User Guide 33B Installing a digital certificate on a USB security token

Purpose of this Guide

The purpose of this guide is to assist SPEAR users to set up a new USB security token and install their digital certificate. Lodging party signing users must store their certificates on a USB security token. If you are exempt from this requirement, please follow User Guide 33A instead.

Notes

1. This guide follows on from ‘User Guide 32 - Applying for a Certificate Manager digital certificate’ or from ‘User Guide 35 – Applying for a standard digital certificate’.
2. Once your certificate has been approved by DigiCert, you will receive an email containing instructions to assist you with installing your certificate.
3. If you have already installed your digital certificate on your computer, follow the steps in ‘User Guide 33C – Importing existing digital certificates onto a USB security token’ instead.

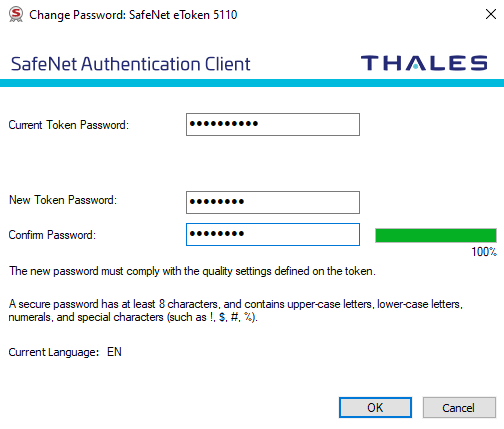
Important - Software required

Please ensure the SafeNet Authentication Client software has been installed prior to commencing the steps below. This can be downloaded from the DigiCert website:

<https://www.digicert.com/StaticFiles/SafeNetAuthenticationClient-x64.msi>

If you experience issues installing this software, please contact your IT department to ensure you have the required privileges.

1. Insert your token and change the password

Once the software has been installed, insert your USB security token into one of your computer’s USB ports. If this is the first time you’ve used this token, the software will prompt you to change your password.

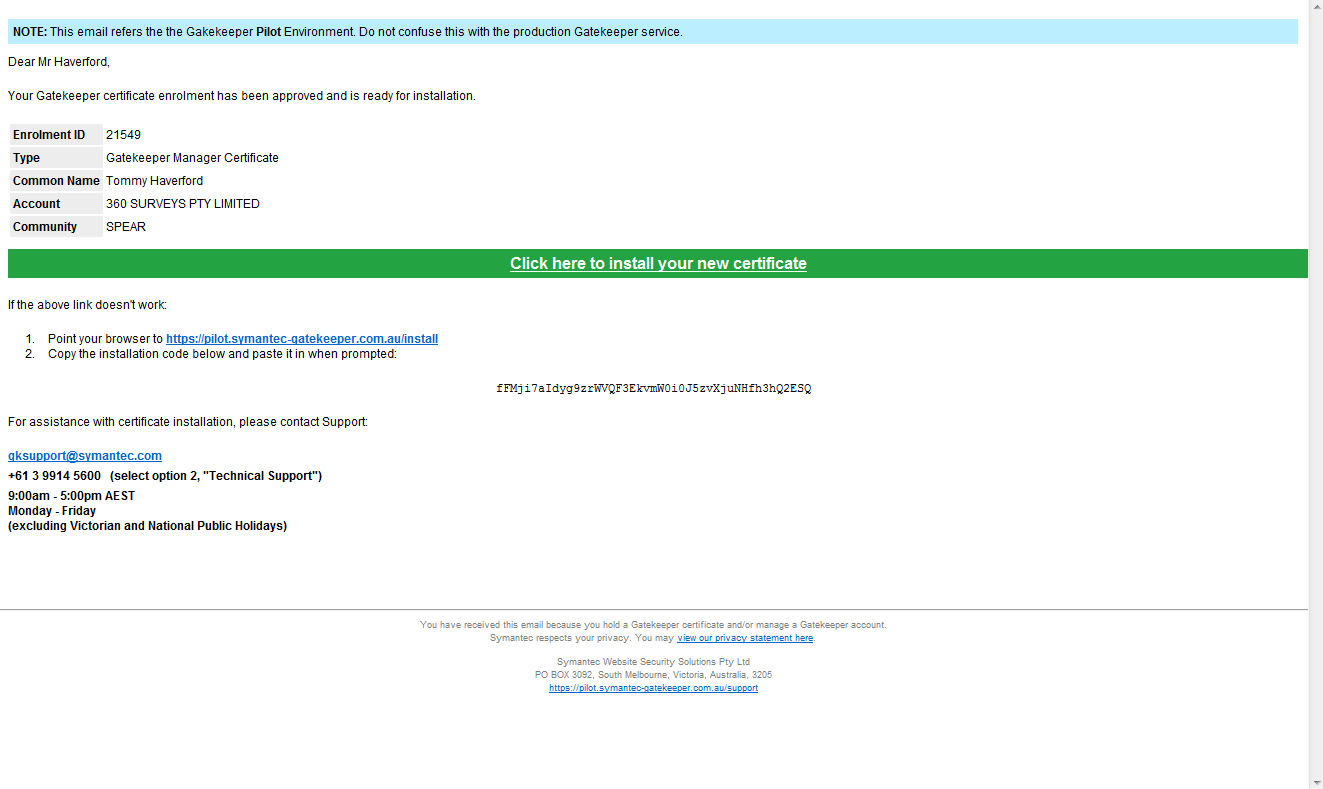
NOTE: The default token password is: 1234567890

