User Guide 33A Installing and backing up your digital certificates – Internet Explorer

Purpose of this Guide

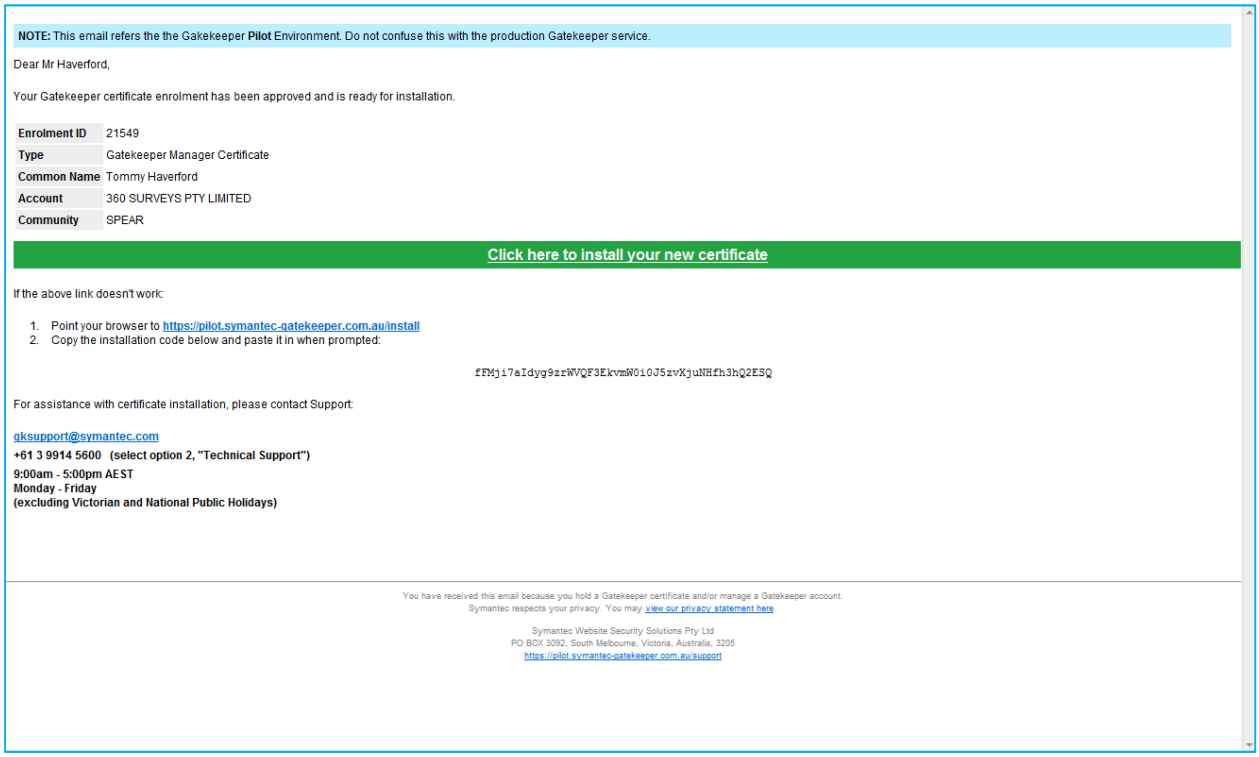
The purpose of this guide is to provide information on how to install and backup your digital certificates using Microsoft Internet Explorer.

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 Digital Signing Certificate as well as your Digital Encryption Certificate. The email will look similar to the sample email shown below.

33.1 Commence Installation

To commence the installation of your certificates, 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:

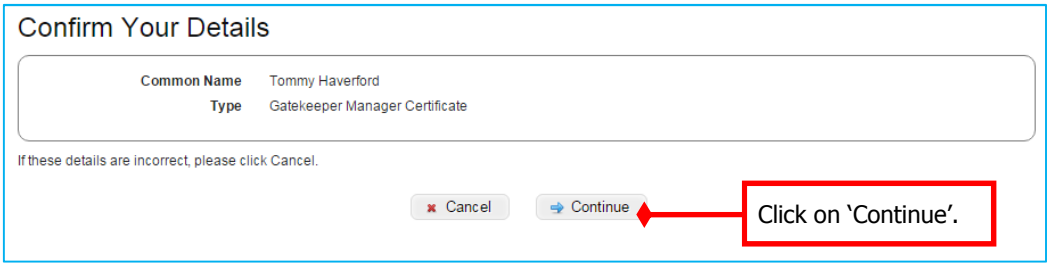
qksupport@symantec.com
+61 3 9914 5600 (select option 2, "Technical Support")
9:00am - 5:00pm AEST
Monday - Friday
(excluding Victorian and National Public Holidays)

You have received this email because you hold a Gatekeeper certificate and/or manage a Gatekeeper account.
Symantec respects your privacy. You may view our privacy statement here.

