Technical Trust Policy

Version 2.0

Last Updated: June 7, 2018

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

Please see Appendix A for detailed trust chain configuration information.

Certificate Filtering

Listed End Points MUST accept any other Participating System messages for which the partner certificate presented meets the requirements of this policy, and passes IETF PKIX 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 certification authorities, etc.) 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. Non-normative: There are other certificates issued by the same Intermediate Certification Authority that are used for non-Carequality purposes and must not be trusted by Carequality.

TLS Cryptographic Configuration

All connections between Participating Systems that are subject to the Carequality Connected Agreement or Carequality Connection Terms MUST use TLS 1.2 or above with mutual authentication as per NIST / FIPS 800-52r1 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf. In order to take advantage of the enhancements available in this version of TLS, TLS 1.2 has been established as the new baseline for all Participating Systems. Participating Systems are permitted to deploy older versions of TLS for non-Carequality purposes, but Participating Systems MUST NOT establish TLS 1.0/1.1 connections **in production** to other Participating Systems. 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 or operating in an equivalent mode of production operation. Non-normative: This approach is designed to provide Participating Systems with a migration path allows those with existing production deployments to upgrade, in a non-breaking manner, to become conformant with the new version of the Carequality Technical Trust Policy document version 2.0.

Specifically, Participating Systems using a validated cryptomodule MUST install, configure, and operate their 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. Participating Systems 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.

Non-normative note: NIST is in the process of updating FIPS 800-52 to revision 2, which includes references to TLS 1.2 as being required, and TLS 1.3 as being required by Jan 1, 2020. Once NIST finalizes FIPS 800-52, the Carequality Technical Trust Policy document will be revisited for likely revision, in coordination with the Carequality community.

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.

Certificate Revocation and Suspended Status Checking

Participating Systems MUST check each transaction to ensure the end entity X.509 certificate used meets the requirements of this Carequality Technical Trust Policy document and is not Revoked, on Hold, or Suspended before establishing trust. Furthermore, participating Systems MUST support Certificate Revocation List (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. Expired certificates MUST not be used to establish trust.

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.

Multiple Trust Chain Support

In order to facilitate normal operational changes with the current Carequality PKI vendor, and to enable redundant PKI vendors, the following policy is established:

a. All Participating Systems MUST support all current trust chains as documented in Appendix A. Non-normatively: Carequality intends to support multiple PKI vendors for redundancy in the future. 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. Participating Systems’ outbound connections CAN continue to support a single outbound trust chain for standard operational use, but MUST be able to switch their outbound trust chain to a secondary trust chain with minimal notice and down time. Participating Systems SHOULD automate this process. Non-normative: This is designed to allow PKI fail-over in the event the primary trust chain becomes inoperable for any reason (such as unscheduled down time).

Subscriber Contact

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-ContactType of “Subscriber”. A Subscriber may have multiple X.509 certificates. A Participating System SHOULD have multiple Subscribers.

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 periodically audits 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

Appendix A – Certificate Trust Chain Configuration

Entrust Root Certificate

Immediately below is the new Entrust June 2017 Root Certificate (provided for your reference). This certificate MUST be obtained via authoritative sources (the End Entity certificate AIA field) and SHOULD be installed in Participating Systems inbound truststores and SHOULD be presented in Participating Systems outbound trust chain. Please follow IT best practices and validate the authenticity and integrity of this certificate before using it:

Serial Number: 4A:A8:A6:0D (1252566541)

```
-----BEGIN CERTIFICATE-----
MIIDpDCCAoygAwIBAgIESqimDTANBgkqhkiG9w0BAQsFADByMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEtMCsGA1UECxMkRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIE5GSSBS
b290IENBMB4XDTE2MTExNjE2MzEwNFoXDTI3MTIxNjE3MDEwNFowcjELMAkGA1UE
BhMCVVMxEDAOBgNVBAoTB0VudHJ1c3QxIjAgBgNVBAsTGUNlcnRpZmljYXRpb24g
QXV0aG9yaXRpZXMxLTArBgNVBAsTJEVudHJ1c3QgTWFuYWdlZCBTZXJ2aWNlcyBO
RkkgUm9vdCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL8fW2c5
Y1H3DBZcF5uwko+I1N9643gEq3PYUU/AtMzRBJ1PFiipWRNyLYPoVaPYr6GUDsrl
TyvQ7LJD5uDOFPxWtGggqcDGFPC8u0MBUvqTvjCMBuGwI55vrjfeW4mZfsoGo+qX
3qHbCRmif/PywciYTnYhArPtM9tZ/9Nyaunpgrk0zKS0G7dgU+aaqW+BQKy8ss6t
1qbcD5HV5laf6nlTXJ0JrMCbUmuUbhNfCp9e+TwS4LtqjPRL5D/pnUkzURyl2F6/
53yZ0M51SJy9hxEnTYHd4QmJp3yR2fDEVI7Ug/6RBgyPSjlnWbuDPDArD+G2yzTs
6tmc1OSDvWYvVUkCAwEAAaNCMEAwDgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/wQF
MAMBAf8wHQYDVR0OBBYEFPrfIwHEquwj461vDTSlDc85ZGVeMA0GCSqGSIb3DQEB
CwUAA4IBAQCc5cuNlP+rF3KHR/UOwlNc6YWLxf2ImQ2Zhv+ULPKczx/pZPELHXnz
kAhTtjpxjpYuH8NHKUxphJEBCL7P7X9zMO66Z5Rso3iwCC95ffYYqJuIxpBn8xuk
Fm3h6sblYlDiMqbQ4wqtNDPMnlvkBbosp2vsr6V5j5jr1Cp/5e6tKuQuCH8iHq8X
5kCvImZEzAf8aAH6pRv3pVswCyxBcPzGHMj4N9RrRFBb462+Sk5q1GMA7roajPpR
Ht7COZNJr2QhWUGSQlavqaaRwYNyeBYuTID8Ihk+VIDdsISQPcor73GMpxK30zym
fDpTdQ0G0+5XayKnMi2NCLO6EPsLvEJJ
-----END CERTIFICATE-----
```

New Entrust 2017 Intermediate Certificate

New Entrust 2017 Intermediate CA certificate (provided for your reference). This certificate MUST be obtained via authoritative sources (the End Entity certificate AIA field) and MUST BE installed in Participating Systems inbound truststores and MUST be presented in Participating Systems outbound trust chain. Please follow IT best practices and validate the authenticity and integrity of this certificate before using it:

Serial Number: 4A:A8:B9:EA (1252571626)

```
-----BEGIN CERTIFICATE-----
MIIH6DCCBtCgAwIBAgIESqi56jANBgkqhkiG9w0BAQsFADByMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEtMCsGA1UECxMkRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIE5GSSBS
b290IENBMB4XDTE3MDUxNjE0MzEzNVoXDTI3MTExNjE1MDEzNVowcTELMAkGA1UE
BhMCVVMxEDAOBgNVBAoTB0VudHJ1c3QxIjAgBgNVBAsTGUNlcnRpZmljYXRpb24g
QXV0aG9yaXRpZXMxLDAqBgNVBAsTI0VudHJ1c3QgTkZJIE1lZGl1bSBBc3N1cmFu
Y2UgU1NQIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoOEqao5H
z2toLgtRAaca84ZyEuQ9QVpZ1RdJEHkFZpLnfx396cjx7ZlwUfmeo41l8NVsgZh8
AVnSdZQLU1rT3Lf2j+4vvHDGhtWTGKQM22obX6n/j1nk66JA6U0pANIWnuHQ9APr
10IugCpVIoYfVWXvuj+Jj8NJKehUdDfv1L3SZwW/KE9Osuadjx+y+jZ3d87Y+8r8
rzmKggqNxrE+xBVpRFxYyVMtWcooAG6YyO7Arp3BlufephNWOjzYr3TCCJyjk02F
yxTlf9WqfhDNguAFGhbL97NRZPKpRLcEc6gHI8VBtGdP+BiDx/c8Kn0tTf3I41yB
jMZ6h7I66502sQIDAQABo4IEhTCCBIEwDgYDVR0PAQH/BAQDAgEGMIIBHQYDVR0g
BIIBFDCCARAwDwYNYIZIAYb6a4FIAwoHATAPBg1ghkgBhvprgUgDCgcCMA8GDWCG
SAGG+muBSAMKBwMwDwYNYIZIAYb6a4FIAwoHBDAPBg1ghkgBhvprgUgDCgcFMA8G
DWCGSAGG+muBSAMKBwYwDwYNYIZIAYb6a4FIAwoHBzAPBg1ghkgBhvprgUgDCgcI
MA8GDWCGSAGG+muBSAMKBwkwDwYNYIZIAYb6a4FIAwoHCjAPBg1ghkgBhvprgUgD
CgcLMA8GDWCGSAGG+muBSAMKBwwwDwYNYIZIAYb6a4FIAwoHDTAPBg1ghkgBhvpr
gUgDCgcOMA8GDWCGSAGG+muBSAMKBw8wDwYNYIZIAYb6a4FIAwoHEDASBgNVHRMB
Af8ECDAGAQH/AgEAMIIBWgYIKwYBBQUHAQEEggFMMIIBSDBQBggrBgEFBQcwAoZE
aHR0cDovL25maXJvb3R3ZWIubWFuYWdlZC5lbnRydXN0LmNvbS9BSUEvQ2VydHNJ
c3N1ZWRUb05GSVJvb3RDQS5wN2MwgcMGCCsGAQUFBzAChoG2bGRhcDovL25maXJv
b3RkaXIubWFuYWdlZC5lbnRydXN0LmNvbS9vdT1FbnRydXN0JTIwTWFuYWdlZCUy
```