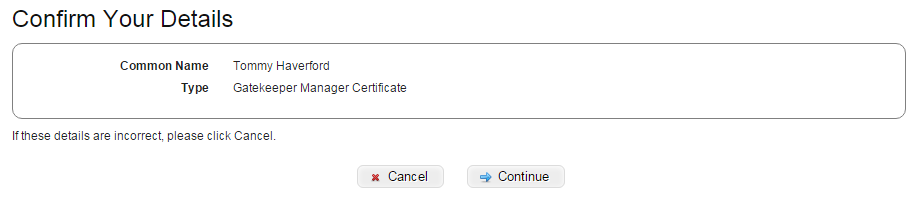
Enter and confirm a new password to protect your USB security token.

This is the password that you will be asked to enter when you digitally sign in SPEAR

2. Open the installation email

You will receive an email from DigiCert when your digital certificate has been issued. To commence the installation process, click on the hyperlink contained in the email from DigiCert.

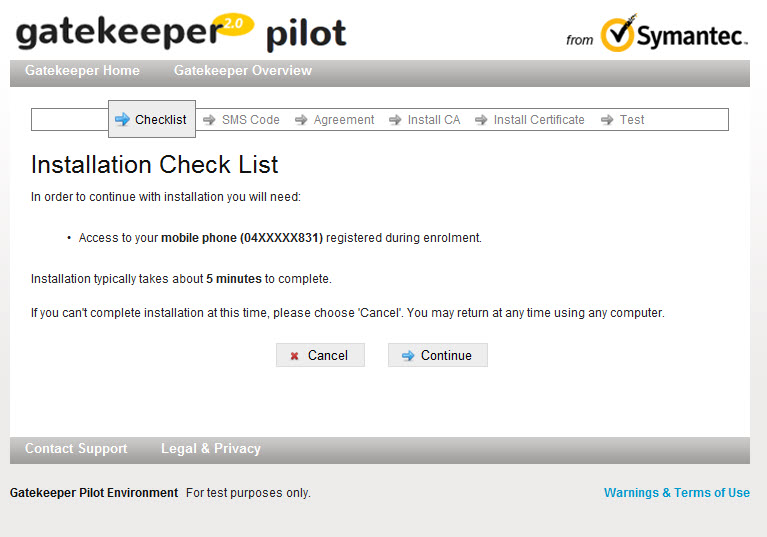


Confirm that the details displayed are correct.

Click on ‘continue’.

