NextGen-Widget-Encrypt-Help

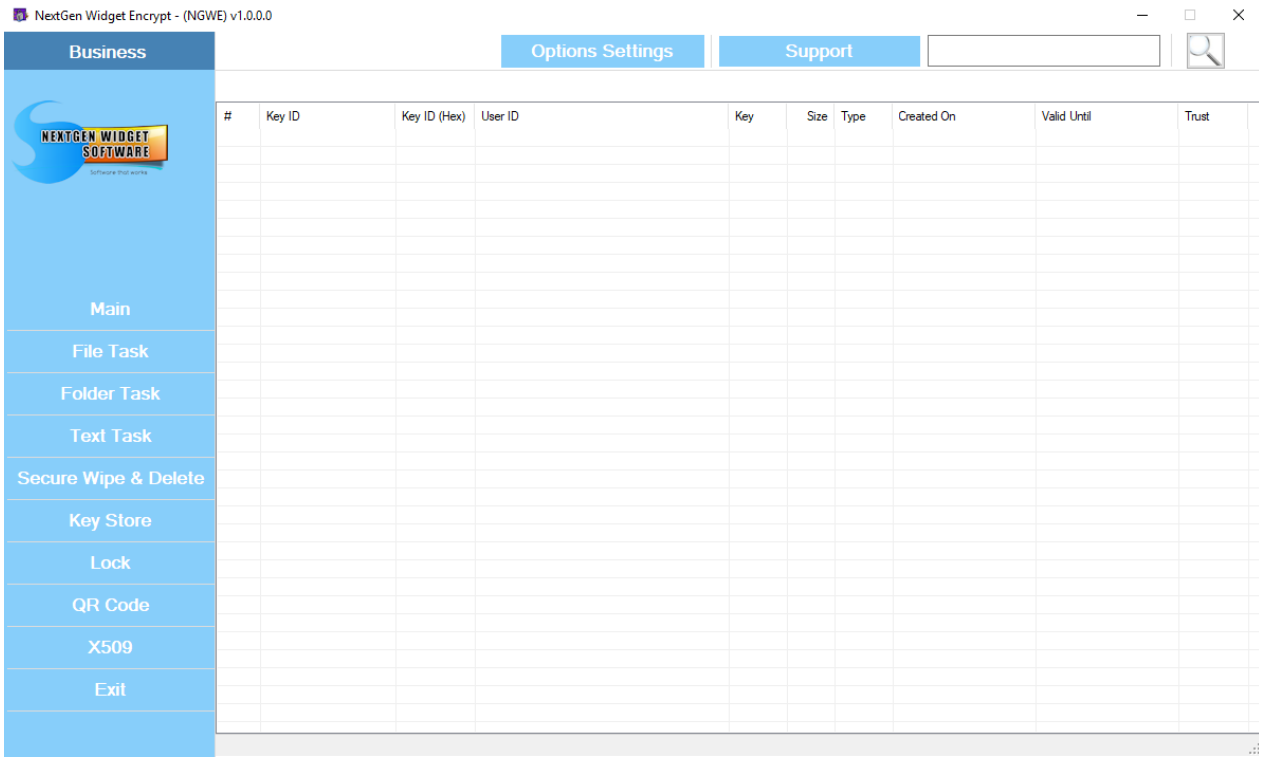
Table of contents

Introduction

NEXTGEN WIDGET ENCRYPT

BY NEXTGEN WIDGET SOFTWARE

A premier GUI for OpenPGP



[Go to Welcome page.]

Welcome

Welcome to NextGen Widget Software's NextGen Widget Encryption NextGen Widget Encrypt program. The OpenPGP operations are performed using DidiSoft OpenPGP Library for .NET.

In our day we take privacy for granted, thinking that every eMail for example is secure or that other Cloud services are all secure when the data is at rest on there servers. Other's think that none of there information is worth anything to anyone so no one wants there information... Wrong!

Just a harmless eMail can revel a boat load of information that a hacker can use to steal your identity.

For example:

=========
eMail: Hi Bob, I'm going on a vacation to Disney World next week for two weeks both Jill and I. We have to leave the dog with Bill because I don't want to leave him at the dog pound. We will meet you at my brothers house in Orlando on Friday 22nd at 3:00 PM.

Jack.
========

Although this is a small example it has some revealing qualities. The biggest one is that it tells a hacker and robber that you'll be away for two weeks and the dog will not be there. If this hacker is working with a burglar, then you may very well have a very big problem. Further this eMail tells the hacker your name, email address and your wife's name just for starters. An easy way to associate an email address with a username is by social media or simply a Google search. Social media can be used to gather all sorts of personal information from this this email.

