Expiration of X.509 Certificate
Questions and Answers

1. How is OTT and IPTV content protected during delivery?
   A: VCAS supports authentication, key distribution and user control and acts as the root Certificate Authority in a PKI hierarchy. It uses X.509 certificates to validate and authorize all content protection communication within the network, including messaging between VCAS sub-system components as well as between the head-end system and mutually authenticated subscriber devices.

   Verimatrix IPTV (ViewRight IPTV) Client versions 3.7.x.x and below and Verimatrix OTT (ViewRight Web) Client versions 3.8.x.x and below use integrated PKI 1024-bit X.509 certificates to establish secure communication with the VCAS head-end. This certificate is referred to as 1k X.509 certificate.

   All VCAS and ViewRight versions 4.x use 2048-bit certificate, referred to as 2k X.509 certificate.

2. When the 1k X.509 client certificate will expire?
   A: X.509 certificates that use PKI 1024-bit key will expiry in October 2024.

3. Will the OTT clients be impacted by X.509 certificate expiration? / Which VR client versions will be impacted due to X.509 certificate expiration?
   A: Yes, all clients with ViewRight version 3.8 and lower will be impacted and need to be upgraded before the expiration date in 2024.

4. For how long the new 2048-bit certificates used by VCAS 4.x are valid?
   A: VCAS and ViewRight version 4.x use 2048-bit certificate that will expire on 19th of January 2038.

5. Is there anything that can be done from the headend to prolong functioning of the clients with 1k certificate?
   A: It is not possible to extend client's certificate expiration date from the headend. Clients perform checks on certificate expiration date which is hardcoded and cannot be changed from the headend. If the client's certificate is expired, the connection is rejected by both – client and server side.

6. Why Verimatrix does not recommend OTA upgrades to extend the end date of 1k certificates?
   A: Upgrading existing old clients would require reissuing new certificate in addition to integration efforts and OTA client upgrade. Considering limitations of reissuing 1k certificate, associated integration risks, low security level of end devices running

End-Of-Life non-supported clients, Verimatrix strongly recommend upgrading to 2k certificates that meet the latest security standards.

7. Will clients with 1k certificates loose studio approvals?
   A: Yes, all clients that cannot handle 2k RSA will lose studio approval. Moreover, local security certification authorities in many countries do not permit the usage of 1K certificates anymore.

8. As clients are checking the expiration date of the X.509 certificate, is it possible to move time back on the headend to prolong functioning of clients with 1k certificate?
   A: It is not possible because clients use sources of time which are not controlled by Verimatrix.

9. Which Verimatrix clients will be affected by X.509 certificate expiration. Should the certificate expiration date be checked on each client type?
   A: There is no need to check the certificate expiration date on each client type, as all IPTV (ViewRight IPTV) Client version 3.7.x.x and Verimatrix OTT (ViewRight Web) Client version 3.8.x.x and lower will be impacted and will lose access to VCAS decryption service causing black screen after the expiration date.