Importing Panels with OCD '.DAT' files.

Author : Carlo Magnaghi Date : 25 March 2008

Note: from version 1.23, certificates are preinstalled; you only need to import certificates if you have deleted them or if they have been updated.

Panels are made available by Ortho Clinical in .DAT format files. Each one of these files contains a digitally signed antigram in ASN.1 DER format. This format warrants that any change in the file, by chance or by part of a malevolent party, may not go unnoticed.

Resolvigen 3 can verify the signature while importing panels from .DAT files.

Getting OCD digital signature certificates.

First of all you should obtain OCD digital signature certificates from your local OCD company. Digital signature certificates contain the public key of the signer entities. Please note that while 'public keys' are by their nature public, you should make sure you obtain them through a trusted source. This is because Resolvigen 3 will later consider trustworthy any information that is signed by the owners of these certificates. OCD certificates are normally made available in a .p7b file (PKCS#7).

Importing digital signature certificates.



In order to be able to verify digital signatures in .DAT files, it is necessary to load digital signature certificates into Resolvigen 3 first.

Log in as 'root': double click on the user name in the bottom right corner of Resolvigen 3 main window, or select Access archive and click on Change user item in Access menu.



In both cases Resolvigen 3 will display the change user dialog. Type 'root' as user name and enter root's password.

| Access Reso | olvigen 3 | | |
|---------------|-----------|-------|----|
| Access | User: | root | ~ |
| Exit Resolvic | Password: | ••••• | ок |

After clicking **OK**, Resolvigen 3 toolbar will turn red; this should be considered as a warning: never leave Resolvigen 3 in root mode unattended: a malevolent user could take a chance to hamper the security features of Resolvigen 3.

Select Change security setup from Access menu; Resolvigen 3 will display the Security settings dialog window.

| Security settings | × | | |
|--|---|--|--|
| Access | | | |
| Password: | | | |
| Enter password to change any of the fields below | | | |
| Access data | | | |
| New password: | | | |
| Retype new: Change | | | |
| Data protection | | | |
| Code: | | | |
| Retype code: Change | | | |
| Options | | | |
| Require login for user access | | | |
| ldentify user editing patient's data | | | |
| Identify user editing RBC data | | | |
| Identify user editing test data | | | |
| Certificates Close | | | |

Click on the Certificates button in the bottom left corner of this window.

| itored certificates | | |
|----------------------|-----------------|--------------------|
| A | dd certificates | Remove certificate |
| Selected certificate | | |
| Subject: - | | |
| lssuer: - | | |
| Time Validity: - | | |
| Serial Number: - | | |
| | | |
| Thumbprint (sha1): - | | |

Click the Add certificates button and select the .p7b file you obtained from OCD.

| 🔇 Open | | | | X |
|--|----------------|---------------------|---|----------------|
| Look in: | 🚞 OCD Panel | 3 | ~ | 1 |
| My Recent Documents Desktop My Documents My Computer | e≊ ocd.p7b | | | |
| S | File name: | ocd.p7b | | <u>O</u> pen |
| My Network Places | Files of type: | PKCS#7 file (*.p7b) | N | <u>C</u> ancel |

P7B files usually contain chains of certificates, each one warranted by a parent certificate, except the first one in the chain, that warrants for itself.

| Do you want to a | dd the following root certificate? |
|------------------|---|
| Subject: | CN=JNJ Root Certification Authority, OU=JNJ Public Key Authorities, O=JNJ, C=US |
| Issuer: | Self Issued |
| Time Validity: | From Monday, December 3, 2001 To Friday, December 3, 2021 |
| Serial Number: | 3c580835 |
| Thumbprint (sha | 1): ac31f8cd b0bb74cb fa066408 1064677b 52273f36 |
| Thumbprint (md8 |): b3efDa27 b6231852 abc72b7a 9d90f57d |

Resolvigen 3 flags self-signed certificates; you should verify these certificates by comparing the thumbprints (both sha1 and md5) with someone you trust, then click the **Yes** button to accept the certificate.

