PDMP TTAC

Prescription Drug Monitoring Program Training and Technical Assistance Center

Prescription Monitoring Program Information Exchange (PMIX) Architecture

Version 1.0

April 2012

Developed in conjunction with:

Alliance of States with Prescription Monitoring Programs

TABLE OF CONTENTS

TABLE OF FIGURES

TABLES

ACKNOWLEDGEMENTS

The Prescription Monitoring Program Information Exchange (PMIX) Architecture is the product of the Alliance of States with Prescription Monitoring Programs Technical Committee under the leadership of Don Vogt, Oklahoma Bureau of Narcotics.

The Alliance Technical Committee members (and invited stakeholders) that participated in the development of the PMIX Architecture document are named below:

- Don Vogt, Alliance of States with Prescription Monitoring Programs, Oklahoma Bureau of Narcotics (Chair)
- Jim Giglio, PDMP Training and Technical Assistance Center, Brandeis University
- Chris Baumgartner, Alliance of States with Prescription Monitoring Programs
- Joe Casar, Kentucky Cabinet for Health and Family Services
- Chad Garner, Ohio State Board of Pharmacy
- Tom Beard, Health Information Designs
- Frank Xavier, Optimum Technology
- Robert Cowan, National Association of Boards of Pharmacy
- Todd Tincher, Appriss
- Jason Heath, Appriss
- Chris Traver, Bureau of Justice Assistance
- Jim Douglas, SEARCH
- Bob Slaski, Open Networks/IJIS Institute

This project was supported 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.

DOCUMENT HISTORY

Date	Version	Editor(s)	Change
11/21/2011	1.0	Bob Slaski	Initial release
5/1/2012	1.0	Bob Slaski	Incorporated Alliance membership review

EXECUTIVE SUMMARY

The Prescription [Drug] Monitoring Program Information Exchange (PMIX) Architecture and associated information technology standards provide the framework to make Prescription Monitoring Program (PMP) interoperability possible and to reduce the risk and cost of implementation.

The PMIX Architecture has four key components:

- Reliable Secure Global Reference Architecture (GRA) Web Services Profile
- National Information Exchange Model (NIEM) data and metadata
- Hub connections (hub to hub capability)
- End-to-end security using Public Key Infrastructure (PKI)

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 PMIX Architecture includes the capability for exchange intermediaries or "hubs" at the state (or territory or district) and national levels as well as hub-to-hub exchanges. Hubs reduce the complexity associated with point-to-point connections to simplify adoption and sustainment.

Paramount to the PMIX Architecture is the complete confidentiality of private information while in transit. The architecture provides for both transport and message level encryption based on an industry standard Public Key Infrastructure (PKI) to maintain the highest level of privacy. The architecture includes full end-to-end message security.

The PMIX Architecture is an overarching framework for standards-based, secure, interoperable, sustainable PMP information exchange.

1 Document Purpose

The PMIX Architecture document provides a cohesive, overarching set of principles that serve as the foundation for:

- PMP systems to exchange prescription history reports with other PMP systems and other authorized organizations using appropriate data and information exchange standards
- Definition of high-level security requirements for information exchanges
- PMP interoperability execution infrastructure to provide security related functions and exchange-facilitating intermediate hubs

The document is a high level overview of the PMIX Architecture and is intended to provide PMP administrators with an overview of the PMIX principles. The PMIX Architecture document is non-normative. The normative specifications are listed in Section 5, Related Documents.

2 Document Scope

The following capabilities are not included within the PMIX Architecture scope:

- The architecture does not provide an application level "ping" health monitoring capability.
- The architecture does not provide for a consolidated logging service, but this will be considered in a future release.

The PMIX Architecture provides for request-multicast or disclosure-aggregation. Request-multicast refers to distributing of a single PMP request to multiple disclosing PMP systems. Disclosure-aggregation refers to the corresponding aggregation of the responses from the multiple disclosing states. Aggregation is the process of collecting the responses and returning them as a single batch. PMIX solutions may also sort and filter the aggregated responses. Sorting/filtering responses is referred to as disclosure-collation. However, these capabilities are not supported between hubs. That is, the PMIX Architecture provides for multiple disclosing PMPs but the interface between hubs will only support individual disclosing PMPs.

3 Background

The Alliance of States with Prescription Monitoring Programs undertook the development of a consensus, national specification (the "PMIX Specification") to enable the interstate sharing of PMP data. Concurrently, the Alliance has supported implementation of an operational interstate data sharing hub which implemented the

PMIX Specification to deliver an operational pilot exchange between Kentucky and Ohio. Other organizations have expressed a desire to take the PMIX Specification and develop independent hub implementations to support data sharing. The National Association of Boards of Pharmacy (NABP) now operates an interstate PMP data sharing hub. In addition, health information exchanges are being established nationwide. To promote interoperability among hub implementations, a rigorous, standards-based approach is needed. Therefore, the PMIX Specification is being extended into a PMIX Architecture, to which these hubs (and any future hub) can conform to promote broader interoperability.

