RxCheck

# Prescription Monitoring Program

# Information Exchange

## *RxCheck State Routing Service*

# SRS Installation & Setup Guide for HCE

| | |
|---|---|
| Delivery On: | **Dec 2021** |
| Version: | **3.0 <draft>** |
| Prepared By: | **IJIS Institute**<br>**Tetrus Corp** |
| Sponsored By: | **Bureau of Justice Assistance** |

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.

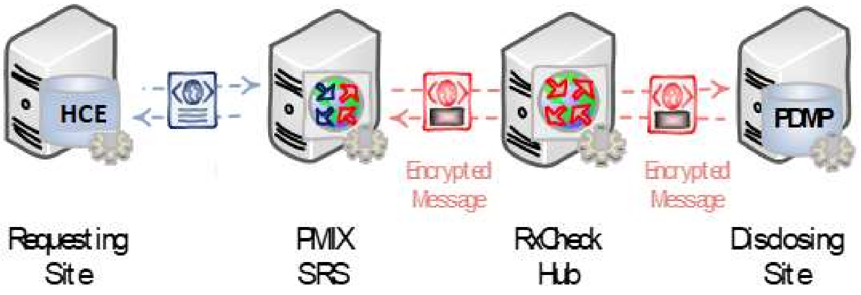
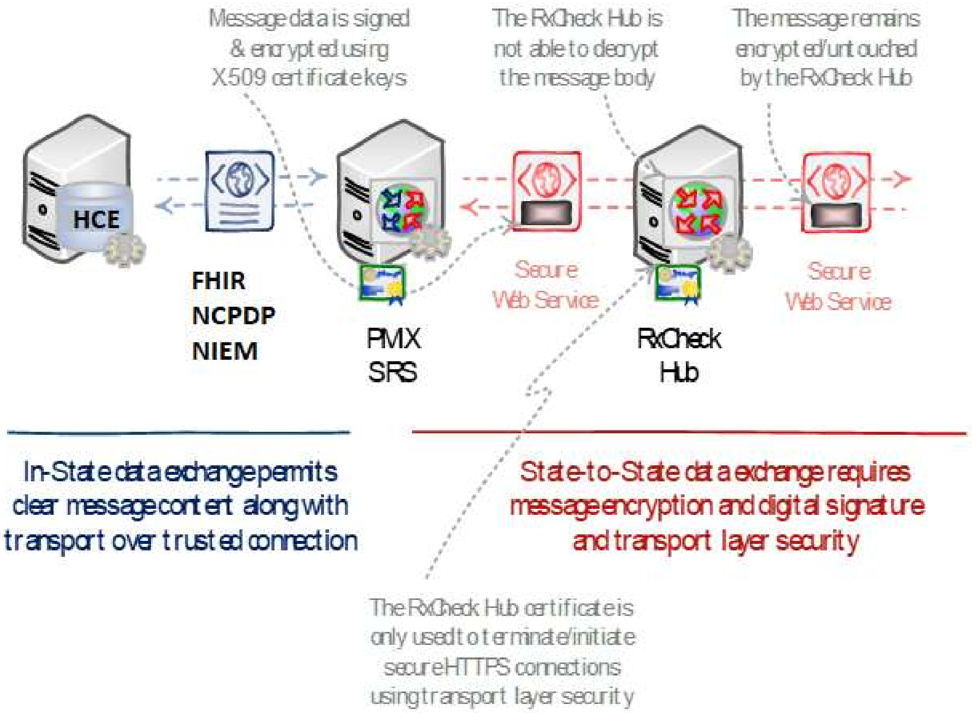


*Figure 1: PMIX Overview*

## 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.



Message data is signed & encrypted using X509 certificate keys

The RxCheck Hub is not able to decrypt the message body

The message remains encrypted/untouched by the RxCheck Hub

In-State data exchange permits clear message content along with transport over trusted connection

State-to-State data exchange requires message encryption and digital signature and transport layer security

The RxCheck Hub certificate is only used to terminate/initiate secure HTTPS connections using transport layer security

