RxCheck

Prescription Monitoring Program

Information Exchange
RxCheck State Routing Service

SRS Docker Deployment

&

Setup Guide for HCE

IJIS Institute

BJA
Bureau of Justice Assistance
U.S. Department of Justice

Contents

Figures

Introduction

Overview

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 concurrent requests can be issued by an HCE system to provide prescription drug histories from as many states as needed.

Specifications

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. Common NIEM exchange data and metadata,
2. Hub connections and
3. End-to-end security (including encryption key management).

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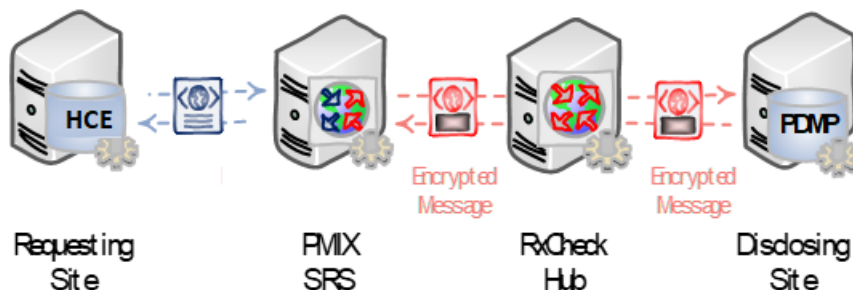

Figure 1: PMIX Overview

RxCheck / SRS Connection

The PMIX service interface utilizes standards-based web services to facilitate communication through hubs to the endpoint systems. The following diagram shows an HCE system connecting to the PMIX RxCheck Hub via the PMIX State Routing Service (SRS). The PMIX SRS enables HCEs to "offload" PMIX functionality such as PMIX compliant service hosting, request/response message validation, role-based site authorization, full message routing and message translation.

Figure 2: PMIX RxCheck/SRS Architecture Detail
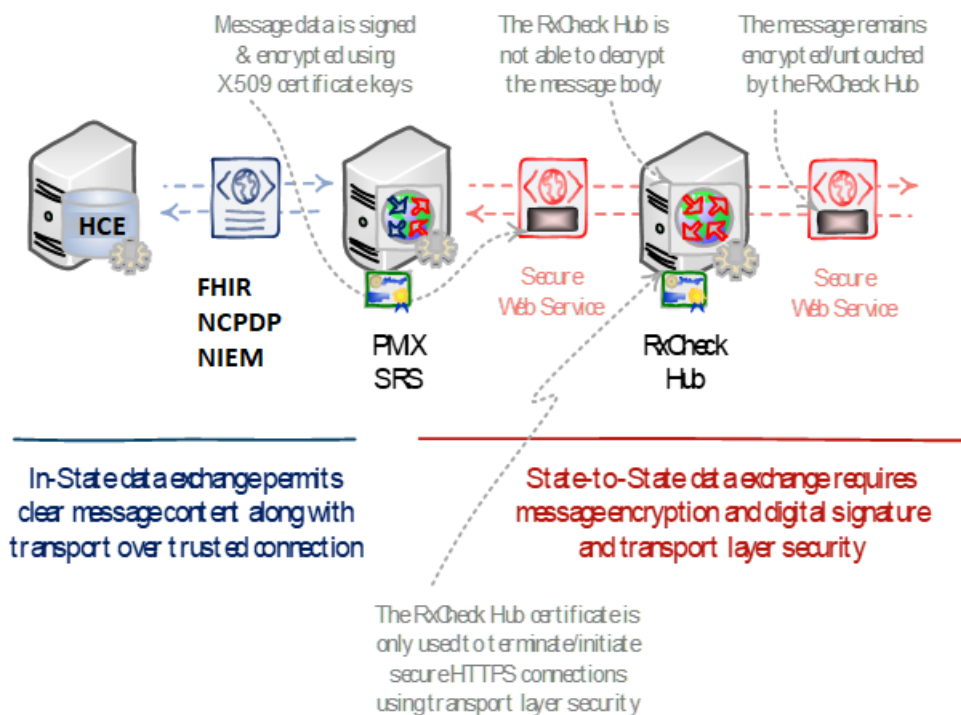
The web service interfaces are protected by a combination of Transport Layer Security (TLS), which provides transport-level encryption and service authentication and message-level encryption, which ensures message privacy and integrity. The PMIX SRS handles all X.509 certificate-based message encryption/decryption involved in communicating over the PMIX secure web service interface.

