RxCheck

Prescription Monitoring Program Information Exchange

RxCheck State Routing Service

SRS Installation & Setup Guide for PDMP

Delivery On:	**Jun 2023**
Version:	**3.1beta**
Prepared By:	**IJIS Institute**
	TetrusCorp
Sponsored By:	**Bureau of Justice Assistance**

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 requests can be issued in sequence by a state PMP 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 basic 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.
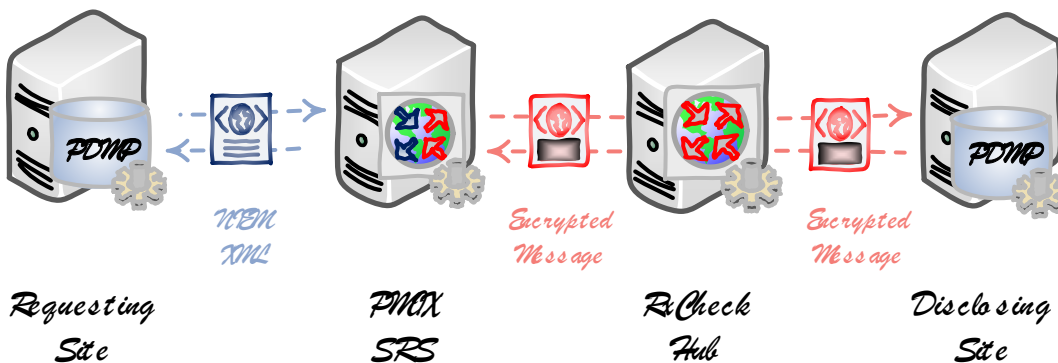

Figure 1: PMIX Overview

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 a state PDMP system connecting to the PMIX RxCheck Hub via the PMIX State Routing Service (SRS). The PMIX SRS enables PDMPs to "offload" PMIX functionality such as PMIX compliant service hosting, request/response message validation, role-based site authorization, full message routing and message translation.
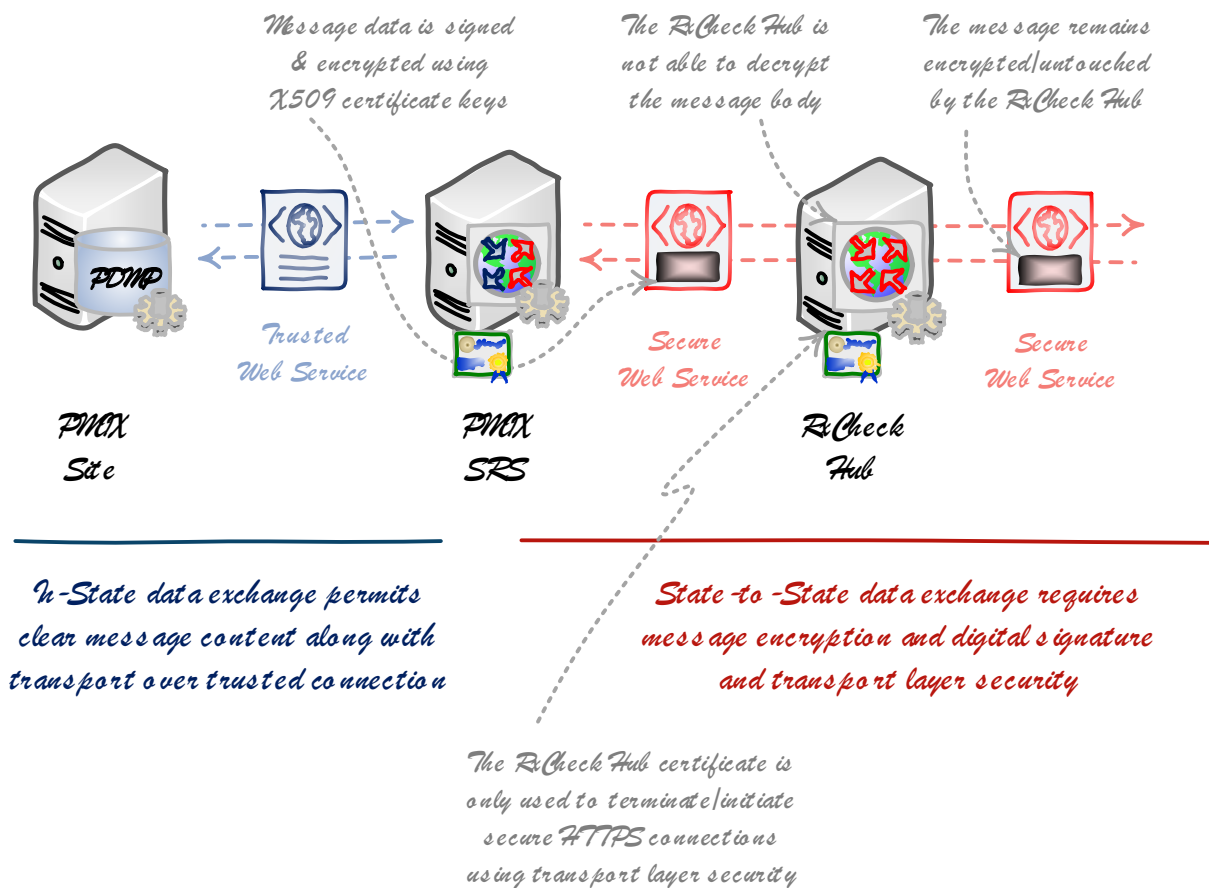

