

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 truststore or 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 truststore or keystore 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 truststore or keystore.

4) **How do I verify that the new certificates are working?**

Once the certificates are renewed on eNETS side (scheduled for **17 June 2025**), you should observe successful HTTPS transactions.

5) **Who should reach out to if any issues?**

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