



Frequently Asked Questions

1) **What is this mTLS certificate used for? What service is using the certificate?**

NETS Click merchants send the host API call to NETS via mTLS connection. The mandatory requirement is the NETS root and intermediate certs should be imported to the trusted CA certs or keystores.

2) **How do I know if I am impacted?**

NETS Click merchants should update the existing mTLS cert to the new host and test out a NETS Click transaction. If there's any connection issue, please import the new root and intermediate certs and try again.

NETS Click merchants are strongly recommended to do same for Production domains, and should there be any issues/difficulties, merchant can still point back to existing domain and troubleshoot together.

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?**

During the UAT testing, if there's no host connection error, or NETS Click payment error after changing to the new domain name, the new certs and new domain are working. Merchant can plan to update in production environment.

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 eNETSTS@nets.com.sg