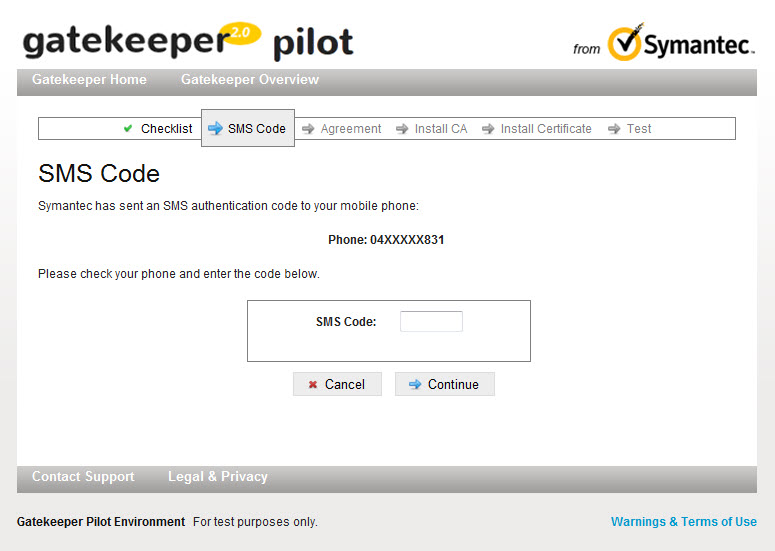
3. Enter SMS code

Have your mobile phone ready.



Click on ‘continue’.

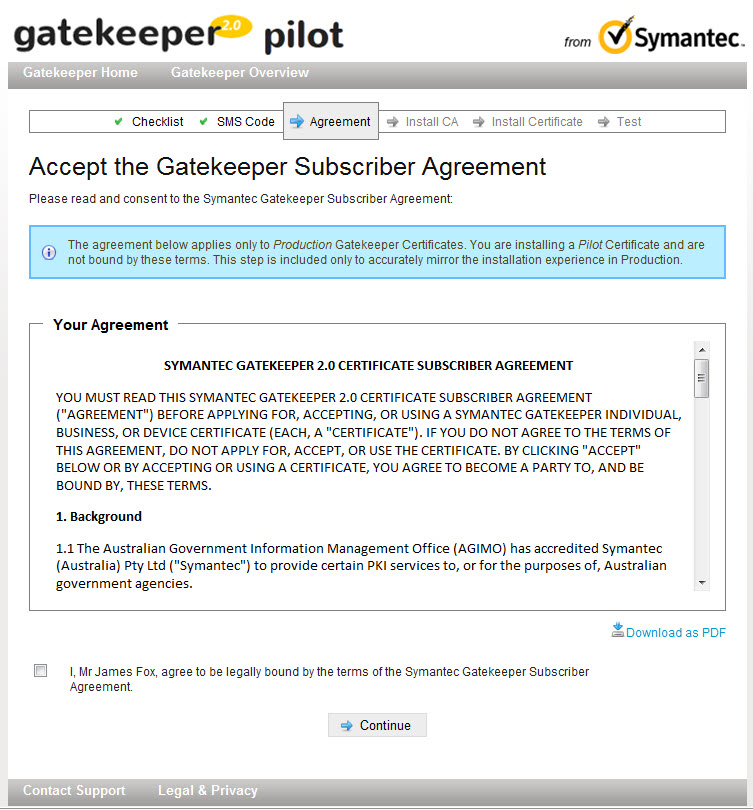
Enter the code sent to your mobile.



Enter code and click continue’.

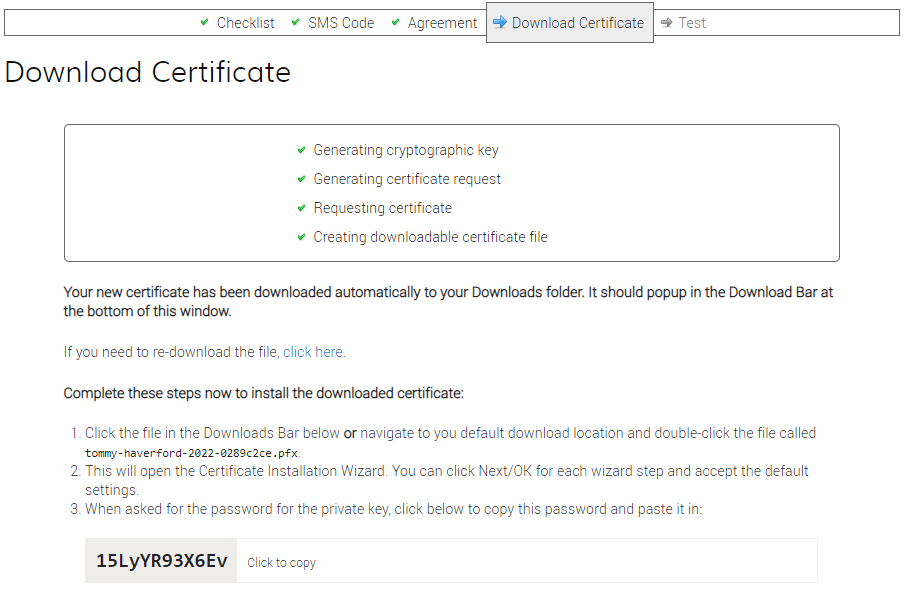
4. Accept the Gatekeeper Subscriber Agreement