Installation Procedure

The steps listed below are intended to provide HCE technical staff with general guidance to augment the information in the PMIX SSP documentation. Please note that implementation may vary depending on HCE's computer system. The IJIS Institute is available to provide technical assistance as needed.

Step 1: Download Package and Prepare the pre-installation checklist
- Download the file ***rxcheck-srs-hce-docker-3.1.zip*** from
  http://builds.rxcheck.org/SRS/v3.1/public_final/hce/
- Fill out and prepare the pre-installation checklist defined in Appendix A

Step 2: Network Preparation
- Configure and validate network connectivity between the State Routing Service and the two endpoint systems:
  - "External" - RxCheck Central Hub
  - "Internal" – HCE System
- The following steps, which are based on a typical configuration process, reflect general network configuration guidance and may need to be tailored to apply to specific environments.
  - **Network Access**
    - Enable the SRS to access the RxCheck Hub
      - Provide the PMIX RxCheck Administrator with the SRS external IP address so that they can configure the RxCheck Hub network firewall
      - Configure the networking components:
        - Add the necessary network address translation (NAT)
        - Add the routing rules needed to route outbound traffic.
        - If necessary, add any outbound firewall rules.
        - If the external IP address is "virtual", ensure any added routing provisions are implemented.

  - **Domain Name Resolution**
    - RxCheck Hub
      - Identity the domain name and network address
      - Ensure the SRS can resolve the domain name to the IP

The following outline provides instructions (On Windows Server) to help acquire and install the X.509 certificate for the PMIX SRS:

- Generate SSL/TLS Custom CSR self-signed certificate (if necessary)
    - Open Microsoft Powershell Window (in Administrator mode)
    - Create the certificate using the following command that will be placed under the local machine and export the PFX and CER version of the certificate to be used in the installer

        ### Create a Self-Signed Certificate

        PS > New-SelfSignedCertificate -Subject "CN=_SITEID_" -KeyLength 2048 -NotBefore (Get-Date) -NotAfter (Get-Date).AddMonths(36) -CertStoreLocation "cert:\LocalMachine\My"

        ```
        PS C:\WINDOWS\system32> New-SelfSignedCertificate -Subject "CN=KK" -KeyLength 2048 -NotBefore (Get-Date) -NotAfter (Get-Date).AddMonths(36)  -CertStoreLocatio
        n "cert:\LocalMachine\My"


          PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

        Thumbprint                                Subject
        ----------                                -------
        8F8747235C7EFF84E04410D5ED1AB18F21C5556D  CN=KK
        ```

        Note: Copy the certificate Thumbprint to be used in the following steps.

        ### Export the Private Key of the Certificate in PFX format

        PS > $mypwd = ConvertTo-SecureString -String "**password**" -Force -AsPlainText

        PS > Get-ChildItem -Path cert:\localMachine\my\[CERTIFICATE-THUMBPRINT] | Export-PfxCertificate -FilePath e:\temp_SITEID_.pfx -Password $mypwd

        ```
        PS C:\WINDOWS\system32> $mypwd = ConvertTo-SecureString -String "kkpass" -Force -AsPlainText
        PS C:\WINDOWS\system32> Get-ChildItem -Path cert:\localMachine\my\8F8747235C7EFF84E04410D5ED1AB18F21C5556D | Export-PfxCertificate -FilePath e:\temp\KK.pfx -P
        assword $mypwd


            Directory: E:\temp

        Mode                LastWriteTime         Length Name
        ----                -------------         ------ ----
        -a----        7/12/2018   6:29 PM           2589 KK.pfx
        ```

        ### Export the Public Key of the Certificate in DER format

        PS > Get-ChildItem -Path cert:\localMachine\my\[CERTIFICATE-THUMBPRINT] | Export-Certificate -Type CERT -FilePath "e:\temp_SITEID_.cer"

        ```
        PS C:\WINDOWS\system32> Get-ChildItem -Path cert:\localMachine\my\8F8747235C7EFF84E04410D5ED1AB18F21C5556D | Export-Certificate -Type CERT -FilePath 'e:\temp'
        KK.cer'
        PS C:\WINDOWS\system32>

            Directory: E:\temp

        Mode                LastWriteTime         Length Name
        ----                -------------         ------ ----
        -a----        7/12/2018   6:35 PM            760 KK.cer
        ```

    Note: You can also create a self-signed certificate using OpenSSL tool.