4 Standards-Based Approach

The use of open, consensus standards promotes interoperability, while preserving local control and retaining the ability to innovate. The Global Advisory Committee (GAC) is a federal advisory committee responsible for the creation of information sharing standards and guidelines in a consensus manner, involving practitioners at all levels of government, national stakeholder organizations, and private industry in order to facilitate information exchange. The GAC developed the National Information Exchange Model (NIEM) and the Global Reference Architecture (GRA), both foundational elements of the PMIX Architecture.

The use of NIEM and GRA ensures compatible data formats and interoperability of the underlying information exchanges including message security. The figure below shows the major components of the PMIX protocol stack and the relationship of NIEM and the GRA within the stack.

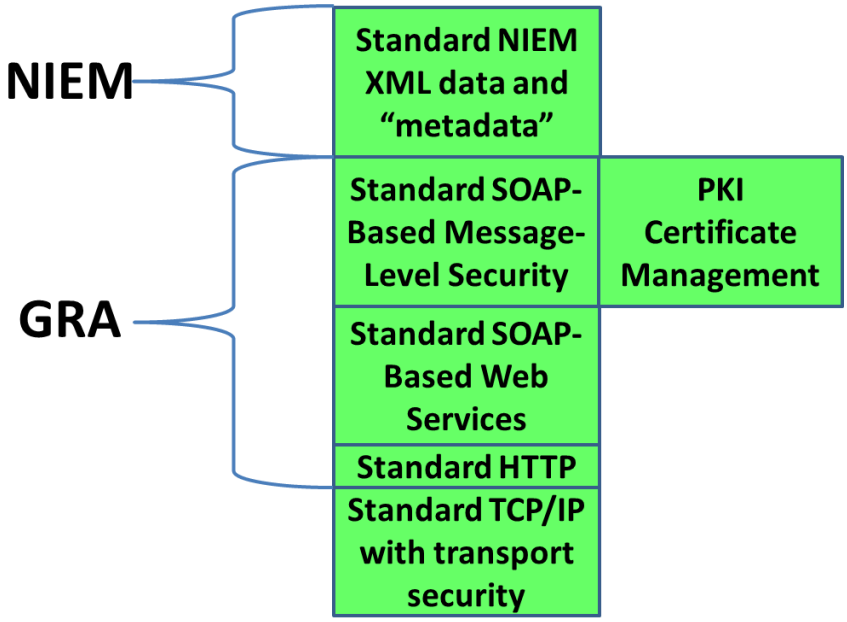


Figure 1 NIEM/GRA Stack

NIEM is based on the World Wide Web Consortium (W3C) eXtensible Markup Language and a number of related advanced data standards. NIEM provides a comprehensive data model and is increasingly being adopted as the basis for health related information exchanges.

The GRA provides a comprehensive framework for standards-based information exchange, that adheres to the concept of a Service Oriented Architecture. The GRA provides a mechanism to define and develop services through the use of service interaction profiles, in particular, the Reliable Secure Web Services Service Interaction Profile. This profile is based exclusively on the use of W3C and Organization for the Advancement of Structured Information Standards (OASIS) standards.

In addition, the GRA defines the concept of an "execution context". The execution context describes the necessary infrastructure behind a service interaction that is not defined directly by the service. In the context of the PMIX Architecture, the main execution context components are the intermediate hubs, the PMIX directory and the PMIX Public Key Infrastructure (PKI). The execution context is to an interoperability infrastructure as the network management capabilities are to a telecommunications network.

5 Related Documents

There are four key specifications which define the PMIX Architecture:

- PMIX Service Specification Package (SSP) V1.0.1 (December 2011)
- PMIX Information Exchange Package Documentation (IEPD) as provided in the PMIX SSP V1.0.1
- PMIX Hub-to-hub Service Specification Package V1.0.0 (April 2012)
- PMIX Execution Context Document V1.0 (May 2012)

These PMIX Architecture documents comply with the respective GRA and NIEM documentation guidelines.

The primary components of a GRA Service Specification Package (SSP) are:

- Service Description
- Service Interface Description
- Reference WSDL
- Reference IEPD

The PMIX Service Specification Package also provides Microsoft .NET and Java reference implementations to facilitate PMP implementation.

The PMIX Hub-to-Hub Service Specification Package specifically defines the hub-to-hub exchange services.

The PMIX Execution Context Document provides a comprehensive description of the PMIX Public Key Infrastructure (PKI) and the PMIX Directory, and will comply with the GRA execution context documentation guideline.

