User Guide 33B Installing and backing up your digital certificates – Mozilla Firefox

Purpose of this Guide

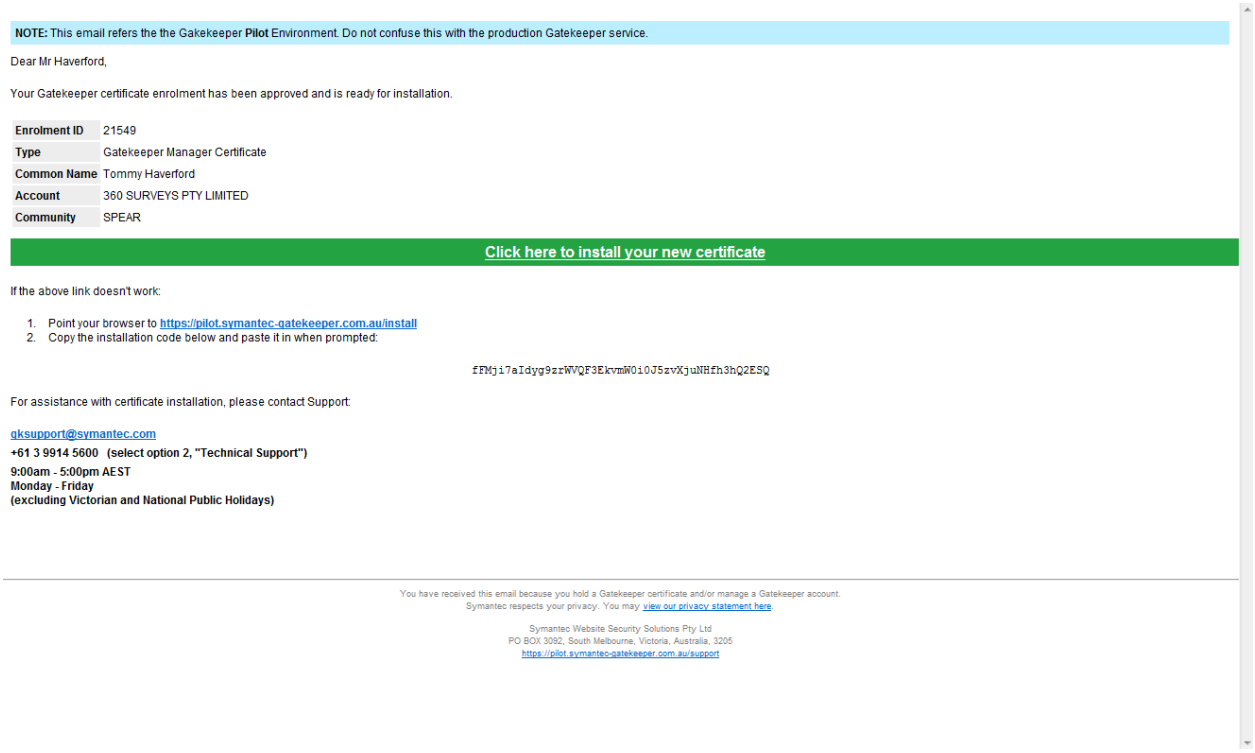
The purpose of this guide is to provide information on how to install and backup your digital certificates using Mozilla Firefox.

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 like 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

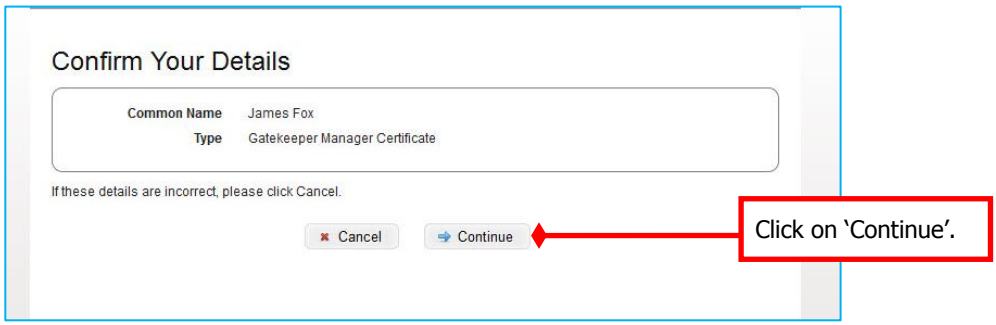
For assistance with certificate installation, please contact Support:

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

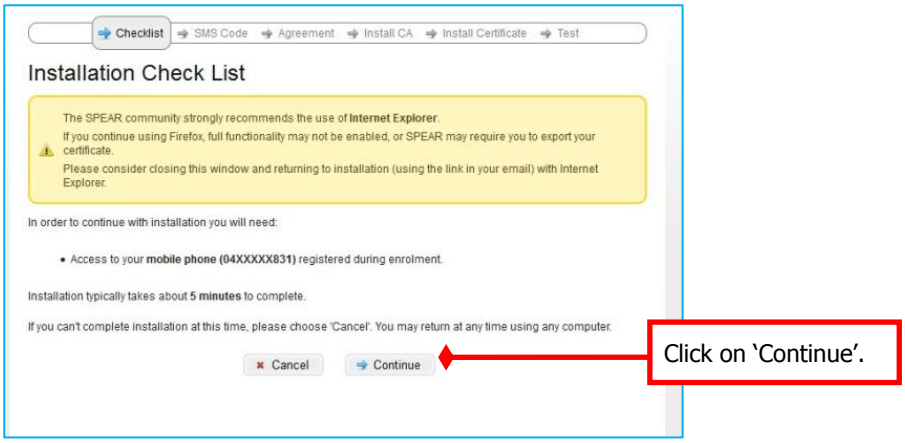
You have received this email because you hold a Gatekeeper certificate and/or manage a Gatekeeper account.
Symantec respects your privacy. You may view our privacy statement here.

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

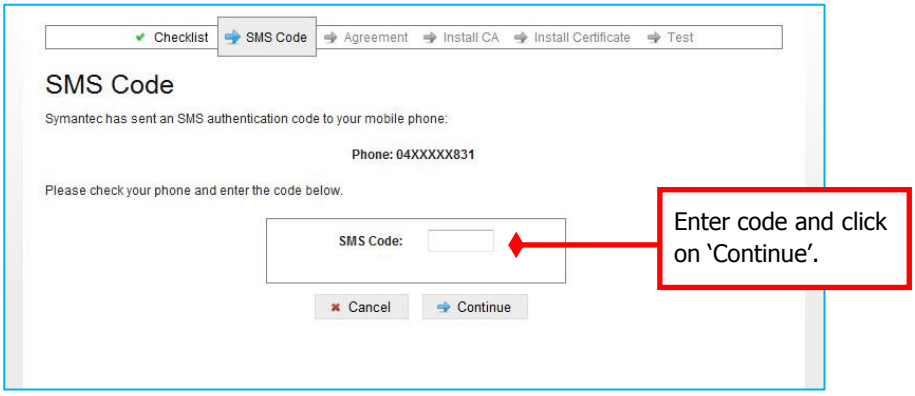
1. Confirm that the details displayed are correct.



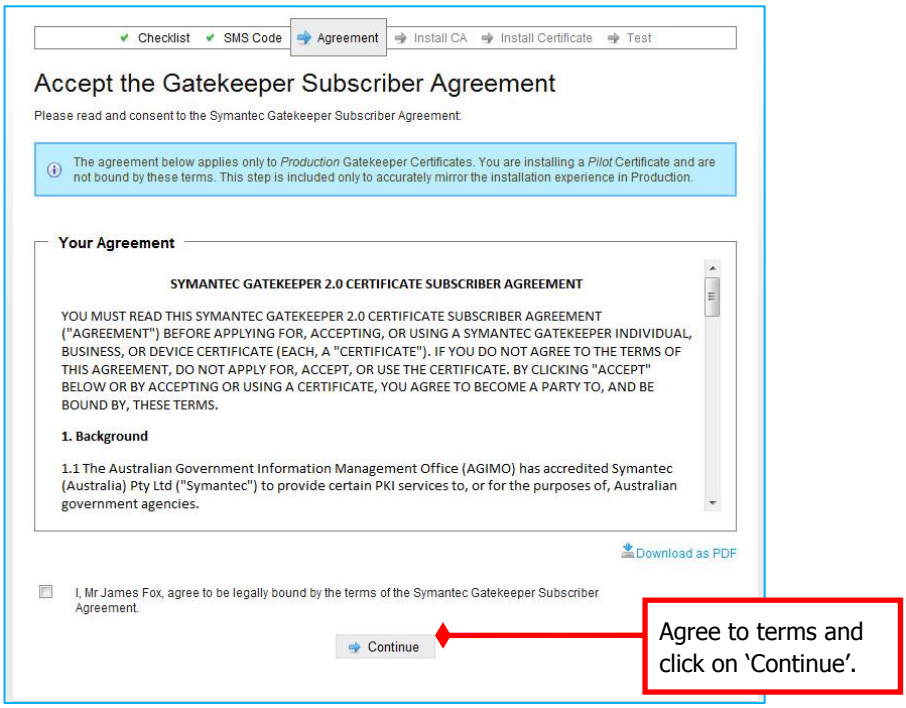
2. Have your mobile phone ready.