Read and agree to the subscriber agreement. A copy can be downloaded for your records.

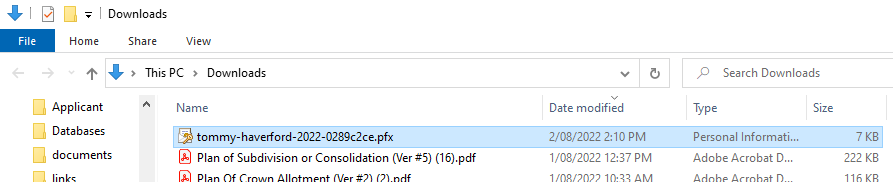


Agree and click ‘Continue’

**5. Download your certificate file**

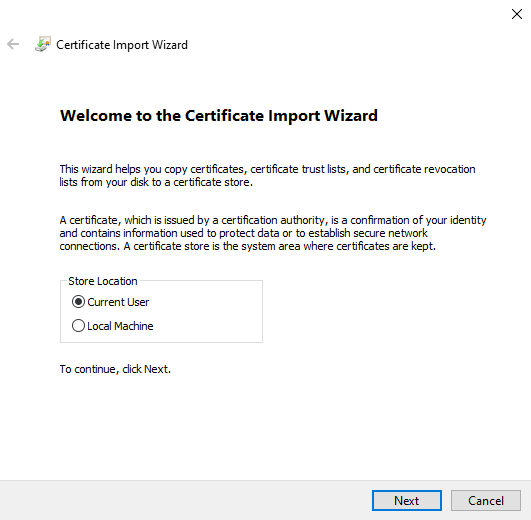
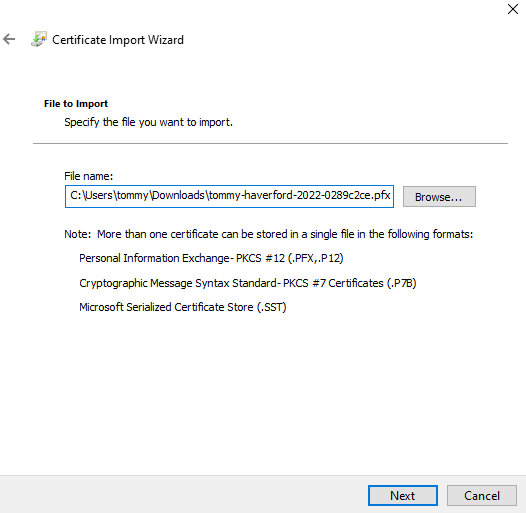
Your digital certificate file will be downloaded automatically. Copy or take note of the temporary password displayed on screen and then open the downloaded certificate file.

You will need this password to install your digital certificate.

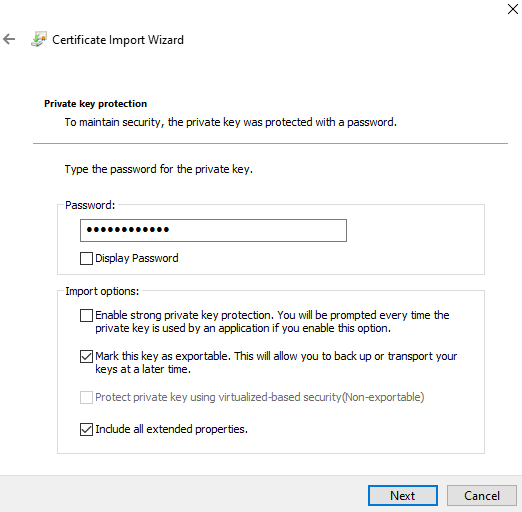
Note: If you are unable to find the file, check your downloads folder.

