



Alliance of States with
Prescription Monitoring Programs

PMIX Architecture

PMIX Architecture Webinar
January 12, 2012

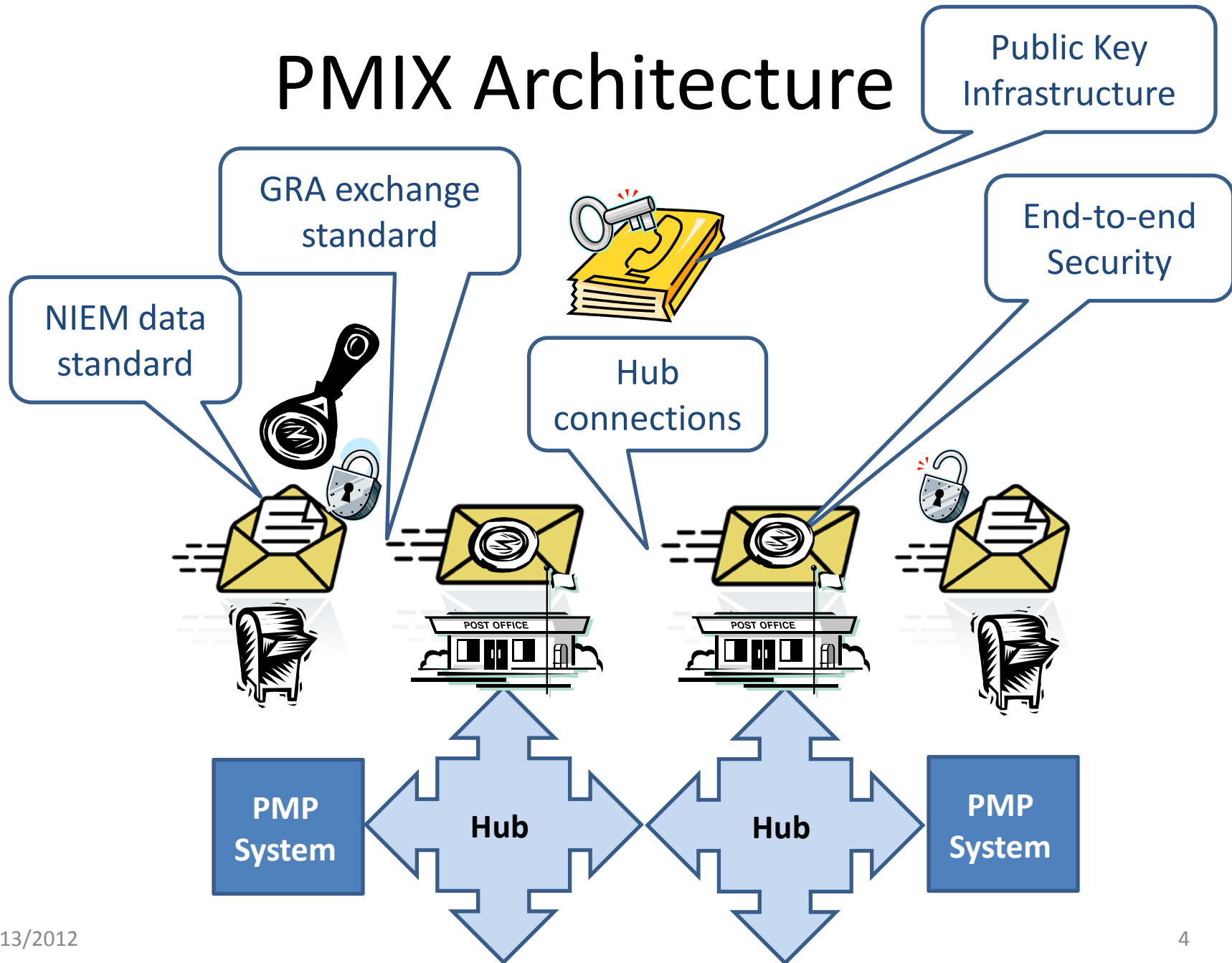
PMIX Architecture Documents

- Prescription Monitoring Program Information Exchange (PMIX) Architecture, Version 1.0, November 2011
- Frequently Asked Questions
http://www.pmpalliance.org/pdf/PMIX%20ARCH%20FAQ_FINAL.pdf