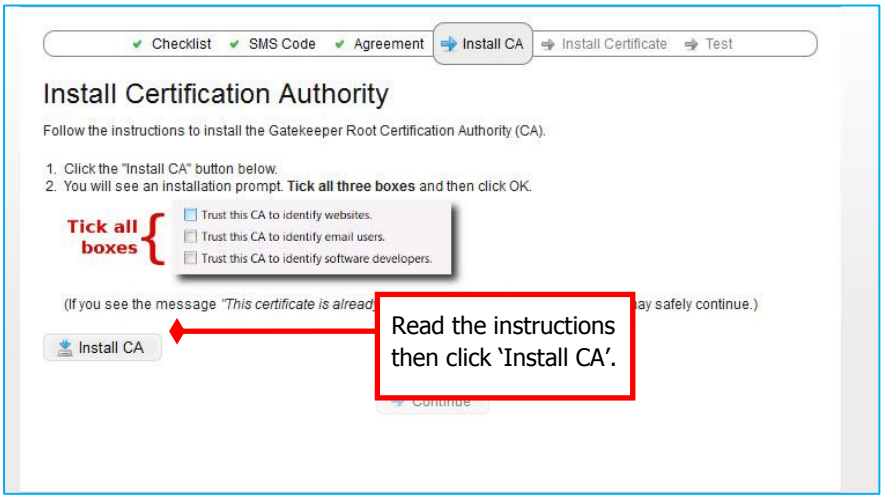
3. Enter the code sent to your mobile



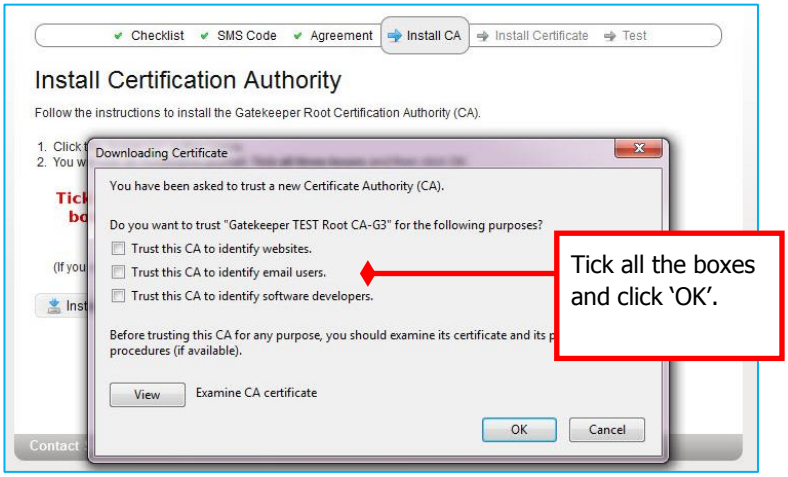
4. Read and agree to the Subscriber Agreement. A copy can be downloaded for your records.



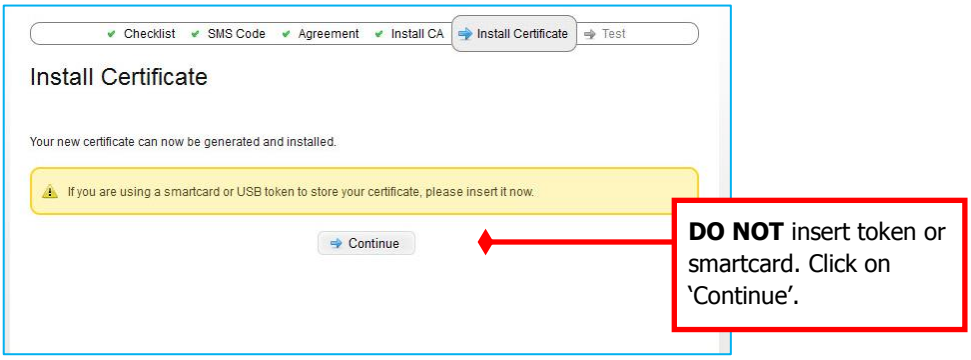
5. Install the Certification Authority.