*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 which serves to augment the information contained in the PMIX SSP documentation. Please note that implementation may vary depending upon 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 following files from http://builds.rxcheck.org/SRS/v3.0/public_final/hce/

  Windows: ***rxcheck-srs-hce-3.0-b<build number>.zip***
  Linux: ***rxcheck-srs-hce-3.0-b<build number>-linux.zip***

- Download and Install latest JDK 11 from AdoptOpenJDK (Linux Only)

  https://adoptopenjdk.net/

  Add following environment variables to the account .profile :

  ```
  export JAVA_HOME=/opt/jdk-11.0.6+10
  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" – 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

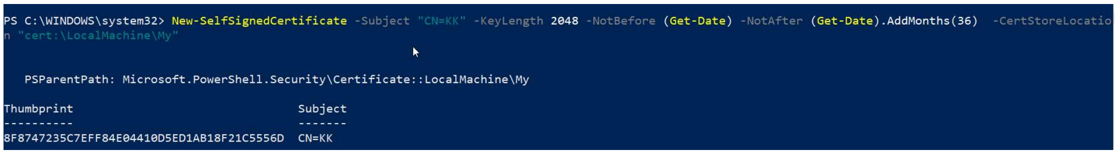
## Step 3: Security

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"



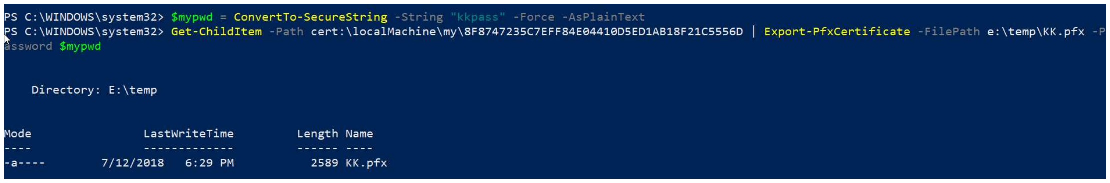
```
PS C:\WINDOWS\system32> New-SelfSignedCertificate -Subject "CN=KK" -KeyLength 2048 -NotBefore (Get-Date) -NotAfter (Get-Date).AddMonths(36)  -CertStoreLocatio
n "cert:\LocalMachine\My"


   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

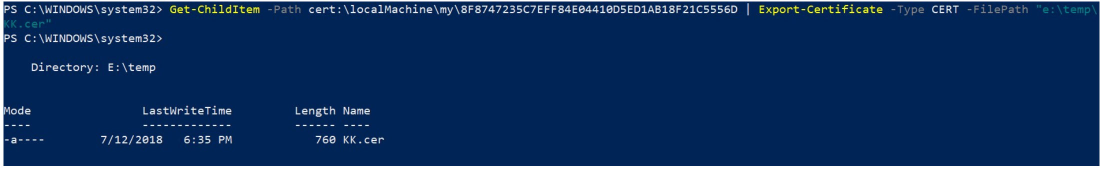
PS > Get-ChildItem -Path cert:\localMachine\my\[CERTIFICATE-THUMBPRINT] | Export-PfxCertificate -FilePath e:\temp_SITEID_.pfx -Password $mypwd



```
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
```

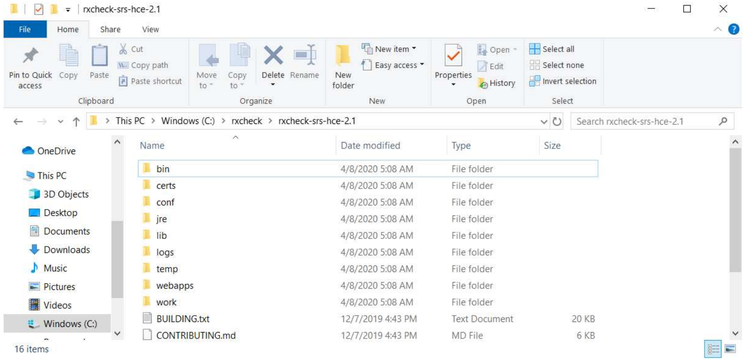
Note: You can also create a self-signed certificate using OpenSSL tool.