MFNlcnZpY2VzJTIwTkZJJTIwUm9vdCUyMENBLG91PUNlcnRpZmljYXRpb24lMjBB
dXRob3JpdGllcyxvPUVudHJ1c3QsYz1VUz9jQUNlcnRpZmljYXRlO2JpbmFyeSxj
cm9zc0NlcnRpZmljYXRlUGFpcjtiaW5hcnkwLgYIKwYBBQUHMAGGImh0dHA6Ly9u
ZmlvY3NwLm1hbmFnZWQuZW50cnVzdC5jb20wggGaBgNVHR8EggGRMIIBjTCB+qCB
96CB9IY5aHR0cDovL25maXJvb3R3ZWIubWFuYWdlZC5lbnRydXN0LmNvbS9DUkxz
L05GSVJvb3RDQTIuY3JshoG2bGRhcDovL25maXJvb3RkaXIubWFuYWdlZC5lbnRy
dXN0LmNvbS9jbj1XaW5Db21iaW5lZDIsb3U9RW50cnVzdCUyME1hbmFnZWQlMjBT
ZXJ2aWNlcyUyME5GSSUyMFJvb3QlMjBDQSxvdT1DZXJ0aWZpY2F0aW9uJTIwQXV0
aG9yaXRpZXMsbz1FbnRydXN0LGM9VVM/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
dDtiaW5hcnkwgY2ggYqggYekgYQwgYExCzAJBgNVBAYTAlVTMRAwDgYDVQQKEwdF
bnRydXN0MSIwIAYDVQQLExlDZXJ0aWZpY2F0aW9uIEF1dGhvcml0aWVzMS0wKwYD
VQQLEyRFbnRydXN0IE1hbmFnZWQgU2VydmljZXMgTkZJIFJvb3QgQ0ExDTALBgNV
BAMTBENSTDEwHwYDVR0jBBgwFoAU+t8jAcSq7CPjrW8NNKUNzzlkZV4wHQYDVR0O
BBYEFGb5JZiuy/vhjACEGdSF/5NW6tamMA0GCSqGSIb3DQEBCwUAA4IBAQAYzB20
TFlb/g4Q/l+evqW05L9MxsayCR+sCXxpi4CtYgeAxWGTTLIUbbRj7vWPGC/aanWr
Was8mRYsJSQRy3SGZJ0cG8bkheIe4Tqm6ALmw2DRaaolDKSJ6yQ+LART0C+Oi8IY
k5BcM6hLpQlm/30UYtvA53AiwTMJVClb7QK+e//4Z0wnDD23PdQXWiUQE9q4+vz3
L+ifgFEljY6EqdKT6dlZVl16xt5gZrrdFlsblPZxuvnnmgl88/qwMd2zfcKTIanP
M+llQt6jM2L3C+PTOBALt9XZyq3Qw1RLfQWsaNcs0/fDOoJfHHw0r9QmMLrBpWJp
7pVxA2WkITMFclBt
-----END CERTIFICATE-----

Specimen End Entity (Server) Certificate

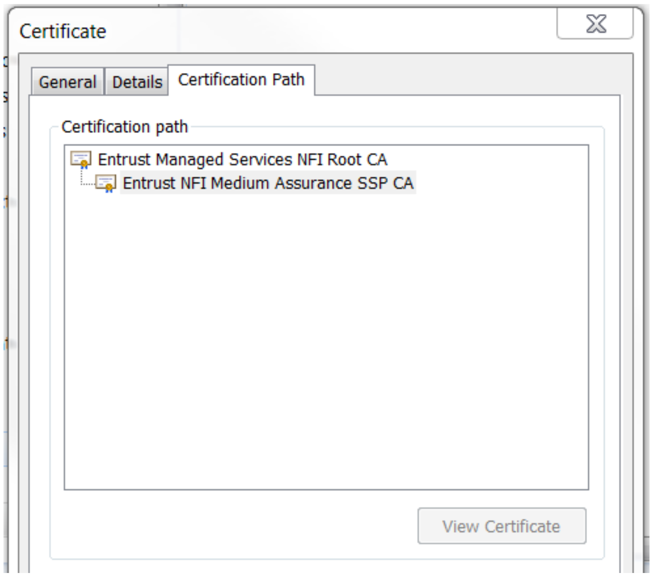
The following is an example revoked and expired production server certificate for Carequality both in Base64/DER format, and textual format. Note that the OCSP and CRL distribution points may need to be added to your outbound firewall white list:

-----BEGIN CERTIFICATE-----
MIIHZDCCBkygAwIBAgIESq909DANBgkqhkiG9w0BAQsFADBxMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEsMCoGA1UECxMjRW50cnVzdCBORkkgTWVkaXVtIEFzc3VyYW5jZSBT
U1AgQ0EwHhcNMTcwNjAyMTMwNzI5WhcNMTgwNjAyMTMzNzI5WjBWMQswCQYDVQQG

```
EwJVUzEQMA4GA1UEChMHSEhTLU9OQzEUMBIGA1UECxMLQ0FSRVFVQUxJVFkxHzAd
BgNVBAMTFmhpZXByb2QwMS5oaWV0ZXhhcy5vcmcwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCkyYgSLLJ+b1YrUtRvUF01mfI/RRjGOKU+3+dIkt8c8TZM
msJVD48qeCao0HaZgP2byhskUyjrJ98uZmGChCPS48DCaBySLGq3NQxk02Kno2ip
T+ZDjDDXHVIHefWEPmjgHWDENGqQcK3d46avgp43toIjBlKmd6NYHtcE4Y65RNwk
qU+OCd8XwVR6nYWdVoGkxkZ5yYrHogjHMI/hQ4ohzSUZRsPH3IxtUuqd2PliHUXS
/paVJOAexRaT6IWeE5oAdiukruLPxuDDFBEqfZjYhvP9GHH4YJksY7P2zfUDsQsa
O/FJXhZxWdMw3of4uooXyncePrYumSh4NWxrAfIXAgMBAAGjggQdMIIEGTAOBgNV
HQ8BAf8EBAMCBaAwEQYJYIZIAYb4QgEBBAQDAgbAMIIBaAYIKwYBBQUHAQEEggFa
MIIBVjCBxwYIKwYBBQUHMAKGgbpsZGFwOi8vbmZpbWVkaXVtc3NwZGlyLm1hbmFn
ZWQuZW50cnVzdC5jb20vb3U9RW50cnVzdCUyME5GSSUyME1lZGl1bSUyMEFzc3Vy
YW5jZSUyMFNTUCUyMENBLG91PUNlcnRpZmljYXRpb24lMjBBdXRob3JpdGllcyxv
PUVudHJ1c3QsYz1VUz9jQUNlcnRpZmljYXRlO2JpbmFyeSxjcm9zc0NlcnRpZmlj
YXRlUGFpcjtiaW5hcnkwWgYIKwYBBQUHMAKGTmh0dHA6Ly9uZmltZWRpdW1zc3B3
ZWIubWFuYWdlZC5lbnRydXN0LmNvbS9BSUEvQ2VydHNJc3N1ZWRUb05GSU1lZGl1
bVNTUENBLnA3YzAuBggrBgEFBQcwAYYiaHR0cDovL25maW9jc3AubWFuYWdlZC5l
bnRydXN0LmNvbTAaBgNVHSAEEzARMA8GDWCGSAGG+muBSAMKBwMwKQYDVR0RBCIw
IIYeSFRUUDovL1dXVy5DQVJFUVVBTElUWS5PUkcvVjAxMIIBrAYDVR0fBIIBozCC
AZ8wggEKoIIBBqCCAQKGQ2h0dHA6Ly9uZmltZWRpdW1zc3B3ZWIubWFuYWdlZC5l
bnRydXN0LmNvbS9DUkxzL05GSU1FRElVTVNTUENBMS5jcmyGgbpsZGFwOi8vbmZp
bWVkaXVtc3NwZGlyLm1hbmFnZWQuZW50cnVzdC5jb20vY249V2luQ29tYmluZWQx
LG91PUVudHJ1c3QlMjBORkklMjBNZWRpdW0lMjBBc3N1cmFuY2UlMjBTU1AlMjBD
QSxvdT1DZXJ0aWZpY2F0aW9uJTIwQXV0aG9yaXRpZXMsbz1FbnRydXN0LGM9VVM/
Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdDtiaW5hcnkwgY6ggYuggYikgYUwgYIx
CzAJBgNVBAYTAlVTMRAwDgYDVQQKEwdFbnRydXN0MSIwIAYDVQQLExlDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0aWVzMSwwKgYDVQQLEyNFbnRydXN0IE5GSSBNZWRpdW0g
QXNzdXJhbmNlIFNTUCBDQTEPMA0GA1UEAxMGQ1JMMjc5MCsGA1UdEAQkMCKADzIw
MTcwNjAyMTMwNzI5WoEPMjAxODAyMTMwMTM3MjlaMB8GA1UdIwQYMBaAFGb5JZiu
y/vhjACEGdSF/5NW6tamMB0GA1UdDgQWBBTfVooxZLqy8lMt1S1q1pS/udafYDAJ
BgNVHRMEAjAAMBkGCSqGSIb2fQdBAAQMMAobBFY4LjIDAgOoMA0GCSqGSIb3DQEB
CwUAA4IBAQCZrqIxuE8FOVpzttA07grgUXOG2KxLTnvHLPMJlKIiNSseaPzdtkdU
G8gtx983A+GdqRx1KOBH7ZFQz+q2RHpZ6K8VurHDru3jCkn8TmCiuP+2Ew9MOSv5
```

```
NqBurCXzfPsSu+ObRfhpdk1AiB6ElFyrNqjwaSDr1FEz1F2lEzCJMnuR1AIxNsa6
xA/XeAASCIXHZur2StmDTiNSUVlFPIY4HyfBg1AB1DWyZw/RT54+aRl94oeY/I/f
IpQ3wV1MK14pbMo4EtA8K0T10VaiZKLLGjZ76kCtbgx9qjoNVPalTEsGMYUr/nFu
5oIQBi8A0MIZ5s6A6QCXxcS3N8Ley15R
-----END CERTIFICATE-----
```