| Stored certificates | 3 | | |
|------------------------------------|---|---------------------------------------|--|
| CN=JNJ Principal | OnLine Certification Authority, OU=JNJ Publi | c Key Authorities, O=JNJ, C=US | |
| | na an de financia de la participación de la construcción de la construcción de la definitación de la definitación En anticipación de la construcción d | Nonlage of the president of the parts | |
| | Add certificates | Remove certificate | |
| Selected certifica | te | | |
| Subject: | CN=JNJ Principal OnLine Certification Authority, OU=JNJ Public Key Authorities, O=JNJ, C=US | | |
| lssuer: | CN=JNJ Root Certification Authority, OU=JNJ Public Key Authorities, O=JNJ, C=US | | |
| Time Validity: | From Monday, December 3, 2001 To Friday, December 2, 2011 | | |
| 2 10 10 10 10 | 3c580837 | | |
| Serial Number: |): 743570cd 20c0508b 09dc3afe_c1a7f78f 0ffd | 6665 | |
| Serial Number: Thumbprint (sha' | | | |

All certificates in chain will be displayed in the **Certificate Store** window. Click **OK** to close this window, the close **Security Settings** window.



You should now double click on 'root' label in the bottom right corner of Resolvigen 3 main window and login again, for example as guest.

| Access Res | olvigen 3 | | |
|--------------|-----------|-------|----|
| Access | | | |
| 1 | User: | guest | ~ |
| S. | Password: | | |
| Exit Resolvi | gen now | | ОК |

Importing Panels from .DAT files.



You may now import Panels from .DAT files: you should obtain .DAT files for the currently active panels from OCD then select **Import Panels** from **Panels** menu. Resolvigen 3 will display the **Import Panels** dialog. By using this dialog you may import Panels from any of the three supported formats:

- Resolvigen 2: this is the format used by Resolvigen 2 and is currently the most often used format.
- Resolvigen XML: this is the native format used by Resolvigen 3.
- OCD Files: this is the format used By OCD to distribute antigrams.

| Import pane | ls | | X |
|----------------------|------------------------|----------------|-----|
| Distribution file ty | pes | | |
| Resolvigen 2 | 🔿 Resolvigen XML 🔘 OCE |) Files (.dat) | |
| Import from folder | | | |
| A:\ | | Cha | nge |
| List of panels | | | |
| Name | Туре | Expiry | |
| | | | |
| | | | |
| | | | |
| | | | |
| | Reloa | ł | |
| Help | | Cancel | ОК |

Select OCD Files (.dat) among the formats listed at the top of the window and click **Change** button to select the folder in which you have stored the .DAT files.



Click **Open** button to check all .DAT files available in the selected directory; please note that the digital signature verification process is quite time consuming, so this step may require some time, especially if several .DAT files are present in the directory.

| Import panel | s | |
|-----------------------|----------------------------|-------------|
| Distribution file typ | es | |
| 🔿 Resolvigen 2 🕻 | 🔵 Resolvigen XML 🧿 OCD Fil | les (.dat) |
| Import from folder | | |
| A:\DAT | | Change |
| List of panels | | |
| Name | Туре | Expiry |
| 8RA179 | Panel A | 08-Mar-2005 |
| 8RB178 | Panel B | 08-Mar-2005 |
| 8S648 | SelectoGen | 08-Mar-2005 |
| 8SS317 | SurgiScreen | 08-Mar-2005 |
| 8SS318 | SurgiScreen | 08-Mar-2005 |
| | Reload |] |
| | | |
| Help | | Cancel OK |

Click **OK** to import all the selected panels; please note that by default only valid Panels are displayed, so if you are importing expired panels for some reason, they will not be immediately displayed in the main window. In this case select **View** \rightarrow **All Panels** in **Panels** menu to display them.

Note: a complete digital signature verification process should check CRLs (Certificate Revocation Lists) on the Internet to make sure that the digital signature certificate signing the document has not been revoked. This step is skipped by Resolvigen 3 because it is often problematic and requires the computer verifying the signature to be connected to the Internet.