

Steps to Verify Certificate Installation

Actions required at your end before the cutover date:

To determine whether you need to import the new intermediate or root certificate, you can list the existing certificate in your truststore or keystore. If you are using Linux servers, follow these steps:

- 1) Confirm you have GlobalSign root and intermediate in your keystore/trust.

To determine whether you need to import the new intermediate or root certificate, you can list the existing certificate in your truststore or keystore. If you are using Linux servers, follow these steps:

- i. Navigate to your keystore / truststore location in your application server
- ii. Enter command: `keytool -list -v -keystore your_keystore_name > /tmp/certificates_list.txt` (Enter your password when prompted)
- iii. Open /tmp/certificates_list.txt and validate if below certificate details are already present.

GS_Chain.cer which is intermediate certificate , serial number :

01ee5f221dfc623bd4333a8557 , valid from : Wednesday, November 21, 2018 8:00:00 AM , valid to : Tuesday, November 21, 2028 8:00:00 AM ,
CN = GlobalSign RSA OV SSL CA 2018

GS_Root.cer which is root certificate , serial number : 04000000000121585308a2,
valid from Wednesday, March 18, 2009 6:00:00 PM, valid to : Sunday, March 18, 2029 6:00:00 PM, CN = GlobalSign

Alternatively, you may use GUI-based tools such as Keystore Explorer to inspect your truststore or keystore.

PS: If the certificates are already present then you do not need to import them to your truststore or keystore.

If the certificates cannot be found, please download and import the root and intermediate certificate from this [link](#).

- 2) Confirm if you are pinning to the base certificate at your end.

uat-api.nets.com.sg (UAT environment) or api.nets.com.sg (Production Environment)

If you are pinning the base certificate download and import the base certificate into your trust/keystore.

- 3) Proceed to arrange for testing after the renewal is completed and share contact details.

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

Please do not remove the existing NETS SSL cert to avoid any unnecessary interruption to your existing connectivity.

We kindly request your assistance in reviewing whether your systems are currently interfacing with any of the above domains, as this may impact connectivity following the SSL certificate renewal.

Please ensure that appropriate testing is conducted in the UAT environment to facilitate a smooth transition to Production.

The new SSL certificates are available for download:

<i>Dates available for download</i>	<i>Environment:</i>	<i>Links</i>
<u>22nd September 2025</u>	<u>UAT</u>	https://developer.nets.com.sg/assets/others/certificates/uat-api.nets.com.sg_2025.zip
<u>8th October 2025</u>	<u>Production</u>	https://developer.nets.com.sg/assets/others/certificates/api.nets.com.sg_2025.zip

Should you have any questions or require further clarification, please do not hesitate to reach out to us at NETSAPIGatewaySupportTeam@nets.com.sg