8966 IDES Packager Overview

Overview

The 8966 IDES Packager comes with 8966 Pro or it can be purchased separately. The Packager will "Package / Encrypt" your data with your private Digital Certificate (Cert) and it will also "Unpackage / Decrypt" files received from IDES using your Cert.

To clarify: the certificate containing the private key is something the customer must get for himself, and must arrange for IDES to recognize (by uploading the public component of the certificate to them) and is highly sensitive. By design for security the IDES Packager does not manage your Cert but it lets the customer browse for the Cert once IDES packager is up. You can browse for the .pfx Cert or if you have a .pem or .key file containing just your private key, and a .crt file with the same names in the same directory, IDES-Packager will accept either file and will find the other one automatically.

Other features include:

- There are two versions **Embedded** is for TPS. It requires a reg code and to reside in it's native directory or it will not run . **Standalone** does not require a code or a special directory.
- There is an unpackage / decrypt mode. Select the Radio Check box at the top for the correct operation.
- Error Checking
  - when a certificate fails verification, information on why is logged to the text box.
  - Validation for XML logs information to the text box. IDES Packager should now reliably prevent you from packaging up a file that would cause problems when sent to IDES including more thorough character escaping to match the IRS's stringent requirements.
  -
- Added drag and drop functionality for selecting your file in step 1 & 2.
- A few UI improvements: notably, double-clicking the log brings up a dedicated window, from which you can save the log to a file (will become useful later when the log is more detailed.)
- Creation of a NIL Report - Only Direct Reporting Non-Financial Foreign Entities (NFFEs) are required to submit nil reports. For all other entities, submission of nil reports is not

mandatory and submission of these reports is optional. While nil reporting might not be required by the IRS, it might be required by the local jurisdiction. Please check with your local tax administration. Nil reports that are submitted must provide Reporting FI information. The report contains Reporting Group, but it does not contain any account reports or pooled reports. Reporting group can be empty or can contain Sponsor or Intermediary information.

Resources:

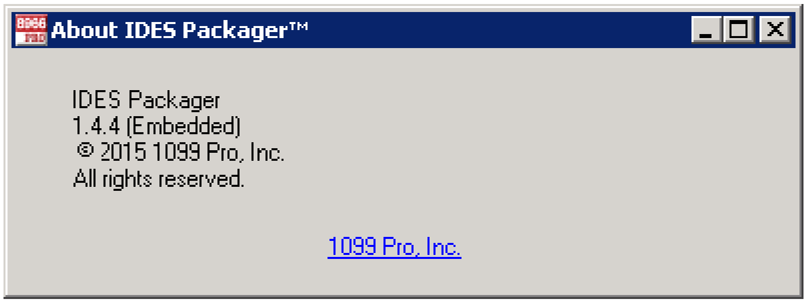
International Data Exchange Service (IDES) - Knowledge Base
https://www.ides-support.com/KnowledgeBase/Index#

8966 Videos - https://www.1099pro.com/videos.asp

Checking for updates to the 8966 Software - From within the 8966 Software click on help & then on Check for updates. If your firewall blocks the update you can download the update directly from https://wiki.1099pro.com/display/PDWA/Support+Download+Site

Checking the IDES Packager Version Number:

Open the IDES Packager. From the 8966 software just click on IDES Packager under #3 on the left. In the packager click on Help & About and you will something similar to :