Step 4: Install Application

Install RxCheck SRS Package

- Unzip the **rxcheck-srs-hce-docker-3.1.zip** file to a folder.

  $ unzip rxcheck-srs-hce-docker-3.1.zip

Configure RxCheck SRS Docker Version

- Change the folder to the home folder

  $cd /home/rxcheck/rxcheck-srs-hce-docker-3.1

- Edit *docker-compose.yml* using an editor like Notepad++ or VI and replace the variables with values listed in the table.

Variable Name	Description
_DOCKER_TAG_	Version tag provided by RxCheck

Configure RxCheck SRS

- Change the folder to "config" folder

  $cd /home/rxcheck/rxcheck-srs-hce-docker-3.1/config

- Copy the PFX file into the "config" folder that was created in Step 3 of the installation.
- Rename *application.yml.template.XXX* file to *application.yml* file
- Edit *application.yml* using an editor like vi or vim and replace the variables with values listed in the table.

Variable Name	Description
APIKEY	API Key provided by RxCheck
SITEID	Site Id provided by RxCheck
_KEYSTORE_FILE_	PFX file name copied to the config folder
KEYPASSWORD	Password for KeyEntry (entered in Step 3)
STOREPASSWORD	Password for the KeyStore (entered in Step 3)

Step 5: Complete SRS Configuration on the RxCheck Console

- Login to RxCheck Console using the credentials provided.
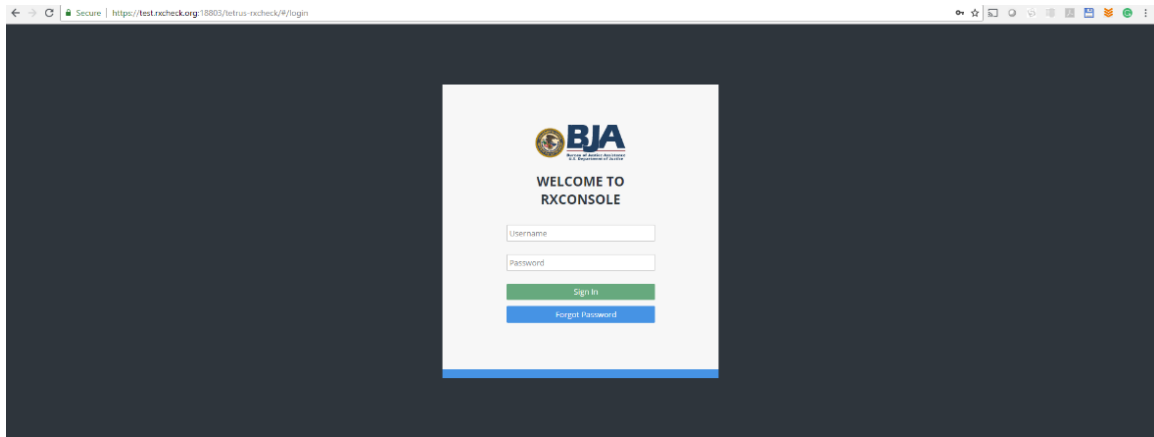
- Setup SRS Outbound Sender Endpoint Security

Set the username and password to secure the endpoints. Leave the fields blank if HTTP Basic Authentication is not required.

Field Name	Description	Default Value
Outbound Username	HTTP Basic Access Authentication Username	
Outbound Password	HTTP Basic Access Authentication Password	

- Upload SRS Public Key to RxCheck Console PKI database

- o Enter Subject name used in Step 3 in the **Private Key Subject** field. Eg: TT
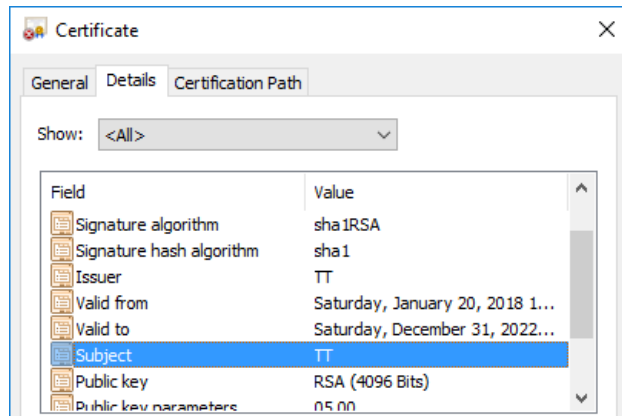
- o Upload the public key. The certificate must be in DER encoded binary X.509 (.cer) format.