Figure 2: PMIX RxCheck/SRS Architecture Detail

The web service interfaces are protected by a combination of secure socket layer, 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 PDMP technical staff with general guidance to which serves to augment the information contained in the PMIX SSP documentation. Please note that implementation may vary depending upon a PDMP'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 following files from http://builds.rxcheck.org/SRS/v3.1/beta/
    Windows: ***rxcheck-srs-pdmp-3.1-b\<build number>beta.zip***
    Linux: ***rxcheck-srs-pdmp-3.1-b\<build number>beta-linux.zip***
- Download and Install latest JDK 11 version from AdoptOpenJDK (Linux Only)
    https://adoptium.net/

    Add the following environment variables to the account .profile :

    export JAVA_HOME=/opt/jdk-11.0.19+17
    export PATH=$JAVA_HOME/bin

- 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" – PDMP 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 they can configure the IJIS 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
  - Enable the SRS to access the State PDMP
    - 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
  - Enable the RxCheck Hub to access the SRS
    - Provide the PMIX RxCheck Administrator with the SRS externally accessible IP address used to connect to the listener
    - Configure the networking components:
      - Add the necessary inbound 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 is able to resolve the domain name to the IP
  - State PMP System
    - Identity the domain name and network address
    - Ensure the SRS is able to resolve the domain name to the IP