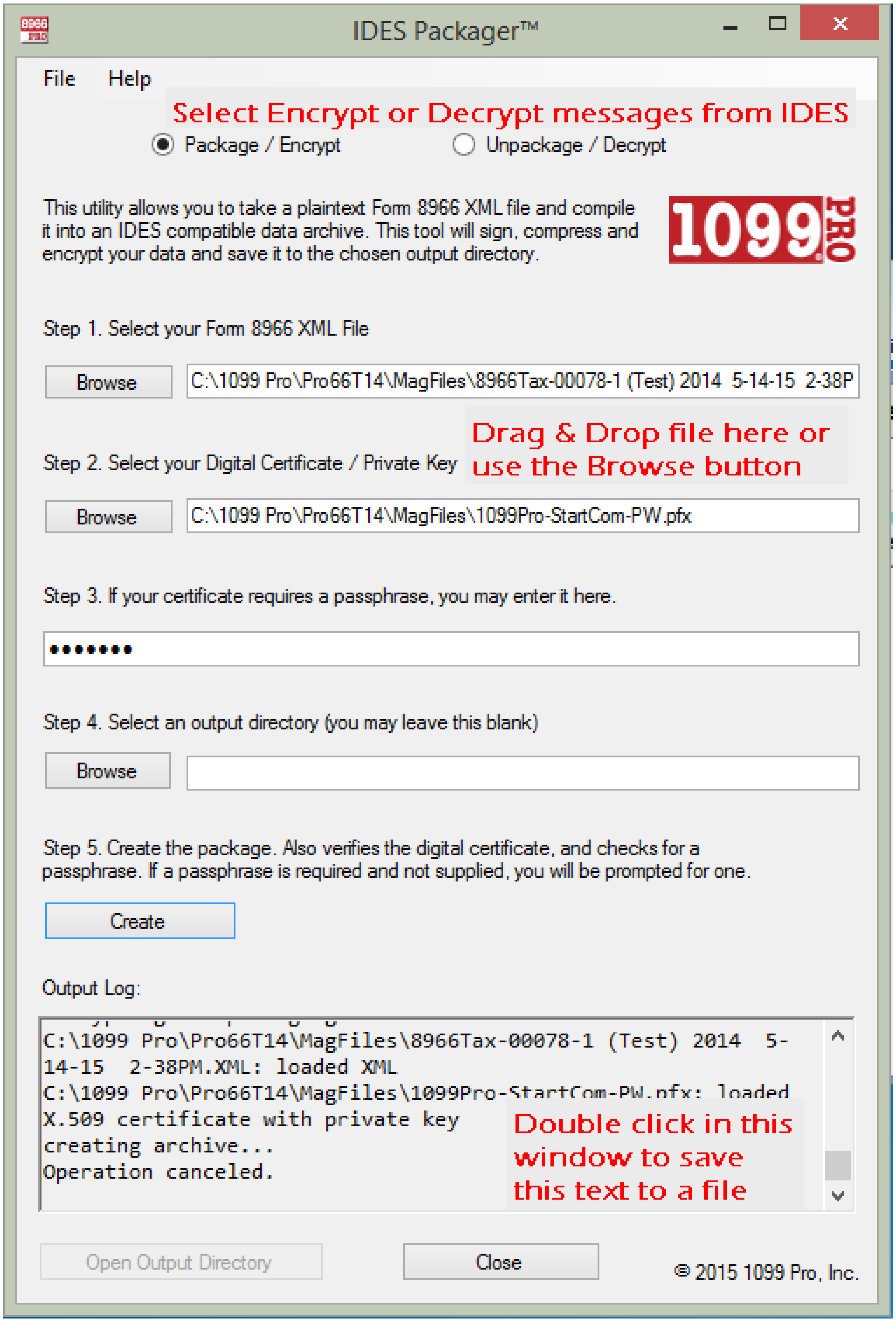


About IDES Packager™

IDES Packager
1.4.4 (Embedded)
© 2015 1099 Pro, Inc.
All rights reserved.

1099 Pro, Inc.

Appendix - IDES Packager Interface



Select Encrypt or Decrypt messages from IDES

● Package / Encrypt ○ Unpackage / Decrypt

This utility allows you to take a plaintext Form 8966 XML file and compile it into an IDES compatible data archive. This tool will sign, compress and encrypt your data and save it to the chosen output directory.