Double-click to open the certificate file.

6. Complete the Certificate Import Wizard

Depending on your Operation System version, the Certificate Import Wizard may look different or present other options. You can generally accept the default values.

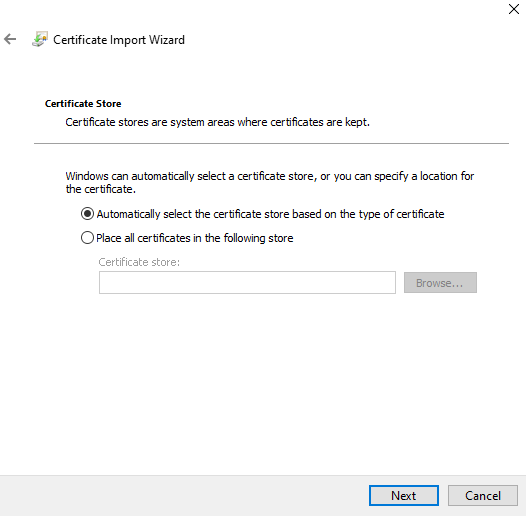
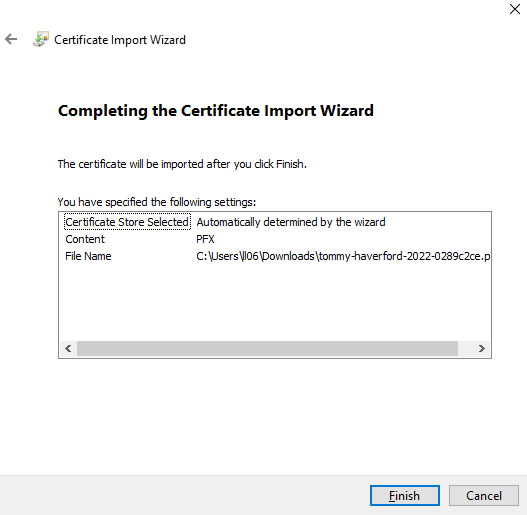
Enter the password copied or noted in the previous step. Ensure you tick ‘Mark this key as exportable’.



Enter or paste the copied password.

You must tick ‘Mark this key as exportable’.

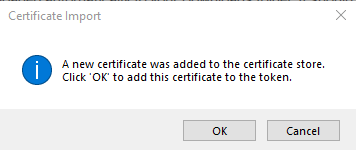
Accept the default values on the following screens.



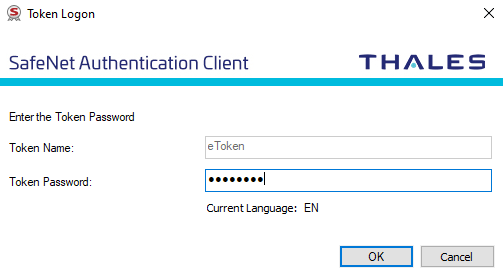
7. Import your digital certificate onto the token

You will be prompted to add the certificate to your token.

Note: This is the password you set in step 1 of this guide.



Enter your token password when prompted.

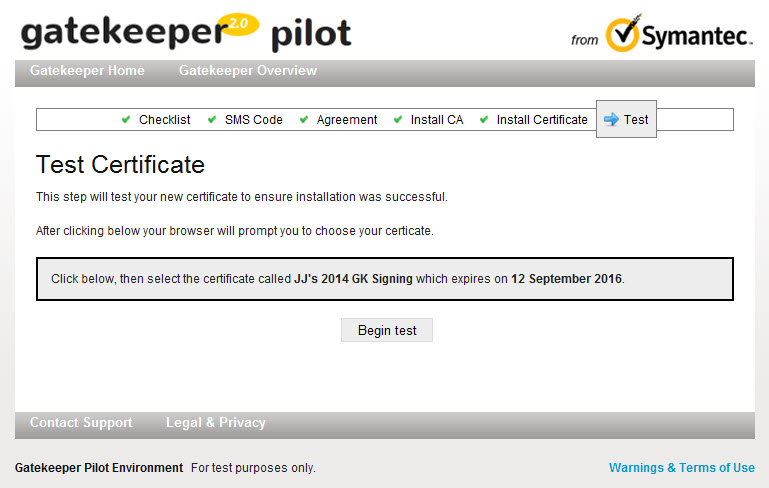


Enter the password you set in step 1 of this guide.