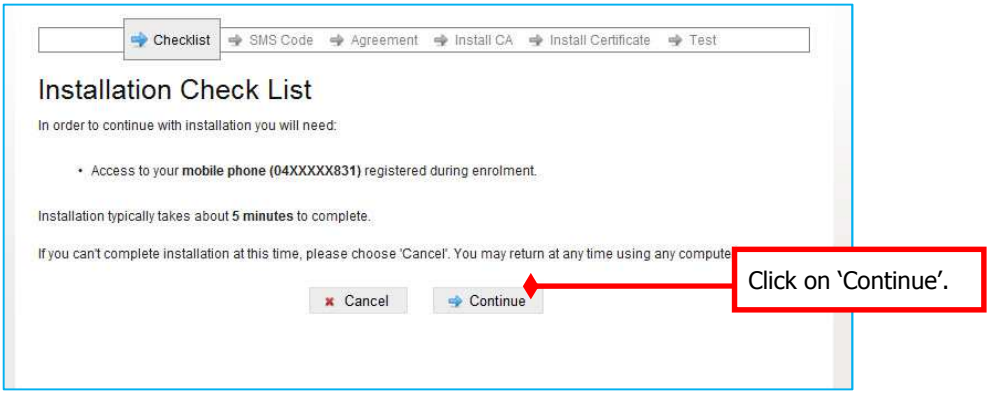
Symantec Website Security Solutions Pty Ltd
PO BOX 3092, South Melbourne, Victoria, Australia, 3205
https://pilot.symantec-gatekeeper.com.au/support

Complete the following steps:

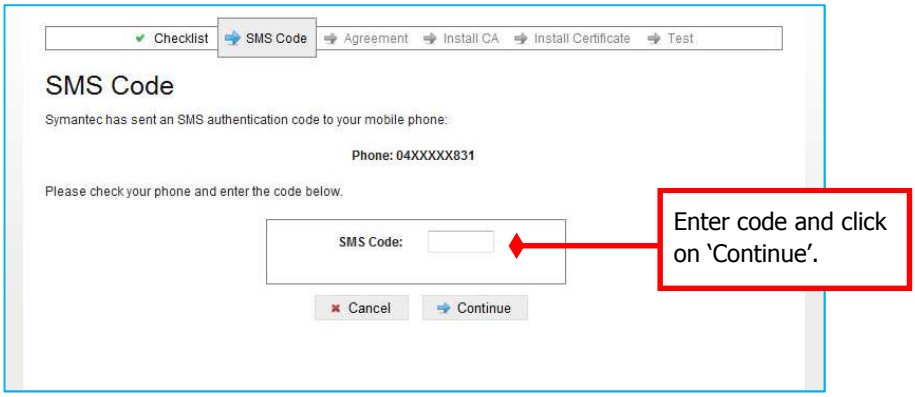
1. Confirm the details displayed are correct.



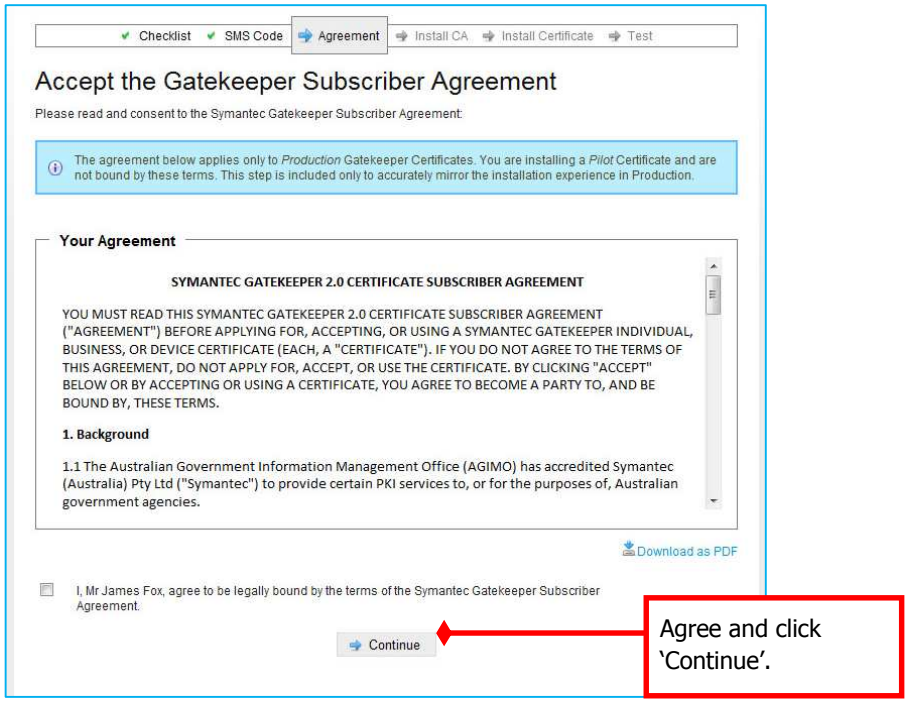
2. Have your mobile phone ready.