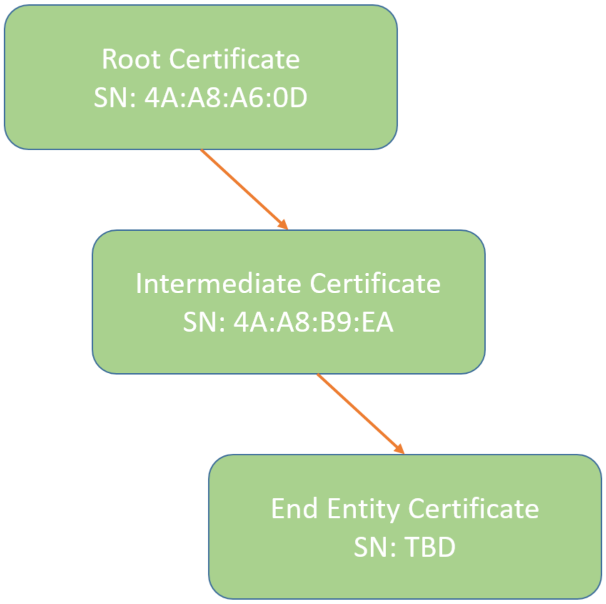
The figure below illustrates the recommended trust chain for Carequality production certificates. Note that this is a three-level trust chain.



Entrust Managed Services NFI Root CA
Entrust NFI Medium Assurance SSP CA

Carequality Standard certification path configuration.

Under the recommended configuration, the gateway root keystores will now have a Entrust Root CA certificate hashed by SHA-256 (with serial number: 4A:A8:A6:0D/1252566541). Also, intermediate keystores will have the Entrust intermediate (a.k.a. subordinate or signing CA) certificate (serial number: 4A:A8:B9:EA/1252571626) which is signed by the Entrust root certificate. Both of these certificates contain keys that were put into operational use on approximately June 1st, 2017 and are thus not interoperable with the prior certificates unless the prior certificates are also installed. The figure below depicts the required outbound trust chains and inbound truststores:



Visual representation of the recommended truststore and keystore configurations.

AIA Issuing CA Certificate File Locations

The AIA file located at the following link contains both the old and new Subordinate CA certificates and is found, authoritatively, in Participating Systems' Sequoia-issued End Entity certificates:

http://nfimediumsspweb.managed.entrust.com/AIA/CertsIssuedToNFIMediumSSPCA.p7c

CRL and OCSP Access Points

In order for Participating Systems to check for revoked or suspended certificates, it may be necessary to allow for outbound access to the CRL distribution point or the OCSP responder network access point. These two URIs MUST be authoritatively obtained from Participating Systems' End Entity certificate extension attributes, but they are listed below for your reference:

X509v3 CRL Distribution Point:
http://nfimediumsspweb.managed.entrust.com/CRLs/NFIMEDIUMSSPCA1.crl

OCSP: http://nfiocsp.managed.entrust.com

(end of file)