

Certificate Centre

Table of Contents

- How do I renew my code signing key that is expired
- How to download my digital certificate
- When importing codesigning certificate using java 2 SDK "keytool", the following error occurs "Keytool error: java.lang.Exception: Failed to establish chain from reply"
- How to convert .pfx (PKCS#12) to a .spc and .pvk files
- How to export my private keys from Internet Explorer
- When importing certificate using Java 2 SDK "keytool" the following error occurs: error keytool: java.lang.Exception: Entry is not an X.509 certificate
- How to request to revoke a digital certificate issued by Ascertia CA
- How to configure MS Outlook to send secure Emails
- Where can I get the Ascertia Root CA certificate from
- How to get a Code Signing Certificate for Trial
- How to buy a Code Signing Certificate

How do I renew my code signing key that is expired

You are required to request a new code signing certificate and to sign your code again with this certificate.

How to download my digital certificate

1. Visit Certification authority site at <https://account.ascertia.com/>
2. Click on "Logon / Register" button to Logon to "Certificate Centre" and type your registered email address / password.
3. After successful login, click on 'View Cart' right below your name.
4. on View Cart page, you can download any of your free certificates.

When importing codesigning certificate using java 2 SDK "keytool", the following error occurs "Keytool error: java.lang.Exception: Failed to establish chain from reply"

Please import "Ascertia Public CA 1" and Ascertia Root CA 2 certificates to establish trust chain of code signing cert. Before you import your code signing certificate issued from Ascertia Free CA in the key store, you can download these Certificates from the following web links:

- Ascertia Root CA 2 from: <http://www.ascertia.com/onlineCA/CA/AscertiaRootCA2.crt>
- Ascertia CA 1 from: <http://www.ascertia.com/onlineCA/CA/AscertiaPublicCA1.crt>

How to convert .pfx (PKCS#12) to a .spc and .pvk files

Using OpenSSL, you can convert a .PFX (PKCS#12) file to a .spc and .pvk file. To download OpenSSL you can use the links as below:

- OpenSSL binary for Windows: <http://www.shininglightpro.com/products/Win32OpenSSL.html>
- Alternatively you can download from OpenSSL website: <http://www.openssl.org/>
- Extract your private key from the {privatekey}.pfx file.

```
Syntax: $>openssl pkcs12 -in {path to pfx file} -nocerts -nodes -out {path to pem_key  
(private key) output file}  
Example: $>openssl pkcs12 -in "E:\Ascertia\codesigning\certs\codesigning1.pfx"  
-nocerts -nodes -out E:\Ascertia\codesigning\certs\codesigning1_key.pem
```

Password: {Type the password of your PFX and press enter button}

- To convert .PEM file to .PVK, download and install the PVK transform utility.

```
Syntax: $> pvk -in {Path to pem file} -topvk -out {path to pvk_key output file}
Example: $> pvk -in E:\Ascertia\codesigning\certs\codesigning1.pem -topvk -out
E:\Ascertia\codesigning\certs\codesigning1.pvk
```

- Extract your certificates (Public key) from the PFX file.

```
Syntax: $> openssl pkcs12 -in {Path to pfx file} -nokeys -out {Path to pem
certificate (public key file)}
Example: $> openssl pkcs12 -in E:\Ascertia\codesigning\certs\codesigning1.pem -nokeys
-out E:\Ascertia\codesigning\certs\codesigning1_cert.pem
```

Password: {Type the password of your PFX and press enter button}

- Transform your PEM file to a SPC file

```
Syntax: $> openssl crl2pkcs7 -nocrl -certfile {path to pem_certs-file} -outform DER
-out {path to spc output file}
Example: $> openssl crl2pkcs7 -nocrl -certfile
E:\Ascertia\codesigning\certs\codesigning1.pem -outform DER -out
E:\Ascertia\codesigning\certs\codesigning1.spc
```

How to export my private keys from Internet Explorer

1. Our digital certificates System is issuing a certificate with private key (in PKCS#12 format). You can get your certificate with private key from Certificate Transactions area under [Certificate Centre](#) section of Ascertia web site.
2. To export your PFX from internet explorer keystore follow the steps as below:
3. Open Internet explorer
4. Click on "Tools >> Internet Options", "Internet Options" dialogue windows will be open
5. Click on "Content" tab
6. Click on "Certificate" button, Certificates dialogue window will open
7. Click the Personal tab and select the certificate to be extracted and click on Export button
8. "Certificate Export Wizard" starts, select "Yes, export the private key"
9. Follow the wizard and choose destination location on your disk and type a file name to save your private key.
10. You will get your-key.pfx file containing your public and private keys for the selected certificate.