Step 3: Security

The following outline provides instructions (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 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
```
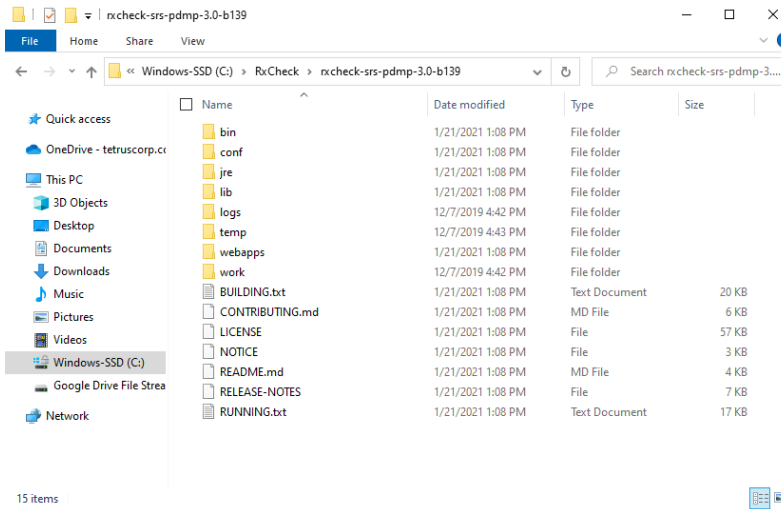
Step 4: Install Application

Install RxCheck SRS Package

- Unzip ***rxcheck-srs-pdmp-3.1-b<build number>beta.zip*** file to a folder.

    <u>Windows:</u>

Linux:

$ unzip rxcheck-srs-pdmp-3.1-b<build number>beta-linux.zip

- Open command prompt and change directory to "**bin**" folder

Windows:

c:\> cd   c:\rxcheck\ rxcheck-srs-pdmp-3.1-b<build number>\bin
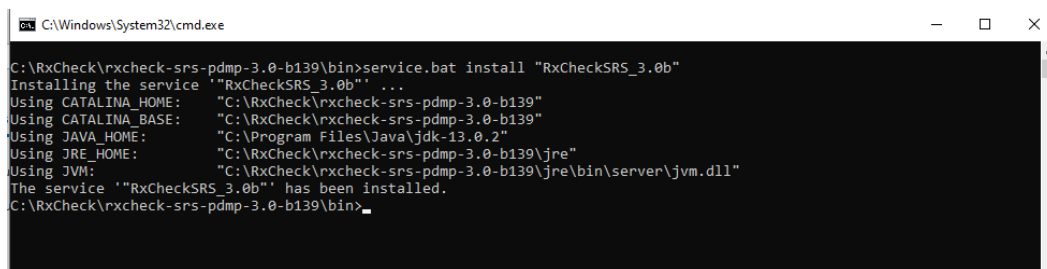
Linux:

$cd /home/rxcheck/ rxcheck-srs-pdmp-3.1-b<build number>-linux/bin

$chmod +x *.sh

- Install RxCheck SRS 3.0 as Windows Service by executing below command. (Windows Only)

Windows:

c:\rxcheck\ rxcheck-srs-pdmp-3.1-b<build number>\bin>service.bat install "RxCheckSRS_3.0"

Configure RxCheck SRS

- Change the folder to "conf" folder

    Windows:

    c:\>cd c:\rxcheck\rxcheck-srs-pdmp-3.1-b<build number>\conf

    Linux:

    $cd /home/rxcheck/rxcheck-srs-pdmp-3.1-b<build number>-linux/conf

- Rename *application.yml.template.XXX* file to *application.yml* file

    Note: Use **application.yml.template.dev** *for beta release*

- Edit *application.yml* using an editor like Notepad++ or VI 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
_FULLPATH_KEYSTORE_FILE_	Full path to PFX certificate file containing the Private Key that was created in Step 3 of the installation.
KEYPASSWORD	Password for KeyEntry (entered in Step 3)
STOREPASSWORD	Password for the KeyStore (default is the same password as key password, entered in Step 3)

Step 5: Complete SRS Configuration on the RxCheck Console

UAT Console URL : https://test.rxcheck.org:18803/tetrus-rxcheck/