6 The PMIX Architecture

The PMIX Architecture requires:

- Reliable Secure Global Reference Architecture (GRA) Web Services Profile
- National Information Exchange Model (NIEM) data and metadata
- Hub connections (hub to hub capability)
- PMP-to-PMP security using Public Key Infrastructure (PKI)

The Architecture requires GRA and NIEM compliance. It also includes optional provisions for state hubs, multiple national hubs, other hubs that may become part of the interoperability infrastructure in the future and even a direct exchange without hubs. It provides end-to-end security by providing the message level encryption of private information from PMP-to-PMP (and transport level encryption of all information when being transmitted between intermediaries over the Internet).

7 Global Reference Architecture Profile (GRA)

The Reliable Secure GRA Web Services Profile 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], which reiterates the full set of GRA non-functional requirements and specifies the standards for conformance. The GRA profile does not require a service to implement every service requirement. Instead, every applicable service requirement must be met using the appropriate standards. The table below lists the GRA service interaction requirements along with the relevance of each GRA to the PMIX Architecture and the associated standards. The key web services standards are WS-Addressing, which enables routing, and WS-Security, which provides end-to-end security.

GRA Service Requirement	PMIX Architecture Standard

[1] GRA Reliable Secure Web Services Service Interaction Profile V1.1, http://it.ojp.gov/docdownloader.aspx?ddid=1134

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
Message Integrity	• Not required
Service Consumer Authentication	• Not required
Non-Repudiation	• Not required
Binary Data	• Not required
Composite Message	• Not required
Service Metadata Availability	• Not required
Service Authentication	• Not required
Identity Attribute Assertion Transmission	• Not required
Transaction Support	• Not Required

Table 1 PMIX Service Requirements

8 Common NIEM Exchange Data and Metadata

The PMIX Architecture requires that data be exchanged in eXtensible Markup Language (XML) in accordance with NIEM and the PMIX IEPDs.

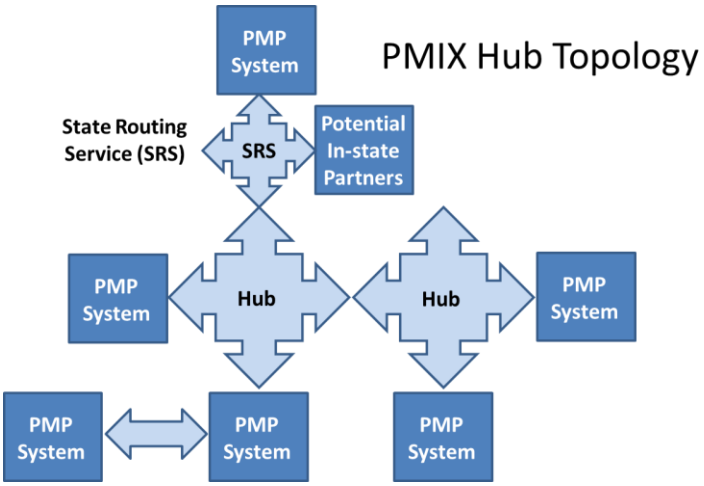
The PMIX Architecture defines two message exchanges: Provide Prescription Drug History and Deliver Deferred Prescription Drug History. All PMIX services operate using the request-response message exchange pattern.

The PMIX Architecture provides for the exchange of unencrypted metadata which can be used to facilitate and control the information exchange. In accordance with the GRA, addressing metadata (requesting entity, disclosing entity(ies), message id(s)) will be exchanged using WS-Addressing. Other metadata, such as requestor role and requester id, has been defined and is documented in the SSPs.

The PMIX Architecture metadata will include provisions for exchanges to/from the requesting entity and multiple disclosing entities associated with a single hub. There are currently no provisions for exchanges to/from the requesting entity and multiple disclosing entities associated with more than one hub, i.e. communicating to multiple

disclosing entities through multiple hubs. That is, the PMIX Architecture provides for multiple disclosing PMPs but the interface between hubs will only support individual disclosing PMPs.

9 Hubs and Hub-to-hub Exchanges



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, must 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.

A State hub, referred to as a State Routing Service (SRS), can be optionally deployed. Use of a SRS provides a state with the ability to more easily add in-state exchanges in the future and can serve as a ready platform for securing end-to-end national exchanges. SRSs can also serve as a bridge for PMP systems built on older or more limited platforms.

The PMIX Architecture requires any hub-to-hub connections to use the PMIX GRA profile. 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.

Conformance for hub-to-hub services can be assessed independent of the PMP-to-hub services.

10 End-to-End Security

A key principle of the PMIX Architecture is the end-to-end encryption of all Protected Health Information (PHI) and Personally Identifiable Information (PII). Encryption/decryption occurs only at the endpoints of each exchange transaction, which limits the potential risk of disclosure en route.