- Click "Save" button on the Site Configurations page.

Step 6: Starting RxCheck SRS

Note: To access and start the container via Docker image download, you'll need specific registry credentials—both a username and password. Get in touch with the RxCheck technical team to secure the required registry login information.

- Change the folder to the home folder

    $cd /home/rxcheck/rxcheck-srs-hce-docker-3.1

- Login to RxCheck container registry.

    $docker login -u <username> -p <password> rxcheck.azurecr.us

- Start the RxCheck SRS container image.

    $docker compose up -d

- Open the service URL below in your browser to confirm that the services are operational.

PMIX2 Outbound SRS	http://localhost:8080/rxoutbound/service/pmix2?wsdl

Note: Replace localhost with the machine name or DNS name associated with the SRS server

Step 7: Conduct Simulator Testing

- Perform a simulator test in which an HCE sends a message to the simulator with state code "QQ" and the simulator can respond back with a message.

Step 8: Integration Testing

- Perform integration testing with an exchange partner; the request will flow from the requesting-state PDMP application to the requesting-state SRS (Option 1) *or* the Custom Proxy (Option 2), to the RxCheck Hub, to the disclosing-state PDMP application (note: the response will follow the same steps in the reverse direction)

Appendix A: Pre-Installation Checklist

The following architecture diagram and pre-installation checklist table will orient the deployment team by identifying important system information prior to the software installation and configuration.

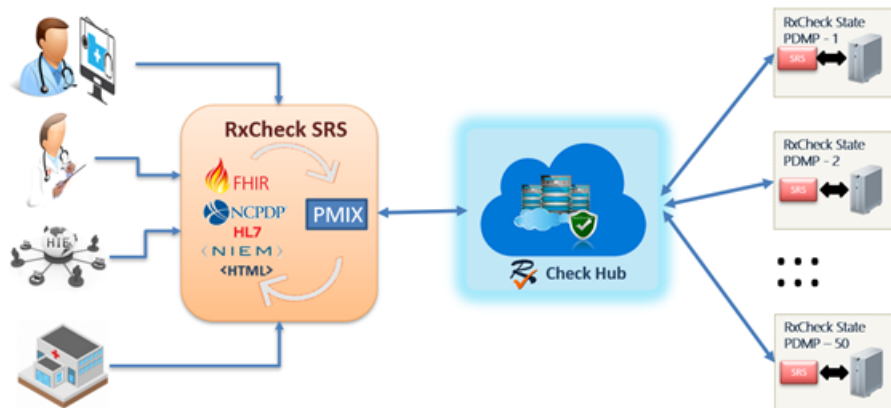| Server Requirements	
Server Type	Virtual Machine or Physical Server
Processor Cores	2
Memory (Free)	6GB for the SRS process
Disk Space (Free)	80GB
Operating System	Linux

Figure 2: Typical RxCheck Integration Architecture Overview

ID	Description	Value
1.	SRS Outbound Host Base URL Address	*http://_____:8080/rxoutbound/service/pmix2*
1.1	Domain Name:	
1.2	IP Address:	
2.	RxCheck Hub Service Host URL Address	*https://uat.rxcheck.org:18803/RxCheck/hub*
2.1	Domain Name:	*uat.rxcheck.org*
2.2	IP Address:	*40.71.234.80*

Table 1: Pre-Installation Checklist (UAT)

ID	Description	Value
1.	SRS Outbound Host Base URL Address	*http://_____:8080/rxoutbound/service/pmix2*

1.1	Domain Name:	
1.2	IP Address:	
2.	RxCheck Hub Service Host URL Address	*https://prod.rxcheck.org:18803/rxcheck/hub*
2.1	Domain Name:	*prod.rxcheck.org*
2.2	IP Address:	*52.227.138.130*

Table 2: Pre-Installation Checklist (PROD)