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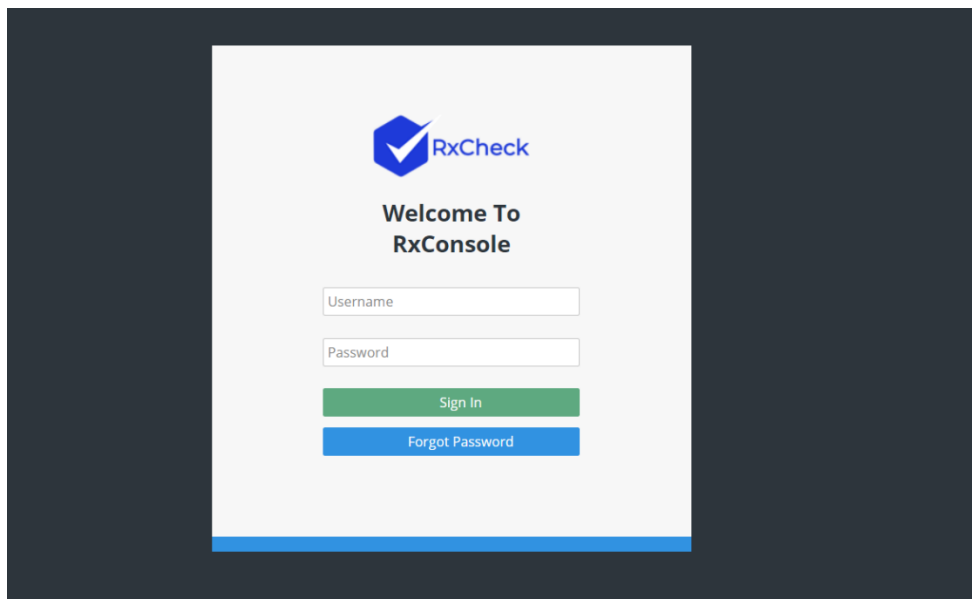
- Setup SRS Outbound Sender Endpoint Security

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	

- Setup SRS Inbound Sender Endpoint

Enter the SRS inbound configuration details for the RxCheck hub to connect to the Inbound SRS service

Field Name	Description	Default Value
Protocol	Select http or https	https

Telephone: (850) 481-PDMP (7367) | Email: pdmpttac@iir.com | Website: www.pdmpassist.org

Domain	Enter a domain name for the SRS Inbound Service instance (Optional – If no domain is specified the system would use the IP Address)	
Port Number	Enter the port number for the SRS inbound service instance (This would be the external port number if there is a firewall NAT)	8443
IP Address	IP address of the server or the external gateway IP address for the SRS inbound Service instance	
IEPD	Select the PMIX version	PMIX2
Inbound URL	The inbound SRS secure URL	https://.../rxinbound/service/pmix2
Inbound Username	HTTP Basic Access Authentication Username	
Inbound Password	HTTP Basic Access Authentication Password	

- Setup PDMP Application Endpoint

Field Name	Description	Default Value
Protocol	Select http or https	
Domain	Enter a domain name for the PDMP Service instance (Optional – If no domain is specified the system would use the IP Address)	
Port Number	Enter the port number for PDMP service instance	
IP Address	IP address of the server of the PDMP service instance	
URL Path	This is the relative path of the application URL suffix	
PDMP Username	HTTP Basic Access Authentication Username	
PDMP Password	HTTP Basic Access Authentication Password	

- Upload SRS Public Key to RxCheck Console PKI database
