

**Prescription Monitoring Program Information Exchange**

**( PMIX )**

**Execution Context  
Version 1.1  
  
July 2013**

**Sponsored by:**



**TABLE OF CONTENTS**

[1 Introduction 5](#_Toc322962480)

[1.1 Overview 5](#_Toc322962481)

[1.2 Purpose 6](#_Toc322962482)

[2 System Overview 7](#_Toc322962483)

[2.1 PMIX Architecture 7](#_Toc322962484)

[2.2 PMIX Topology Overview 8](#_Toc322962485)

[2.3 PMIX System Components 9](#_Toc322962486)

[3 REACHABILITY 10](#_Toc322962487)

[3.1 Network Infrastructure 10](#_Toc322962488)

[3.2 Message Transport 10](#_Toc322962489)

[4 WILLINGNESS 11](#_Toc322962490)

[4.1 Network infrastructure security 11](#_Toc322962491)

[4.2 Identity provisioning and management 11](#_Toc322962492)

[4.3 Shared security infrastructure 13](#_Toc322962493)

[4.4 Security policy infrastructure 15](#_Toc322962494)

[5 AWARENESS 18](#_Toc322962495)

[6 INTERMEDIARIES 19](#_Toc322962496)

[6.1 Message Router 19](#_Toc322962497)

[6.2 Orchestration 20](#_Toc322962498)

[6.3 Transformer 21](#_Toc322962499)

[6.4 Validation 21](#_Toc322962500)

[7 Operational Considerations 24](#_Toc322962501)

[7.1 Performance and Availability 24](#_Toc322962502)

[7.2 Scalability 24](#_Toc322962503)

[7.3 Maintainability and Supportability 24](#_Toc322962504)

[8 Appendix A — References 25](#_Toc322962505)

[9 Appendix B — Acronyms 25](#_Toc322962506)

[10 Appendix C — Document History 26](#_Toc322962507)

[11 Appendix D — PMIX LDAP Structural Hierarchy 27](#_Toc322962508)

[12 Appendix E — PMIX Roles 28](#_Toc322962509)

**FIGURES**

[Figure 1: PMIX Architecture Overview 7](#_Toc322962510)

[Figure 2: PMIX Hub Topology 8](#_Toc322962511)

[Figure 3: PMIX Architecture Standards 8](#_Toc322962512)

[Figure 4: PMIX Component Overview 9](#_Toc322962513)

[Figure 5: High Level LDAP Overview 13](#_Toc322962514)

[Figure 6: Authorization Configuration Scenario 16](#_Toc322962515)

[Figure 7: WS-Addressing 19](#_Toc322962516)

[Figure 8: Request Profile Usage Example 22](#_Toc322962517)

**TABLES**

[Table 1: X.509 Certificate Attributes 12](#_Toc322962518)

[Table 2: LDAP Specifications 13](#_Toc322962519)

[Table 3: Authorization Hierarchy and Structure 15](#_Toc322962520)

[Table 4: Message Routing Metadata 20](#_Toc322962521)

[Table 5: Request Profile Structure & Hierarchy 21](#_Toc322962522)

**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 is supported by Grant No. 2010-DG-BX-K088 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 U.S. Department of Justice.*

# Introduction

## Overview

In the context of a service-oriented architecture (SOA) 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. GRA web services are based on the Organization for the Advancement of Structured Information Standards (OASIS) Web Services Profiles.

The PMIX Execution Context provides a method for describing and documenting the set of infrastructure elements, process entities, policy assertions, and agreements identified as part of a specific, real interaction between a service consumer and a service. Execution context forms a communication and policy path between a service consumer with needs and a service that provides the functionality. It was developed in accordance with the GRA Execution Context Guidelines (<http://it.ojp.gov/docdownloader.aspx?ddid=1170>).

## Purpose

The PMIX Execution Context is intended to define the infrastructure components, including network and server equipment and software necessary to form a real, physical, secure, communication path, for data transmission capability, between a consumer and service. This path may contain equipment and software necessary for the reliable transmission of data, including transient message storage capabilities and the processing or handling of messages in transit.