6. A download certificate window will display.



7. Install Certificate. Do not install your certificates to a smartcard or USB token.

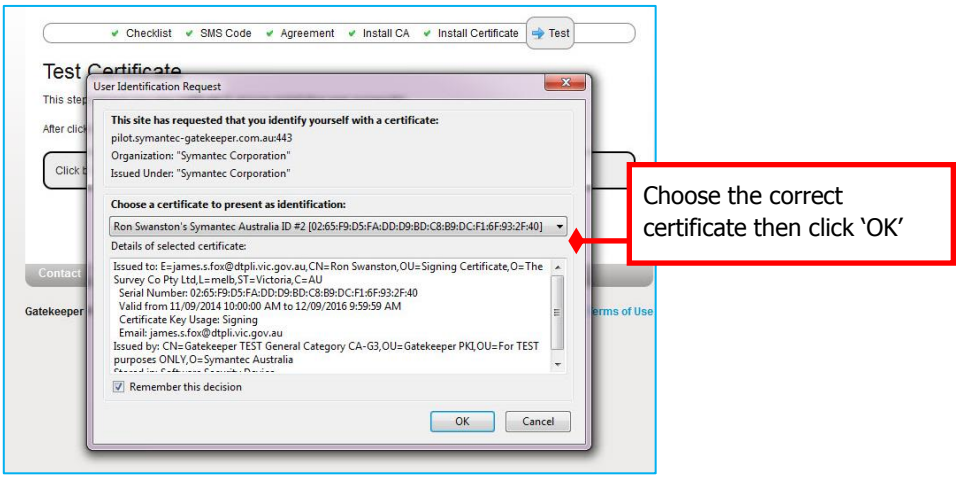


8. A message will be displayed that certificates have been installed. Click 'OK'

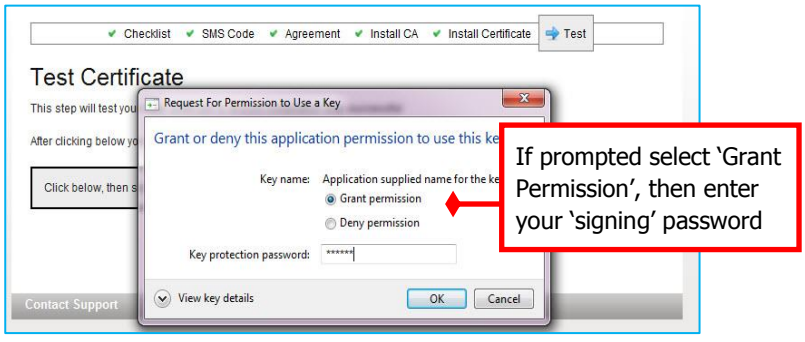
9. All items on the Install certificate screen should now be ticked. Click 'Continue'