Executive Summary

- PMIX Architecture 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)

PMIX Architecture



Purpose

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

Background

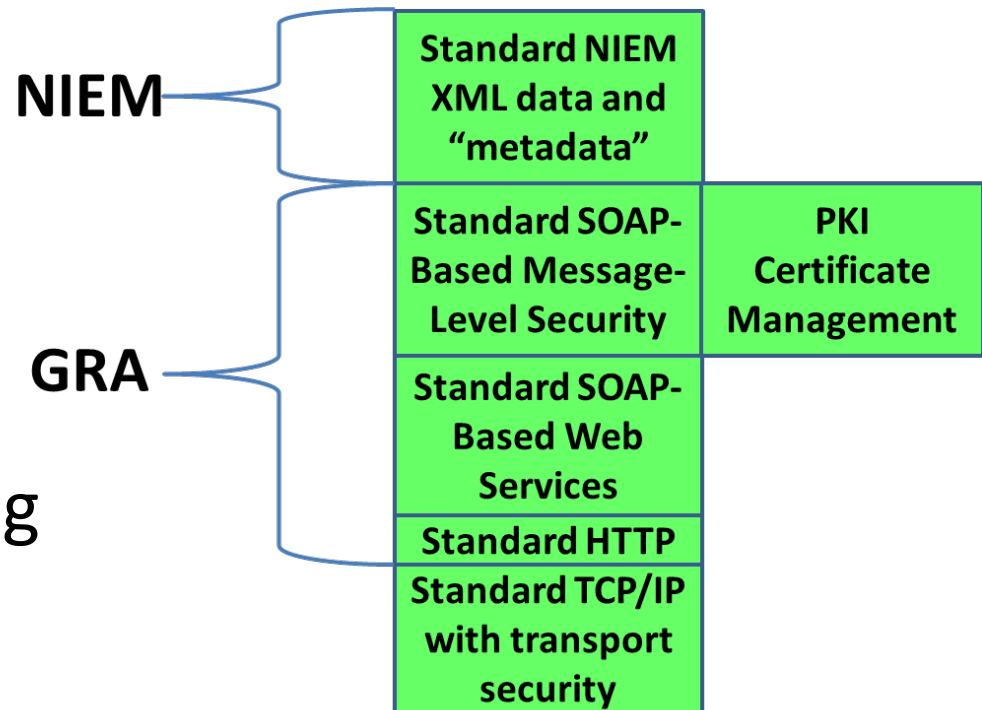
- PMIX specifications
<http://pmpalliance.org/content/prescription-monitoring-information-exchange-pmix>
- National Association of Boards of Pharmacy PMP Interconnect
<http://www.nabp.net/programs/pmp-interconnect/nabp-pmp-interconnect/index.php>
- RxCheck
[http://www.pmpalliance.org/pdf/20111227%20PMIX SSP v 1.0.1.zip](http://www.pmpalliance.org/pdf/20111227%20PMIX%20SSP%20v%201.0.1.zip)

Standards-Based Approach

- Open, consensus standards promotes interoperability, while preserving local control and retaining the ability to innovate
- 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
- GAC developed the National Information Exchange Model (NIEM) and the Global Reference Architecture (GRA), both foundational elements of the PMIX Architecture

NIEM and GRA

- Use of NIEM and GRA ensures compatible data formats and interoperability of the underlying information exchanges including message security



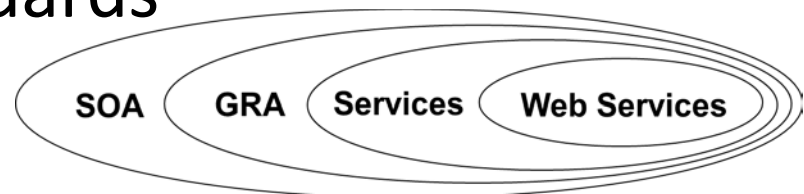
NIEM

- 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



GRA

- GRA provides a comprehensive framework for standards-based information exchange, that consistent with Service Oriented Architecture
- 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 based exclusively on the use of W3C and Organization for the Advancement of Structured Information Standards (OASIS) standards



