HDA
Healthcare Distribution Alliance
HEALTH DELIVERED

VRS Provider Network: Policy for Communication of Certificate Expiry and Renewal

The VRS Provider Network-Subgroup for Lookup Directory (LD) Readiness is a group of VRS Lookup Directory solution providers that have requestor/responder customer records for the purpose of responding to requests for verification. The failure to maintain up-to-date VRS certificates results in connectivity failures and other inefficiencies. The VRS Advisory Board has adopted this policy to support the activities of these solution providers when communicating the expiration and renewal of certificates.

This policy is intended to cover the following defined certificates:

- **Client certificate**:
  Definition: The certificate providers send with their LD interactions to identify themselves.
  Usage: The LD system uses a client certificate to authenticate itself during push/pull interactions with other LD systems.

- **Secure Socket Layer (SSL)[1] certificate on the endpoint:**
  Definition: The certificate used by a provider to enable the HTTPS protocol on their endpoint, ensuring secure communication between the server and the client.
  Usage: SSL certificates are used for encrypting the connection between two systems. To check the SSL certificate on another provider's endpoint, visit the provider's endpoint in the browser and examine the certificate.

Communication Policy for Service Providers

Following these steps and recommendations will enable clear, secure and efficient communication among solution providers when communicating certificate changes.

1. The VRS Registry should be used to maintain designated contact information for receiving certificate communication changes. For immediate access, ***only*** public URLs should be shared using the VRS Registry on the VRS SharePoint. Solution providers should not share private keys on the VRS Registry.
2. Provide renewed certificates at least 30 days before expiry.
3. To avoid service disruptions, provide and apply replacement certificates at the designated date and time from the issuer. Spontaneous changes may be caused by various events (i.e. compromised private keys, system build, updates, etc.) that require widespread communication and immediate troubleshooting and maintenance across the network.
4. Use a special email subject for email blasts regarding critical certificate changes. Recommended labels are provided below:

[1] SSL is a security protocol that encrypts data transmitted between a web server and a browser, creating a secure connection.

a. Notification: [Label] Certificate Expiring in 60 Days
b. Warning: [Label] Certificate Expiring in 30 Days
c. Urgent Notice: [Label] Certificate Expiring in 7 Days
d. Critical Notice: [Label] Certificate has Expired – Check VRS Registry for New Certificate URL
e. Critical Notice: Service Disruption - Certificate Replacement

Further, email subject labels should include qualifiers to differentiate between test and production environments, such as 'SSL for Test,' 'SSL Certificate for Production,' 'Client Certificate for Test,' and 'Client Certificate for Production.'

5. Contact the respective LD Provider when a connectivity issue is encountered.