In accordance with the Execution Context Guidelines, the Execution Context is described in the following four infrastructure areas:

* Reachability
  + Defined by the GRAas “the existence of a communication path or channel that allows a service consumer and service to communicate with one another.”
* Willingness
  + The GRA concept includes the scope of interaction permitted between the service consumer and service provider.
* Awareness
  + Described as service registries and/or repositories that provide the capability for content management, authentication/authorization and data validation.
* Intermediaries
  + Defined as any component that receives messages from a consumer and, subsequently as a service consumer, interacts with another service.

# System Overview

## PMIX Architecture

The purpose of the PMIX Architecture was to establish a set of information exchange standards and specifications to facilitate systems exchange of prescription history reports with other PMP systems and other authorized organizations. In addition, the PMIX Architecture defined the high-level addressing and security requirements for information exchange and the PMP interoperability execution infrastructure for security related functions and exchange-facilitating intermediate hubs.



Figure 1: PMIX Architecture Overview

The PMIX Architecture relies on GRA standards including NIEM compliant content structure and semantics to provide optional provisions for state hubs, interstate hubs, other hubs that may become part of the interoperability infrastructure in the future and even a direct exchange without hubs (see Figure 2). The architecture specifies dual security mechanisms, transport level encryption of all information transmitted between intermediaries and end-to-end message level security from PMP-to-PMP.

## PMIX Topology Overview

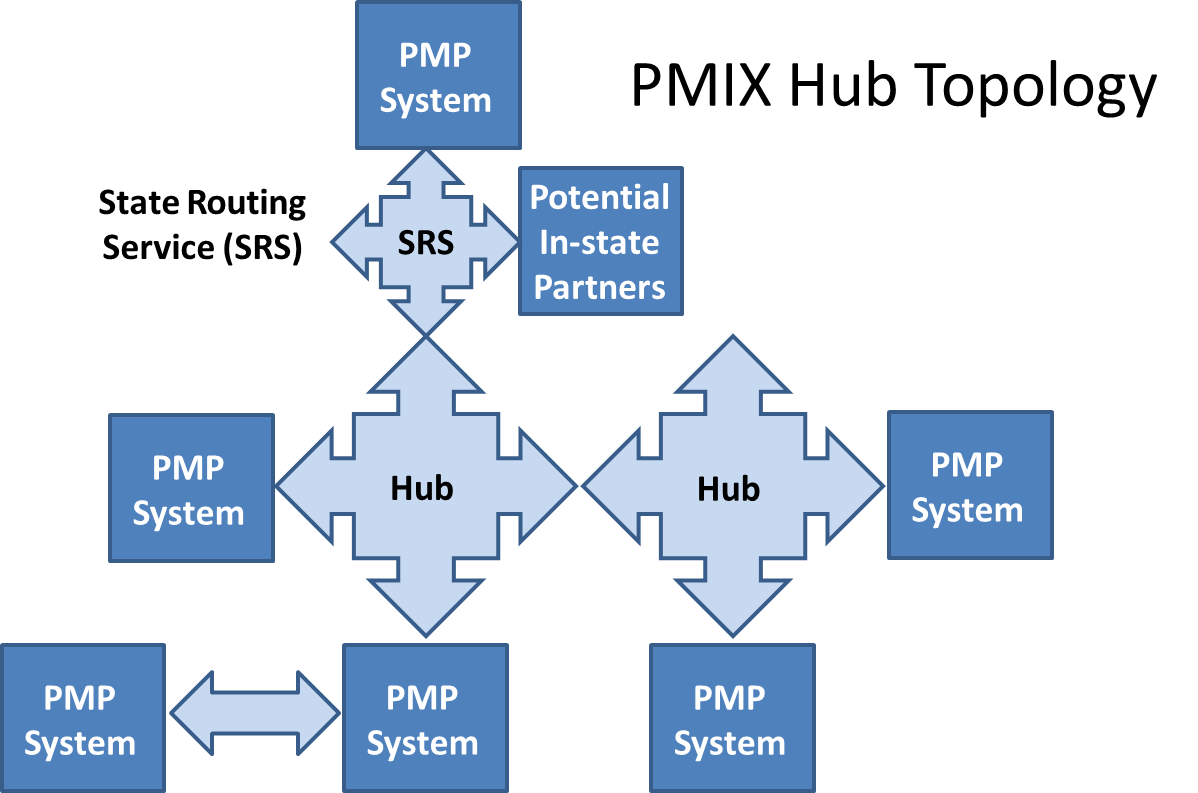
 A hub provides secure routing services to direct information exchanges as required. The hub approach limits the need to provide multiple State network security configurations. In addition, hubs can exchange data through other hubs. Hubs, referred to more technically in the GRA as intermediaries, must support the same standards for transport, addressing and security.