PMIX Execution Context

- GRA defines the concept of an “execution context” which is the infrastructure behind a service interaction that is not defined directly by the service
- PMIX execution context components include the intermediate hubs, the PMIX directory and the PMIX Public Key Infrastructure (PKI)
- Execution context provides an interoperability infrastructure analogous to the routers and network management system in a network

GAC Standards

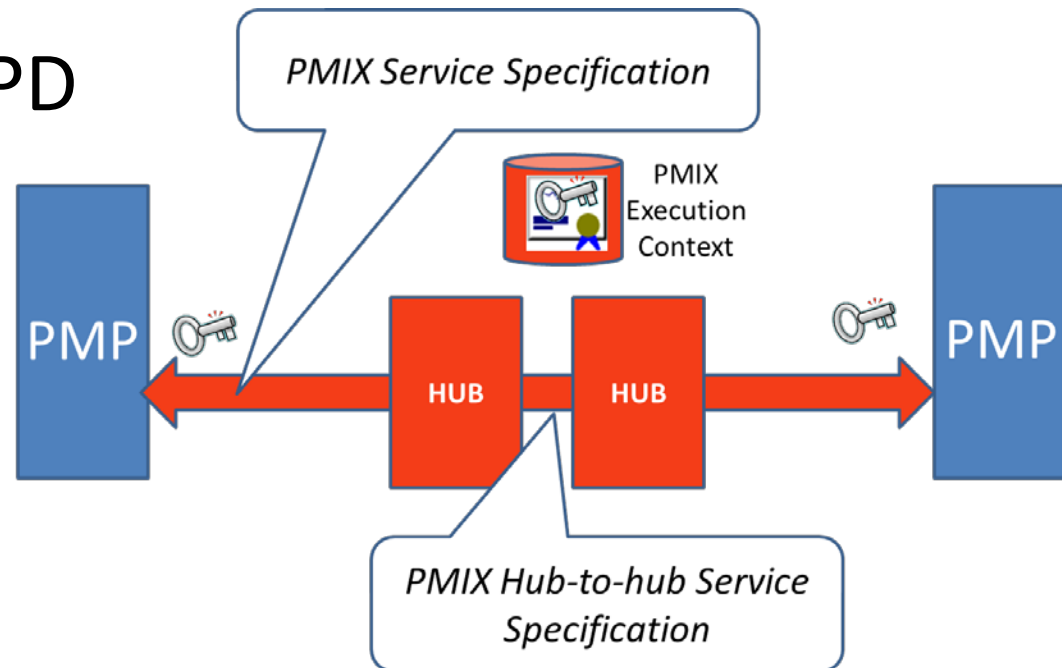
- Data
 - XML and National Information Exchange Model
PMIX Information Exchange Package Documentation
- Exchange
 - Reliable Secure Web Services and the Global Reference Architecture (GRA) Service Specification Package (one stop programming)
- Security
 - GRA Web Services Security

Related Documents

- 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 (TBD 2012)
- PMIX Execution Context Document V1.0 (TBD 2012)

GRA Service Specification Package (SSP)

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



PMIX Architecture Principles

- 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)

Global Reference Architecture Profile

- Reliable Secure GRA Web Services Profile specifies standards from the W3C and OASIS, including a standard service interface and WS-Security (plus transport security)
- Key web services standards are WS-Addressing, which enables routing, and WS-Security, which provides end-to-end security
- GRA Reliable Secure Web Services Service Interaction Profile V1.1
<http://it.ojp.gov/docdownloader.aspx?ddid=1134>

