User Guide 33C Installing Lodging Party digital certificates on a USB security token – Internet Explorer

Purpose of this Guide

The purpose of this guide is to provide information on how to install your digital certificates on a USB security token using Internet Explorer. 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 or 33B 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 Symantec, you will receive an email containing instructions to assist you with installing your certificate. The email will look similar to the sample email shown in 33.3 below.
3. Whilst SPEAR can be used with any supported browser (including Google Chrome, Mozilla Firefox or Internet Explorer), you **must** use Internet Explorer to install your certificate.

33.1 Install the eToken software

If not already installed, download the Safenet Authentication Client software for your relevant operating system from the DigiCert website:

https://knowledge.digicert.com/generalinformation/INFO1982.html

Once downloaded, run the file to install the software, selecting the default options throughout.

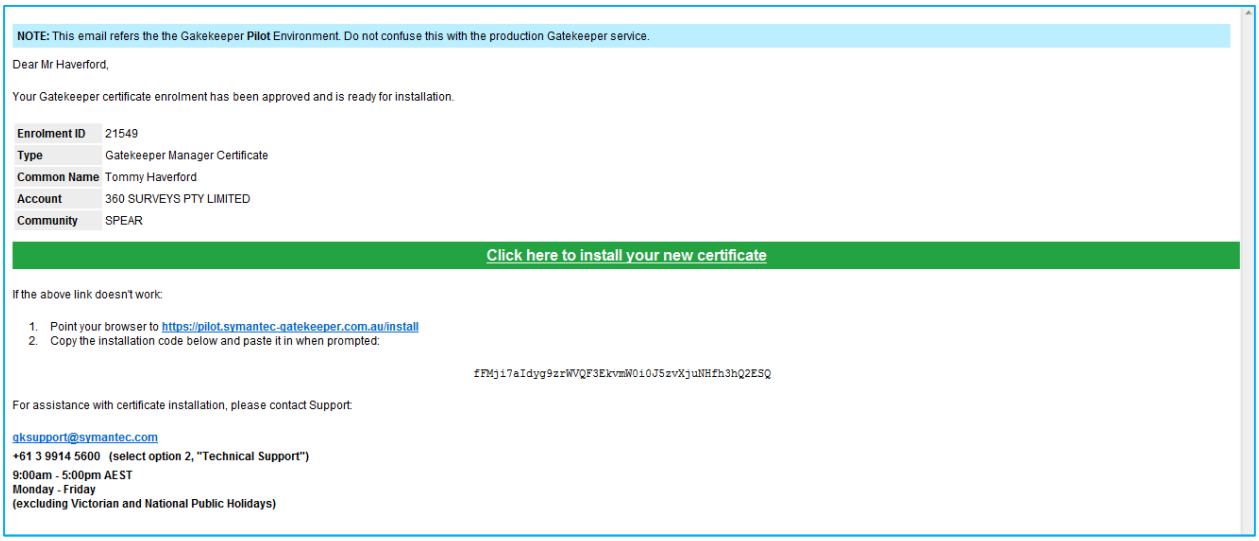
33.2 Change your eToken password

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

33.3 Install your certificate

To commence the installation of your certificate, click on the hyperlink contained in the email sent to you from Symantec.



NOTE: This email refers the the Gakekeeper **Pilot** Environment. Do not confuse this with the production Gatekeeper service.

Dear Mr Haverford,

Your Gatekeeper certificate enrolment has been approved and is ready for installation.

Enrolment ID	21549
Type	Gatekeeper Manager Certificate
Common Name	Tommy Haverford
Account	360 SURVEYS PTY LIMITED
Community	SPEAR

Click here to install your new certificate

If the above link doesn't work:

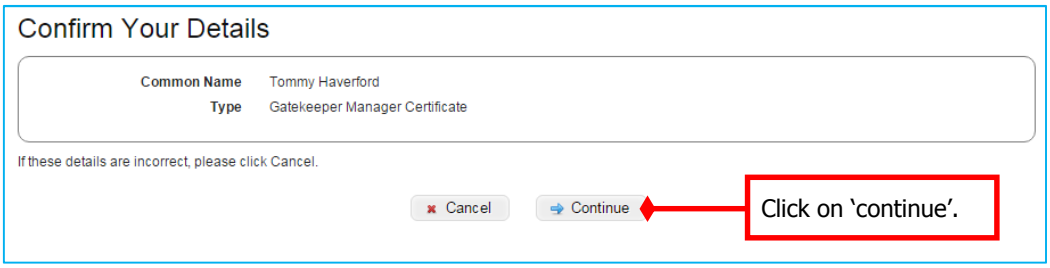
1. Point your browser to https://pilot.symantec-gatekeeper.com.au/install
2. Copy the installation code below and paste it in when prompted:

fFMji7aIdyg9zrWVQF3EkvmW0i0J5zvXjuNHfh3hQ2ESQ

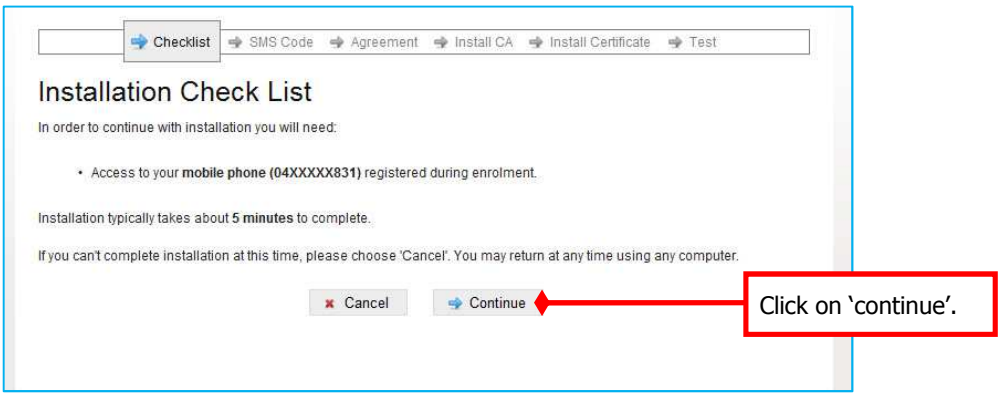
For assistance with certificate installation, please contact Support:

qksupport@symantec.com
+61 3 9914 5600 (select option 2, "Technical Support")
9:00am - 5:00pm AEST
Monday - Friday
(excluding Victorian and National Public Holidays)

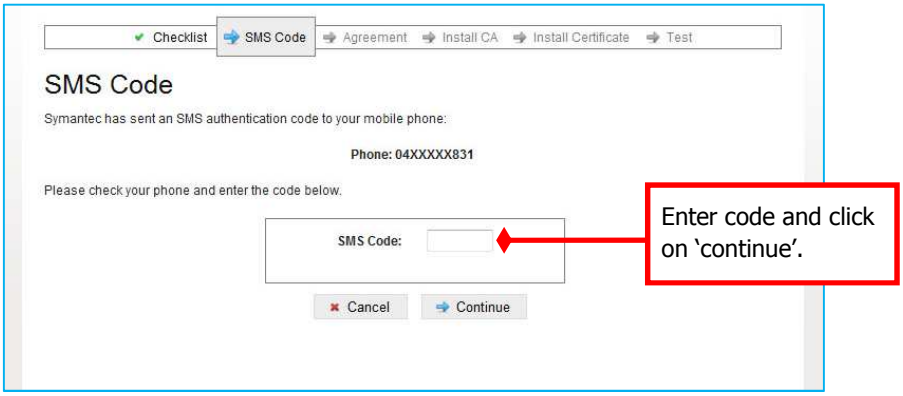
Confirm that the details displayed are correct.



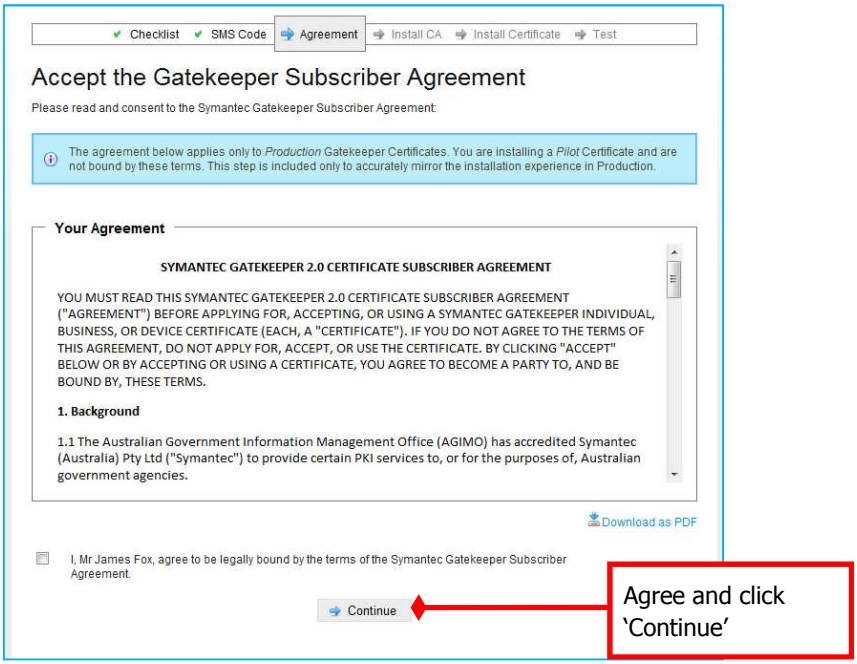
Have your mobile phone ready.