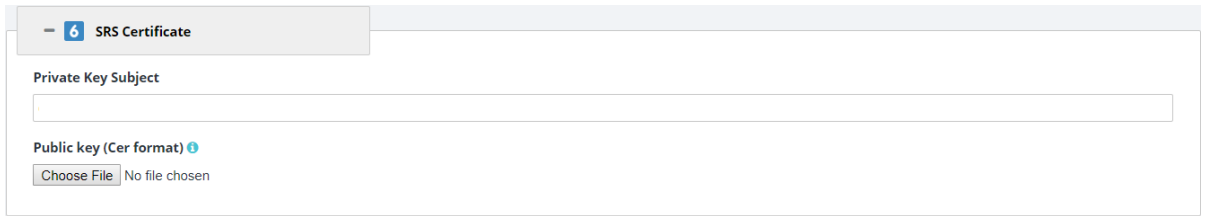
- o Enter Subject name used in Step 3 in the ***Private Key Subject*** field. Eg: TT
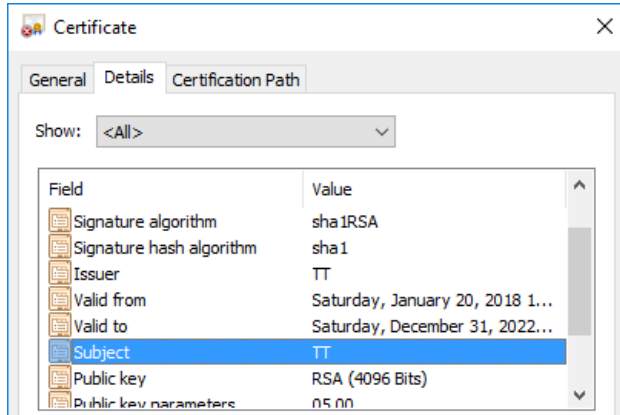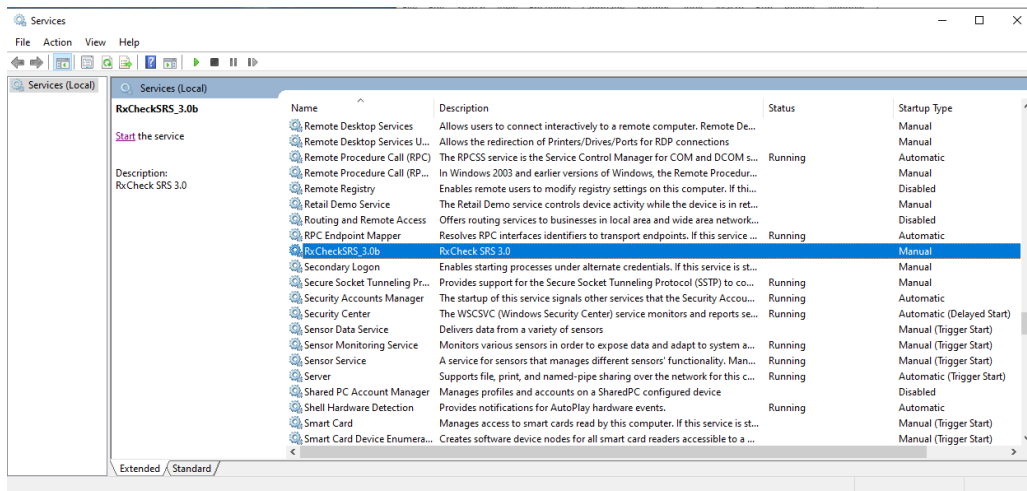

- o Upload the public key. The certificate must be in DER encoded binary X.509 (.cer) format.

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

Step 6: Starting RxCheck SRS 3.1

- Open Windows Services Manager. To open Windows Services, Run *services.msc* to open the Services Manager. Here you will be able to start, stop, disable, delay Windows Services. (Windows Only)

- Find Service "**RxCheckSRS_3.1b**" and change the Start Type to "*Automatic*" (Windows Only)
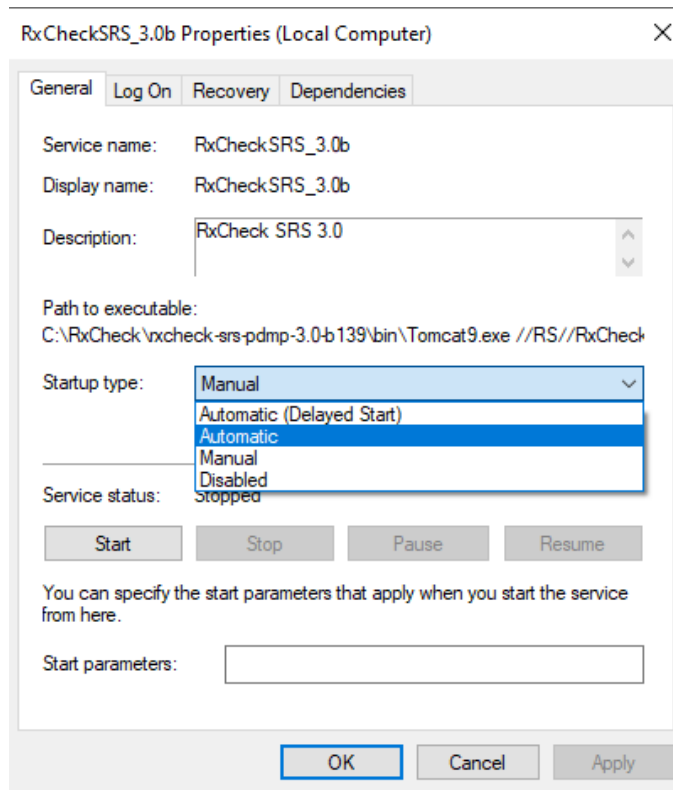
- Right click on the service name and "Start" the service. (Windows Only)
- Run the **startup.sh** from **bin** folder to start the SRS process (Linux Only)

- Open the following Service URLs in a browser to verify the services are running

PMIX Inbound SRS	https://localhost:8443/rxinbound/service/pmix2?wsdl
PMIX 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 State PDMP sends a message to the simulator with state code "GG" 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.
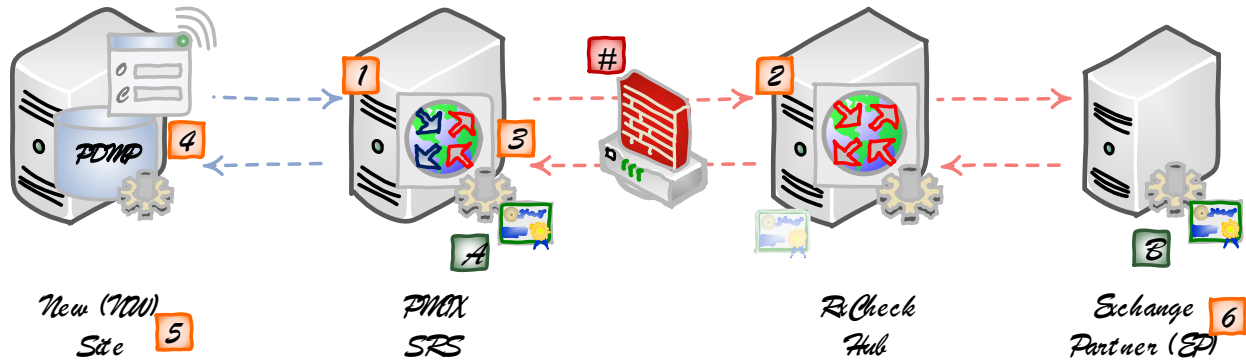

Figure 3: PMIX RxCheck/SRS Architecture Detail

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://test.rxcheck.org:18803/RxCheck/hub*
2.1	Domain Name:	*test.rxcheck.org*
2.2	IP Address:	*13.90.244.183*
3.	SRS Inbound Host Base URL Address	https://_____:8443/rxinbound/service/pmix2
3.1	Domain Name:	
3.2	IP Address:	
4.	New site PDMP Application URL Address	
4.1	Domain Name:	
4.2	IP Address:	
5.	New site unique qualifier (NW)	
6.	Exchange partner unique qualifier (EP)	
A.	The new site's PMIX SRS certificate	