Step 1. Select your Form 8966 XML File

C:\1099 Pro\Pro66T14\MagFiles\8966Tax-00078-1 (Test) 2014 5-14-15 2-38P

Drag & Drop file here or use the Browse button

Step 2. Select your Digital Certificate / Private Key

C:\1099 Pro\Pro66T14\MagFiles\1099Pro-StartCom-PW.pfx

Step 3. If your certificate requires a passphrase, you may enter it here.

••••••••

Step 4. Select an output directory (you may leave this blank)

Step 5. Create the package. Also verifies the digital certificate, and checks for a passphrase. If a passphrase is required and not supplied, you will be prompted for one.

Output Log:

```
C:\1099 Pro\Pro66T14\MagFiles\8966Tax-00078-1 (Test) 2014  5-
14-15  2-38PM.XML: loaded XML
C:\1099 Pro\Pro66T14\MagFiles\1099Pro-StartCom-PW.pfx: loaded
X.509 certificate with private key
creating archive...
Operation canceled.
```

Double click in this window to save this text to a file

© 2015 1099 Pro, Inc.

Appendix – How to get the valid times for a certificate embedded in a .PFX file

If the IDES notifies you that the encrypted upload certificate differs from the digital cert you have on file we recommend that you upload your digital certificate to the IDES site again

If you haven't already, you should extract the third certificate from their PFX as described in https://ides.desk.com/customer/portal/articles/1895247-exporting-a-single-certificate, and upload that to IDES. If that's the certificate IDES already had, it'll do no harm, and if it's not, then it'll fix their problem.

Then recreate your encrypted package using the same certificate again and send it to the IDES again and see if it works. If you still get the error from IDES then it is possible to look at the certificate dates you have and compare them with the IDES site. If the dates don't match it would be a clear indicator that the cert used for encryption is different than the cert the IDES site has. Follow the below instructions to get the cert date from your local PC. Assuming that didn't fix the problem, we might be able to learn something with this:

If you have the standalone IDES Packager, open a command prompt in the directory where `ides-packager.exe` is, extract the attached ZIP file into that directory, and run it with the following command line:

```
ides-packager.exe "000000.00000.TA.124 - Valid.xml" --recipient=1099pro_certificate.crt
```

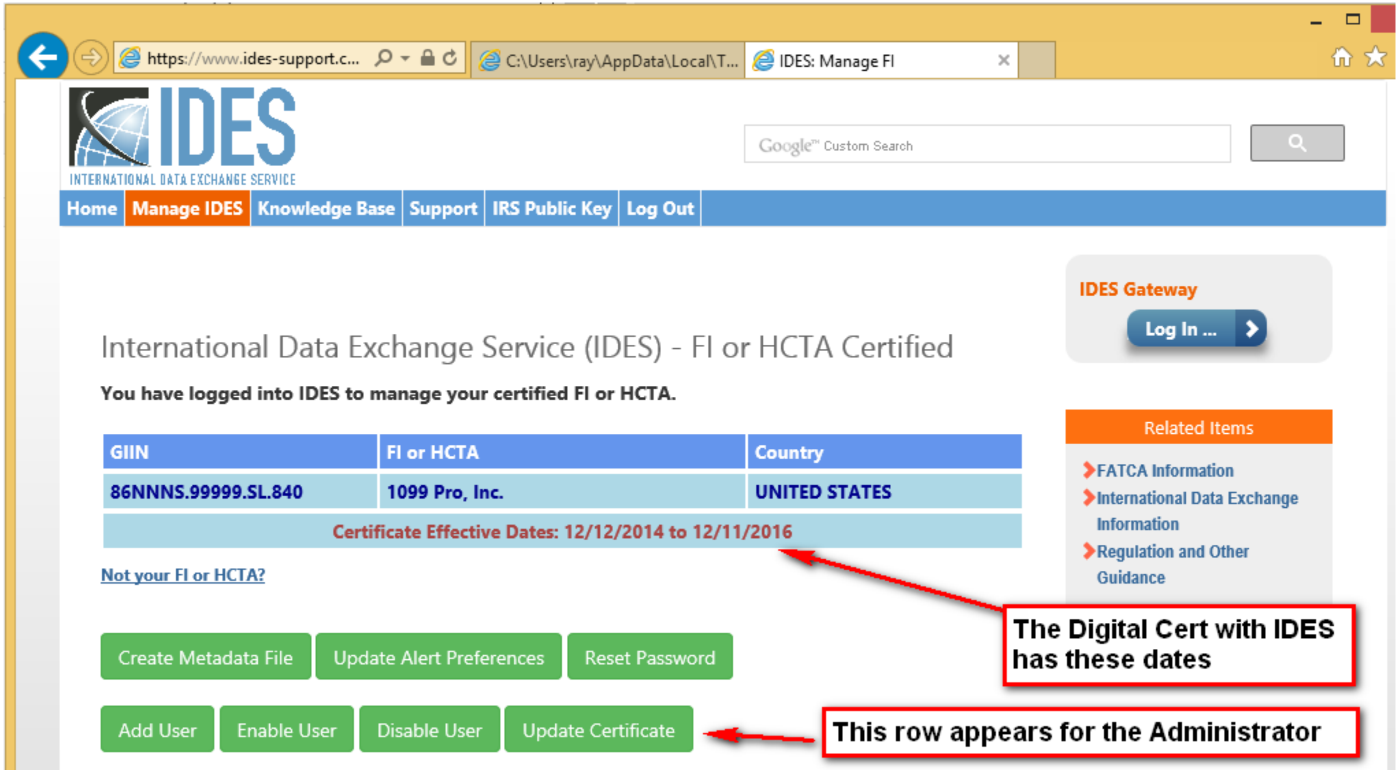
IDES Packager should open up as usual, with Step 1 already filled in. Then they should fill out the rest of the steps as usual, create a package, and then send that package to us, along with their certificate. It's important that they NOT send us the PFX (that contains their private key), but the third certificate embedded within the PFX, which is what they uploaded to IDES at some point in the past.