3. Enter the code sent to your mobile.

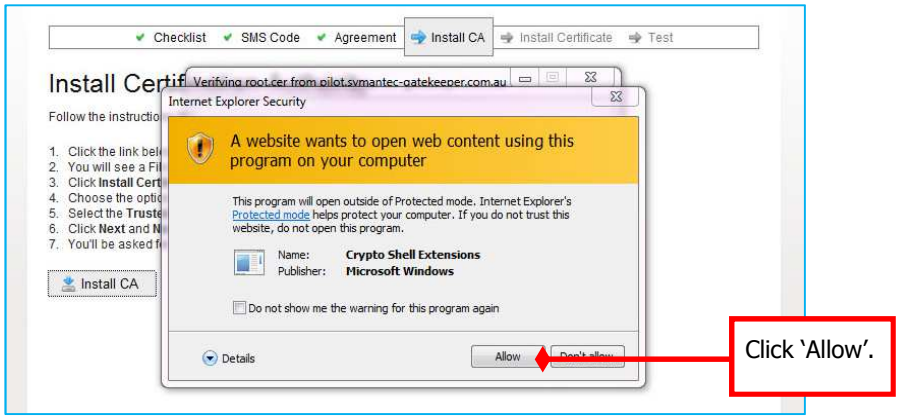


4. Read and agree to the subscriber agreement. A copy can be downloaded for your records.

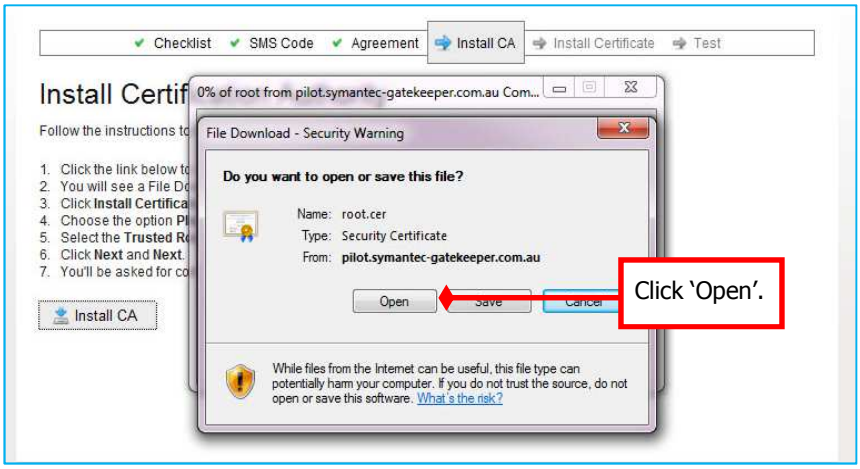


5. Install the Certification Authority.

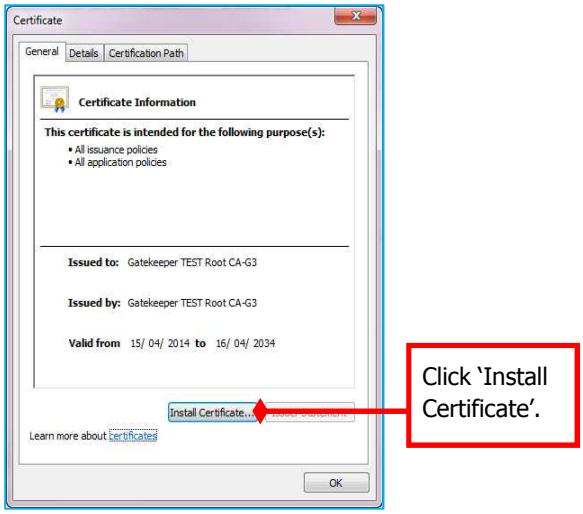
6. An Internet Explorer Security warning will display.