When importing certificate using Java 2 SDK "keytool" the following error occurs: error keytool: java.lang.Exception: Entry is not an X.509 certificate

It seems that the contents of your saved.p7b (certificate information store) or .cer (certificate file) are not valid. Are you able to open and view the .p7b or .cer file that you are trying to import? Copy the contents of certificate started from "-----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----" and paste in **Notepad**, remove all of the spaces, save it as text (.txt) document and rename the file extension from .txt to .p7b or .cer , this will resolve your problem.

How to request to revoke a digital certificate issued by Ascertia CA

There is no revocation mechanism supported for Digital Certificate, however if you want to revoke your digital certificate, send a signed email to support@ascertia.com with the details about your certificate to be revoked and we will analyze the request.



Revocation mechanism will be available soon for Low cost digital certificates.

How to configure MS Outlook to send secure Emails

To configure MS outlook to send secure emails follow the steps as below:

1. Open Microsoft Outlook. Click on 'File' menu, select 'Options' and Outlook Options screen will be displayed.
2. Click on 'Trust Center' from left panel, click on 'Trust Center Settings' button and Trust Center screen will be displayed.
3. Click on 'Email Security' from left panel. Now click on 'Import/Export' button and 'Import/Export Digital ID' screen will be displayed. Now select 'Import existing Digital ID from a file' option, browse and select your .pfx file, enter your .pfx file password in Password field of 'Import/Export Digital ID' screen, and press OK button to save settings.
4. Now on Trust Center screen, check 'Add digital signature to outgoing messages' option under Encrypted e-mail and click OK button to save settings.
5. Now on Outlook Options screen, click OK button to save settings.

New email message:

1. Compose a new email in Outlook.
2. Before to send the message, click the options button in the new message window. (Alternately, select Options from the View menu in the new message window). Click the check boxes for the options you want (either Sign, Encrypt, or both). Send the message. The message will show up in Outlook with small icons denoting that it has been signed or encrypted.



Before sending an encrypted email you must have certificate of that person which you want to send encrypted email. To get this, have them send you a signed email. In outlook, open the email and then right click on the person's email address, and select the option to add them to your contact list. Their key will be automatically added to the list of people you can decrypt from.

Decrypting Email from other people:

- To decrypt email from other people, you must have private key (associated with this public key) in your user key store.
- When the other person sends you an encrypted email, you may not be able to read it in the preview pane of Outlook. To view the message, open the message, and outlook will automatically decrypt it for you.

Save Digital Certificate from signed email:

- Digital Signature validity windows will be open
- Click on "View Certificate" button to view the certificate and all its detail.
- "View Certificate" dialogue window will be open, click on "Details" tab.
- Click on "Copy to file" button. This will start the digital certificate export wizard that will allow you to export the digital certificate of your contact person.
- Follow the certificate export wizard instructions to export the certificate on your hard disk.

Add new contact in outlook contacts and associate the certificate:

- Open MS Outlook, click on "File" Menu >> click on "New" >> Contacts
- New Contact window will be open, to add new contact click on "General" and type the general details (Name, email, phone numbers etc) of contact.
- Click on "certificates" tab, click on import button to import the certificate in outlook contacts, browse and select the path for respective certificate that you saved on the disk, click on "Open" button.
- Now you can send email to this person.

When you receive a signed message, you can save the digital certificate of sender in your Contacts List. You first need to click on the signed icon represented as ??

Where can I get the Ascertia Root CA certificate from

You can download the Ascertia Root CA certificate from the following link: <http://www.ascertia.com/onlineCA/CA/AscertiaRootCA2.crt>

How to get a Code Signing Certificate for Trial

Follow these steps:

- Register <https://account.ascertia.com/register> on our website and login to web portal: <https://account.ascertia.com/login>
- Click "Try Free Certificate".
- Click the "Try" button for the desired certificate to use it for trial purpose (30 days)

- Fill in the mandatory information to generate the certificate and click the "Submit" button.
- Click the Download icon available in the "PFX file" column to download the PFX of the desired certificate.

How to buy a Code Signing Certificate

Follow these steps:

- Register <https://account.ascertia.com/register> on our website and login to web portal: <https://account.ascertia.com/login>
- Click "Try Free Certificate".
- Select duration of the desired certificate from the drop down list as its validity period.
- Click the "Buy" button for the desired certificate.
- Fill in the mandatory information to generate the certificate and click the "Submit" button.
- Click the "Download" icon available in the "PFX file" column to download the PFX of the desired certificate.