Figure 2: PMIX Hub Topology

The PMIX Architecture requires any hub-to-hub connections to use the PMIX GRA profile. A State hub or State Routing Service must also comply with the execution context. A hub must be able to route messages using the WS-Addressing standard and must be able to relay encrypted content using WS-Security.



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)

Figure 3: PMIX Architecture Standards

## PMIX System Components

The PMIX service interface complies with the GRA Web Services Reliable Secure Service Interaction Profile and the GRA Execution Context Guidelines.

The PMIX service interface utilizes standards-based web services to facilitate communication through hubs to the 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 ensures message privacy and integrity.

Figure 4 below depicts an overview of PMIX interface components, including two sample endpoint systems separated by two disparate hub implementations. The web service interface illustrates the secure nature of the web service communication and the complete end-to-end message encryption.



Figure 4: PMIX Component Overview

In addition, the diagram shows the open standard LDAP directory service repository that will store digital certificates, used for transport and message level security, as well as site role based authorization information and validation rules.

# REACHABILITY

## Network Infrastructure

*Network infrastructure provides a physical path for service participants to reach out to each other and share the information.*

The PMIX network infrastructure uses the public Internet to support the transmission of data between all site participants that are providers and/or consumers of the PMIX services and supports all of the messaging protocols identified in the PMIX Service Interface Description Document (SIDD).

The shared network infrastructure execution context requires that the network support data transport via TCP/IP between all partner locations at which consumer and provider systems will be deployed. The network must provide adequate bandwidth to support message exchange that complies with response times specified in service policies and contracts. To the extent that service interaction requirements are implemented through reliance on network reliability and security, the network must satisfy reliability/availability and security requirements specified in service policies and contracts. The network must permit the transmission of secure HTTP (HTTPS) traffic (on non-standard TCP ports) between the partner locations.

Static IP addresses are used as an additional assurance that access is from an authorized service consumer.

## Message Transport

The shared execution context must allow service providers to deploy and manage components called service containers, which are defined as follows. A service container:

• Receives messages and, based on the service action being invoked, interacts with one or more adapters to accomplish the service’s real-world effect

• Manages the lifecycle of adapters (including configuration/initiation, disposal, and threading/concurrency issues)

A service container must be capable of receiving and properly handling any message that conforms to a service interaction profile defined within this architecture.

The shared execution context must specify and/or provide software components or application programming interfaces (APIs) that service consumer systems will use or invoke in order to send messages. These components or APIs must support the sending of any message that conforms to the reliable web services interaction profile as customized for the PMIX Architecture (see Appendix A).

# WILLINGNESS

## Network infrastructure security

The shared execution context specifies a secure HTTP communication channel leveraging Secure Socket Layer (SSL), which establishes a secure, encrypted tunnel between the service consumer and the service provider. SSL is based on a cryptographic system that uses separate keys to encrypt and decrypt the data − a public key known to everyone and a private or secret key known only to the recipient of the message.

In order to support the SSL requirement, the shared execution context must support the use of third party certificate authorities for digital certificate issuance, revocation, and provisioning for the service policy/contract requirements for message confidentiality. Also, since the security requirements cannot be met solely at the transport level, digital certificates (third party or self-signed) will also be used to provide message level security. SSL certificates are managed locally and are not stored in the PMIX Directory.

## Identity provisioning and management

To support the identity provisioning and management requirements of the PMIX Architecture, the shared execution context requires a public key infrastructure that relies on X.509 digital certificates which can be used for authentication, confidentiality, nonrepudiation, and message integrity functions.