I know you have seen all the sites that find people or group relatives, ages and phone numbers. Then there's the sites that linkup email addresses with names and addresses or phone numbers. So now, the hacker has put together a profile on you just with this little bit of information.

Most of us give out more information than that and attach PDF's to an email that may have Banking information or perhaps Mortgage information because we're applying for a Mortgage. Even some government sites don't require encryption when they accept resumes and other personal information. In todays world most things are done via email with no thought of security. Just look at most sites and you'll see that email is the root of a new evil. Here, let's look at the NYS Department of Motor Vehicles "Medical Certification Unit" for example. This unit receives Medical Certification and Medical Documents, but has one of the ways to receive Medical Documents in unsecure email without posting a OpenPGP public key so you could email an encrypted document. Granted, a lot of people see this process as being too difficult and rather take the chance of their personal information being discovered and used criminally.

Cloud services are just another way to say "I don't want to manage the data, you do it". The problem with "you do it" is that you have know idea how that data is secured on someone else's computer. Just think of the big box stores that had credit card numbers stolen or the 145.5 million that had there credit stolen with an additional 2.4 million Americans that only had their names and a partial driver's license number stolen by the attackers. If these companies had there data encrypted at rest, then the stolen information would have been useless to the thefts. How many times do you get a letter that says a particular company has been breached and your information was stolen. In a lot of these cases and will claim that no personal data was stolen, but how do you actually know that.

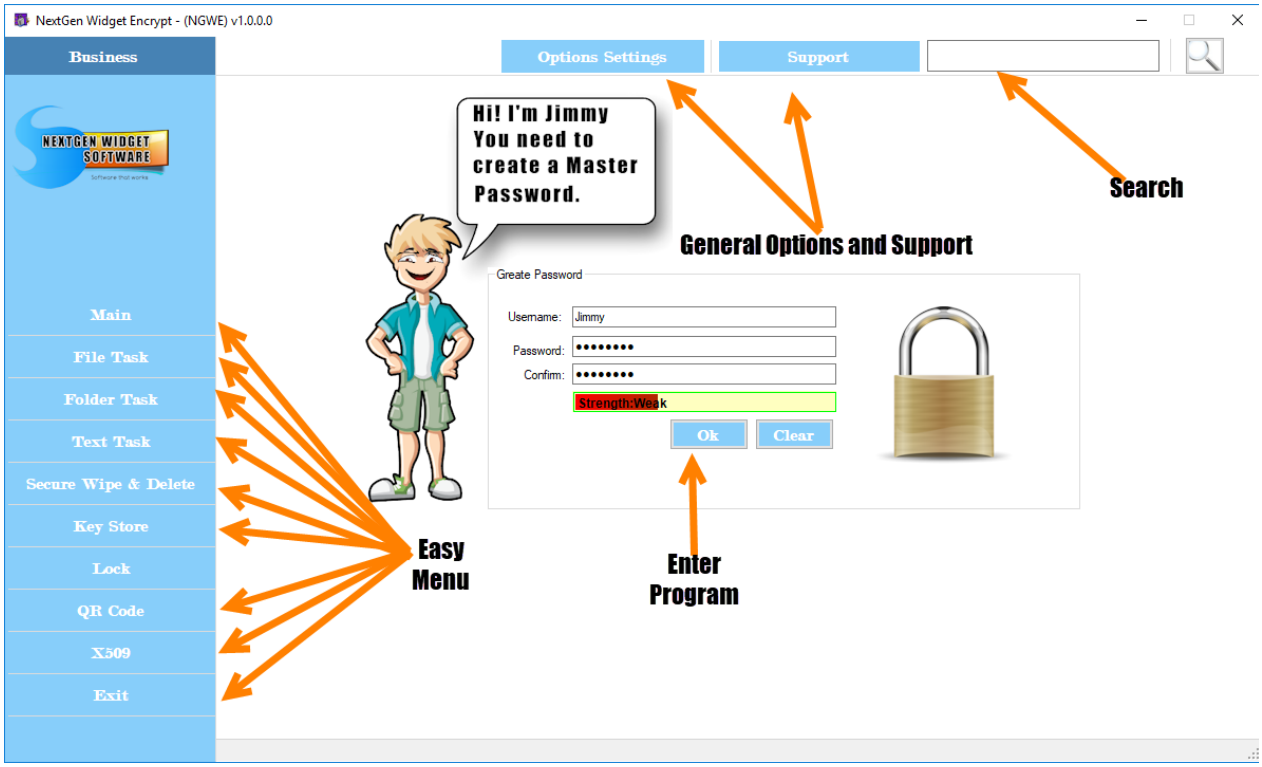
This is just a very, very small example of why we need encryption and why I made "NextGen Widget Encrypt". NextGen Widget Encrypt uses OpenPGP and it makes it easy to use Public Key Infrastructure, (PKI) Encryption. The interfaces are easy to understand and easier to use. NextGen Widget Encrypt has a smooth look that's easy on the eyes, plus all

the needed functions that makes OpenPGP top dog in the game like; Text, File and Folder Task, Secure Wipe and Delete, QR Code generating and X509 Certificate generation.

