exchange.

* Dispensed prescription date range (KY required, OH: required)
  + RequestPrescriptionDateRange (complex)
    - RequestPrescriptionDateRangeBegin
      * “2008-11-01”
    - RequestPrescriptionDateRangeEnd
      * “2010-11-30”
* Patient birthdate, name and other identifiers, and contact info
  + RequestPatient (complex)
    - PersonBirthDate (complex)
      * Date (KY: required, OH: required)
        + “1967-08-13”
    - PersonName (complex)
      * PersonGivenName (KY: required, OH: required)
        + “User2\_F”
      * PersonMiddleName (KY: optional, OH: optional)
        + “User3\_M”
      * PersonSurName (KY: required, OH: required)
        + “User1\_L”
    - PersonSSNIdentification (complex)
      * IdentificationID (KY: optional, OH: ignored)
        + “222222222”
    - PersonPrimaryContactInformation (complex)
      * ContactTelephoneNumber (complex)
        + FullTelephoneNumber (complex)

TelephoneNumberFullID (KY: ignored, OH: optional)

“123-123-1233”

* + - * ContactMailingAddress (complex)
        + Structured Address (complex)

LocationStreet (complex)

StreetFullText (KY: required, OH: optional)

“Test Street 2”

LocationCityName (KY: required, OH: ignored)

“Columbus”

LocationStateUSPostalServiceCode (KY: required, OH: ignored)

“OH”

LocationPostalCode (5-digit, KY & OH: required)

“44444”

* + - PersonStateIssuedIdentifier (complex)
      * IdentificationID (KY: optional, OH: ignored)
        + “RR123456”
      * IdentificationJurisdictionText (KY: optional, OH: ignored)
        + “OH”

# Data Outputs

It is anticipated that elements contained in a response will be utilized for display to the user who initiated the request. Hence it is not a as critical to gain prior agreement between the exchange partners on what elements would be required, optional, or ignored (as was the case above for the request elements being used to feed the disclosing state database queries).

The recommendation with regard to request responses, then, is for each state to fetch the sample instance (in the file “PMIX\_NIEM\_2.0\_Request\_Response\_Instance.xml”) of the PMIX request response schema in the enclosed PMIX IEPD.

# Data Provenance

The data exchanged by this service originates at the participating partner PMP systems. The provenance of the data will be restricted to the data available from the specific participating state PMP system.

# Behavior Model

The diagram provided below further describes the behavior model of the service and how the service actions interact with each other.



Figure 9: Behavior Model of PMIX Exchanges

Each state is assumed to have a State Routing Service (SRS) that performs the same exchange services within the state as the hub between states. The SRS interacts through an Application Program Interface (API) that is incorporated into the PMP systems.

# Action Model

The tables below contain information about each individual service action.

|  |  |  |
| --- | --- | --- |
| Action Name | | Provide Prescription Drug History |
| Action Purpose | | |
| This action is used to by participating PMP systems to provide prescription drug history. | | |
| Action Inputs | Action Outputs | |
| RequestType   * Disclosing state id * Request id * Request metadata role * Patient Drug History Request (see IEPD) | ResponseType   * Response type (header) * Patient Drug History Report(s) if any (see IEPD) | |
| Action Provenance | | |
| The provenance of this action is the same as the provenance of the service.  The Action includes addressing information (disclosing state id). | | |

Table 2: Provide Prescription Drug History

# Process Model

The Service delivers the prescription history as the initial response to the request if available. Only one patient request is associated with any one message.

The hubs act as a Simple Object Access Protocol (SOAP) intermediary rather than a web service proxy. A SOAP intermediary preserves the end-to-end web service relationship between states.

The Figure below shows a Business Process Modeling Notation (BPMN) diagram for the PMIX interstate exchange.



Figure : PMIX Service Business Process Modeling Notation

The sequence diagram provided below further describes the behavior model of the service and how the service actions interact with each other.



Figure 11: PMIX Sequence Diagram

# Appendix A — References

* PMIX Trusted Service Interface Description v1.1.0, July 2013
* PMIX Secure Service Interface Description v1.1.0, July 2013
* PMIX Execution Context Document v1.0, April 2012
* PMIX NIEM 2.0 Information Exchange Package Documentation
* ijis\_pmix\_III\_niem\_2\_0\_iepd\_v0\_20\_20101207
* GRA Web Services Service Interaction Profile v1.3
* GRA Reliable Secure Web Services Service Interaction Profile v1.2

# Appendix B — Acronyms

API Application Programming Interface

GRA Global Justice Reference Architecture

NIEM National Information Exchange Model

PMIX Prescription Drug Monitoring Information Exchange

SOAP Simple Object Access Protocol

SRS State Routing Service

W3C World Wide Web Consortium

WCF Windows Communication Framework

WS-I Web Services Interoperability

WSDL  Web Services Description Language

XML [eXtensible Markup Language](http://en.wikipedia.org/wiki/XML)

# Appendix C — Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Change |
| 1/2011 | 1.0 Rev B | Bob Slaski, Open Networks | For PMP Committee review |
| 3/2011 | 0.1 | Scott Serich, IJIS Institute | Incorporating PMP Committee feedback |
| 5/2011 | 0.2 | Scott Serich, IJIS Institute | Incorporating additional PMP Committee feedback |
| 6/2011 | 0.3 | Scott Serich, IJIS Institute | Incorporating final PMP Committee feedback |
| 7/2011 | 1.0 DRAFT | Scott Serich, IJIS Institute | Technical editing pass |
| 6/2012 | 1.0.1 | Bob Slaski, Open Networks | Updated to SSG 1.0 |
| 9/2012 | 1.0.2 | Bob Slaski, Open Networks | Updated to reflect community comments |
| 7/2013 | 1.1.0 | Todd Seymour,  Open Networks | Revisions to reflect consolidation of State-to-Hub and Hub-to-Hub specifications. |

1. GRA Reliable Secure Web Services Service Interaction Profile V1.1, <http://it.ojp.gov/docdownloader.aspx?ddid=1134> [↑](#footnote-ref-1)