The following outline provides an overview of the X.509 certificate structure:

|  |  |
| --- | --- |
| Attribute | Description |
| Version # | X.509 certificate version number (in practice always 3). |
| Serial Number | A unique identifier for the certificate. |
| Algorithm ID | The algorithm used to create the digital signature. |
| Issuer Name | The name of the certificate issuer. |
| Validity Period | The period during which the certificate is valid. |
| Subject Name | The name of the subject represented by the certificate. |
| Subject Public Key Info | The public key algorithm. |
| Issuer Unique Identifier | The identifier for the issuer. (optional) |
| Subject Unique Identifier | The identifier for the subject. (optional) |
| Extensions | Extensions can be used to store additional information, such as Key Usage or Alternative Names. (optional) |
| Signed Hash of Cert data | The hash of the preceding fields encrypted using the issuer's private key, which results in a digital signature. |

Table 1: X.509 Certificate Attributes

## Shared security infrastructure

An open standard Lightweight Directory Access Protocol (LDAP) directory service is utilized to facilitate the storage and management of digital certificates. In addition, the directory service also stores site information such as contacts, role based authorization and rule base business rules.

The following table lists the relevant LDAP specifications:

|  |  |
| --- | --- |
| Reference | Description |
| RFC4511 | LDAP Protocol |
| RFC4512 | Directory Information Models |
| RFC4513 | Authentication Methods and Security Mechanisms |
| RFC4514 | String Representation of Distinguished Names |
| RFC4515 | String Representation of Search Filters |
| RFC4516 | Uniform Resource Locator |
| RFC4517 | Syntaxes and Matching Rules |
| RFC4518 | Internationalized String Preparation |
| RFC4519 | Schema for User Applications |
| RFC4523 | Schema Definitions for X.509 Certificates |

Table 2: LDAP Specifications

The PMIX interface utilizes the LDAP Directory Service as a standards-based repository to facilitate the authentication and authorization of service subscribers as well as the implementation of business rules such as validation.



Figure 5: High Level LDAP Overview

The LDAP directory service schema will be extended by standard LDAP Data Interchange Format files which establish the basic structural foundation of the repository. A complete listing of the PMIX Directory is provided as an appendix. The following outline describes the main categories of data objects that have been added to the standard LDAP structure to represent PMIX control data.

* **pmixSite:**
  + The base data structure which contains general site information and a container structure for all other associated configuration data
* **pmixSenderRoles:**
  + The Sender Roles data values identify the outbound “sending” roles that have permission to send requests, including the disclosing sites for which the roles have been authorized
* **pmixAuthSites:**
  + The Authorized Sites configuration data specify the requesting site roles that are authorized to sending inbound requests
* **pmixContacts:**
  + The contact data contains the structure needed to represent technical and administrative contact persons
* **pmixSiteCertificate:**
  + The Site Certificate data value provides all the fields necessary to represent the digital certificate binary and associated metadata
* **pmixRequestProfiles:**
  + A site’s Request Profiles represent the full set of request required field combinations supported by their PMP application
* **pmixRoutingData:**
  + The routing data section contains repository fields that store information pertaining to client endpoints and routing
* **pmixServiceHost:**
  + The service host section establishes repository fields that represent the host service endpoint information, including type, address, etc.

## Security policy infrastructure

The security policy infrastructure represents the collection of components implemented in the central hub(s) as well as the endpoint systems that implement the access control requirements for the PMIX service transactions. The authorization functions will leverage data stored in the **pmixSenderRoles** and **pmixAuthSites** LDAP structures to provide the necessary role-based security. The following table provides an overview of the authorization hierarchy and structure.

|  |  |  |
| --- | --- | --- |
| LDAP Object | Type | Occurrence |
| pmixSite | Object Class | Multiple |
| * pmixSenderRoles | Container | Single |
| * + pmixSenderRole | Object Class | Multiple |
| * + - pmixRoleAuthorizedStateRole | Attribute | Multiple |
| * pmixAuthSites | Container | Single |
| * + pmixAuthSite | Object Class | Multiple |
| * + - pmixSiteAuthorizedStateRole | Attribute | Multiple |

Table 3: Authorization Hierarchy and Structure

Sender authorization and sender roles will be validated to the extent possible.

Required field validation can be performed at any hub subject to the following rules;

   a. If there is no required field set (request profile), consider the request to be valid

   b. If there is one required field set, validate the required fields

A listing of all roles is provided as an Appendix.

The following diagram shows a working example of the LDAP Directory Service authorization entries required for a **Doctor** at the **GG** PMP Site to send a PMIX Request to the **TT** PMP Site.



