**Modified and New VNFRQTS Requirements for HTTPS Authentication**

*R-763774* - The xNF ~~PNF~~ **MUST** support a HTTPS connection to the DCAE VES Event Listener.

N-1: The xNF **SHOULD** support Certificate Authentication for authenticating HTTPS connections to the DCAE Event Listener.

N-2: If the xNF supports Certificate Authentication, then when the xNF sets up a HTTPS connection to the DCAE Event Listener, the xNF **MUST** provide its own X.509 certificate to the DCAE VES Event Listener and the Subject Name **MUST** uniquely identify the xNF according to [RFC 5280](https://tools.ietf.org/html/rfc5280).

N-3: If the xNF supports Certificate Authentication, then the xNF **MUST NOT** support Basic Authentication for authenticating HTTPS connections to the DCAE Event Listener.

N-4: If the xNF does not support Certificate Authentication, then the xNF **MUST** support Basic Authentication for authenticating HTTPS connections to the DCAE Event Listener.

*R-01427* – Ifthe xNF supportsBasic Authentication, then the xNF ~~The PNF~~ **MUST** support the provisioning of security and authentication parameters (HTTP username and password) in order to be able to authenticate with DCAE VES Event Listener ~~(in ONAP)~~.

~~Note: In R3, a username and password are used with the DCAE VES Event Listener which are used for HTTP Basic Authentication.~~

Note: The configuration management and provisioning software are specific to a vendor

architecture.

*R-894004* - Ifthe xNF supportsBasic Authentication, then ~~W~~when the xNF ~~PNF~~ sets up a ~~HTTP or~~ HTTPS connection to the DCAE VES Event Listener ~~collector~~, it **MUST** provide a username and password to the DCAE VES Event Listener ~~collector for HTTP Basic Authentication~~ in the Authorization header. Note: HTTP Basic Authentication has 4 steps: Request, Authenticate, Authorization with Username/Password Credentials, and Authentication Status as per RFC7617 ~~and RFC 2617~~.

*R-49109* – The xNF ~~VNF~~ **MUST** support HTTP~~/~~S using TLS v1.2 or higher with strong cryptographic ciphers.

*~~R-579051~~* ~~- The PNF~~ **~~MAY~~** ~~support a HTTP connection to the DCAE VES Event Listener.~~

**New ONAP Security Requirements**

O-1: DCAE VES Listener MUST support 4 options for authentication of HTTPS connections

1. Certificate only enabled (auth.method = certOnly)
2. Basic Authentication only enabled (auth.method = basicAuth)
3. Certificate and Basic Authentication enabled (auth.method = certBasicAuth)
4. No authentication performed (auth.method = noAuth)

O-2: If auth.method = certOnly, DCAE VES Listener MUST authenticate the HTTPS client as follows:

* 1. For a client with a valid certificate, DCAE VES Event Listener MUST pass the client authentication and MUST use the Subject Name in the certificate as the client identity for authorization according to [RFC 5280](https://tools.ietf.org/html/rfc5280).
	2. For a client with no or an invalid certificate, DCAE VES Event Listener MUST fail the client authentication.
	3. DCAE VES Event Listener MUST NOT consider client basic authentication credentials.

O-3: If auth.method = basicAuth, DCAE VES Event Listener MUST authenticate the HTTPS client as follows:

1. For a client with correct basic authentication credentials, DCAE VES Event Listener MUST pass the client authentication and MUST use the username in the Authorization header as the client identity for authorization.
2. For a client with no or incorrect basic authentication credentials, DCAE VES Event Listener MUST fail the client authentication.
3. DCAE VES Event Listener MUST NOT consider client certificate credentials.

O-4: If auth.method = certBasicAuth, DCAE VES Event Listener MUST authenticate the HTTPS client as follows:

1. For a client with a valid certificate, DCAE VES Event Listener MUST pass the client authentication and MUST use the Subject Name in the certificate as the client identity for authorization according to [RFC 5280](https://tools.ietf.org/html/rfc5280).
2. For a client with no or an invalid certificate and with correct basic authentication credentials, DCAE VES Event Listener MUST pass the client authentication and MUST use the username in the Authorization header as the client identity for authorization.
3. For a client with no or an invalid certificate and with no or incorrect basic authentication credentials, DCAE VES Event Listener MUST fail the client authentication.

O-5: If auth.method = noAuth, DCAE VES Event Listener MUST pass the HTTPS client authentication. For a client with a valid certificate, DCAE VES Event Listener MUST use the Subject Name in the certificate as the client identity for authorization according to [RFC 5280](https://tools.ietf.org/html/rfc5280). For a client with no or an invalid certificate and with basic authentication credentials, DCAE VES Event Listener MUST use the username in the Authorization header as the client identity for authorization.

O-6: DCAE Event Listener MUST authorize the HTTPS client using the identity derived during authentication.

O-7: If auth.method = certOnly or certBasicAuth, then DCAE MUST provide an Event Listener that is able to authenticate HTTPS clients using mutual certification authentication for TLS.

O-8: If auth.method = basicAuth or certBasicAuth, then DCAE MUST provide an Event Listener that is able to authenticate HTTPS clients using Basic Auth over HTTPS where the TLS is established using 1-way certification authentication.