Because they'll be using our certificate as the recipient (instead of the default IRS certificate), we will be able to decrypt the package, and verify that the key they used to sign the XML corresponds to the certificate they give us.

Appendix – Comparing the IDES Digital Certificate dates to your Certificate

This test compares the dates of the IDES Digital Cert with the dates of the Digital Cert you are using. First we will get the dates of the IDES Digital Cert & then we will get the dates of the PFX cert and compare them. If they are different then that's a problem. If they are the same it proves nothing as you might have one or more Digital Certs with the same dates.

1. Login to IDES and your dates are shown as below.



International Data Exchange Service (IDES) - FI or HCTA Certified

You have logged into IDES to manage your certified FI or HCTA.

GIIN	FI or HCTA	Country
86NNNS.99999.SL.840	1099 Pro, Inc.	UNITED STATES
Certificate Effective Dates: 12/12/2014 to 12/11/2016		

The Digital Cert with IDES has these dates

This row appears for the Administrator

2. On your computer with the Digital Cert do the following where is the name of your FILE.PFX Digital Certificate. Compare this with the NotBefore: and NotAfter: dates as shown below.

In a command line, run:

```
certutil -dump FILE.PFX
```

It will prompt for the password, and once entered output some information. Look for two lines beginning "NotBefore:" and "NotAfter:"

Sample output using this approach on our IDES certificate/key pair:

```
C:\Users\8966\Desktop\Projects\IDES>certutil -dump Input\1099Pro-
StartCom-PW.pfx
Enter PFX password:
================ Certificate 0 ================
================ Begin Nesting Level 1 ================
Element 0:
Serial Number: 02b69f
Issuer: CN=StartCom Class 2 Primary Intermediate Server CA,
OU=Secure Digital Certificate Signing, O=StartCom Ltd., C=IL
NotBefore: 12/12/2014 10:45 AM
NotAfter: 12/11/2016 9:11 PM
Subject: E=webmaster@1099pro.com, CN=*.1099pro.com, O=1099
Pro, Inc., L=Calabasas, S=California, C=US
Non-root Certificate
Cert Hash(sha1): f0 61 a8 58 b3 72 0f c7 fc e4 0e 4a 85 a8 45 81 15 9f
b0 40
----------------  End Nesting Level 1  ----------------
  Provider = Microsoft Enhanced Cryptographic Provider v1.0
Encryption test passed
CertUtil: -dump command completed successfully.
```