Figure 6: Authorization Configuration Scenario

In the event that the requesting and/or disclosing authorization has not been configured properly, then the Hub will throw the SOAP fault:

<s:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
 xmlns:s="http://www.w3.org/2003/05/soap-envelope"  
 xmlns:a="http://www.w3.org/2005/08/addressing">  
 <s:Header>  
 <a:Action s:mustUnderstand="1">http://www.w3.org/2005/08/addressing/soap/fault</a:Action>  
 </s:Header>  
 <s:Body>  
 <s:Fault>  
 <s:Code>  
 <s:Value>s:Sender</s:Value>  
 <s:Subcode>  
 <s:Value>**AuthorizationError**</s:Value>  
 </s:Subcode>  
 </s:Code>  
 <s:Reason>  
 <s:Text xml:lang="en-US">

**The Requesting Role is not authorized for the Disclosing State.**

</s:Text>  
 </s:Reason>  
 <s:Node>https://test.rxcheck.org:18803/2010/12/pmix/router</s:Node>  
 <s:Role>**RxCheck** Hub</s:Role>  
 </s:Fault>  
 </s:Body>  
</s:Envelope>

# AWARENESS

As a result of the sensitive nature of the patient data and system components contained in the PMIX environment, all service interactions will be governed by legal agreements between exchange partners. Therefore, since system participation is highly controlled, an on-line service registry, which enables a service consumer to dynamically locate and access the service, is not required. Rather, the service specification and execution context documentation will be distributed to each new participant.

# INTERMEDIARIES

The PMIX shared execution context provides specific detailed information regarding the services support by the intermediate hub(s). The following sections discuss the message router, data flow orchestration and data field validation that must be implemented by a PMIX Hub.

## Message Router

The PMIX service interface uses a request/response “message exchange pattern” (referred to as the MEP in the standards specifications) to provide simple processing in the case that the prescription drug history is readily available. The request/response message exchange patterns will rely on SOAP faults to return any error data back to the original calling application.

The PMIX web service interface leverages the WS-Addressing specification to facilitate intermediate routing through each hub system. Figure 7 below demonstrates the WS-Addressing (wsa) routing data essential for PMIX interactions.



Figure 7: WS-Addressing

The following SOAP message example demonstrates the actual custom PMIX Metadata header along with the WS-Addressing header elements.

<soap:Envelope xmlns:soap="**http://www.w3.org/2003/05/soap-envelope**" xmlns:pmix="**http://www.pmix.gov**">

<soap:Header xmlns:wsa="**http://www.w3.org/2005/08/addressing**">

<pmix:MetaData>

<pmix:Requestor>**Dr. Abc**</pmix:Requestor>

<pmix:RequestorRole>**Pharmacist**</pmix:RequestorRole>

<pmix:RoutingData>

<pmix:DisclosingState>**P2**</pmix:DisclosingState>

<pmix:RequestID>**12345**</pmix:RequestID>

<pmix:RequestingState>**P1**</pmix:RequestingState>

</pmix:RoutingData>

</pmix:MetaData>

<wsa:Action>**http://www.pmix.gov/pmp/ProvidePrescriptionDrugHistory**</wsa:Action>

<wsa:To>**urn://p2/**</wsa:To>

<wsa:From>**urn://p1/**</wsa:From>

</soap:Header>

…

The following table describes the <soap:Header> metadata elements:

|  |  |  |
| --- | --- | --- |
| Parameter | Description | Location |
| Metadata   * Requestor * Requestor Role * RoutingData * RequestID * RequestingState * DisclosingState | Metadata includes information about the requestor, including role and routing information, which contains the Request ID (a unique message identifier) and the requesting/disclosing state two character postal code. | SOAP header |
| WS-Addressing   * Action * To * From | The Action is an identifier that uniquely identifies the semantics implied by a message. The wsa:To element identifies the target destination, while the wsa:From identifies the source endpoint. | SOAP header |

Table 4: Message Routing Metadata

## Orchestration

The PMIX shared execution context is expected to be expanded for orchestration of PMIX request multicasting and message aggregation.

## Transformer

The PMIX shared execution context does not specify any components for message transformation since the intermediary message level security ensures that all payload data is encrypted during transit through the hub(s).