Enter the code sent to your mobile.

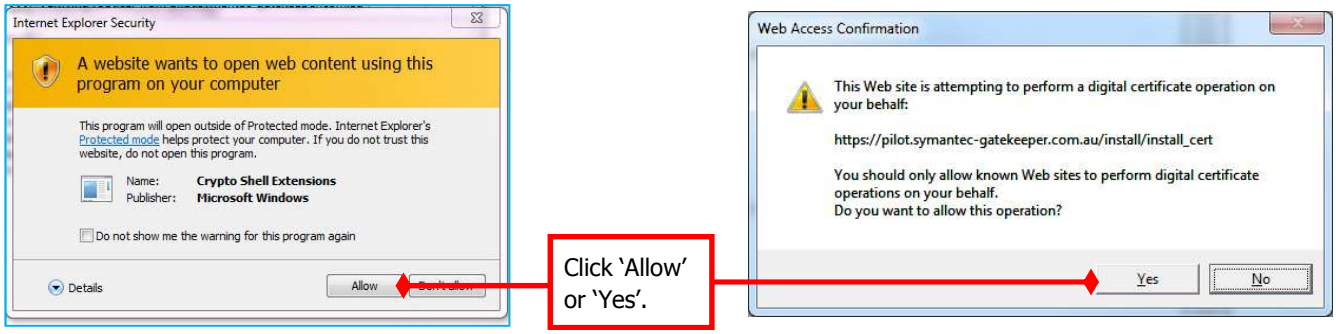


Read and agree to the subscriber agreement. A copy can be downloaded for your records.

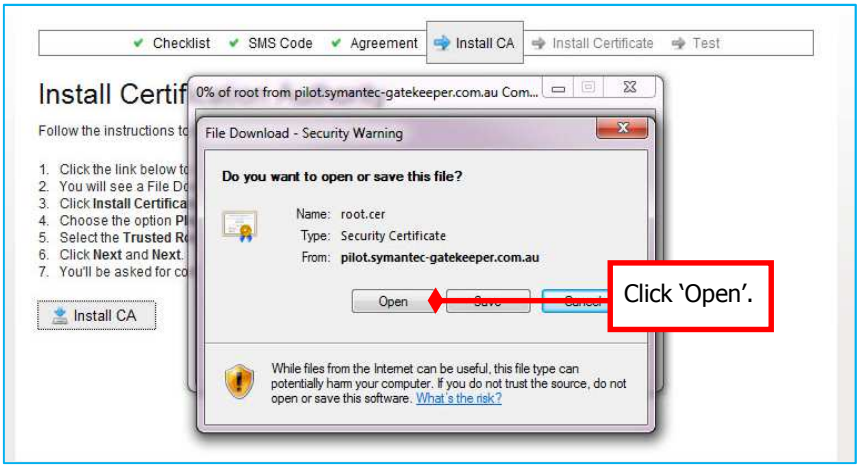


Install the Certification Authority.

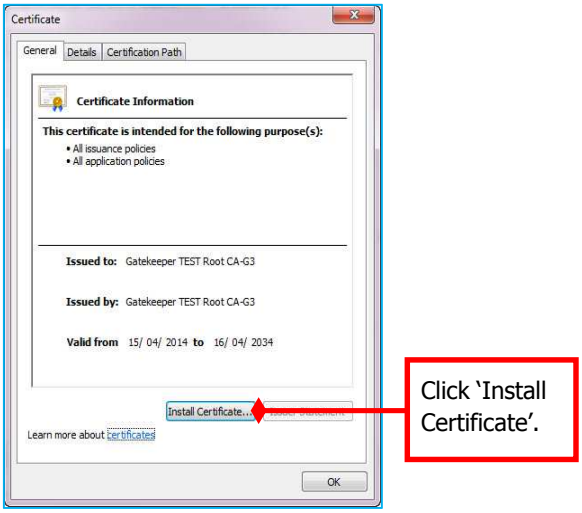
NOTE: Click 'Allow' or 'Yes' on any Internet Explorer Security Warnings that appear throughout the installation process.