PMIX Service Requirements

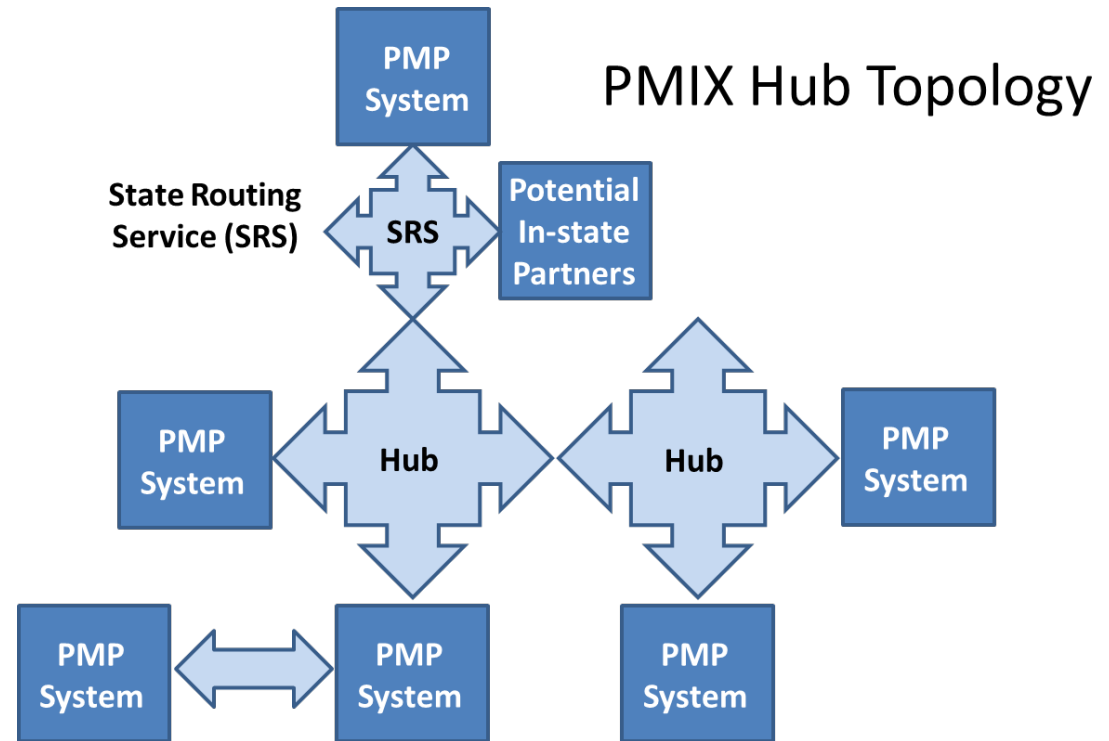
GRA Service Requirement	PMIX Architecture Standard
Simple Message	✓ XML (NIEM) ✓ SOAP
Message Exchange Pattern	✓ Request-Response
Interface Description	✓ Web Service Description Language (WSDL) 1.1
Message Confidentiality	✓ Transport Layer Security ✓ OASIS Security Profile 1.1 w/XML Encryption
Message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

Common NIEM Exchange Data/Metadata

- Data is exchanged in eXtensible Markup Language (XML) in accordance with NIEM and the PMIX IEPDs
- Request-response message exchanges: Provide Prescription Drug History and Deliver Deferred Prescription Drug History
- Metadata for control of the information exchange is unencrypted
- Addressing metadata (requesting entity, disclosing entitie(s), message id(s)) exchanged using WS-Addressing
- Additional metadata, such as requestor role and requester id, defined and documented in the SSPs
- The PMIX Architecture metadata will include provisions for exchanges to/from the requesting entity and multiple disclosing entities

Hubs and Hub-to-hub Exchanges

- A hub provides secure routing services to direct information exchanges
- Hubs can exchange data through other hubs



Hubs and Hub-to-hub Exchanges

- Hub-to-hub connections must use the PMIX GRA profile, e.g. a hub must be able to route messages using the WS-Addressing standard and must be able to forward encrypted data without intervention using WS-Security
- Conformance for hub-to-hub services can be assessed independent of the PMP-to-hub services
- State hub, referred to as a State Routing Service (SRS), can be optionally deployed
 - 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
 - Bridge for PMP systems built on older or more limited platforms

End-to-End Security

- 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
- 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