Appendix – Advanced Debugging, How to check your own signed XML

Failed Signature Check Notification (NSC)

1. **Why did my organization receive this notification?**
   The IRS could not validate the digital signature on the payload file with the IDES file ID, transmission ID and timestamp, with your organization's valid public key on IDES.
2. **What do I need to do as a result of this notification?**
   Please re-sign the file using the procedures provided in the IDES User Guide, available on the IRS IDES Home, and your local encryption software package and recreate and upload the transmission to IDES following all procedures (see the IDES User Guide, available on the IRS IDES Home) for transmission preparation and upload. The IRS will send another notification to you through IDES once your file has been downloaded and processed further.

The method below provides a way for the user to check their own signed XML. Contact TS@1099pro.com if IDES cannot match your encrypted upload to the digital certificate uploaded to IDES. Customers will need to download the **DEV** version, not the standalone, and will have to run the encryption from the command line, and then the signature-checking command. I would like them to do this to a file that actually gets sent to IDES. Here is a log of a session that tries to demonstrate the process.

```
> ides-packager --version
ides-packager 1.4.7 (dev)

Copyright (C) 2015 1099 Pro, Inc.
All rights reserved.
> dir
Volume in drive C has no label.
Volume Serial Number is 5E6A-1AD9

Directory of C:\Users\Pro\Desktop\Projects\IDES

05/11/2015  01:23 PM    <DIR>          .
05/11/2015  01:23 PM    <DIR>          ..
02/11/2015  12:41 PM             6,790 000000.00000.TA.124 - Valid.xml
04/22/2015  09:40 AM             2,710 1099Pro-StartCom-PW.crt
03/10/2015  01:18 PM             4,677 1099Pro-StartCom-PW.pfx
               3 File(s)         14,177 bytes
               2 Dir(s)  352,842,268,672 bytes free

> ides-packager "000000.00000.TA.124 - Valid.xml" 1099Pro-StartCom-PW.pfx --test --
output output
Please enter the passphrase for 1099Pro-StartCom-PW.pfx, then press Enter
```

```
creating archive...
output file: 000000.00000.TA.124 - Valid.xml
output file: 000000.00000.TA.124_Payload.xml
output file: 000000.00000.TA.124_Payload.zip
output file: 000000.00000.TA.124_Payload
output file: 000000.00000.TA.840_Key
output file: 000000.00000.TA.124_Metadata.xml
output file: 20150511T082345601Z_000000.00000.TA.124.zip

> ides-packager --check-signature output\000000.00000.TA.124_Payload.xml 1099Pro-StartCom-PW.crt
signature verification SUCCEEDED
This XML was signed by:
  E=webmaster@1099pro.com, CN=*.1099pro.com, O="1099 Pro, Inc.",
  L=Calabasas, S=California, C=US (F061A858...)
```

Notes:

1) The first two commands are just for demo purposes.
2) The encryption is done with the third command. The --test flag causes ides-packager to output all of its intermediate files along with the result archive. This means that the signed XML is output, unencrypted, which is important because the encrypted output cannot be decrypted by anyone but the IRS. In this example, the signed but unencrypted XML is 000000.00000.TA.124_Payload.xml, and the encrypted archive (which may be uploaded to IDES if the source data is real) is 20150511T082345601Z_000000.00000.TA.124.zip.
3) The fourth command checks the signature on the signed XML to verify that it was created correctly. Notice that we used a different certificate file. The CER file contains only the certificate, not the private key. ForeignBank can use the file they sent us earlier, ides.cer at that point. This should be exactly the same file they uploaded to IDES.