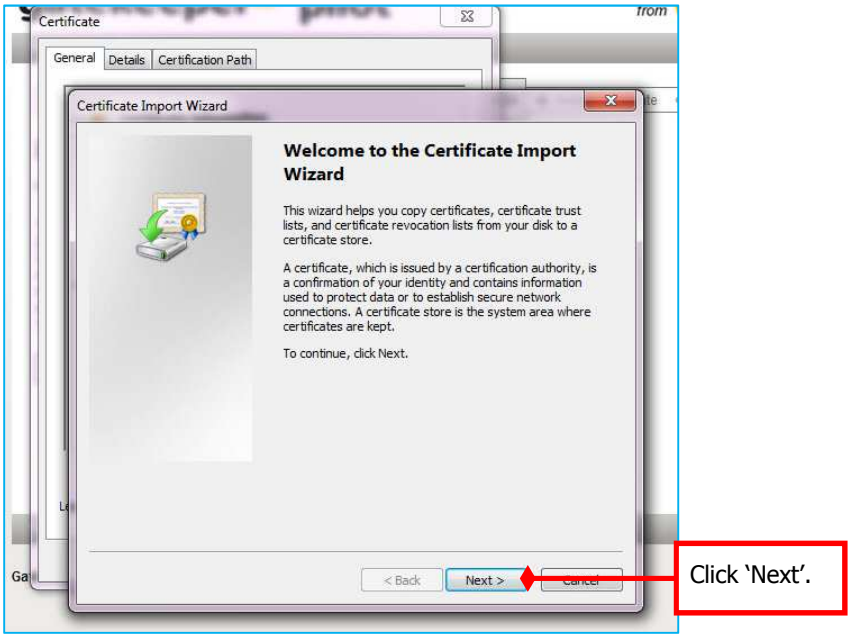
Click the 'Open' button on the downloaded file.



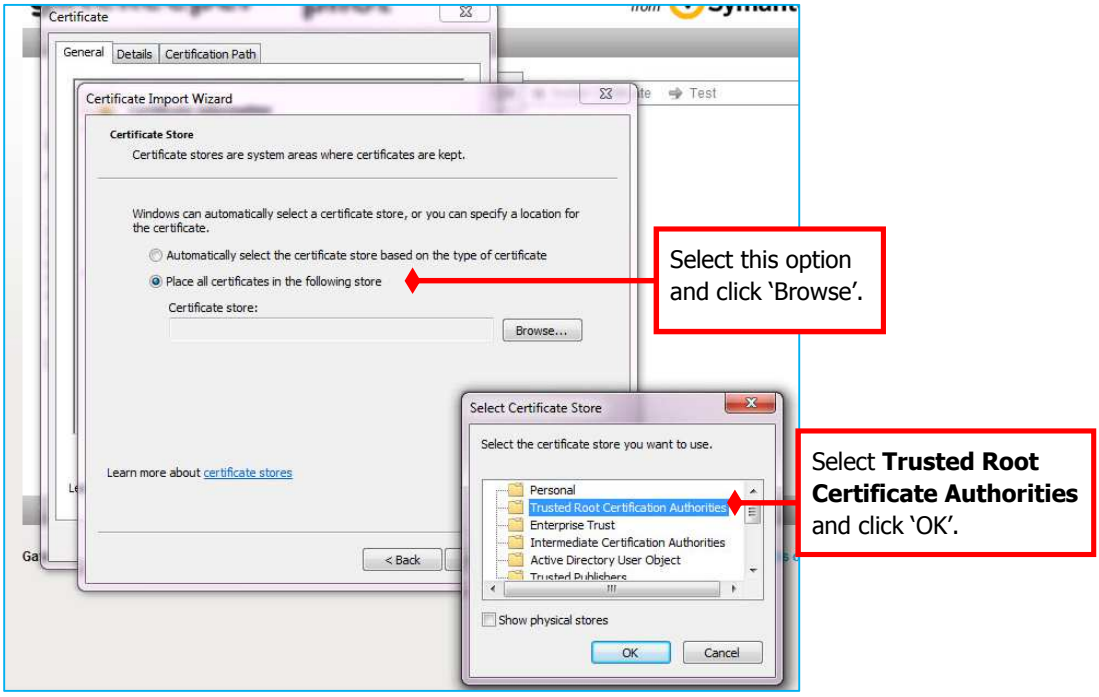
Click 'Install Certificate'.