Transport and Message Security

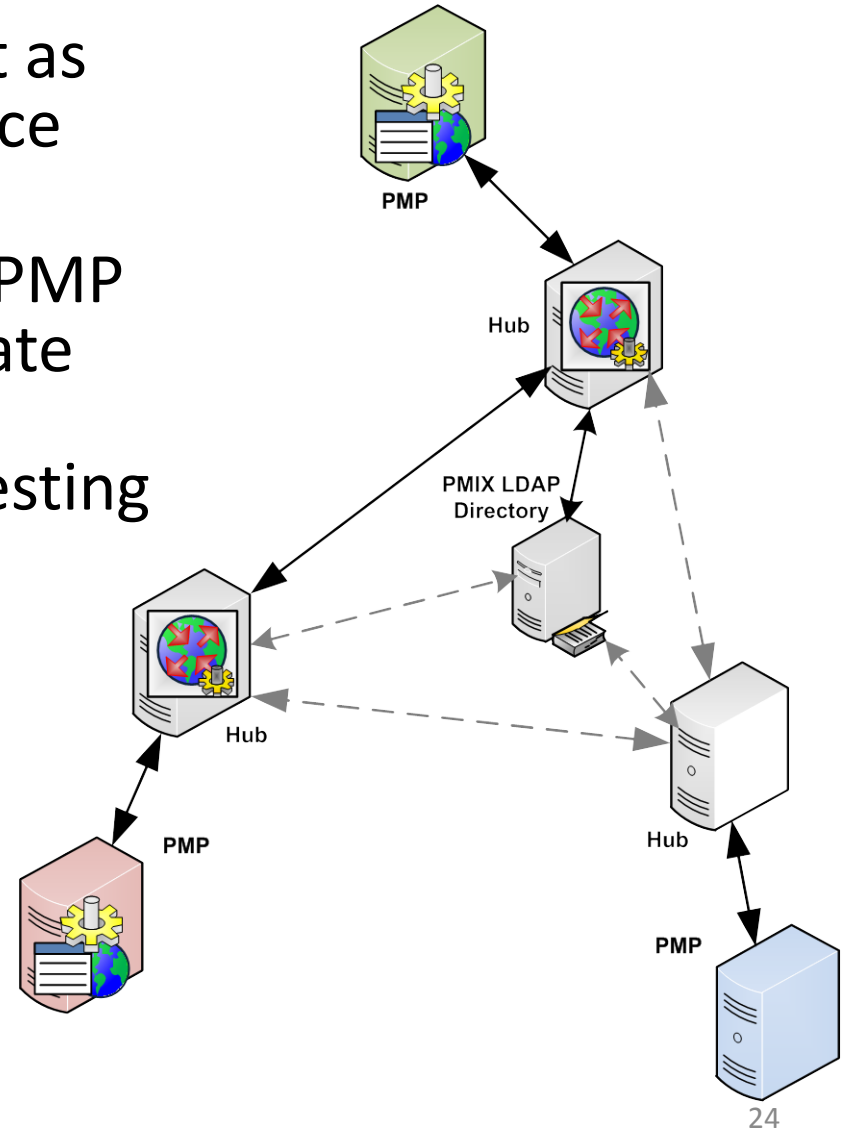
- Transport level encryption of the entire PMIX exchange (meaning the XML document defined the PMIX NIEM IEPD) during transmission as well as end-to-end encryption of the content of the actual core PMIX request and response
- Message level encryption is performed in accordance with the GRA, which specifies the OASIS Basic Security Profile using WS-Security with XML encryption using NIST Advanced Encryption Standard (256 bit)

