Certificate Centre - KB Articles

Table of Contents

- How to fix Publisher can not be verified error on web pages with DLL / ActiveX controls signed with code signing certificate issued by Ascertia
- Sign jar files using JARSIGNER utility
- How to enable trust on Ascertia CA hierarchy in Firefox?
- 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?
- From where I can get Ascertia Root CA ?

How to fix Publisher can not be verified error on web pages with DLL / ActiveX controls signed with code signing certificate issued by Ascertia

Download Ascertia Root CA 2 and Ascertia Public CA 1 (the Intermediate CA Certificate, the issuer of your secure email digital certificate) and import these certificates in Internet Explorer (user key store). To download Ascertia Root CA 2 and Intermediate CA certificate use the links as below:

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

Once downloaded on hard disk, double click on these files one by one, click on “Install Certificate” and proceed with the installation wizard.

If you want to import these CA certificates in Firefox, then open Firefox, go to the above mentioned URL and select all options as shown below:

Once done restart your web browser and retry to access the webpage.

ⓘ It will be required to import Ascertia certification authority certificates on every desktop PC that will access the application or ActiveX control signed by code signing certiticate issued by Ascertia.

Sign jar files using JARSIGNER utility

You can sign your jar files Using JARSIGNER utility, that is bundled with Java SDK. Before to proceed you are required to download your code signing certificate with private key (PFX/ PKCS#12 file) issued by Ascertia Public CA 1 on your hard disk and follow the steps as below:

Jar Signing Command Syntax:

```
C:\Program Files\Java\jdk1.6.0_13\bin>JARSIGNER.exe –verbose –keystore {Path to PFX (PKCS#12) file} –storepass “{private key password}” –storetye {keystore type, i.e. PKCS12} {Path of JAR file to sign} {Signer alias, i.e. code signer certificate alias, (your name / CN value in certificate is signer certificate alias)}
```

Jar Signing Command Example:

```
C:\Program Files\Java\jdk1.6.0_13\bin>JARSIGNER.exe -keystore E:\Ascertia\codesigning\certs\codesigning1.pfx -storepass "password" -storetype PKCS12 E:\Ascertia\codesigning\Java\asc_pdf-s.jar andy
```

Signed Jar Verification Syntax:

To get detailed information of Jar signer the syntax is as below:

```
J:\Program Files\Java\jdk1.6.0_13\bin>jarsigner -verify {Path of the jar file to verify}
```

```
C:\Program Files\Java\jdk1.6.0_13\bin>JARSIGNER –verbose –certs -verify {Path of the jar file to verify}
```

Signed Jar Verification example:

```
J:\Program Files\Java\jdk1.6.0_13\bin>jarsigner –verbose –certs –verify E:\Ascertia\codesigning\Java\asc_pdf-s.jar
```

How to enable trust on Ascertia CA hierarchy in Firefox?

To build trust on Ascertia CA hierarchy in Firefox, you are required to import Ascertia Root CA certificate and Ascertia intermediate CA certificates in Firefox keystore. To import Ascertia Certification Authorities certificates, open Firefox and visit the URL's as below:

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

Firefox will display a "Downloading Certificate" dialogue, select all options as shown below:

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 http://www.ascertia.com/OnlineCA/default.aspx
2. Click on “Logon / Register” button to Logon to “Certificate Centre” and type your registered email address / password. On successful logon your web browser will be redirected to Certificate transactions main page.
3. Click on your desired certificate to view its contents.
4. Web browser will redirect to Certificate Transaction details page.
5. Click on appropriate button to download your digital certificate.
6. Browse the location to save your digital certificate, and click on save button.

1. Visit Certification authority site at http://www.ascertia.com/OnlineCA/default.aspx
2. Click on “Logon / Register” button to Logon to “Certificate Centre” and type your registered email address / password. On successful logon your web browser will be redirected to Certificate transactions main page.
3. Click on your desired certificate to view its contents.
4. Web browser will redirect to Certificate Transaction details page.
5. Click on appropriate button to download your digital certificate.
6. Browse the location to save your digital certificate, and click on save button.

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

See Article **“How to get a codesigning certificate and how to configure it”** to know more about how to import code signing certificate.

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**OR** http://www.slproweb.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 the PVK transform utility from http://www.drh-consultancy.demon.co.uk/pvk.html

```
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 .cert 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:

- Open Microsoft outlook. Click on “Tools” menu >> select “Options” >> go to the “Security” tab.
- If you already imported the secure email certificate then skip step 3 and 4 in this article
- To import the digital certificate click on “Import/Export” button.
- Click on “Browse” button, select the path to your certificate with private key (*.pfx file), type the private key password for your selected secure email certificate, type a name of Digital ID, and click on “OK” to complete secure email certificate import wizard in MS outlook (it

will be stored in logged in user’s key store).

- Click the “Settings” button. In Certificates and Algorithms area, click “choose” button and select your certificate for signing certificate and encryption certificate. Click “OK” in the “Change security settings” window.
- If you want to encrypt every outgoing message, click the check boxes “Encrypt contents and attachments for outgoing messages” under encrypted emails section of Security tab.
- If you want to sign every outgoing message, click the check boxes “Add digital signature to outgoing messages” under encrypted emails section of Security tab.

> ⓘ If you only want to digitally sign / encrypt selective messages, skip the steps 6 and 7 and follow instructions in step

- Compose a new email in Outlook.
- 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 ??

From where I can get Ascertia Root CA ?

You can download the Ascertia Root CA certificate from the following link:http://www.ascertia.com/OnlineCA/cacert.aspx?linkID=40.