Technical Trust Policy

Version 4.0

Updated: Jul 31, 2023

Table of Contents

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

Certificate Authority (CA): the entity that issues digital certificates for the Carequality 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 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.

Sponsor: The person responsible for acting as the requestor for a Carequality 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 Subscriber Agreement. Every Sponsor must create an account with the designated Certificate Authority and be Identity Proofed as defined (typically IAL2) by the CA.

Subscriber: The organization that is requesting the certificate. Each Subscriber must be registered with the Certificate Authority that issues the organization its Carequality certificate.

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.

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 any Carequality designated Certificate Authority is governed by its own rules. Production 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 send an email to techsupport@carequality.org asking for a Production certificate. It is recommended that the person who will be the Implementer's Sponsor send this email to Tech Support. After this request is sent, a ticket will be opened in the Carequality Customer Relationship Management (CRM) tool. This ticket will be reviewed by the Implementer's Carequality Program Manager to sign-off on this request. In order to be issued their initial Production certificate, Implementers must complete a series of onboarding steps before a Production certificate is issued. The respective Program Manager shall ensure all of these steps are completed before permitting the certificate to be issued. Certificate renewals are also subject to review, to ensure the Implementer is in good standing, and allowed to participate further in the Use Case.

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 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.

Test (or Validation) certificates are also available upon request. Unlike a Production certificate request, Identity Proofing for a Test certificate is not required. Requests for Test certificates can also be made by sending an email to techsupport@carequality.org asking for such. The ticketing and Program Manager review process as described above (for Production certificates) also applies.

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 and Carequality Connections (CCs) MAY deploy as either a single-tenant gateway or multi-tenant gateway. In either scenario there is a one-to-one relationship between the single X.509 certificate and the Fully Qualified Domain Name (FQDN) of the Listed End Point published in the Directory.

For clarity, a Carequality Implementer with multiple CCs hosted behind a single gateway, MAY be deployed with only one X.509 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 each/all of those CCs is/are 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 X.509 certificate being issued to each CC.

Server Name Indication (SNI) Support

All Implementer and CC initiating gateways must support the ability to initiate requests using TLS Server Name Indication (SNI) [1]. All Implementer and CC responding gateways must:

1) Support the ability to successfully process SNI inbound requests even if the responding gateway does not host multiple tenants OR;

2) Establish a TLS connection to the correct virtually-hosted tenant.

Subject Alternative Name (SAN) Use

Carequality X.509 certificates may use Subject Alternative Names for two purposes. The Certificate Authority 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 Carequality. A Subject Distinguished Name type SAN field indicating the Common Name of the certificate Subject may also be denoted, but only if specifically requested by the Implementer or CC.

[1] The HTTPS-Only Standard: Server Name Indication (SNI) - https://https.cio.gov/sni/

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 that are secured by a X.509 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 (CN) 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 within the Carequality framework.

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 800-52r2 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.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 (a "Validated Crypto Module"). Non-normative: This approach is designed to provide Participating Systems with a migration path that 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 3.0.

Specifically, Participating Systems using a Validated Crypto Module MUST install, configure, and operate their FIPS 140-2 Validated Crypto Module 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 invalidated crypto module must configure their crypto module to operate in the same manner as a Validated Crypto Module and must disable unsecure or weak functionality such as 3DES encryption or MD5 hashes.

IP Address Allow Listing

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 allow listing for either outbound or inbound connections. Participating Systems MUST NOT implement an IP allow list 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 allow listing, 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. 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.

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 MAY continue to support a single outbound trust chain for standard operational use, but Participating Systems MUST be able to switch their outbound trust chain to a secondary trust chain with minimal notice and downtime. 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 downtime.)

Other Uses

X.509 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 may be subject to downtime due to Carequality activities such as certificate revocation or directory entry changes. Other uses of Carequality Listed End Points, and X.509 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 1.2 or greater with mutual authentication for all transactions.

The same fully qualified domain name (FQDN) and port combination MUST 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 Certificate Information

Implementers and Participating Systems are responsible for maintaining up-to-date contact information and Sponsor information, along with up-to-date entries in the Carequality Directory. 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 Participating System SHOULD have multiple Sponsors. The Certificate Authority 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 Identity Proofing process for that organization.

Per the CA provider utilized by Carequality, all certificate recipients must be Identity Proofed and sign a Subscriber Agreement before being issued a Production certificate. Industry guidelines state that identity proofing is valid for a period of 2 years. This process indicates the person officially authorized by Carequality Participating Systems as the Sponsor for purposes of receiving and accepting responsibility for the secure use and management of the Carequality X.509 certificate and its associated keys. The Sponsor will be identity-proofed per NIST 800-63A IAL2 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 techsupport@carequality.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) Every 12 months, the signed certificate will expire and need to be re-issued. The CA shall attempt to notify the Sponsor on file approximately 60-90 days prior to the certificate expiration to begin the renewal process.
4) The Sponsor is responsible for ensuring that the X.509 certificate and access codes are maintained securely at all times.

Appendix A – Certificate Trust Chain Configuration

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

CRL Access Point

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 points. The URIs MUST be authoritatively obtained from Participating Systems' 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

Appendix B – Carequality Patient Request Identity Verification Policy

Overview

When processing data requests initiated by a patient (Patient Request), it is imperative that the patient's information is disclosed only to the patient to whom that information belongs. This is typically accomplished by having the Patient authenticate directly with the data source, but in cases where such an authentication workflow is either undesirable or infeasible, additional mechanisms are needed.

