Technical Trust Policy

Version 1.2

Last Updated: May 20, 2016

Introduction

Carequality creates a community of trusted exchange partners who rely on each organization's adherence to the terms of the Carequality Connected Agreement, Carequality Connection Terms, and Use Case Implementation Guides. Trust in the community relies on the mutual responsibilities embodied within these terms but can only be fully realized if participants have certainty 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 system that hosts an end point listed in the Carequality Directory, or directly originates a request to such an end point (a "Participating System"), must conform to the requirements outlined in this Policy, which constitute technically enforceable evidence that the organization has met the associated criteria for being a Carequality Participating System.

Individual Use Case Implementation Guides may specify different requirements from those outlined in this Policy and in such a case the Implementation Guide will take precedence.

Definitions

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

Policy Binding: Associating a X.509 digital certificate with a given policy environment. See also the *Binding* section of this document.

Listed End Point: A web service technical URL hosted by a Participating System that is listed in the Carequality Directory.

Server Certificate: An X.509 version 3 certificate issued to an End Entity. Note that Carequality only issues one type of certificate, and that same type of certificate is expected to be used by both peers for a Carequality 2-way-TLS connection.

Subscriber: The single person responsible for acting as the sponsor for a Carequality X.509 certificate. The Subscriber is responsible for secure acquisition, installation, and management of the full life cycle of the certificate as per the Entrust Subscriber Agreement.

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

Certificate Issuance Process

The actual process for issuing certificates by this CA is governed by Entrust rules under compliance with the Federal Bridge Certification Authority (FBCA) program. Certificates are only issued for entries in the Carequality Directory. However, not all Carequality Directory entries will have their own, separate certificate. See the section entitled Multi-Tenant Gateways for more information.

The initial step in the issuance process is for the Carequality Implementer to prepare and send a Carequality V1 Certificate Package to Carequality support staff as per the instructions in the package. At a high level, once the package is securely uploaded to a Carequality encrypted file storage area, it will be

reviewed by staff, and then the certificate acquisition codes will be issued to the designated person at the Carequality Connection.

Carequality support staff will accept Carequality Certificate Packages from any of the three points of contact listed on the Implementer's Carequality Implementer Application, or from any staff member identified by one of those three contacts as being authorized to submit these Packages. The submission of a Package for a Carequality Participating System will serve as the Implementer's indication that the Carequality Connection is approved to participate in exchange activities via the Carequality Framework, through that Implementer.

Once the Carequality V1 Certificate Package has been received, Carequality support staff will review the contents to ensure the appropriate requirements have been meet, including, but not limited to:

- Confirming that the Carequality Participating System is approved as having satisfied the business and legal process for being issued a certificate and being listed in the Carequality Directory
- Ensuring the Subscriber is correctly identity proofed
- Contains the signed Entrust FBCA subscriber agreement
- Contains the directory and certificate technical information

Carequality support staff will then issue codes to the Subscriber so that the certificate can then be signed, obtained and installed. Carequality support staff then validate the certificate installation as described below. Once the Participating System successfully completes any production validation required by the relevant Implementation Guide(s), it will officially enter into production operational status.

More detailed steps within this general process are subject to change based on experience, technical developments, and updates to the underlying Entrust processes. Carequality will provide additional, up-to-date information on process details to those who begin the certificate request process. This information may take the form of a separate document, an online FAQ page, or some other appropriate mechanism.

Policy Binding

Policy Binding is the process of associating a given X.509 digital certificate to the Carequality trust domain.

Policy Binding occurs when the following four conditions are satisfied:

1) The End Entity (a.k.a. server) 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 End Entity certificate possesses a Subject Distinguished Name attribute with an Organizational Unit (OU) component of CAREQUALITY;
3) The End Entity certificate has at least one Subject Alternative Name Extension type of URI and value of "HTTP://WWW.CAREQUALITY.ORG/V01"; and
4) The End Entity 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 "CAREQUALITY". 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 "HTTP://WWW.CAREQUALITY.ORG/V01".

Multi-Tenant Gateways

Carequality Implementers can deploy as either a single-tenant gateway or multi-tenant gateway. In the single-tenant case, there is a one-to-one relationship between X.509 certificates, and Carequality Connections (CCs). In the multi-tenant case, there is more than one CC per X.509 certificate. Both scenarios are allowed.

A Carequality Implementer with multiple CCs hosted behind a single gateway, MAY be deployed with only one certificate for all of their CCs. In this case, a single certificate will be issued for that Implementer and that Implementer will be entered into the Directory. Subsequently, as that Implementer's CCs become ready to exchange, each CC will be added to the Directory, but no additional certificate will need to be issued since it is behind the same gateway. Stated differently, multi-tenant scenarios will result in one Carequality Directory entry per CC, but will not result in a separate Carequality certificate being issued to each CC.

