eHealth Exchange

Operating Policy and Procedure

Subject: eHealth Exchange Digital Credentials		
Status: FINAL – Approved by CC	**Policy #: OPP-9**	
Effective Date: 8/1/2020	**Version: 6**	**Page 1 of 7**

I. Purpose

eHealth Exchange digital certificates, are issued, managed, held and revoked in accordance with the DURSA under the authority of the eHealth Exchange Coordinating Committee (Coordinating Committee). These certificates serve as the "Digital Credentials" referenced in the DURSA and are used by eHealth Exchange Participants to authenticate to each other prior to the transmission of Message Content, to encrypt the communications channel for the exchange of Message Content, and to digitally sign certain components of the Message Content.

eHealth Exchange Digital Credentials are only intended to be used to exchange Message Content between eHealth Exchange Participants and networks contracted for exchange, as governed by the DURSA and Coordinating Committee. This OPP clarifies several deployment options.

Use of Digital Credentials for other purposes or for exchanging data with organizations who are not eHealth Exchange Participants and on networks contracted for exchange, increases risk to those Participants. For example, use of Digital Credentials for other uses creates a dependency, putting other uses and applications at risk since the Digital Credentials may be revoked, held, or re-issued in accordance with the DURSA and Coordinating Committee.

II. Policy

1. While it is discouraged, eHealth Exchange Participants may, at their own risk, utilize eHealth Exchange Digital Credentials (which are x.509 digital certificates) for purposes other than to secure eHealth Exchange gateway 2-way-TLS connections and signing components of eHealth Exchange transacted messages, with the following conditions:
    a. Signed public certificate and private key may only be used to facilitate the security of messages transacted for healthcare-related purposes and/or DURSA Permitted Purposes.
    b. Signed public certificate and private key may only be used to secure only SOAP or REST based transport or for digital signatures creation or validation.
    c. Private keys may only be installed in a Secure Environment, and must never be duplicated outside of that Secure Environment or shared in any way.
    d. Private keys may only be installed in a Secure Environment that is also acting as the eHealth Exchange Participant gateway.

eHealth Exchange Participants may:

a. Install the eHealth Exchange root certificate on any server.
b. Install the eHealth Exchange intermediate certificate on any server.
c. Install the eHealth Exchange public key and signed server certificate on any server.

These other uses would not be supported by eHealth Exchange or governed by the Coordinating Committee; however, the eHealth Exchange certificate support processes would still apply.

Organizations incur risk of a certificate being revoked, held, or re-issued at any time and could thus experience unexpected operational outages for systems using eHealth Exchange x.509 certificates for other purposes.

2. Configure their Secure Environment to only allow eHealth Exchange Participant access

Participants must configure their eHealth Exchange gateway to only accept inbound requests from other eHealth Exchange Participants and/or the eHealth Exchange Hub, other than as allowed in section II(1) above. Configuration of each environment is unique, and thus eHealth Exchange Support Staff are unable to provide authoritative and complete configuration requirements. However, Participants must meet the following requirements, at a minimum, and with the exceptions as permitted in II(1) above:

   a. Have implemented x.509 certificate filtering to prevent non-eHealth Exchange certificates from being accepted at the 2-way-TLS layer.
   b. Have implemented x.509 certificate revocation checking to prevent “held”, or “revoked” eHealth Exchange certificates from being accepted at the 2-way-TLS layer.
   c. Have implemented x.509 certificate revocation checking to prevent expired, corrupted, or other invalid eHealth Exchange certificates from being accepted at the 2-way-TLS layer.
   d. Have implemented their PRODUCTION Secure Environment so that it does not accept eHealth Exchange VALIDATION certificates, and vice versa.

3. TLS Version 1.2 Conformance Statements

Prior to the approval of these statements, the baseline for the eHealth Exchange was TLS 1.0. The intent of this document is to establish TLS 1.2 as the new baseline for all eHealth Exchange gateways, and to help ensure that gateways do not establish TLS 1.0/1.1 connections, in production, to other eHealth Exchange gateways, while still allowing TLS 1.0/1.1 to be deployed at the gateway.