## Validation

In order to implement the required PMIX request parameter validation, each PMIX intermediary must be able to access the global site request parameter requirements and compare the rules against the metadata associated with the in-transit message. The PMIX execution context specifies that the global set of site request parameter requirements will be stored in the distributed LDAP directory service as request profiles. Each request profile will identify a unique set of request parameters that would establish the minimum inquiry data for the request. A site has the option to support one or more search / request profiles as appropriate based on the PMP rules. The following table shows the LDAP repository structure and hierarchy for a request profile.

|  |  |  |
| --- | --- | --- |
| LDAP Object | Type | Occurrence |
| pmixConfiguration | Container | Single |
| * pmixRequestProfiles | Container | Single |
| * + pmixRequestProfile | Object Class | Multiple |
| * + - pmixRequiredDataElement | Object Class | Multiple |
| * + - * pmixRequiredDataElementName | Attribute | Single |
| * + - * pmixRequiredDataElementXPath | Attribute | Single |
| * + - * pmixRequiredDataElementDesc | Attribute | Optional |

Table 5: Request Profile Structure & Hierarchy

The request profile configuration and site references are depicted in the following diagram.



Figure 8: Request Profile Usage Example

In the event that the required data elements in the message header do not match a destination site request profile, then the hub will throw the SOAP fault:

<s:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
 xmlns:s="http://www.w3.org/2003/05/soap-envelope"  
 xmlns:a="http://www.w3.org/2005/08/addressing">  
 <s:Header>  
 <a:Action s:mustUnderstand="1">http://www.w3.org/2005/08/addressing/soap/fault</a:Action>  
 </s:Header>  
 <s:Body>  
 <s:Fault>  
 <s:Code>  
 <s:Value>s:Sender</s:Value>  
 <s:Subcode>  
 <s:Value>**ValidationError**</s:Value>  
 </s:Subcode>  
 </s:Code>  
 <s:Reason>  
 <s:Text xml:lang="en-US">

**The Disclosing State does not have a search profiles that validates the request message**.

</s:Text>  
 </s:Reason>  
 <s:Node>https://test.rxcheck.org:18803/2010/12/pmix/router</s:Node>  
 <s:Role>**RxCheck** Hub</s:Role>  
 </s:Fault>  
 </s:Body>  
</s:Envelope>

# Operational Considerations

## Performance and Availability

The infrastructure must be available as necessary to support the most stringent availability requirements specified in service policies and contracts. Based on existing implementations of information exchanges to be deployed on the infrastructure in the future, the infrastructure must at a minimum be available seven days per week, 24 hours per day, with a 99.99% probability of availability.

## Scalability

The infrastructure must be capable of a limited initial deployment (consisting of perhaps no more than one service and one consumer), while being capable of scaling to hundreds of services and consumers.

## Maintainability and Supportability

The infrastructure must provide administrators with intuitive interfaces for configuration, deployment/management of service interfaces and service containers, and maintenance.

# Appendix A — References

PMIX Service Description Document Version 1.0.1

PMIX Service Interface Description Document Version 1.0.1

Global Reference Architecture Execution Context Guidelines Version 1.1

Global Reference Architecture Framework Version 1.9

# Appendix B — Acronyms

API Application Programming Interface

GRA Global Reference Architecture

NIEM National Information Exchange Model

OASIS Organization for the Advancement of Structured Information  
Standards

PMIX Prescription Drug Monitoring Information Exchange

RS WS SIP Global Reference Architecture Reliable Secure Web Services   
Service Interaction Profile

SOAP Simple Object Access Protocol

SRS State Routing Service

W3C World Wide Web Consortium

WCF Windows Communication Framework

W/S Web Services

WSDL  Web Services Description Language

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

# Appendix C — Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Change |
| 4/2012 | 1.0.0 | Todd Seymour, Bob Slaski,  Open Networks | Initial PMIX Execution Context |
| 7/2013 | 1.1.0 | Todd Seymour,  Open Networks | PMIX Execution Context Re-release |