Trust Chain

Except as described in the Other Uses section of this document, Listed End Points MUST be configured to transmit, receive, and accept exactly and only the following three-level trust chain: The Participating System Server certificate, the Entrust Intermediate (Signing) CA certificate, and the Entrust Root CA (self-signed) certificate, as defined below:

- The Entrust Root (self signed) CA cert:
  - serial number: 4a a7 c2 6d
  - issued 9/9/2009
  - valid until 9/9/2019
  - issuer OU = Entrust Managed Services NFI Root CA, OU = Certification Authorities, O = Entrust, C = US
  - subject OU = Entrust Managed Services NFI Root CA, OU = Certification Authorities, O = Entrust, C = US

- The Entrust Intermediate (Signing) CA cert:
  - serial number: 4a a7 f7 19
  - issued 5/23/2011
  - valid until 8/23/2019
  - issuer OU = Entrust Managed Services NFI Root CA, OU = Certification Authorities, O = Entrust, C = US
  - subject OU = Entrust NFI Medium Assurance SSP CA, OU = Certification Authorities, O = Entrust, C = US

- Participating Systems Server cert:
    - serial number/dates (customer specific)
    - issuer OU = Entrust NFI Medium Assurance SSP CA, OU = Certification Authorities, O = Entrust, C = US
    - subject CN = (your FQDN), OU = CAREQUALITY, O = HHS-ONC, C = US

Certificate Filtering

Listed End Points MUST accept any other Participating System messages for which the partner certificate presented meets the requirements of this policy, is intact, is correctly Bound, is within its validity period, is not revoked, and is not on hold, unless the relevant Use Case's non-discrimination requirements allow messages to be rejected from a particular sender or group of senders.

All Participating Systems that initiate requests to Listed End Points MUST allow outbound connectivity to any Listed End Point for the relevant Use Case and which are secured by a server certificate that is intact, is correctly bound, is within its validity period, is not revoked, and is not on hold, unless the relevant Use Case's non-discrimination requirements allow the initiator to refrain from sending messages to a particular Listed End Point or group of Listed End Points.

For purposes of communication via the Carequality Framework, and except in accordance with the Other Uses section below, 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 Chain listed above with a common name consistent with the Listed End Point and with an Organizational Unit of CAREQUALITY. Alternatively, instead of filtering based on the Subject Organizational Unit, the end point MAY filter based on the above chain of trust, plus the Subject Alternative Name, as described in the *Policy Binding* section of this policy document, and if is a member of the eHealth Exchange, it MUST filter access as specified in the *eHealth Exchange and Carequality Dual Trust Domain Considerations* section of this document.

TLS Cryptographic Configuration

All connections between Participating Systems that are subject to the Carequality Connected Agreement or Carequality Connection Terms MUST use TLS 1.0 or above with mutual authentication as per NIST / FIPS 800-52r1 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf. In addition, Participating Systems must deploy a cryptographic subsystem listed on the NIST Cryptographic Module Validation program, running in FIPS mode as per http://csrc.nist.gov/groups/STM/cmvp/validation.html

IP Address Whitelisting

The number of connections afforded by the Carequality Framework and the requirements for most organizations under Carequality's Non-Discrimination principle may present significant logistical challenges for those who would attempt to implement IP address whitelisting for either outbound or inbound connections. Participating Systems MUST NOT implement an IP whitelist unless fully complying with the applicable Implementation Guide's non-discrimination requirements allows the Participating System to accept messages only from a known, static set of other participants.

Ports

As noted above with respect to IP whitelisting, maintenance of firewall or other connectivity rules presents significant logistical challenges if done individually for all Listed Endpoints. In order to allow restrictions on the ports opened both inbound and outbound and to avoid firewall maintenance for individual connections, Listed Endpoints MUST use one of the following ports for inbound services requests:

- 443
- 4437
- 14430

Participating Systems that originate messages to Listed Endpoints MUST allow outbound communication on all three of the above-listed ports.

Revocation Checking

Participating Systems MUST check each transaction to ensure the certificate meets the requirements of this policy. Furthermore, participating Systems MUST support Certificate Revocation Lists (CRL) checking. Participating Systems MAY support Online Certificate Status Protocol (OCSP) responder network service checking. Note that only valid certificates (within their validity period) should be checked for revocation status as expired certificates, for example, are normally not listed as revoked.

Validation

Carequality Support Staff will conduct a periodic limited scope, security test to help ensure the security of the Carequality operational environment. This test will utilize technical controls designed to prevent Protected Health Information ("PHI") from being accessed during the test with such controls open to inspection by Participants Systems' Subscribers. THIS SECURITY TEST IS NOT A REPRESENTATION OF PROPER SECURITY CONFIGURATION, nor is it a substitute for a Participating System security audit. Any identified deficiency will be treated as a business confidential/need to know only disclosure with the Carequality support staff working privately with Participating System to remediate such identified defects using Information Security "Responsible Disclosure" guidelines.

eHealth Exchange and Carequality Dual Trust Domain Considerations

For those organizations that are authorized to exchange messages under both the eHealth Exchange and Carequality, the following section applies.

