Frequently Asked Questions

1) **What is this SSL certificate used for? What service is using the certificate?**
   SSL certs are used to establish a secure connection from the merchant's server to eNETS endpoints. If your server initiates an HTTPS connection, the updated root and intermediate certificates must be present in your keystore to avoid connection failures.

2) **How do I know if I am impacted?**
   If your systems connect to the above-mentioned eNETS URLs using HTTPS and rely on local keystore/truststores, you may be impacted. Please check whether GlobalSign CA is already in your environment.

3) **What do I need to do, and what are the steps**?
   Please reach out to your IT team to review and import the new root and intermediate certificates into your application's keystore or truststore.

4) **How do I verify that the new certificates are working?**
   Once the certificates are renewed on eNETS side, you should observe successful HTTPS transactions.

5) **Who should I reach out to if I face any issues?**
   If you require further assistance or face any issues, please contact us at NETSAPIGatewaySupportTeam@nets.com.sg

Network for Electronic Transfers (Singapore) Pte Ltd
351 Braddell Road • #01-03 • Singapore 579713
T +65 6272 0533 F +65 6272 2334 W www.nets.com.sg
Co. Reg. No. 198500065G GST Group Reg. No. M90370546E