The PMIX Architecture requires transport level encryption of the entire PMIX exchange (meaning the XML document defined the PMIX NIEM IEPD) during transmission as well as end-to-end encryption of the content of the actual core PMIX request and response. In particular, no PII or PHI data can be unencrypted outside of the requesting or disclosing entities. Metadata, such as that pertaining to routing between entities and user role, is not encrypted except during the actual transmission.

Message level encryption is performed in accordance with the GRA, which specifies the OASIS Basic Security Profile. This profile specifies the use of WS-Security with XML encryption using NIST Advanced Encryption Standard (256 bit).

The PMIX Web Service Description Language (WSDL) provides security policy statements that define all the exchange security requirements, including the specific XML elements to be encrypted (example below).

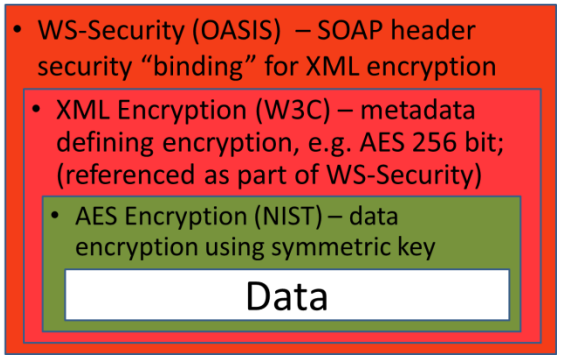


Figure 2 WS-Security Components

```
<wsp:Policy wsu:Id="WsBasicProfile_ProvidePrescriptionDrugHistory_Input_policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SignedParts xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        </sp:SignedParts>
        <sp:EncryptedParts xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
          <sp:Body/>
        </sp:EncryptedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
```

Figure 3 PMIX Security Policy Example

The PMIX Architecture specifies the need for Public Key Infrastructure (PKI). PKI is based on digital certificates with public and private keys used for both transport level and message level security. The PMIX PKI supports X.509 certificate use and storage including certificate revocation. Each PMP system will be required to have a certificate and publish the certificate to the PMIX directory. Certificates can either be self-signed or issued by a third party.

The architecture provides for a shared infrastructure to support certificate/key management capabilities and basic directory services. In particular, the architecture includes a PMIX Directory Service that supports secure access and update using the Lightweight Directory Access Protocol (LDAP). The PMIX Directory, also known as the PMIX LDAP Server, will provide for X.509 certificate management as well as PMP contact and service requirement information. The PMIX Directory will provide an entry for each participating PMP which will include the certificate/public key, PMP contact information, authorized requesting entities, authorized disclosing entities and authorized requestor roles. The PMIX Directory will be available through secure connection to all hubs and PMP systems.

11 PMIX Architecture Summary

The Alliance of States with Prescription Monitoring Programs 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 architecture requires 1) Compliance with the 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 requires the use of the GRA Reliable Secure Web Services Service Interaction Profile. The GRA specifies profiles of standards from the W3C and OASIS, including a standard service interface and WS-Security. Specifically, the following W3C and OASIS standards are required: SOAP, WS-Security and WS-Addressing.

The architecture requires that data be exchanged in eXtensible Markup Language (XML) in accordance with the PMIX IEPDs. The architecture defines two message exchanges: Provide Prescription Drug History and Deliver Deferred Prescription Drug History. PMIX “addressing” data (requesting entity, disclosing entity(ies), message id(s)) will be exchanged using WS-Addressing.

The architecture provides for any number of national exchange hubs as well as standard hub-to-hub connections using the PMIX GRA profile. 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. State hubs, named State Routing Services (SRSs) in PMIX, can be optionally deployed.

The architecture requires that all Personally Identifiable Information (PII) and Personal Health Information (PHI) be encrypted from entity-to-entity by performing transport level encryption of the entire PMIX exchange during transmission as well as end-to-end message level encryption of IEPD contents in accordance with the GRA (OASIS Basic Security Profile). This profile specifies the use of WS-Security with XML encryption using NIST Advanced Encryption Standard (256 bit).

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 architecture and associated standards provide the framework to make interoperability possible and to reduce the risk and cost of implementation. There is a strong push to establish nationwide governance and create multilateral agreements. In terms of technology, the PMIX Architecture is based on broadly supported industry and government open standards to facilitate and reduce the corresponding cost of nationwide participation.

12 Appendix A - REST Interoperability

The PMIX Architecture used the Web Services Interoperability exchange methodology based on the SOAP standard. REpresentational State Transfer (REST) is a widely used, alternative exchange methodology that does not include a standard profile for reliable secure messaging. A specific strategy has been developed that will enable interoperability between GRA compliant SOAP-based systems and REST-based systems.