The eHealth Exchange has a substantially similar technical trust design. The biggest two technical differences are that the eHealth Exchange uses an X.509 Subject Distinguished Name component of OU=NHIN, instead of OU=CAREQUALITY, and that the eHealth Exchange is silent on the topic of Subject Alternative Names. In order to establish trust domain interoperability the following approaches are required. Note that this section does not set policy related to trust or distrust between Carequality or the eHealth Exchange, it only establishes the technical means to enforce appropriate policy (such as legal agreements governing exchange between the eHealth Exchange Participant and the Carequality Participating System).

eHealth Exchange Participants wishing to trust Carequality Participating Systems can either add trust for all Carequality Listed End Points, and then add exceptions, or they may choose to distrust all Carequality Listed End Points and then add exceptions. To add trust, or distrust, all of the entire Carequality trust domain, the eHealth Exchange Participant MUST either 1) add filtering to allow or disallow exchange with partner certificates with an OU=CAREQUALITY, or 2) add filtering to allow or disallow exchange with partner certificates with a Subject Alternative Name of "HTTP://WWW.CAREQUALITY.ORG/V01". To add trust, or distrust, for a specific Carequality Listed End Point, the eHealth Exchange Participant MUST add filtering for a CN=<FQDN of the Carequality Listed End Point>. Note that the requirements of the *Certificate F*iltering and *Trust Chain* sections of this document still apply.

In a similar, but not identical manner, Carequality Participating Systems wishing to trust eHealth Exchange Participants can either add trust for all eHealth Exchange Listed End Points, and then add exceptions, or they may choose to distrust all eHealth Exchange Participants and then add exceptions. To add trust, or distrust, for the entire eHealth Exchange trust domain, the Carequality Participating System MUST add filtering to allow or disallow exchange with partner certificates with a Subject DN component of OU=NHIN (note that the eHealth Exchange certificates do not have Subject Alternative Names consistently populated at this time). To add trust, or distrust, for a specific eHealth Exchange Participant, Carequality Participating Systems MUST add filtering for a CN=<FQDN of the eHealth Exchange Participant Gateway>.

In the case where an existing eHealth Exchange Participant also seeks to declare that it is a member of Carequality, the eHealth Exchange Participant will receive a new X.509 certificate issued as per this document. The eHealth Exchange Participant is then expected to bind their Carequality certificate to a new port number, or use an entirely new FQDN.

In the case where an existing Carequality Participating System also seeks to declare that it is a member of the eHealth Exchange, the Carequality Participating System will be issued a new X.509 certificate issued as per the eHealth Exchange standard process. The Carequality Participating System is then expected to bind their eHealth Exchange certificate to a new port number, or use an entirely new FQDN. Note that in the future, Sequoia expects to issue single certificates with multiple OUs in the Subject allowing for one OU for Carequality and one OU for the eHealth Exchange.

In both of the above cases, the remainder of this document continues to apply.

Accuracy

Since the X.509 certificate Subscriber may need to be consulted to perform administrative functions on the certificate, the Participating System MUST accurately maintain its X.509 certificate Subscriber information in the Carequality Directory at all times. Each X.509 certificate must have a Subscriber listed in the Carequality Directory with a Person-Contact Type of "Subscriber". A Subscriber may have multiple X.509 certificates.

Other Uses

Carequality issued certificates and Listed End Points may be used for non-Carequality purposes, provided that the organization to which the certificate is issued understands that such a use is not supported by Carequality, and that the organization accepts the risk that the system be subject to

downtime due to Carequality activities such as certificate revocation, or directory entry changes. Other uses of Carequality Listed End Points, and certificates, MUST BE for substantially similar uses (such as for exchanging clinical and administrative data using web services), MUST be compatible with the maintenance of a secure data center, and MUST only use TLS 1.0 or greater with mutual authentication for all transactions.

The same fully qualified domain name (FQDN) and port combination should not be used for production Carequality activity and non-production activity of any sort, even if the non-production activity is substantially similar in other ways to Carequality activity.

Participating Systems are not otherwise constrained by Carequality, and the servers, networking appliances, and other elements of the Participating System's deployment environment may also be used for whatever other purposes the organization judges to be appropriate, as long as the support of these other uses does not conflict with the requirements of this document, any relevant Implementation Guide, or other Carequality Policy.