B.	The partner site's PMIX SRS certificate	
#	Network Configuration (Firewall, Router)	

Table 1: Pre-Installation Checklist (UAT)

Telephone: (850) 481-PDMP (7367) | Email: pdmpttac@iir.com | Website: www.pdmpassist.org

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/pmix2*
2.1	Domain Name:	*prod.rxcheck.org*
2.2	IP Address:	*52.227.138.130*
3.	SRS Inbound Host Base URL Address	https:// _____:8443/rxinbound/service/pmix2
3.1	Domain Name:	
3.2	IP Address:	
4.	New site PDMP Application URL Address	
4.1	Domain Name:	
4.2	IP Address:	
5.	New site unique qualifier (NW)	
6.	Exchange partner unique qualifier (EP)	
A.	The new site's PMIX SRS certificate	
B.	The partner site's PMIX SRS certificate	
#	Network Configuration (Firewall, Router)	

Table 2: Pre-Installation Checklist (PROD)

Appendix B
Customizing SRS

1. *Changing Server Ports*

   By default, the RxCheck SRS service runs on ports 8080 (http) and 8433 (https). If necessary, different ports can be configured in *server.xml* file located in

   c:\rxcheck\rxcheck-srs-pdmp-3.1-b<build number> \conf folder.

   o For HTTP port, modify the below XML element. Change the port 8080 to a desired port.

   `<Connector port="`**`8080`**`" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443" />`

   o For HTTPS port, modify the below XML elements. Change the port 8443 to a desired port.

   `<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="`**`8443`**`" />`

   `<Connector SSLEnabled="true" clientAuth="false" keystoreFile="conf/keystore.jks" keystorePass="rxchecksrs" maxThreads="150" port="`**`8443`**`" protocol="HTTP/1.1" scheme="https" secure="true" sslProtocol="TLS"/>`

   `<Connector port="8009" protocol="AJP/1.3" redirectPort="`**`8443`**`" />`

2. *Changing Server Certificate*