Public Key Infrastructure

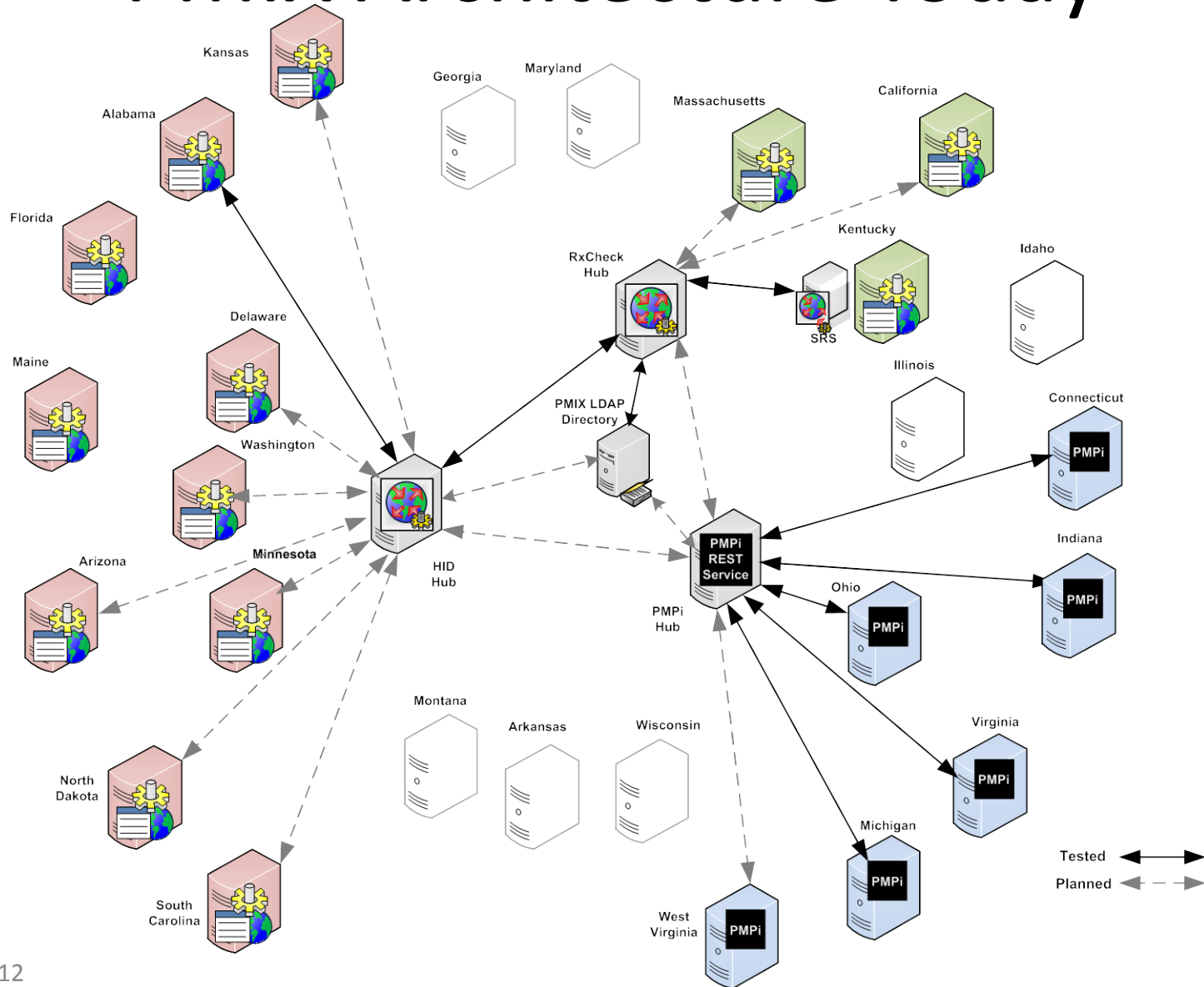
- PKI is based on digital certificates with public and private keys
- Certificates are used for both transport level and message level security
- PMIX PKI supports X.509 certificate use and management including certificate revocation
- Shared infrastructure to support certificate/key management capabilities and basic directory services

PMIX Directory

- X.509 certificate management as well as PMP contact and service requirement information
- Record for each participating PMP which will include the certificate w/public key, PMP contact information, authorized requesting entities, authorized disclosing entities and requestor roles
- Available through secure connection to all hubs and PMPs
- Secure access and update using the Lightweight Directory Access Protocol (LDAP)



PMIX Architecture Today



REST Interoperability

- PMIX Architecture is based on 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

REST Interoperability

