Federated Identity Service

Export & Import Software Certificates
(For Users with FIS Basic, Secure Email, and Medium Software Certificates)

Version 2.0
Exostar, LLC
August 25th, 2014
Table of Contents
Purpose .................................................................................................................................1
Exporting Certificates .......................................................................................................1
Importing Certificates .......................................................................................................5
Increasing Certificate Security Level ................................................................................11
Purpose
This guide has been created for the users who need to back-up their certificates. This guide will provide you information on the process to export the certificates for safe-keeping and importing backed-up certificates.

Exporting Certificates

**IMPORTANT:** The instructions for exporting and importing your digital certificate are intended for certificate backup purposes only. Users should maintain control of their digital certificates at all times and it is recommended that users apply strong passwords to their certificates during export. For additional information on your organization’s policies regarding certificate usage and storage, please contact your organization’s IT or Security Office.

Follow the steps below to export the certificate:

1. Open an Internet Explorer browser window
2. Click Tools/Internet Options/Content/Certificates (see below)

![Internet Options](image)

3. The following screen will be presented. From the Personal tab, highlight the certificate marked ‘Identity’ and click Export.
4. Click the option ‘Yes, export the private key’ and click Next.

5. Click the options ‘Include all certificates in the certification patch if possible’ and click Next.
6. Apply a password to the certificate. Click Next.

Note: You must remember this password. It will be used during the certificate import process.

7. Browse for a location to store your certificate. Click Browse... For security reasons, it is important that you maintain control of your digital certificate at all times.
8. Enter your first and last name as the File name. The Save as Type should be *.pfx. Click Save

Note: In order to label this certificate as your ‘Identity’ certificate, enter ‘(Identity) follows your last name. This enables you to identify your certificates correctly.
9. The file path will be populated, click Next>

10. Click Finish

11. You should receive an ‘Export was successful’ message. Click OK.

You have successfully exported your digital certificate! If you have multiple certificates, back-up each certificate by following this process.

**Importing Certificates**

Follow the steps below to import the certificates that you backed up previously.
1. Open an Internet Explorer browser window
2. Click Tools/Internet Options/Content/Certificates

3. From the Personal tab, Click Import.

4. The Import Wizard will open, click Next>
5. Browse for the .pfx file (certificate) you saved during the export process. Click Browse.
6. Make sure you are browsing for file type .pfx and choose the certificate labeled 'Identity' and click Open.

7. The certificate file path will be populated. Click Next>.
8. Enter the password that you applied to the certificate during the export process (Step 9 above). Optionally, check the box to Enable Strong Key protection to be prompted for this password each time this certificate is leveraged.

9. Choose the ‘Automatically select…’ option and click Next>
10. Click ‘Finish’

11. The ‘Importing new private exchange key’ window is displayed. At this point you have the option to increase the security level of the certificate.

**NOTE:** If you wish to increase the security level, click on Set Security Level and follow the steps provided in Increasing Certificate Security Level section for next steps.

To leave your security level at Medium, click OK

12. You should receive an ‘Import was successful’ message. Click OK
You have completed the certificate import process. If you need to import additional certificates, follow the process until you have imported all certificates.

**Increasing Certificate Security Level**

In the previous section, we covered the Import of Digital certificates. As a corporate policy, you may also be required to add additional Security level for your certificate. At Exostar, we encourage you to set the security level for your Medium Level of Assurance Certificates to High.

1. Starting from Step 11 of the ‘Importing Certificate’ process above, click the Set Security Level button

2. Choose the High option. Click Next>
3. Enter a CryptoAPI Private Key Password, confirm password then click Finish.

Note: Please remember this password. When using your certificate to access ForumPass, you will be prompted for this CryptoAPI password after selecting your certificate.

![](image1.png)

4. Security level will now be set to High. Click OK

![](image2.png)

5. You should receive ‘Import was successful’ message

![](image3.png)

You have successfully imported your digital certificate with High Security Level!