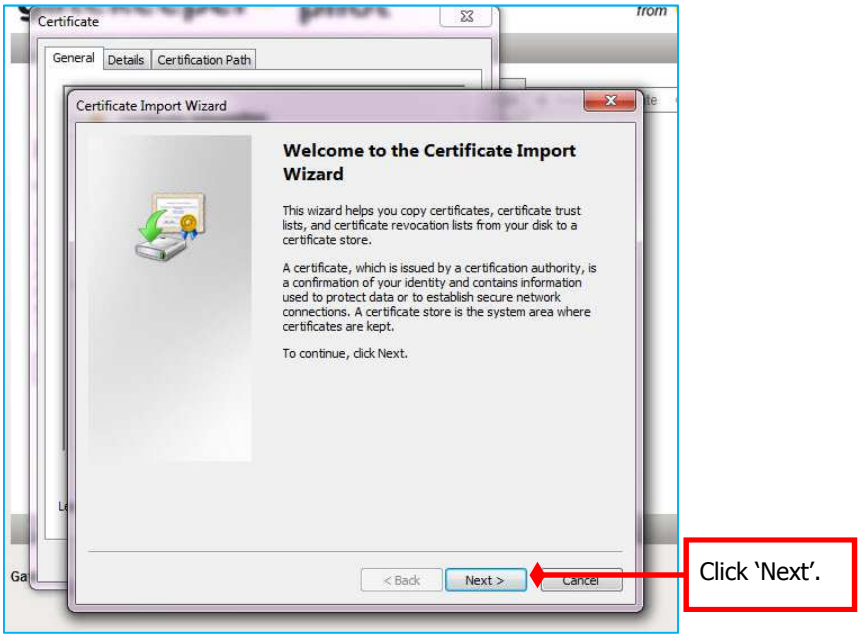
7. A file download warning opens.



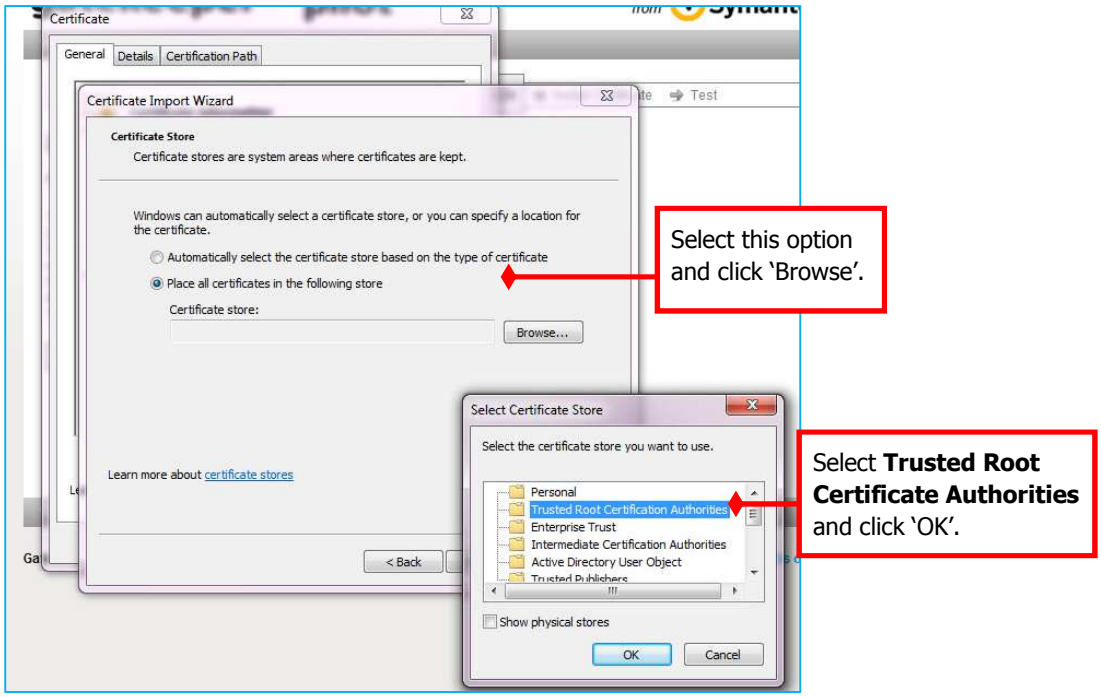
8. The certificate screen is now displayed.