The rational for these changes is to:

   a. Update the TLS connections to utilize the currently available TLS 1.2 enhancements.
   b. Create precise text that is unambiguous, and testable.
   c. Allow gateways to deploy older versions of TLS, for non-eHealth Exchange purposes, while confirming that such gateways are configured to use TLS 1.2 for eHealth Exchange transactions.

d. Establish TLS 1.2 as the mandatory baseline for interoperability.
e. Provide a migration path to allow organizations with existing production deployments to upgrade, in a non-breaking manner, to become conformant with this new document.

This section contains only the normative text. Use of SHOULD, MUST, etc. are as per IETF formal definitions. Each statement is organized in the form of a document unique conformance statement identifier, followed by conformance text, followed by one or more associated test case definitions.

- **CONF001**: Conformance statement: Gateways MUST NOT establish connections using SSL 2.0.
- **CONF002**: Conformance statement: Gateways MUST NOT establish connections using SSL 3.0.
- **CONF003**: Conformance statement: Gateways SHOULD NOT establish connections using TLS 1.0.
- **CONF004**: Conformance statement: Gateways SHOULD NOT establish connections using TLS 1.1.
- **CONF005**: Conformance statement: Gateways MUST establish connections using TLS 1.2.
- **CONF006**: Conformance statement: Gateways that allow establishment of connections with TLS 1.0 and TLS 1.1 MUST only negotiate connections with TLS 1.1.
- **CONF007**: Conformance statement: Gateways that allow establishment of connections with TLS 1.0 and TLS 1.2 MUST only negotiate connections with TLS 1.2.
- **CONF008**: Conformance statement: Gateways that allow establishment of connections with TLS 1.1 and TLS 1.2 MUST only negotiate connections with TLS 1.2.
- **CONF009**: Conformance statement: Gateways that allow establishment of connections with TLS 1.0, TLS 1.1 and TLS 1.2 MUST only negotiate connections with TLS 1.2.

Gateways MUST also exchange using the highest strength cipher suite and key establishment mechanisms available to both Participants. Participants SHOULD use a TLS service listed on the most recently updated FIPS 140-2 Module Validation Lists as being validated, and not revoked, under the Cryptographic Module Validation Program:

- http://csrc.nist.gov/groups/STM/cmvp/
- Lists at http://csrc.nist.gov/groups/STM/cmvp/validation.html.

Participants using a validated cryptomodule MUST install, configure, and operate the FIPS 140-2 validated cryptomodule in either an approved or an allowed mode including, without limit, approved security requirements:

- http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf, approved security functions
- http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf, approved protection profiles
- http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexb.pdf, random number generation
- http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf, and key establishment techniques
- http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexd.pdf as listed in the latest version of:
  - http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf.

Participants using an unvalidated cryptomodule must configure their cryptomodule to operate in the same manner as a validated cryptomodule and must disable insecure or weak functionality such as 3DES encryption or MD5 hashes.

Ciphersuite Tests:

- **CONF010**: Conformance statement: Gateways MUST reject a connection when presented with a ciphersuite categorized as LOW.
- **CONF011**: Conformance statement: Gateways MUST reject a connection when presented with a ciphersuite categorized as eNULL.
- **CONF012**: Conformance statement: Gateways MUST reject a connection when presented with a ciphersuite categorized as aNULL.
- **CONF013**: Conformance statement: Gateways MUST reject a connection when presented with a ciphersuite categorized as EXPORT (which includes EXPORT40 and EXPORT56).
- **CONF014**: Conformance statement: Gateways MUST reject a connection when presented with a ciphersuite categorized as DES.
- **CONF015**: Conformance statement: Gateways MUST reject a connection when presented with a ciphersuite categorized as 3DES.
- **CONF016**: Conformance statement: Gateways MUST reject a connection when presented with a ciphersuite categorized as RC2.
- **CONF017**: Conformance statement: Gateways MUST reject a connection when presented with a ciphersuite categorized as RC4.
- **CONF018**: Conformance statement: Gateways MUST reject a connection when presented with a ciphersuite categorized as MD5.

III. Procedure

Delegation of Rights

The Coordinating Committee has designated Healtheway, Inc. (d/b/a/ The eHealth Exchange) and its staff ("eHealth Exchange Support Staff") to provide operational support to eHealth Exchange Participants and the Coordinating Committee, including but not limited to the set of responsibilities outlined in OPP #1.

In addition, the Coordinating Committee has delegated responsibility to eHealth Exchange and its eHealth Exchange Support Staff to facilitate the security testing necessary to implement the policies in OPP #9 described above.

