ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Technical Trust Requirements

Applicability: QHINs

Table of Contents

1 Introduction

Trust among entities participating in the Trusted Exchange Framework and Common Agreement (TEFCA) relies on the mutual responsibilities embodied within the Common Agreement and Qualified Health Information Network (QHIN) Technical Framework (QTF)[1] and certainty among participating entities that transactions are being sent to, and received from, the systems of other organizations bound by those same terms.

To ensure this level of trust, any QHIN[2] that hosts an end point listed in the RCE Directory Service[3] (a Listed End Point), or directly originates a request to such an end point, must conform to the requirements outlined in this document.

2 Definitions

Certificate Authority (CA): the entity that issues digital certificates for the TEFCA ecosystem. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.

X.509 certificate: An X.509 version 3 certificate issued to an end entity. Note that the RCE only issues one type of certificate, and that same type of certificate is expected to be used by both peers for a QHIN-to-QHIN 2-way-TLS connection. X.509 Server Certificate requirements are specified in the QTF.

Subscriber: The organization that is requesting the certificate.

Sponsor: The person responsible for acting as the requestor for an RCE certificate. The Sponsor is generally responsible for secure acquisition, installation, and management of the full life cycle of the certificate as per the CA's requirements.

2-Way-TLS: Use of IETF Transport Layer Security with authentication of both end points in the internet communication pathway[4].

[1] As defined in the Common Agreement
[2] As defined in the Common Agreement
[3] As defined in the Common Agreement
[4] *The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446

Policy Binding: Associating an X.509 digital certificate with a given policy environment.

Listed End Point: A web service technical URL hosted by a QHIN that is listed in the RCE Directory Service.

Universal Resource Identifier (URI): A method of identifying a resource available via the internet. Example: https://www.xyz.org.

3 Certificate Issuance Process

The process for issuing certificates by any RCE-designated CA is governed by the rules of that CA. Production certificates are only issued for entries in the RCE Directory Service. However, not all RCE Directory entries will have their own separate certificate. See the section entitled Gateway Designation for more information.

3.1 Non-Production Certificate

A non-production certificate is required for conformance and non-production partner testing. To request a non-production certificate, the Sponsor must send an email to QHINtechsupport@sequoiaproject.org. After this request is received, a ticket will be opened in the RCE Customer Relationship Management (CRM) tool. This ticket will be reviewed by the RCE prior to approval. Note that unlike for a production certificate, identity proofing for a non-production certificate is not required.

3.2 Production Certificate

To obtain an initial production certificate, the QHIN's Sponsor must send an email to QHINtechsupport@sequoiaproject.org requesting a production certificate. Every Sponsor must create an account with the designated CA and be identity proofed, as further detailed in the RCE Certificate Information section below. After the RCE receives the request, a ticket will be opened in the RCE CRM tool. Prior to being issued an initial production certificate, QHINs must complete all necessary Onboarding[5] steps through Phase 3 of the Onboarding and Designation[6] process[7]. The RCE shall ensure all Onboarding is completed before permitting the certificate to be issued. Certificate renewals are also subject to review, to ensure the QHIN is in good standing and allowed to continue participation as a Designated QHIN.

[5] As defined in the Common Agreement
[6] As defined in the Common Agreement
[7] https://rce.sequoiaproject.org/qhin-process/

4 Policy Binding

Policy Binding is the process of associating a given X.509 digital certificate to the RCE trust domain. Policy Binding occurs when the following four conditions are satisfied:

1) The Listed End Point certificate possesses a Subject Distinguished Name attribute with a single Common Name (CN) component equal to the Fully Qualified Domain Name (FQDN) of the Listed End Point;
2) The Listed End Point certificate possesses a Subject Distinguished Name attribute with an Organizational Unit (OU) component of "RCE";
3) The Listed End Point certificate has at least one Subject Alternative Name Extension type of URI and value of "WWW.SEQUOIAPROJECT.ORG/V01"; and
4) The Listed End Point certificate is issued by the trust chain defined herein.

Note that there may be multiple OU values for any given certificate, but only one of those is required to be "RCE". There also may be multiple Subject Alternative Name values, but only one of those is required to be of type URI with a value of "WWW.SEQUOIAPROJECT.ORG/V01".

5 Gateway Designation

For clarity, a QHIN with multiple Participants[8] and Subparticipants[9] hosted behind a single gateway will be deployed with only one X.509 certificate for all of their Participants and Subparticipants. In this case, a single certificate will be issued for that QHIN, and that QHIN will be entered into the RCE Directory Service. Subsequently, as that QHIN's Participants and Subparticipants become ready to exchange, each Participant and Subparticipant will be added to the directory, but no additional certificate will need to be issued by the RCE since all of those Participants and Subparticipants are behind the same gateway. Stated differently, multi-tenant scenarios will result in at least one RCE Directory Service entry per Participant and Subparticipant but will not result in the RCE issuing a separate X.509 certificate being issued to each.

6 Subject Alternative Name (SAN) Use

RCE X.509 certificates may use Subject Alternative Names for two purposes. The CA will automatically set this field as noted in the Policy Binding section of this document via a URI data type field indicating that this X.509 certificate is for the RCE. A Subject Distinguished Name type

[8] As defined in the Common Agreement
[9] As defined in the Common Agreement

SAN field indicating the Common Name of the certificate Subject may also be denoted, but only if specifically requested by the QHIN.