Click 'Next' on the 'Certificate Import Wizard' screen.

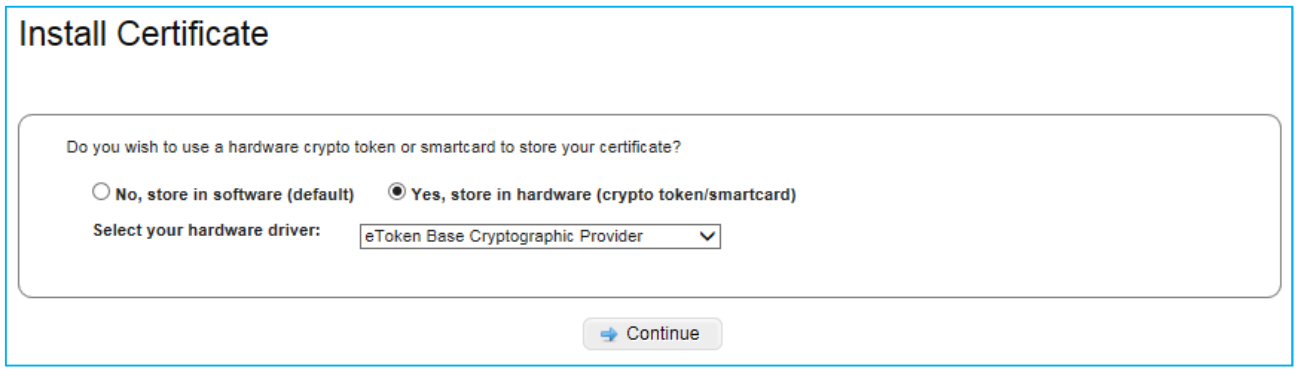


Select the 'Trusted Root Certificate Authorities' certificate store.

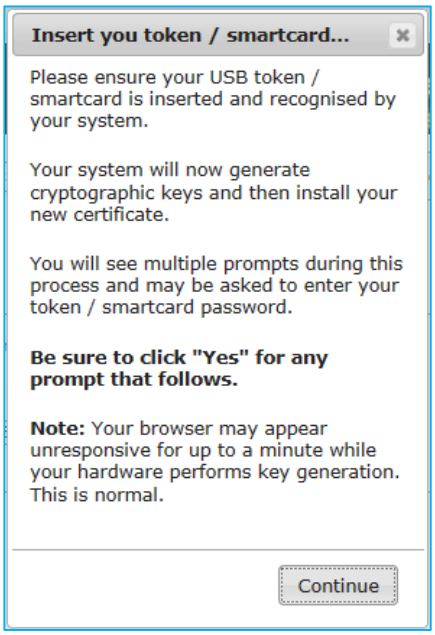


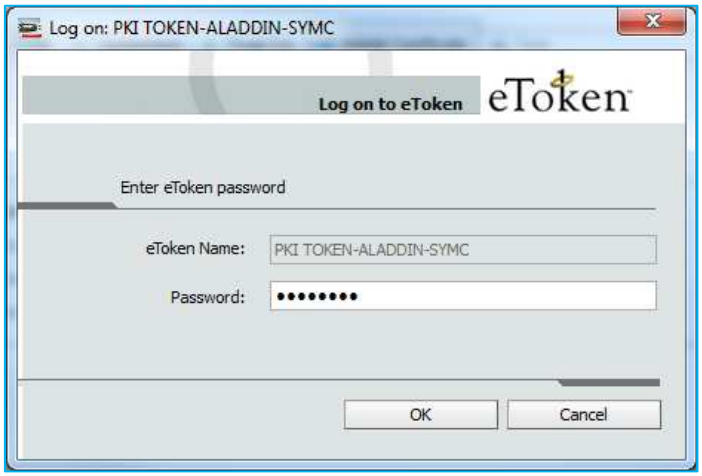
Click 'Next' and then 'Finish'. A window will pop up to confirm installation was successful. Click 'OK' to close any open windows and return to the Symantec installation process before continuing to the next step.