## Step 4: Install Application

### Install RxCheck SRS Package

- Unzip ***rxcheck-srs-hce-3.0-b<build number>.zip*** file to a folder.

  Windows:



| Name | Date modified | Type | Size |
|---|---|---|---|
| bin | 4/8/2020 5:08 AM | File folder | |
| certs | 4/8/2020 5:08 AM | File folder | |
| conf | 4/8/2020 5:08 AM | File folder | |
| jre | 4/8/2020 5:08 AM | File folder | |
| lib | 4/8/2020 5:08 AM | File folder | |
| logs | 4/8/2020 5:08 AM | File folder | |
| temp | 4/8/2020 5:08 AM | File folder | |
| webapps | 4/8/2020 5:08 AM | File folder | |
| work | 4/8/2020 5:08 AM | File folder | |
| BUILDING.txt | 12/7/2019 4:43 PM | Text Document | 20 KB |
| CONTRIBUTING.md | 12/7/2019 4:43 PM | MD File | 6 KB |

  Linux:

  ***$ unzip rxcheck-srs-hce-3.0-b<build number>-linux.zip***

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

  Windows:

  ***c:\> cd   c:\rxcheck\rxcheck-srs-hce-3.0-b<build number>\bin***

  Linux:

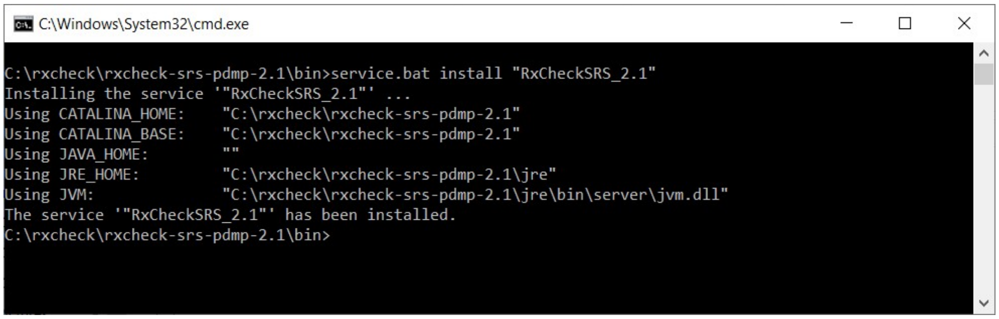
  ***$cd /home/rxcheck/rxcheck-srs-hce-3.0-b<build number>/bin***

  ***$chmod +x *.sh***

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

  Windows:

  ***c:\rxcheck\rxcheck-srs-hce-3.0-b<build number>\bin>service.bat install "RxCheckSRS_3.0b<build number>"***



```
C:\rxcheck\rxcheck-srs-pdmp-2.1\bin>service.bat install "RxCheckSRS_2.1"
Installing the service '"RxCheckSRS_2.1"' ...
Using CATALINA_HOME:    "C:\rxcheck\rxcheck-srs-pdmp-2.1"
Using CATALINA_BASE:    "C:\rxcheck\rxcheck-srs-pdmp-2.1"
Using JAVA_HOME:        ""
Using JRE_HOME:         "C:\rxcheck\rxcheck-srs-pdmp-2.1\jre"
Using JVM:              "C:\rxcheck\rxcheck-srs-pdmp-2.1\jre\bin\server\jvm.dll"
The service '"RxCheckSRS_2.1"' has been installed.
C:\rxcheck\rxcheck-srs-pdmp-2.1\bin>
```

### Configure RxCheck SRS

- Change the folder to “conf” folder

Windows:

***c:\> cd c:\rxcheck\rxcheck-srs-hce-3.0-b<build number>\conf***

Linux:

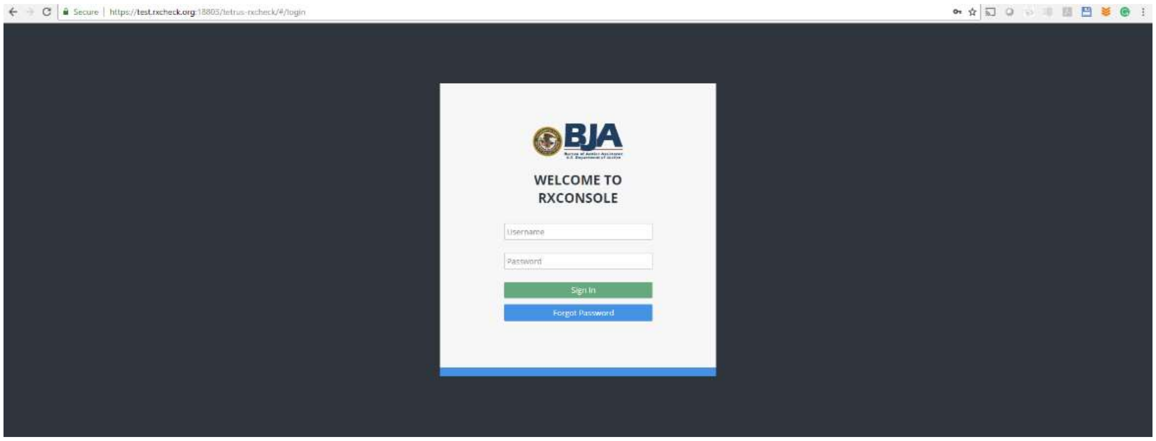
***$cd /home/rxcheck/rxcheck-srs-hce-3.0-b<build number>-linux/conf***

- Rename *application.yml.template.XXX* file to *application.yml* file
- Edit *application.yml* using an editor like Notepad++ or VI and replace the variables with values listed in the table.

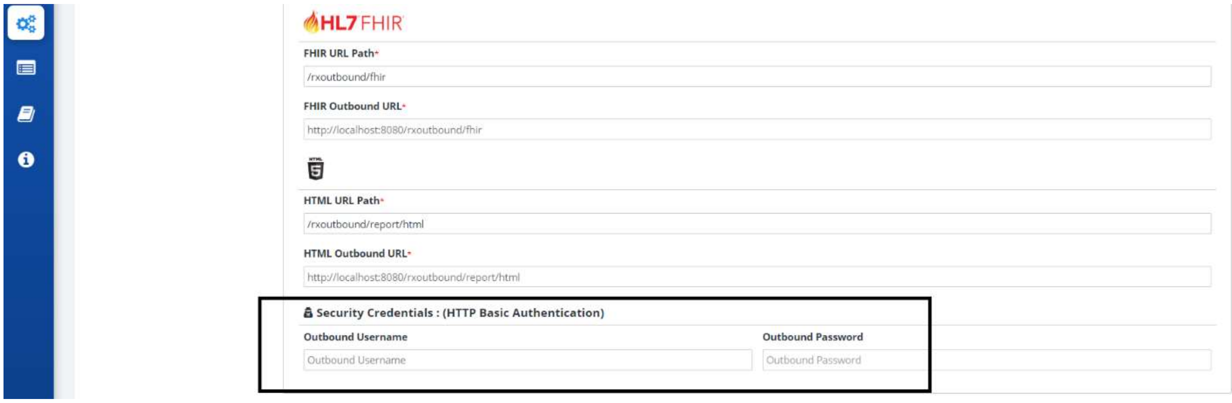
| **Variable Name** | **Description** |
|---|---|
| _APIKEY_ | API Key provided by RxCheck |
| _SITEID_ | Site Id provided by RxCheck |
| _FULLPATH_KEYSTORE_FILE_ | Full path to PFX certificate file containing the Private Key that was created in Step 3 of the installation. |
| _KEYPASSWORD_ | Password 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

- Login to RxCheck Console using the credentials provided.


