Public Key Infrastructure Procedure

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>December 26, 2019</td>
<td>Chief Information Security Officer</td>
</tr>
</tbody>
</table>

**Purpose of Procedure**
The purpose of this procedure is to define the procedures for uses and management of Public Key Infrastructure.

**What is Public Key Infrastructure (PKI)**
Public Key Infrastructure (PKI) is a system of processes, technologies, and policies that allows one to encrypt and sign data. Digital certificates that authenticate the identity of users, devices, or services can be issued to create secure connections for both public web pages and private systems, i.e. VPNs, WiFi, Wiki pages, and other services. PKIs secure messages from end-to-end; the message is encrypted at the sender’s device, and decryption is done at the recipient’s device. No third-party can intercept sensitive data with end-to-end encryption.

**PKI Uses**
PKI is typically used for the following:
- Securing Webpages
- Encrypting Files
- Authenticating and Encrypting Email(s)
- Authenticating Nodes to Wireless
- Authenticating VPN Connections

**HSX PKI Certificate Processes**
HSX utilizes various services to obtain and manage interface certificates. These services include Amazon Web Services (AWS), DigiCert, and Let’s Encrypt.

Amazon Web Services
- All AWS certificates are automatically updated upon expiration
DigiCert
- DigiCert sends automated notifications that specific certificates are expiring at 90-, 60-, 30-, and 3-day intervals
- Notifications are sent to the HSX Support Desk and the HSX Chief Technology Officer

HSX PKI Certificate Processes

1. [https://www.digicert.com/pki/](https://www.digicert.com/pki/)
• HSX Mirth systems trigger alerts about expiring certificate – these notifications are triggered when a specific Mirth Connect box is loaded

HSX Certificate Management
HSX utilizes certificate management services through AWS and Digicert. In addition to these online monitors and notifications, HSX also compiled and maintains a Certificate Management Matrix, as pictured below. The Maxtix tracks each cert’s Request Date and Expiration Date. If a cert is no longer in use or has been rolled up into a multi-domain cert, it is noted within Column K. This Matrix was developed in July 2019 and will continued to be used going forward.

<table>
<thead>
<tr>
<th>Common Name</th>
<th>Alias</th>
<th>Cert that Covers</th>
<th>Cert Managed By</th>
<th>Issuer</th>
<th>Date of Last Update</th>
<th>Cert Request/Valid</th>
<th>Cert Expiration</th>
<th>Renewal Type</th>
<th>Common Name</th>
<th>Notes, Comments, Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface.hsqep.org</td>
<td>interface.hsqep.org</td>
<td>ConvertServer - HSA Hosted</td>
<td>DigitCert</td>
<td>2019-09-06</td>
<td>2020-09-13</td>
<td>interface</td>
<td>Current</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface.hsqep.org</td>
<td>interface.hsqep.org</td>
<td>ConvertServer - HSA Hosted</td>
<td>DigitCert</td>
<td>2017-07-09</td>
<td>2019-10-08</td>
<td>interface</td>
<td>Expired</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>prod.hsqep.org</td>
<td>prod.hsqep.org</td>
<td>ConvertServer - HSA Hosted</td>
<td>DigitCert</td>
<td>2016-09-27</td>
<td>2017-10-03</td>
<td>prod</td>
<td>No longer in use - roll up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>query.hsqep.org</td>
<td>query.hsqep.org</td>
<td>ConvertServer - HSA Hosted</td>
<td>DigitCert</td>
<td>2017-04-13</td>
<td>2017-09-19</td>
<td>query</td>
<td>Expired</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>test.hsqep.org</td>
<td>test.hsqep.org</td>
<td>ConvertServer - HSA Hosted</td>
<td>DigitCert</td>
<td>2019-08-24</td>
<td>2020-08-04</td>
<td>test</td>
<td>Current</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>connprof1.hsqep.org</td>
<td>connprof1.hsqep.org</td>
<td>ConvertServer - HSA Hosted</td>
<td>Self Signed</td>
<td>2015-06-25</td>
<td>2015-08-04</td>
<td>M/Cert1</td>
<td>Current</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>connprof2.hsqep.org</td>
<td>connprof2.hsqep.org</td>
<td>ConvertServer - HSA Hosted</td>
<td>Self Signed</td>
<td>2015-06-25</td>
<td>2015-08-04</td>
<td>M/Cert2</td>
<td>Current</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>connprof3.hsqep.org</td>
<td>connprof3.hsqep.org</td>
<td>ConvertServer - HSA Hosted</td>
<td>Self Signed</td>
<td>2015-06-25</td>
<td>2015-08-04</td>
<td>M/Cert3</td>
<td>Current</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Internal Certificate Update Process
• HSX receives notification of expiring cert via Support Desk
• Support Desk creates a Jira Ticket for Development Triage review
A new cert is requested with the same domain name or rolled up into an overarching, multi-domain cert
  - Example: connecttest.hsxsepa.org will be renewed with the same name
  - Example: interface.hsxsepa.org is now a roll up of internal.interface.hsxsepa.org, interface2.hsxsepa.org, and prod.hsxsepa.org

The Dev Team will put in the request to DigiCert (or another certificate authority vendor) for approval by the HSX CTO
Once approved, the new cert is available for download
HSX Dev Team and Support Desk will complete outreach to impacted members with a two to three (2-3) week window of completing the cert cutover
  - HSX works with each Member (or Member’s vendor) to complete the certificate update – phone calls and screenshares are scheduled on an as needed basis
  - HSX provides the cert’s public key, cert, and root CA to Member/Vendor
  - HSX never distributes certificate private keys
  - HSX provides member a hard cut-over date to have the new cert applied to their end of the interface – on the predetermined date and time, HSX completes the cert cutover
This date is typically three to five (3-5) days prior to the cert expiration

Testing is completed once the new cert has been applied to both ends of the interface

- HSX monitors impacted Member interfaces and troubleshoots as needed

**External Interface Certs and Client Certs Update Process**

HSX receives notification of Member and Client cert updates and expirations via the HSX Support Desk. The Member will submit a ticket with the new cert(s) for test and/or prod interfaces.

Hello HSX,

Please open up an IBM support ticket to work with them to replace the HSX expiring certificates.

- Expires 16-jan-20 /CN=HSXProd
- Expires 18-Jan-20 /CN=HSXTest

Any questions, please let us know.

Thank you,

The Support Desk will create a Jira ticket that includes the Member's name, the interface type, channel name(s), and date of expiration/cutover. The Development team will review the ticket during their daily Dev Triage meeting for assignment and completion.

HSX will then work with the member to coordinate cutover prior to the expiration date; this includes any necessary troubleshooting calls and screensharing.

If the client's certificate is managed by HSX, please refer to the Internal Certificate process that is listed above.
<table>
<thead>
<tr>
<th><strong>Responsible Owner:</strong></th>
<th>CISO</th>
<th><strong>Contact:</strong> email</th>
<th><a href="mailto:Brian.wells@healthshareexchange.org">Brian.wells@healthshareexchange.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approved By:</strong></td>
<td>Brian Wells</td>
<td><strong>Version #</strong></td>
<td>1.0</td>
</tr>
</tbody>
</table>
| **Current Approval Date:** | December 26, 2019 | **Review Date:** | December 18, 2022  
October 9, 2021  
October 17, 2020  
December 26, 2019 |
| **Date Procedure to go into Effect:** | December 26, 2019 |