During the installation process, you will be asked whether you wish to use a hardware crypto token to store your certificate. Click 'Yes, store in hardware' and select 'eToken Base Cryptographic Provider' from the hardware driver drop-down list.

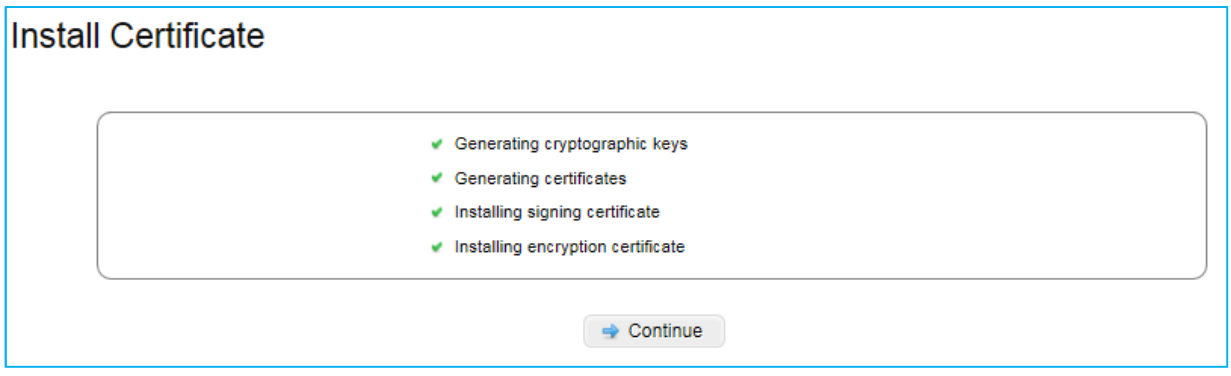


When prompted to insert your token, ensure it is inserted into one of your computer's USB ports. You will then be prompted to enter your token password to install the certificate.



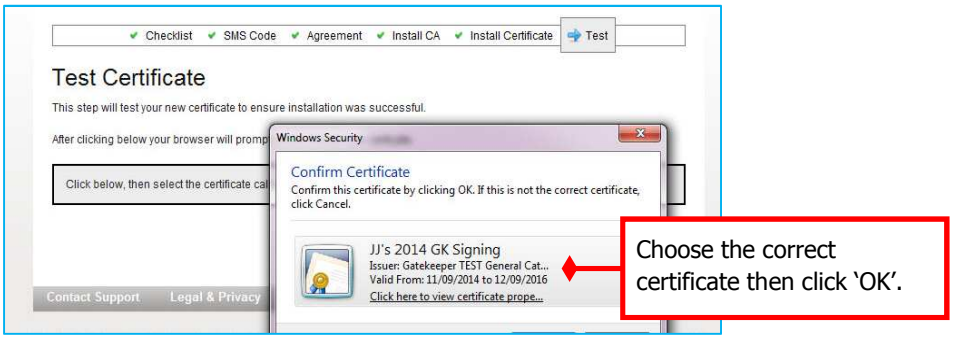


NOTE: Installation may take a few minutes and the light on your token will flicker during this time. Please wait for green ticks to be displayed against all items before continuing.

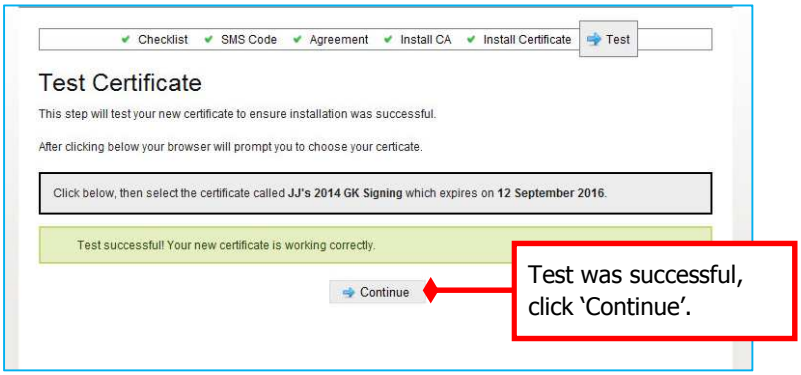


Following installation, you will be asked to test your certificate.

Select your new certificate to test.



Enter your token password when prompted.



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.

33.3 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:

- Visiting the SPEAR website www.spear.land.vic.gov.au/SPEAR.
- Contacting the SPEAR Service Desk on 9194 0612 or email spear.info@delwp.vic.gov.au