10. Test Certificate

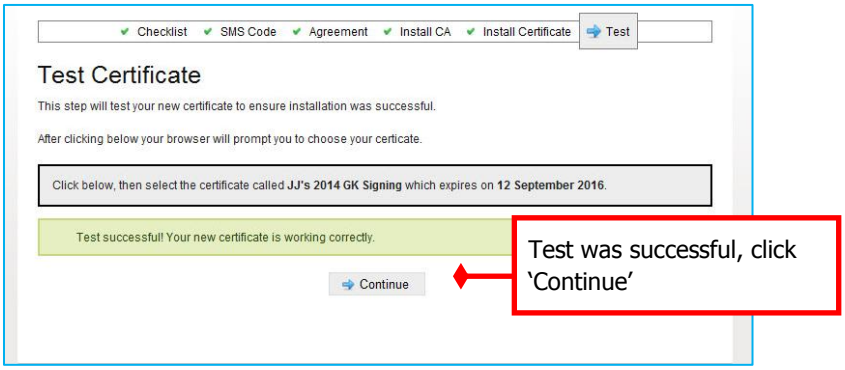
11. Select certificate to test



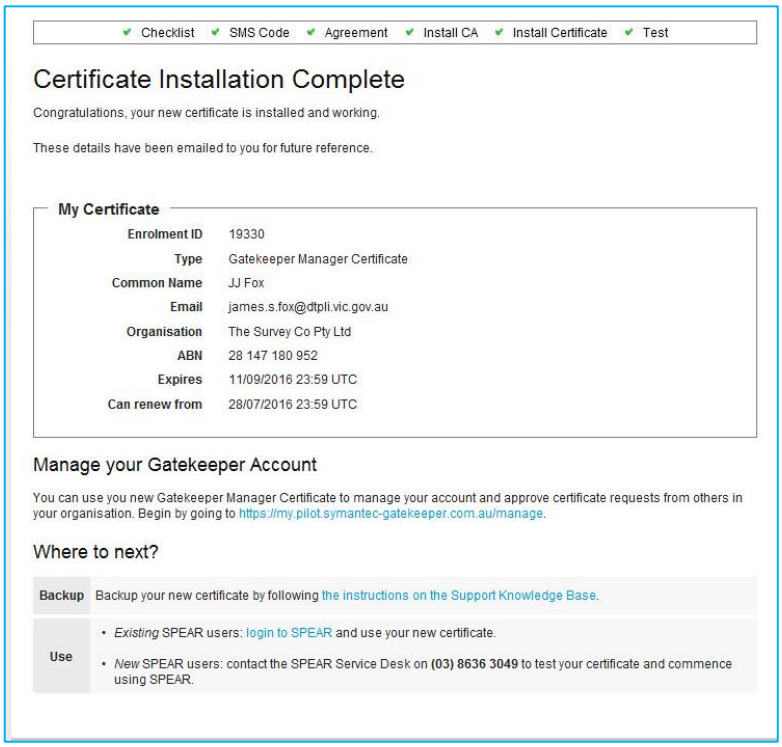
12. Enter your signing password



13. Test completed successfully

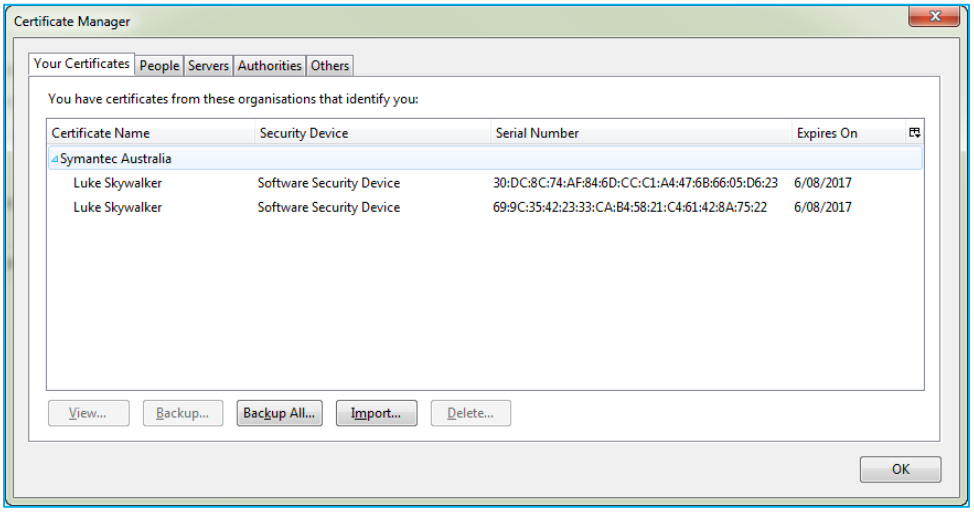


14. The certificate installation has now completed successfully. To back up your certificates, please continue with the following:

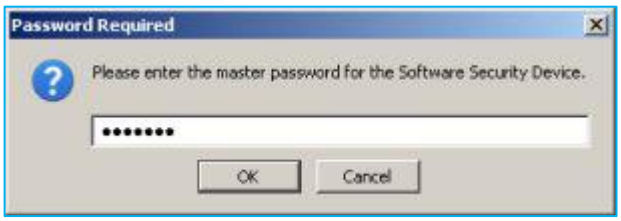


33.2 Certificate backup from Firefox

15. In the current browser window go to the Tools menu, select Options. Go to the Privacy & Security section and scroll down to the Certificates section. Click the 'View Certificates' button, select the Your Certificates tab.



16. Select both certificates and click 'backup'
17. Choose a location for the file and an appropriate filename - if you are backing up your signing certificate, a suggested filename is "SPEAR Signing Cert 2009". Click the 'Save' button.
18. If you have set a Master Password for Firefox, you will be prompted for it here - enter your Firefox password, then click the 'OK' button.



19. Choose a password to protect your certificate backup. The password you choose cannot be recovered or changed, so be sure to remember it! Once you have entered and confirmed your password, click the OK button.

Once you have backed up both of your certificates, you should have one file with .p12 extension to the file names.

If you wish to ensure that your Digital Signing Certificates have been backed up correctly into your selected folder, use Windows Explorer and look for the file with .p12 extension. SPEAR recommends that you burn the Digital Signing 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.

As Firefox puts certificates in its own certificate store you must reimport your certificates into the Windows certificate store so they can be used in SPEAR. Please refer to User Guide 36_Importing Digital Certificates into Certificate Store

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