# Appendix D — PMIX LDAP Structural Hierarchy

* pmixConfiguration  (*1-1)*
  + pmixRequestProfiles *(1-1)*
    - pmixRequestProfile *(1-oo)*
      * pmixRequiredDataElement *(1-oo)*
        + pmixRequiredDataElementName *(1-1)*
        + pmixRequiredDataElementXPath *(1-1)*
        + pmixRequiredDataElementDesc *(0-1)*
* pmixSites  *(1-1)* 
  + pmixSite   *(1-oo)*
    - pmixSiteDisplayName  *(1-1)*
    - pmixSiteDescription  *(1-1)*
    - pmixSiteStatus  *(1-1)*
    - pmixRequestProfileReferences *(1-1)*
      * pmixRequestProfileReference *(0-oo)*
    - pmixSenderRoles  *(1-1)*
      * pmixSenderRole  *(0-oo)*
        + pmixDisplayName  *(1-1)*
        + pmixRoleAuthorizedStateRole  *(1-1)*
    - pmixAuthSites *(1-1)*
      * pmixAuthSite *(1-oo)*
        + pmixDisplayName  *(1-1)*
        + pmixSiteAuthorizedStateRole  *(1-1)*
    - pmixContacts  *(0-1)*
      * pmixContactPerson  *(1-oo)*
        + pmixContactType  *(1-1)*
        + pmixContactName  *(1-1)*
        + pmixContactTitle  *(0-1)*
        + pmixContactAddressStreet  *(0-1)*
        + pmixContactAddressCity  *(0-1)*
        + pmixContactAddressState  *(0-1)*
        + pmixContactAddressPostalCode  *(0-1)*
        + pmixContactEmailAddress  *(1-oo)*
        + pmixContactPhone  *(*1*-oo)*
    - pmixSiteCertificate *(1-1)*
      * pmixCertUserCertificate *(0-1)*
      * pmixCertPublicKeyLength *(1-1)*
      * pmixCertPublicKeyAlgorithm *(1-1)*
      * pmixCertPublicKeyData *(1-1)*
      * pmixCertFriendlyName *(0-1)*
      * pmixCertSubjectCommonName *(1-1)*
      * pmixCertSubjectAlternative *(1-1)*
      * pmixCertDomainIdentity *(1-1)*
      * pmixCertThumbprint *(1-1)*
      * pmixCertStatusIndicator *(1-1)*
      * pmixCertExpirationDate *(1-1)*
    - pmixSystemConnectionData
      * pmixSystemType *(1-1)  [RxCheck, PMPi, HID]*
      * pmixSystemEndpoint *(1-1)*
      * pmixSystemIPAddress *(1-1)*
      * pmixSystemDnsName *(1-1)*

# Appendix E — PMIX Roles

|  |  |
| --- | --- |
| Category | Role |
| Dispensers | Dispensing Prescribers |
| Dispensers | IHS Dispensers |
| Dispensers | Military Prescribers |
| Dispensers | Pharmacies |
| Dispensers | Pharmacy Technicians |
| Dispensers | VA Dispensers |
| Law Enforcement | ATF |
| Law Enforcement | Corrections |
| Law Enforcement | DEA |
| Law Enforcement | Drug Courts |
| Law Enforcement | FBI |
| Law Enforcement | FDA |
| Law Enforcement | HHS |
| Law Enforcement | Homeland Security |
| Law Enforcement | Local |
| Law Enforcement | Medicaid Fraud Investigators |
| Law Enforcement | Military Police |
| Law Enforcement | Multijurisdictional Task Forces |
| Law Enforcement | OIG |
| Law Enforcement | Parole |
| Law Enforcement | Probation |
| Law Enforcement | State Attorney General |
| Law Enforcement | State Criminal Justice Department |
| Law Enforcement | State Drug Control Agents |
| Law Enforcement | State Police |
| Law Enforcement | State Prosecutors (District or Commonwealth Attorneys) |
| Law Enforcement | US Attorney |
| Law Enforcement | VA Investigators |
| Miscellaneous | Child Protective Services |
| Miscellaneous | Medical Examiner/Coroner |
| Miscellaneous | Peer Assistance Programs/Recovering Health Professions Programs |
| Miscellaneous | State Medicaid Programs |
| Miscellaneous | Workers' Compensation |
| Prescribers | Dentists |
| Prescribers | IHS Prescribers |
| Prescribers | Medical Interns |
| Prescribers | Medical Residents |
| Prescribers | Military Prescribers |
| Prescribers | Naturopathic Physicians |
| Prescribers | Nurse Practitioners/Clinical Nurse Specialist |
| Prescribers | Optometrists |
| Prescribers | Pharmacists |
| Prescribers | Physician Assistants |
| Prescribers | Physicians (MD, DO, DPM) |
| Prescribers | Psychologists |
| Prescribers | VA Prescribers |
| Prescribers | Veterinarians |
| Regulatory Agencies | Licensing Board Investigators |