7 Trust Chain

Production (PRD) Environment Trust Bundle:
https://bundles.directtrust.org/bundles/sequoiaProjectProdTrustBundle.p7b

Validation (VAL) Environment Trust Bundle:
https://bundles.directtrust.org/bundles/sequoiaProjectValTrustBundle.p7b

The above trust bundles include everything you need, but the individual Root and Intermediate certificates for VAL and PRD in .PEM format can also be found here: https://desk.zoho.com/portal/directtrust/en/kb/articles/individual-root-and-intermediate-pem-files

Certificate Revocation List (CRL) Access Point:
In order for QHINs to check for revoked or suspended certificates, it may be necessary to allow for outbound access to the CRL distribution points. The URIs MUST be authoritatively obtained from QHINs' end entity certificate extension attribute and can also be found here for your reference: https://desk.zoho.com/portal/directtrust/en/kb/articles/certificate-revocation-lists-crls

8 Certificate Filtering

Listed End Points MUST accept any other QHIN messages for which the other QHIN's certificate presented meets the requirements of this policy and passes validation (is intact, is correctly bound, is within its validity period, is not revoked, is not on hold, and is signed by one of the designated intermediate signing CAs.

All QHINs must allow outbound requests to any Listed End Point that is secured by an X.509 certificate that is intact, is correctly bound, is within its validity period, is not revoked, and is not on hold.

For purposes of QHIN-to-QHIN communication, all Listed End Points must also be configured to accept only certificates that meet the specifications in this policy and that are issued by the trust chains listed above with a Common Name (CN) consistent with the Listed End Point and with an Organizational Unit of "RCE". Alternatively, instead of filtering based on the Subject Organizational Unit, the Listed End Point MAY filter based on the above trust chain, plus the Subject Alternative Name, as described in the Policy Binding section of this policy document. Other certificates issued by the same CA that are used for exchange outside QHIN-to-QHIN purposes MUST NOT be trusted for QHIN-to-QHIN exchange.

9 Ports

To allow restrictions on the ports opened, both inbound and outbound, and to avoid firewall maintenance for individual connections, Listed End Points MUST use one of the following TCP ports for inbound services requests:

- 443
- 4437
- 14430

QHINs MUST allow outbound communication on all three of the above-listed ports.

10 Certificate Revocation and Suspended Status Checking

QHINs MUST check each transaction to ensure the destination X.509 certificate used meets the requirements of this RCE Technical Trust Requirements document and is not revoked, on hold, or suspended before establishing trust. Furthermore, participating systems MUST support Certificate Revocation List (CRL) checking. QHINs MAY support Online Certificate Status Protocol (OCSP) responder network service checking. Only valid X.509 certificates (within their validity period) should be checked for revocation status. Expired certificates, for example, are normally not listed as revoked. Expired certificates MUST not be used to establish trust.

11 Multiple Trust Chain Support

To facilitate normal operational changes with the current RCE CA vendor, and to enable redundant CA vendors, the following policy is established:

a. All QHINs MUST support all current trust chains, as documented in the Trust Chain section above. Non-normative: The RCE intends to support multiple CA vendors for redundancy. This requirement also facilitates orderly transitions to newer trust chains from the same vendor as certificates naturally expire or are re-issued over time.

b. QHINs' outbound connections MAY continue to support a single outbound trust chain for standard operational use, but QHINs MUST be able to switch their outbound trust chain to a secondary trust chain with short notice from the RCE and with minimal downtime. QHINs SHOULD automate this process. Non-normative: This is designed to allow CA fail-over in the event the primary trust chain becomes inoperable for any reason (such as unscheduled downtime).

12 RCE Certificate Information

QHINs are responsible for maintaining up-to-date contact information and Sponsor information, along with up-to-date entries in the RCE Directory Service. Failure to maintain correct contact and Sponsor information, particularly if the Sponsor is no longer employed by the organization, may result in delays in renewing or re-issuing certificates, which may, in turn, result in production connectivity failures when certificates expire. To prevent this, a QHIN SHOULD have multiple Sponsors. The CA will track certificate expiration dates and reach out to the designated Sponsor(s) 60-90 days in advance of the Subscriber's certificate expiring. Ideally, this should allow enough time to renew the certificate even if a new Sponsor must go through the identify proofing process for that organization.

Per the CA providers utilized by the RCE, all certificate recipients must be identity proofed and sign a Subscriber Agreement before being issued a production certificate. This process indicates the person officially authorized by the QHIN as the Sponsor for purposes of receiving and accepting responsibility for the secure use and management of the RCE X.509 certificate and its associated keys. The Sponsor will be identity-proofed per NIST 800-63A Identity Assurance Level 2 guidelines.

Additional items to be aware of:

1) If the X.509 certificate becomes compromised, or decommissioned, or otherwise needs to be revoked, then the Sponsor MUST immediately send an email to QHINtechsupport@sequoiaproject.org, which will be acknowledged, indicating that the certificate should be revoked.
2) In the event of a key compromise, please contact the RCE immediately, 24 hours a day, so the certificate can be revoked, as described in step #1.
3) Per the CA, certificates have an expiration date and need to be re-issued prior to expiration. The CA will attempt to notify the Sponsor on file approximately 60-90 days prior to the certificate expiration to begin the renewal process, but ultimately it is the responsibility of the certificate holder to maintain a valid certificate.
4) The Sponsor is responsible for ensuring that the X.509 certificate and access codes are maintained securely at all times.

This program is supported by the Office of the National Coordinator for Health Information Technology (ONC) of the U.S. Department of Health and Human Services (HHS) under grant number 90AX0026, Trusted Exchange Framework and Common Agreement – Recognized Coordinating Entity (RCE) Cooperative Agreement Program, in the amount of $5,101,000 with 100 percent funded by ONC/HHS. This information or content and conclusions are those of the author and should not be construed as the official position or policy of, nor should any endorsements be inferred by ONC, HHS or the U.S. Government.