Frequently Asked Questions

1) **What are the leaf, intermediate and root certificates used for?**
   The SSL/TLS server certificate (leaf certificate) is used to establish a secure HTTPS connection to a NETS endpoint. The new leaf certificate will be issued under the new GlobalSign intermediate certificate, which chains to the new GlobalSign root certificate. Your system must be able to validate and trust this certificate chain to connect successfully.
2) **How can I check whether this update applies to my systems?**
   This update is relevant to systems that connect via HTTPS to eNETS (including the eNETS Admin Portal), NETSClick or Online QR API endpoints. Systems that do not trust the new GlobalSign certificate chain may encounter connection errors when certificates under the new chain are deployed. We recommend that your IT team or service provider review the truststore or keystore used for these connections against the root and intermediate certificate details listed above.
3) **What action is recommended?**
   We recommend that your IT team or service provider check for both certificates using the verification steps above. If either is missing, we recommend downloading the certificate package using the NETS link provided and importing the missing certificate(s) into the truststore or keystore used by your application. If both are already present, no additional import is required. This review does not involve renewing your own SSL/TLS certificate.
4) **Who should I contact for assistance?**

   If you require further assistance or face any issues, please contact us at enetsts@nets.com.sg or enetsps@nets.com.sg.