   A default self-signed certificate is included in the package for SSL/TLS transport layer. This <u>must</u> be replaced by either a new self-signed certificate or a certificate purchased from a CA in the production environment.

   o Creating a self-signed certificate.

   `C\>keytool -genkey -keyalg RSA -alias selfsigned -keystore `**`keystore.jks`**` -storepass `**`rxchecksrs`**` -validity 720 -keysize 2048`

   o Copy the self-signed certificate keystore keystore.jks file to *c:\rxcheck\rxcheck-srs-pdmp-3.1-b<build number>\conf folder*

3. *Separate instances for Outbound and Inbound Services*

   If desired, separate instances of Outbound and Inbound SRS's can be installed on the same server or on a different sever by following the steps 1 through 6. This might be required due to the local network security requirements or for achieving higher performance throughput.

   Based on the type of service you are installing, delete the other .war file from *c:\rxcheck\rxcheck-srs-pdmp-3.1-b<build number>\webapps folder.*

4. *Increasing JVM memory*

   By default, the Java process heap size is set for minimum 3072MB and maximum 6144MB. This must be changed to higher memory for production environment.

Memory parameters can be changed in service.bat file located in c*:\rxcheck\rxcheck-srs-pdmp-3.1-b<build number> \bin.* You may need to uninstall and reinstall the service.
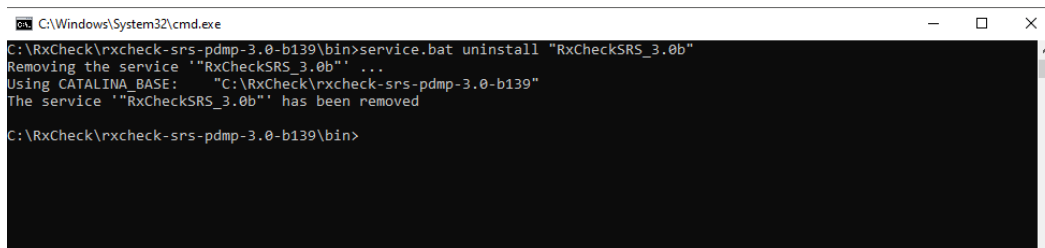
if "%JvmMs%" == "" set JvmMs=__3072__

if "%JvmMx%" == "" set JvmMx=__6144__

5. *Uninstalling RxCheck SRS*

To uninstall SRS process, execute command.

c:\rxcheck\rxcheck-srs-pdmp-3.1-b<build number>\bin>service.bat uninstall "RxCheckSRS_3.1b"

Telephone: (850) 481-PDMP (7367) | Email: pdmpttac@iir.com | Website: www.pdmpassist.org