VRS Current Security Approach

- Solution providers and network participants who intend to provide their own requesting or responding services are currently utilizing a TLS mutual authentication approach exchanging X.509 certificates.
- Certificates can either be self-signed or issued by a public certificate authority.
- Certificates are exchanged on a one-to-one basis with entities listed in the Registry (at a minimum) so that all entities are known to everyone else in the network.
- Managing certificate validity and expiration dates is something that will need to be taken care of during onboarding between solution providers or those building their own requesting or responding services.
- Certificates should have a limited validity of no more than 2 years and a new certificate should be provided at least 90 days in advance of expiry.