Secure | https://test.rxcheck.org:18803/tetrus-rxcheck/#/login
BJA
WELCOME TO RXCONSOLE
Username
Password
Sign In
Forgot Password

- Setup SRS Outbound Sender Endpoint Security



HL7 FHIR

FHIR URL Path*

/rxoutbound/fhir

FHIR Outbound URL*

http://localhost:8080/rxoutbound/fhir

HTML URL Path*

/rxoutbound/report/html

HTML Outbound URL*

http://localhost:8080/rxoutbound/report/html

Security Credentials : (HTTP Basic Authentication)

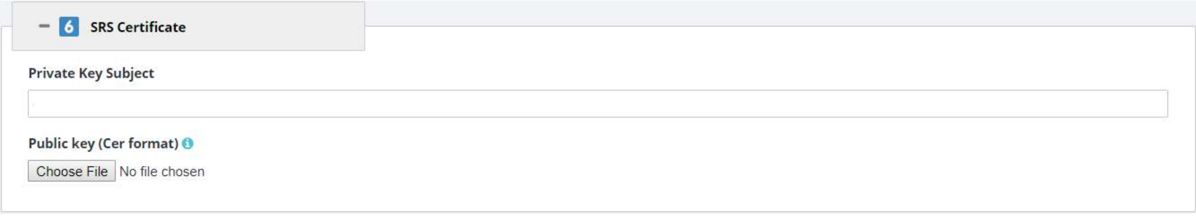
Outbound Username: Outbound Username

Outbound Password: Outbound Password

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

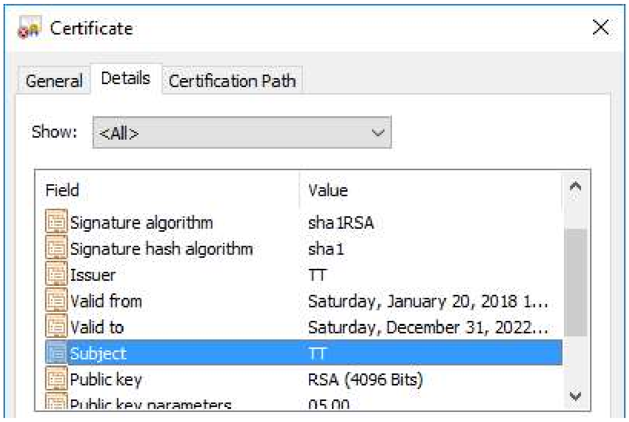


6 SRS Certificate

Private Key Subject

Public key (Cer format)

  - Enter Subject name used in Step 3 in the ***Private Key Subject*** field. Eg: TT



Certificate

Show: <All>

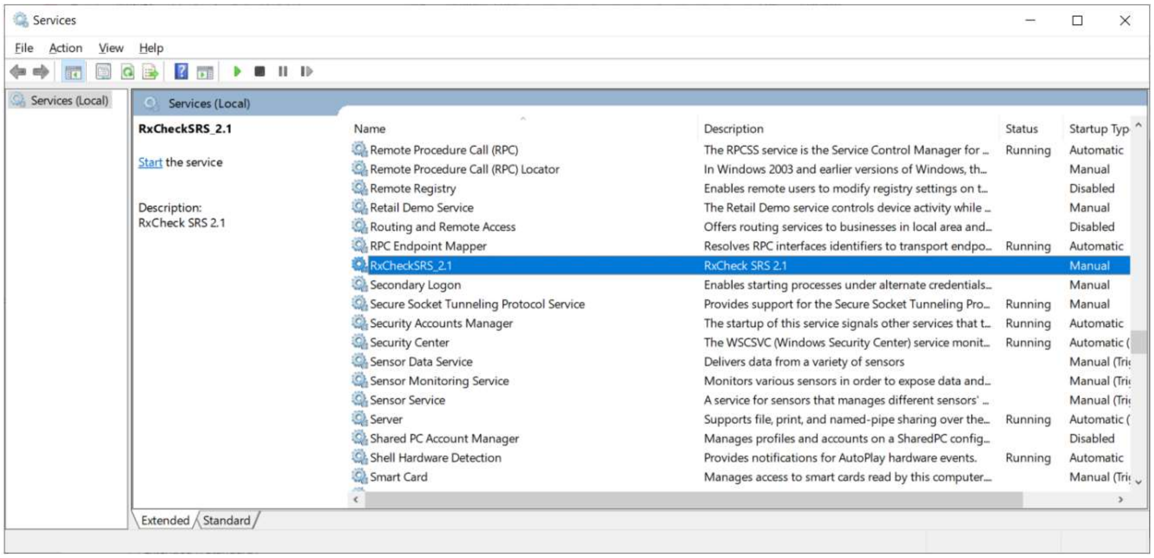
| Field | Value |
|---|---|
| Signature algorithm | sha1RSA |
| Signature hash algorithm | sha1 |
| Issuer | TT |
| Valid from | Saturday, January 20, 2018 1... |
| Valid to | Saturday, December 31, 2022... |
| Subject | TT |
| Public key | RSA (4096 Bits) |
| Public key parameters | 05 00 |