9. The certificate import wizard opens.



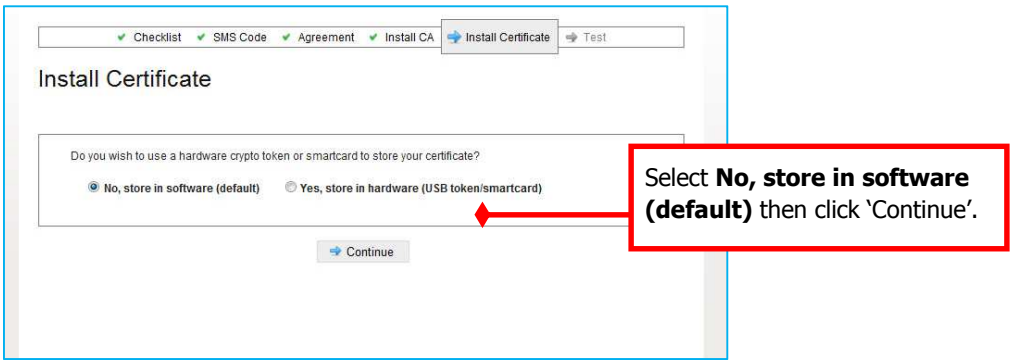
10. Select the certificate store.



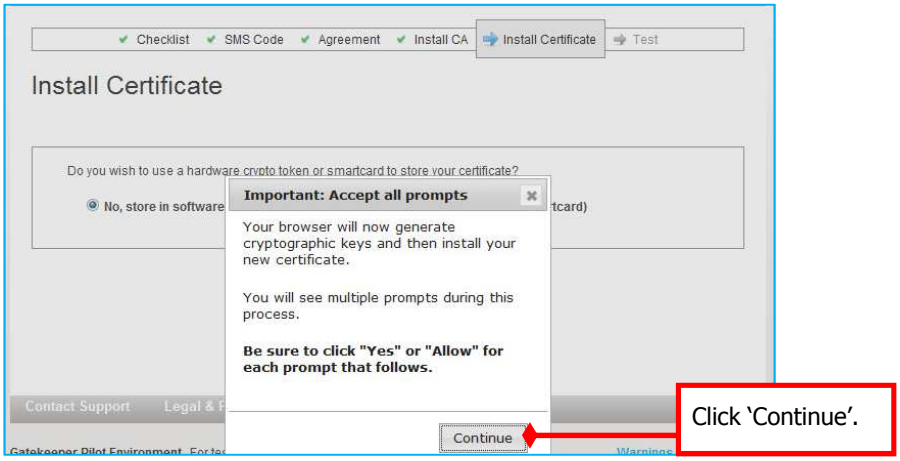
11. Click 'Next' then 'Finish'.

12. A window will pop up to confirm installation was successful. Click 'OK' to close the windows then click 'Continue'.

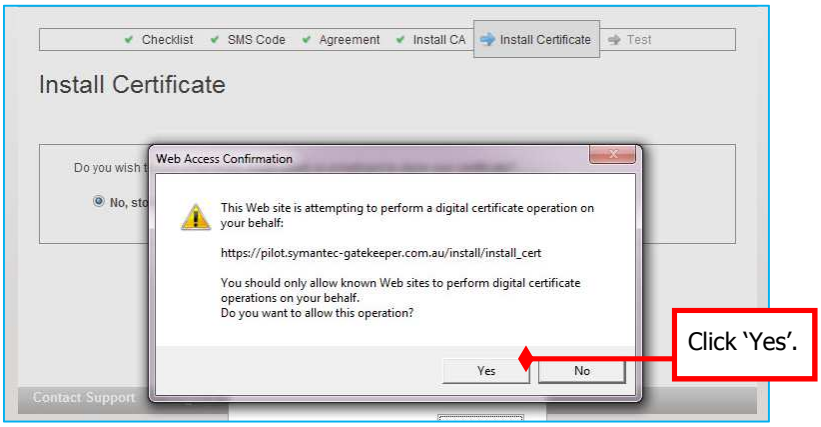
13. Install Certificate.



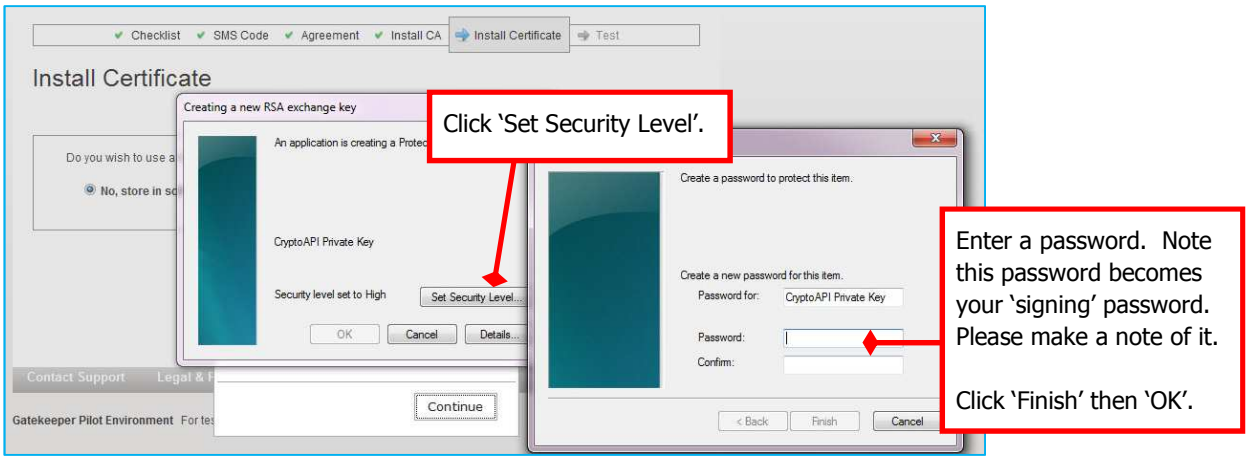
14. A message to accept or allow all prompts displays.