A window will pop up to confirm the certificate was imported successfully. Click ‘OK’ to close any open windows and return to the DigiCert installation process before continuing to the next step.

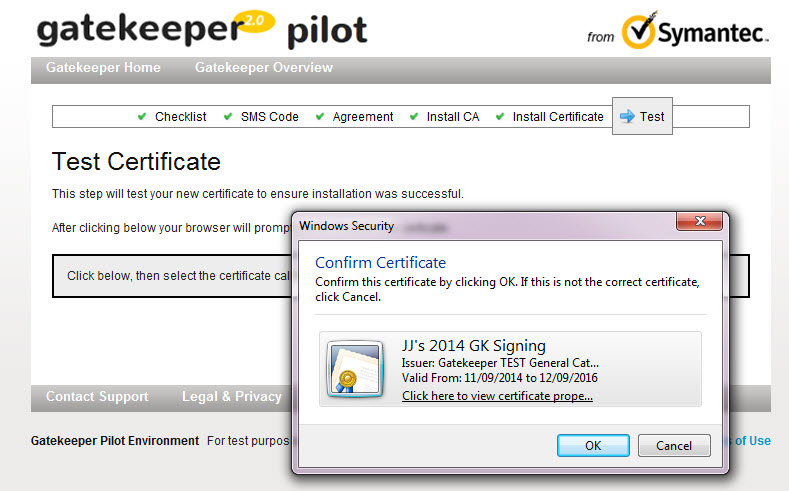
8. Test your digital certificate with DigiCert

Following installation, you will be asked to test your certificate.



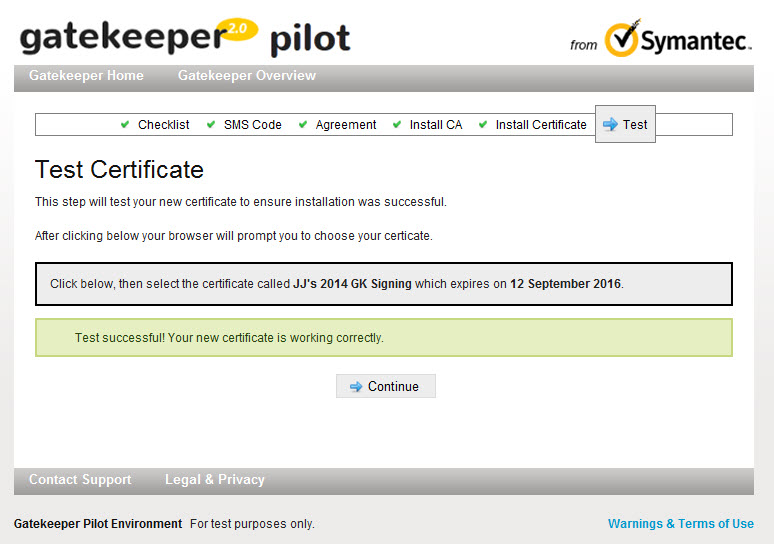
Read the instructions then click ‘Begin Test’.

Select your new certificate to test.



Choose the correct certificate then click ‘OK’.

Enter your token password when prompted.



Test was successful, click ‘Continue’.

Once the test has been completed successfully, the installation process is complete. There is no need to back up your certificate as it is stored securely on the USB security token.

What next?

Certificate Manager digital certificate holders can now approve standard digital certificates for other members of your organisation. Please refer to User Guide 37 - Certificate Manager guide to managing certificates.

If you will be using your certificate in SPEAR to sign key documents, you can now test it. Please see User Guide 34 – Testing your digital certificate for more information.

Need more information?

Further information on this topic can be found by:

* Speaking with your IT department if you’re unable to install the software
* Visiting the SPEAR website [www.spear.land.vic.gov.au/SPEAR](http://www.spear.land.vic.gov.au/SPEAR).
* Contacting the SPEAR Service Desk on 9194 0612 or email [spear.info@delwp.vic.gov.au](mailto:spear.info@delwp.vic.gov.au)