Just jump right into it by navigating to "Getting Started" link to show you all the functions of the all new NextGen Widget Encrypt software.

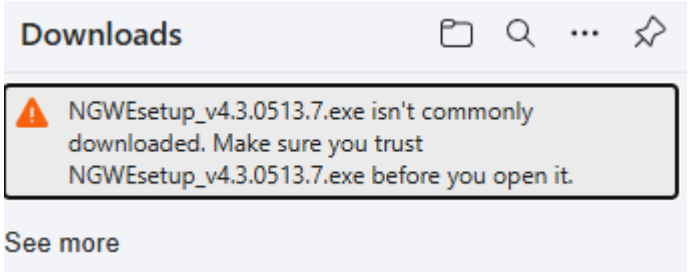
DISCLAIMER OF WARRANTIES

Getting Started

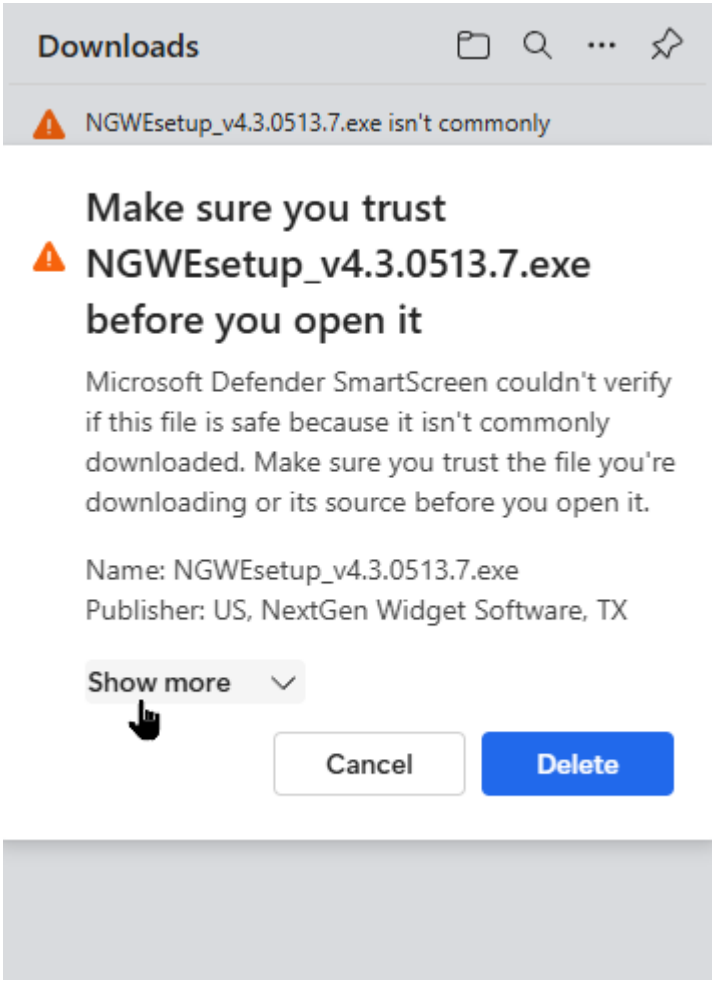


Setup and Install

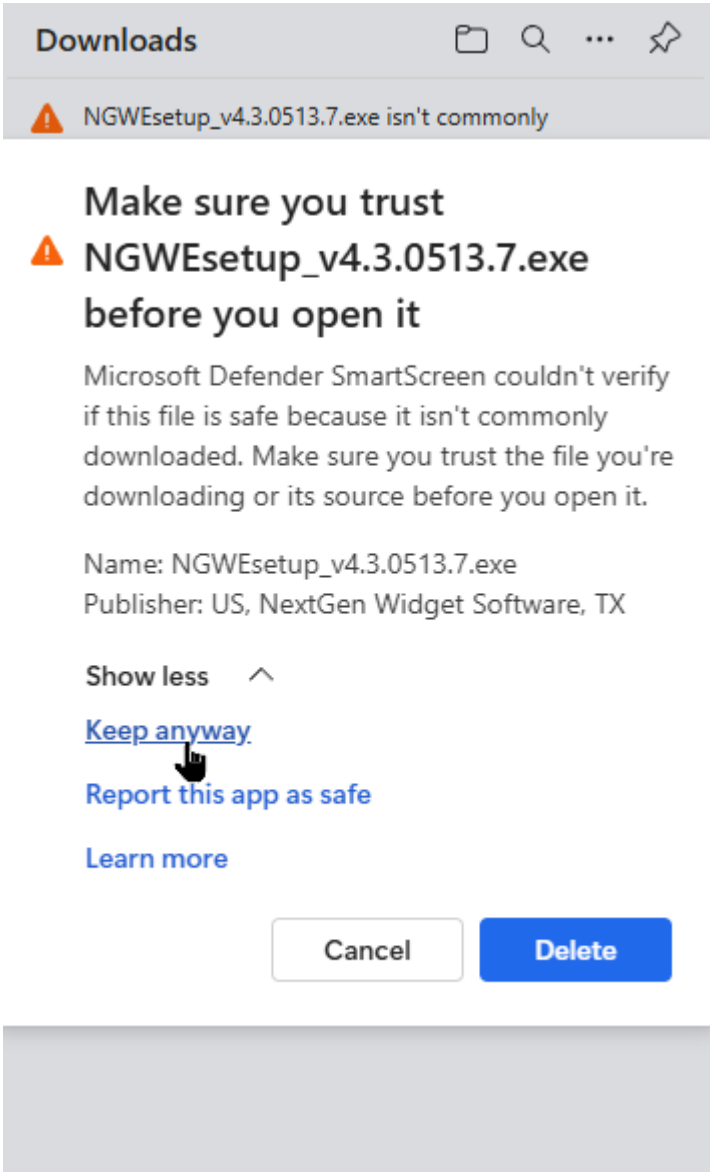
When downloading the program from the website you may get trust message. This software can be trusted.



Just click on the… And select "Keep" and click the "Show more" down arrow.



Now, Just select "Keep anyway".