  - 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

- 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)



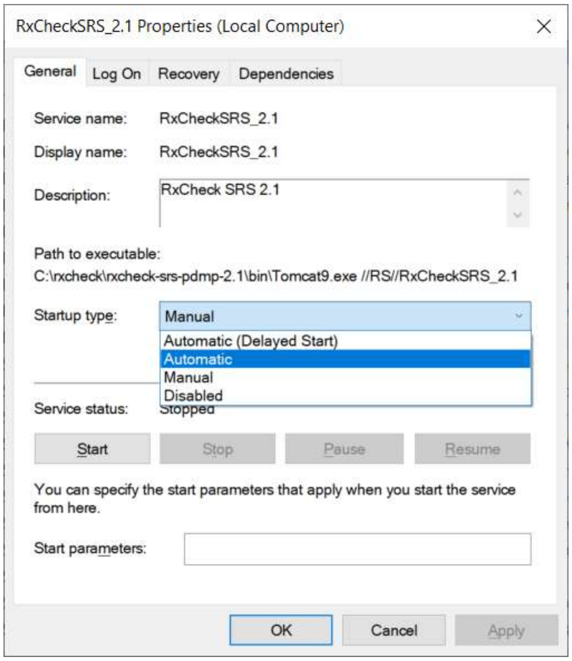
**RxCheckSRS_2.1**

Start the service

Description:
RxCheck SRS 2.1

| Name | Description | Status | Startup Typ |
|---|---|---|---|
| Remote Procedure Call (RPC) | The RPCSS service is the Service Control Manager for ... | Running | Automatic |
| Remote Procedure Call (RPC) Locator | In Windows 2003 and earlier versions of Windows, th... | | Manual |
| Remote Registry | Enables remote users to modify registry settings on t... | | Disabled |
| Retail Demo Service | The Retail Demo service controls device activity while ... | | Manual |
| Routing and Remote Access | Offers routing services to businesses in local area and... | | Disabled |
| RPC Endpoint Mapper | Resolves RPC interfaces identifiers to transport endpo... | Running | Automatic |
| RxCheckSRS_2.1 | RxCheck SRS 2.1 | | Manual |
| Secondary Logon | Enables starting processes under alternate credentials... | | Manual |
| Secure Socket Tunneling Protocol Service | Provides support for the Secure Socket Tunneling Pro... | Running | Manual |
| Security Accounts Manager | The startup of this service signals other services that t... | Running | Automatic |
| Security Center | The WSCSVC (Windows Security Center) service monit... | Running | Automatic ( |
| Sensor Data Service | Delivers data from a variety of sensors | | Manual (Tri |
| Sensor Monitoring Service | Monitors various sensors in order to expose data and... | | Manual (Tri |
| Sensor Service | A service for sensors that manages different sensors' ... | | Manual (Tri |
| Server | Supports file, print, and named-pipe sharing over the... | Running | Automatic ( |
| Shared PC Account Manager | Manages profiles and accounts on a SharedPC config... | | Disabled |
| Shell Hardware Detection | Provides notifications for AutoPlay hardware events. | Running | Automatic |
| Smart Card | Manages access to smart cards read by this computer... | | Manual (Tri |