15. A web access confirmation message is displayed. Click 'yes' or 'allow'

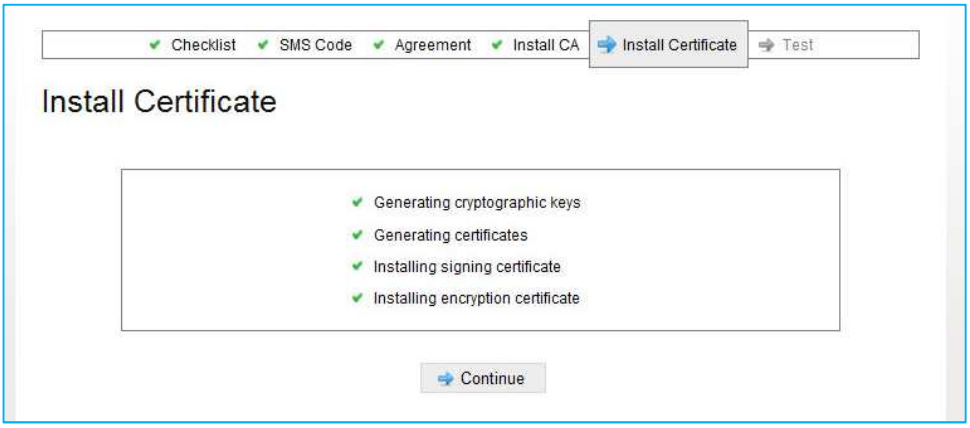


16. Creating a new RSA key.

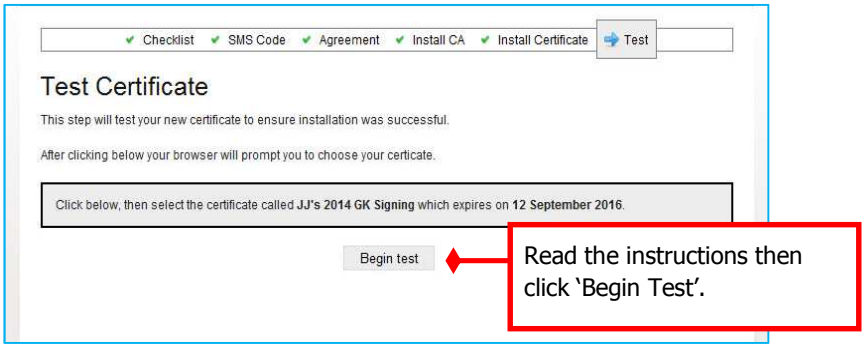


17. The above step will need to be repeated. Enter the same password as you entered the first time.

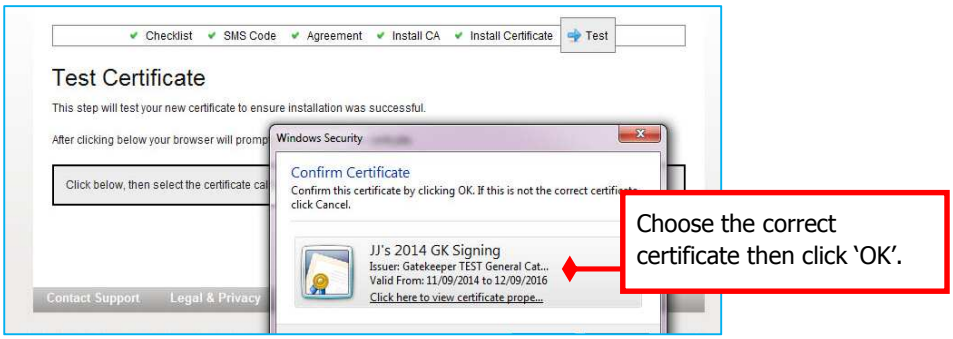
18. The installation is complete when all items are ticked. Click 'Continue'.