This appendix details an exchange pattern within a federated trust framework (Carequality) in which a Query Initiator facilitating a Patient Request query must partner with a Credentialing Service Provider (CSP) to identity proof the patient to at least IAL2 prior to sending requests to the data sources (Carequality Implementers and CCs). The CSP must provide a signed, technical token (IAL2 Claims Token) containing the patient's demographics to the Patient Request Initiator, as part of the IAL2 identity verification service. By policy, the Patient Request Initiator must provide this token to the Query Responder within the Patient Discovery (XCPD) transaction.

Trusted Credential Service Providers

Carequality Implementers or their CCs that initiate queries for Patient Request must use one or more of an approved a set of trusted CSPs that has been vetted and approved by a certifying body selected by Carequality which will be authorized to perform IAL2 identity verification services for Carequality Query Initiators. Carequality's website will link to all approved certifying bodies. Each CSP will provide an endpoint to share a JSON Web Key Set (JWKS) which a Query Responder can use to validate an identity token issued by that CSP. After verifying a patient's identity on behalf of the Query Initiator, the CSP SHALL make available to that Query Initiator a signed OpenID Connect token.

The Query Initiator SHALL relay the CSP-provided OpenID Connect token to the Query Responder using an additional SAML attribute statement ("id_token") containing the OIDC token in Query-Based Document Exchange or as an additional element ("id_token") within the Carequality extension in the FHIR Use Case.

OpenID Token Construction (IAL2 Claims Token)

OpenID Connect (OIDC) is an authentication protocol which specifies how to exchange a user's identity. OIDC closely integrates with the OAuth 2.0 authorization method. By specifying its use in the QBDE and FHIR Use Case exchange, we anticipate and align the exchange of patient identity with future exchange methods. In healthcare, OIDC is built into the HL7 SMART on FHIR specification and is also the *de facto* standard for FHIR exchange internationally.

The OpenID Connect Core specification describes many optional capabilities. This specification makes use of OIDC's ID Token. The following requirements apply:

- Public Keys Published as Bare JWK Keys: The CSP SHALL publish public keys as bare JWK keys (which MAY also be accompanied by X.509 representations of those keys).
- Signed ID Token: The CSP SHALL support Signing ID Tokens with RSA SHA-256.
- Claims: The CSP SHALL include the below claims.

OpenID Connect JWT headers

OIDC JWT Header	
alg	Hardcoded to “RS256”.
kid	Identifies which key to use from the JWKS.
typ	Hardcoded to “JWT”.

OIDC JWT Body	**Description**
aud	HCID of the Query Initiator as a URI. For example urn:oid:<oid> (per RFC 3001).
iat	When the CSP issued the token.
iss	The base URL of the CSP at which the JWKS is accessible.
jti	Unique identifier for the JWT.
Demographics that MUST be included or use “Unknown” in your response	
given_name	
family_name	
date of birth	
address	See list and definition of address elements, below. Allow multiple addresses (array) if supported by the CSP.
Demographics that MUST be included if known	
historical_address	See list and definition of address elements, below. Allow multiple addresses (array) if supported by the CSP.
middle_name	
middle initial	
suffix	
email	
phone_number	
SSN	
SSN Last four digits	
ZIP+4	
Sex	

OIDC JWT Body Address Object	**Optionality**
formatted	OPTIONAL
street_address	REQUIRED, IF KNOWN
city	REQUIRED, IF KNOWN
state	REQUIRED, IF KNOWN
zip_code	REQUIRED, IF KNOWN
country	REQUIRED, IF KNOWN

Example OIDC JWT

```
{
      "alg":"RS256",
      "kid":"toW9jMUSN/5/L3iwaQGdTmNDuhvp/JcAZVH/cOJ6OrE=",
      "typ":"JWT"
} {
      "aud":"hci1",
      "iat":1666280632,
      "iss":”https://csp.example.com”,
      “sub”:” f7bdf590-2fc4-4718-8f33-043c8f96b66d”,
      “jti”:”bcb9533e-1cc1-48bd-848b-b4200ea504b9”,
      “given_name”:”John”,
      “family_name”:”Schmidt”,
      “middle_name”:”Jacob Jingleheimer”,
      “nickname”:”Ed”,
      “email”:”jjjs@example.com”,
      “email_verified”:true,
      “phone”:”555-555-5555”,
      “gender”:”M”,
      “birthdate”:”Unknown”,
      “address”:{
            “formatted”:” 1060 West Addison Street, Chicago, IL 60613 USA”,
            “street_address”:” 1060 west Addison Street”,
            “locality”:”Chicago”,
            “region”:”Illinois”,
            “postal_code”:”60613”,
            “country”:”USA”
            },
      “http://www.carequality.net/OIDC/claim/mothers_maiden_name”:”Vetter”,
      “http://www.carequality.net/OIDC/claim/principle_care_provider_id”:”293
84572342”,
      “http://www.carequality.net/OIDC/claim/birth_place_address”: {
            “formatted”:”1060 West Addison Street, Chicago, Illinois 60613
USA”,
            “street_address”:”1060 west Addison Street”,
            “locality”:”Chicago”,
            “region”:”Illinois”,
            “postal_code”:”60613”,
            “country”:”USA”
            },
      “http://www.carequality.net/OIDC/claim/birth_place_name”:”Peaceful
Valley Hospital”
}
```

JSON Web Key Set URL

The CSP signs with a private key and publishes the corresponding public key at <iss>/.well-known/openid-configuration per OpenID Connect Discovery. For example, if the ID token’s iss element is https://csp.example.com, the CSP’s JSON Web Key Set (JWKS) document would be available at: https://csp.example.com/.well-known/openid-configuration.

Query Initiators and Query Responders use the public key to verify the CSP’s signature on demographics included in the JWT. Therefore, the CSP SHALL provide the JWKS publicly without requiring authentication.

CSP are encouraged to rotate encryption keys as described in OpenID Connect Core.