- Find Service “***RxCheckSRS_3.0b<build number>***” and change the Start Type to “*Automatic*” (Windows Only)



Service name: RxCheckSRS_2.1

Display name: RxCheckSRS_2.1

Description: RxCheck SRS 2.1

Path to executable:
C:\rxcheck\rxcheck-srs-pdmp-2.1\bin\Tomcat9.exe //RS//RxCheckSRS_2.1

Startup type: Manual

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

- 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

| | |
|---|---|
| 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 a HCE 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.

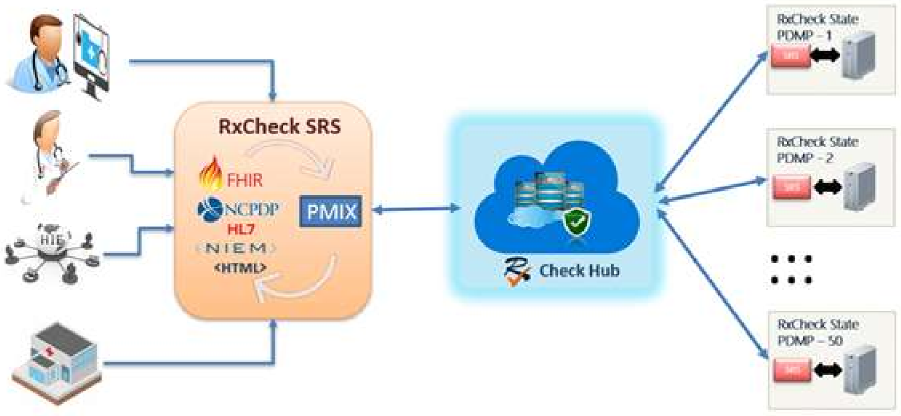


*Figure 2: Typical RxCheck Integration Architecture Overview*

| 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)*

# 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-hce-3.0-b<build number>\conf* folder.

   - 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" />
     ```

   - 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 must be replaced by either a new self-signed certificate or a certificate purchased from a CA in production environment.

   - Creating a self-signed certificate.

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

   - Copy the self-signed certificate keystore *keystore.jks* file to *c:\rxcheck\apache-tomcat-8.5.32\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-hce-3.0-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.

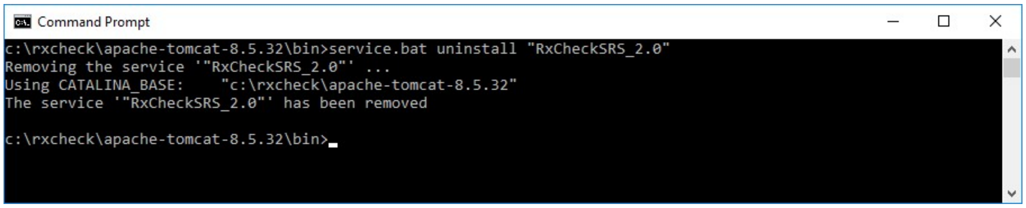
Memory parameters can be changed in setenv.bat (Windows) or setenv.sh (Linux) file located in the *bin* folder. You may need to uninstall and reinstall the service for changes to on windows server.

5. Uninstalling RxCheck SRS

   To uninstall SRS process, execute command.

   Windows:

   ***c:\rxcheck\rxcheck-srs-hce-3.0-b<build number>\bin>service.bat uninstall "RxCheckSRS_3.0b<build number>"***



```
c:\rxcheck\apache-tomcat-8.5.32\bin>service.bat uninstall "RxCheckSRS_2.0"
Removing the service '"RxCheckSRS_2.0"' ...
Using CATALINA_BASE:    "c:\rxcheck\apache-tomcat-8.5.32"
The service '"RxCheckSRS_2.0"' has been removed

c:\rxcheck\apache-tomcat-8.5.32\bin>
```