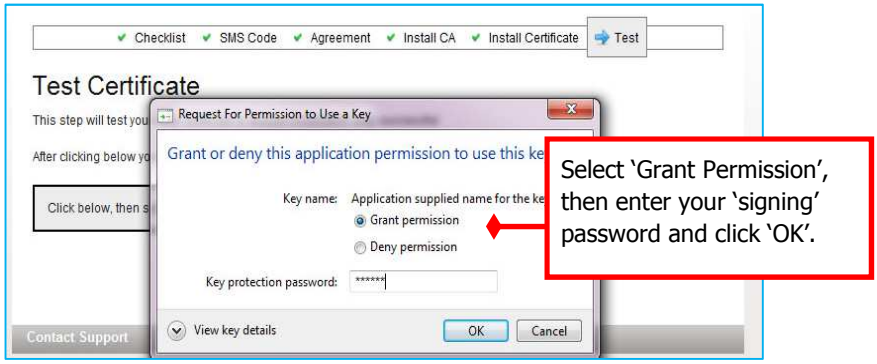
19. Test certificate.



20. Select certificate to test.

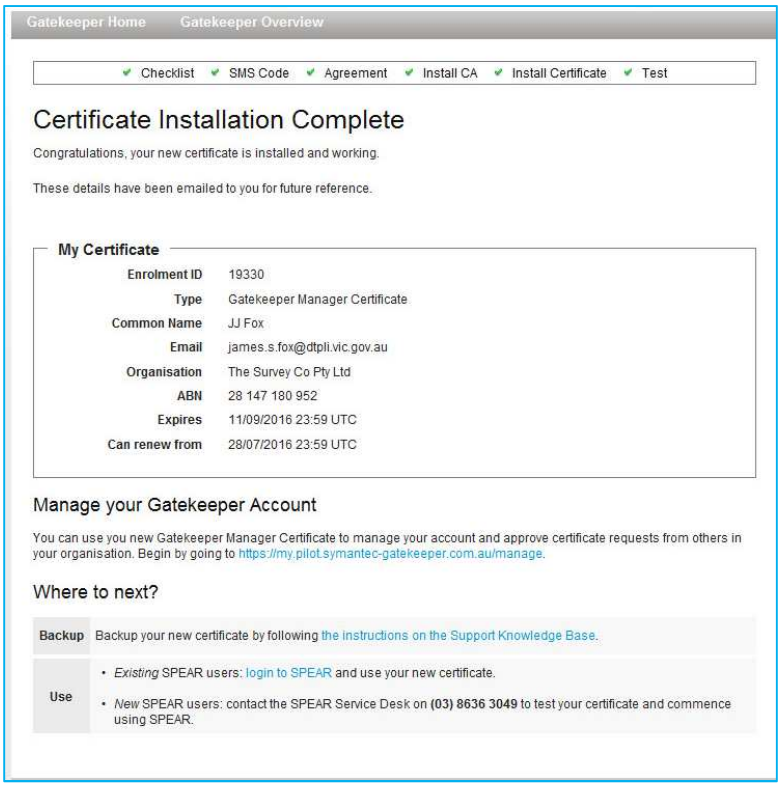


21. Enter your signing password.



22. Test completed successfully.

23. The certificate installation has now completed successfully. Please continue with the following section to back up your certificates.



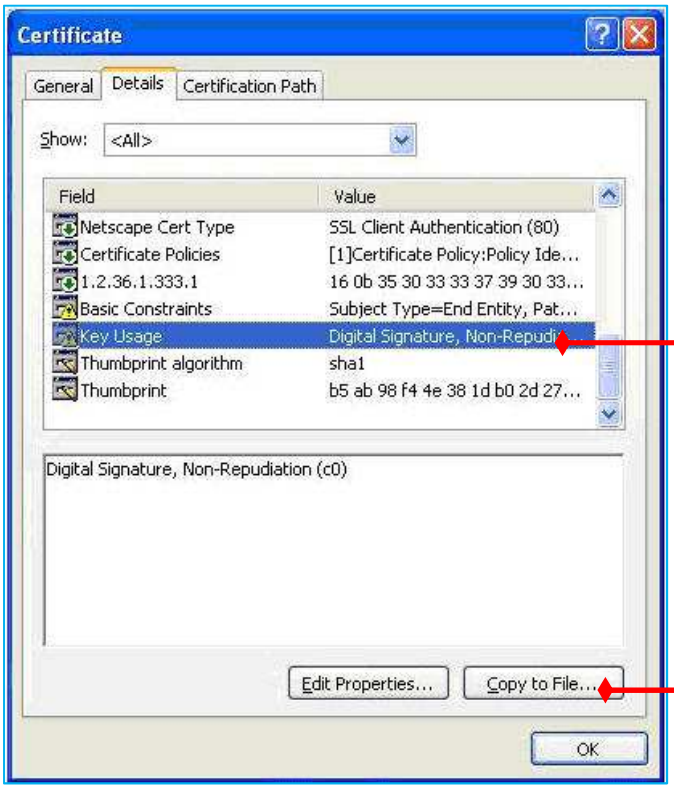
33.2 Certificate backup from Internet Explorer

24. Using the current open browser window: Navigate to the **Personal** tab in Certificates in Internet Explorer: Go to the Tools menu, select 'Internet Options', then go to the Content tab, and click 'Certificates' button.