~~Subscriber Information~~Identity Verification

- Applicants and participants should work with the Certificate Authority vendor to complete required ~~Subscriber~~ identity verification and signatures of any required forms.
- Any changes to a ~~Subscriber's~~ verified resource's information will be handled by the Certificate Authority vendor.

Renewal Information

- The Certificate Authority vendor will track the expiration dates of the x.509 certificate and notify each organization's' Subscriber in advance of the expiration date.
- Each participant must also track their own expiration dates.

IV. Definitions

Applicant: The entity or agency that submits an Application for Participation.

DURSA – Data Use and Reciprocal Support Agreement

Federal Bridge Certificate Authority (FBCA) - The certification authority designed to create trust paths among individual agency PKIs by allowing discrete PKIs to trust digital certificates issued by other entities whose policies have been mapped and cross-certified with the FBCA

Public Key Infrastructure (PKI) – The system employed by the eHealth Exchange to manage X.509 certificates used for the purposes of data encipherment, and message signature generation.

Responsible Disclosure – A practice developed by the Information Security community to ensure that identified vulnerabilities in security-related systems are resolved in a manner that protects the privacy and operational integrity of impacted systems until the vulnerability is remediated. A key component of this process is to only provide the vulnerability information on a need to know basis.

REST – An acronym for Representational State Transfer which is a method of information exchange that uses a web-browser-like approach to contact message content. This method is used by the HL7 FHIR® standard.

Secure Environment – In the context of this OPP, a secure environment is defined as a single computer, in a data center with appropriate physical and software access controls to prevent inappropriate access by unauthorized people or systems. A secure environment also optionally includes a high availability cluster of computers designed to mimic the cryptographic behavior of a single system, and it also includes a disaster response data center operated to closely mimic the behavior of the primary data center.

SOAP – A method of transacting message content exchange using XML. This method is used by the eHealth Exchange Patient Discovery, Messaging Platform, Access Consent Policies, and other specifications.

Subscriber/Sponsor – A Subscriber or Sponsor refers to the person a Participant has officially authorized to receive and accept responsibility for the secure use and management of the Participant's x.509 public certificate and its associated keys. This individual must be able to enter into binding legal agreements on behalf of the Participant.

Transport Layer Security (TLS) – A method the eHealth Exchange uses to create secure (private, intact, and authentic) communications channels between Participants.

All other capitalized terms, if not defined herein, shall have the same meaning as set forth in the DURSA.

V. References

"Restatement II of the Data Use and Reciprocal Support Agreement (DURSA)", Version Date: August 13, 2019

a. Section 14, Privacy and Security
b. Section 17.01, Disclaimers-Reliance on a System
c. Section 19, Term, Suspension and Termination

FBCA

According to the Federal Public Key Infrastructure Policy Authority's (FPKIPA) November 8, 2018 "Decision Brief on Health Information Technology (Health IT) Use of Public Key

Infrastructure technologies and Federal Public Key Infrastructure accreditation requirements" distributed by Federal PKI Policy Authority Co-Chairs LaChelle LeVan and Tim Baldridge, "Public Key Infrastructure systems utilized to identify and authenticate web services to Nationwide Health Information Network exchanges and systems operated by non-federal entities are not required to be accredited by the Federal Public Key Infrastructure Policy authority, or any systems or trust frameworks governed under its authority."

VI. Related Policies and Procedures

a. OPP #1: Participation – Review and Disposition of Applications for Participation
b. OPP #3: Participation – Changes, Suspension, Termination

VII. Version History

ID	Date	Comments
1	3/27/14	Drafted policy, based upon recommendations from Policy & Technical Task Group
2	4/1/14	Minor editorial revisions
3	4/1/14	Minor editorial revisions
4	7/20/15	Revised to reflect Healtheway name change to eHealth Exchange
5	1/10/16	Added section #3, additional definitions, plus a certificate "hold" status text
6	1/11/16	Additional clarifications related to testing and Subscriber responsibilities
7	1/15/16	Additional text related to the DURSA, new definitions, and clarifications on delegated responsibility.
8	9/12/17	Added TLS Version 1.2 requirements and conformance statements and Dual Trust Support requirements to Policy section
9	6/2020	Updated language to reflect newest DURSA amendment changes; Updated formatting for consistency and readability
10	9/2020	Updated language to reflect shift of Certificate Authority vendor and FBCA change.