Carequality V1 Certificate Package

Carequality support staff will issue an X.509 certificate upon receipt of a properly completed Carequality V1 Certificate Package. Implementers requiring their own certificates should submit the package on their own behalf. For any Carequality Participating Systems requiring their own certificates, the Sponsoring Implementers SHALL work with each relevant Carequality Participating System to complete and submit the Carequality V1 Certificate Package. This package contains the information needed for Carequality support staff to finish identity proofing the Subscriber, and then issue a production certificate and add the Implementer or Participating System into the Carequality Directory.

The Carequality V1 Certificate Package Manifest:

1. Carequality Certificate Authority / Directory Listing Form
2. Entrust Subscriber Agreement
3. Entrust Identity Proofing Form

The documents in the Carequality V1 Certificate Package should be completed, as per the below instructions, and returned to Carequality by being uploaded to Carequality's file share service. Specific information and access will be provided to those Implementer staff members who are authorized to upload files. Carequality will provision such access to each of the contacts identified on the Implementer's Application, and/or up to three additional individuals identified by one of those three contacts as being authorized to submit the packages on behalf of the Implementer.

Implementers and Participating Systems are responsible for maintaining up-to-date contact information and Subscriber information, along with up-to-date entries in the Carequality Directory. Failure to maintain correct contact and Subscriber information, particularly if the Subscriber 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 if certificates expire.

Instructions

Since Carequality utilizes an FBCA cross certified Managed Certification Authority provider, all Carequality Connections must complete and return a notarized Entrust Subscriber Identity Verification form, and an Entrust Subscriber Agreement, upon each key issuance or a maximum of every 20 months. These forms indicate the person officially authorized by Carequality Participating Systems to receive and accept responsibility for the secure use and management of the Carequality Connection's X.509 public certificate and its associated keys. This individual (the "Subscriber"), will be identity proofed, in person, by a licensed Notary Public and will be required to show the Notary several forms of identification. Once the Entrust Subscriber Identity Verification form, and the Entrust Subscriber Agreement forms have been completed, they should be scanned along with a photocopy of the Subscriber identification sources (driver's license, etc.) and the Notary Public's certificate. This set of 3 files should then be uploaded to the designated Carequality secure file storage service. After a successful upload of the files to the Carequality share, the person performing the upload should send an email to techsupport at sequoiaproject dot org with the name of the new folder containing the files for this certificate. A Carequality support staff member will respond with the next steps, which for a properly completed package, will be to provide the certificate acquisition codes directly to the X.509 certificate Subscriber.

The package will be stored on the Carequality secure, encrypted, file system for future reference and audits. *Note that contrary to instructions in the forms, the agreements should be returned to the Carequality support staff, not Entrust*. Entrust has the authority to periodically audit the Carequality records to assure compliance with their processes.

Additional items to be aware of:

1) If the certificate becomes compromised, or decommissioned, or otherwise needs to be revoked, then the Subscriber MUST immediately send an email to techsupport at sequoiaproject dot org, which will be acknowledged, indicating that the certificate should be revoked.
2) In the event of a key compromise, please contact Carequality immediately, 24 hours a day, so the certificate can be revoked, as described in step #1.
3) Approximately every 12 months, the signed certificate will expire and need to be re-issued. Carequality Participating Systems are responsible for contacting the Carequality support staff approximately 3 weeks prior to the certificate expiration to request a new certificate. More advanced notice is permitted if needed to allow for proper Carequality Participating System internal deployment planning.
4) The Subscriber is responsible for ensuring that the X.509 certificate, and access codes, are maintained securely at all times.

Carequality V1 Certificate Package Manifest

When returning the package to Carequality, please create a new folder on the Carequality file share in the following format:

- FQDN-port#
- Where “FQDN” is the name of the Carequality Participating System Fully Qualified Domain Name, and the “port#” is the port that this certificate will be bound to.

Then, under that new folder, please upload three files:

- Completed Carequality Certificate Authority / Directory Listing Form
- Completed Entrust Subscriber Agreement
- Completed Entrust Identity Proofing Form

An example for a hospital called “HOSPITAL ABC”:

- PROD01.HOSPITAL-ABC.ORG-443
  - 2016-01-01-HOSPITAL-ABC-Carequality-Certificate-Authority-Directory-Listing-Form.XLSX
  - 2016-01-01-HOSPITAL-ABC-Entrust-Subscriber-Agreement.PDF
  - 2016-01-01-HOSPITAL-ABC-Entrust-Identity-Proofing-Form.PDF

Another example for an Integrated Delivery Network called “IDN XYZ”:

- GATEWAY.IDN-XYZ.COM-443
  - 2016-01-01-IDN-XYZ-Carequality-Certificate-Authority-Directory-Listing-Form.XLSX
  - 2016-01-01- IDN-XYZ-Entrust-Subscriber-Agreement.PDF
  - 2016-01-01- IDN-XYZ-Entrust-Identity-Proofing-Form.PDF