25. Your two new Gatekeeper certificates are shown. Because they appear to be identical, you will need to identify each one, double-click on the first certificate.

Double click on a certificate. (**Do not** choose the IMPORT option).

26. Go to the Details Tab. Scroll to the bottom of the list, and then click on the item called Key Usage. Note what is shown in the box below:



Digital Signature, Non-Repudiation is your signing certificate.

Key Encipherment, Data Encipherment is your encryption certificate.

Click 'Key Usage'.

Click 'Copy to File'.

NOTE: Remember which certificate you're backing up - it will assist when choosing a filename for your backup in Step 26.

27. Certificate Export Wizard. Click 'Next' on the first screen, then select 'Yes, export the private key' on the second screen.

Select 'Yes' to export the private key

NOTE: Failing to do this step will result in your backup files being in the incorrect format.

Click 'Next>'.

28. Select Export File Format.

Tick the boxes for:
- **Include all certificates** in the certification path if possible
- **Enable strong protection**

Click 'Next>'.

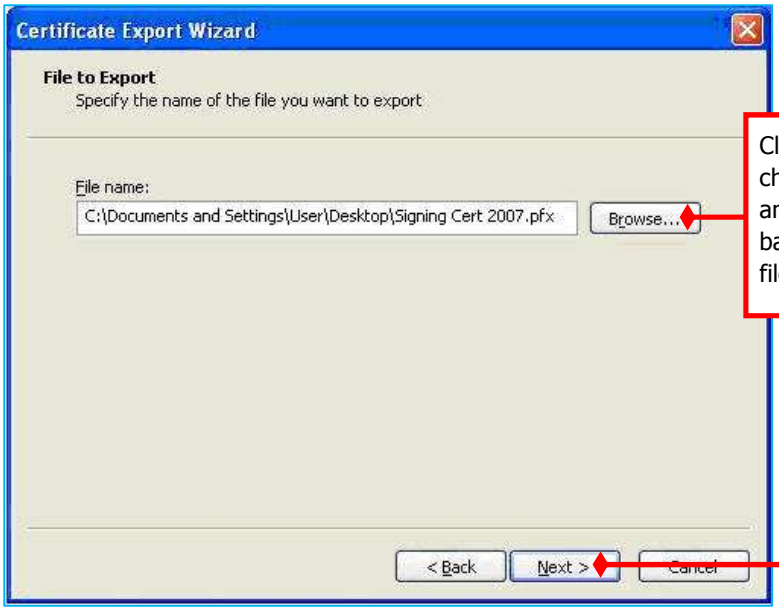
29. Choose a password for security of your backed-up certificate. Use at least one uppercase and one non-alphabetic character and preferably 8 characters.

Securely record your password for future reference. It cannot be recovered or changed!

Click 'Next>'.

30. Choose a location and name for your backed-up certificate.

Suggested filenames for your backed up certificates are 'Freds signing cert2009' and 'Freds encryption cert2009' file/certificate.



Click 'Browse' to choose a location and name for your backup file/certificate.

The backed-up certificates should be placed somewhere secure such as a regularly backed up drive.

Click 'Next'.

31. Depending on the security level that you have when enrolling for your certificate, you may be presented with a box asking for a 'CryptoAPI Private Key' password - this is the password you chose when you enrolled. **NOTE: Neither Symantec nor SPEAR can recover or reset this password for you!** High Security requires a password. Medium security does not require a password.

Enter the password you chose when you first enrolled.

If you are not prompted for a password, simply click on 'OK'.

Click 'OK'.

32. You need to repeat the backup process for the other certificate.

Go back to Step 21 of this User Guide, select the second certificate and repeat the Export process.

Once you have backed up both of your certificates, you should have two files with .pfx extensions to the file names.

If you wish to ensure that your digital certificates have been backed up correctly into your selected folder, use Windows Explorer and look for two files with .pfx extensions. SPEAR recommends that you burn the digital certificate files to CD or store them on a USB memory stick, as well as your network server to ensure they are not lost if you change PCs or have a major disk failure.

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 digital 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