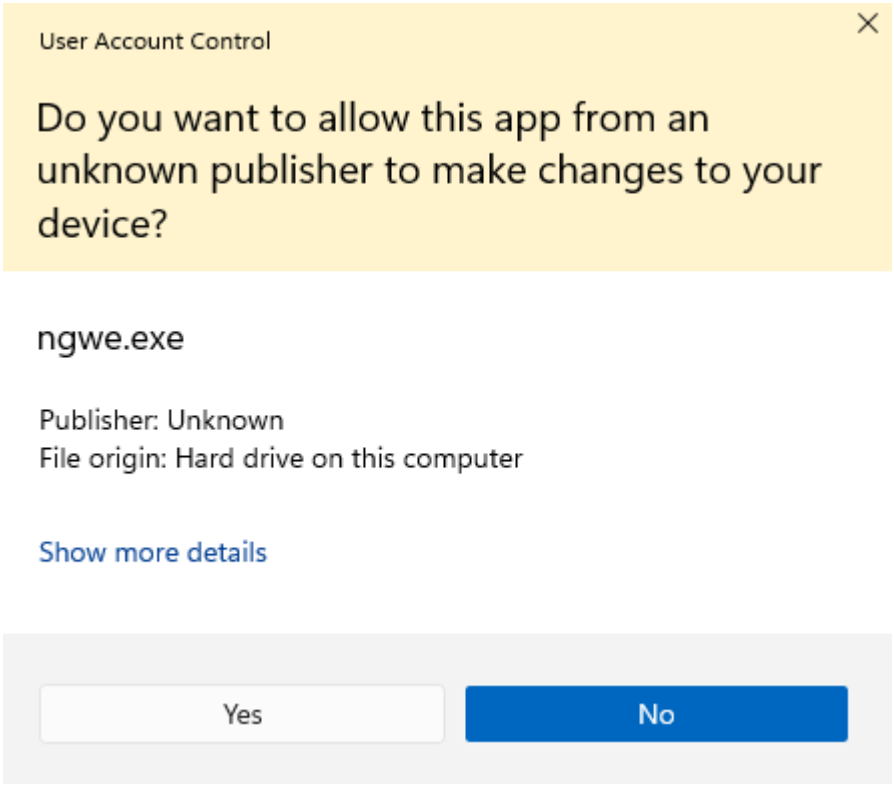
Now just go to the directory that the setup file was saved to an double-click.

Set up and install is a simple process. Just double-click on the set up installer Set up and install is a simple process. Just double-click on the set up installer. While it's on your PC you will see a shield over the icon. Once you double-click on the installer you will see the User Account Control (UAC) which says Publisher "unknown" unless you turn this off. This is because the program does not have a Root CA certificate in the Microsoft certificate store.

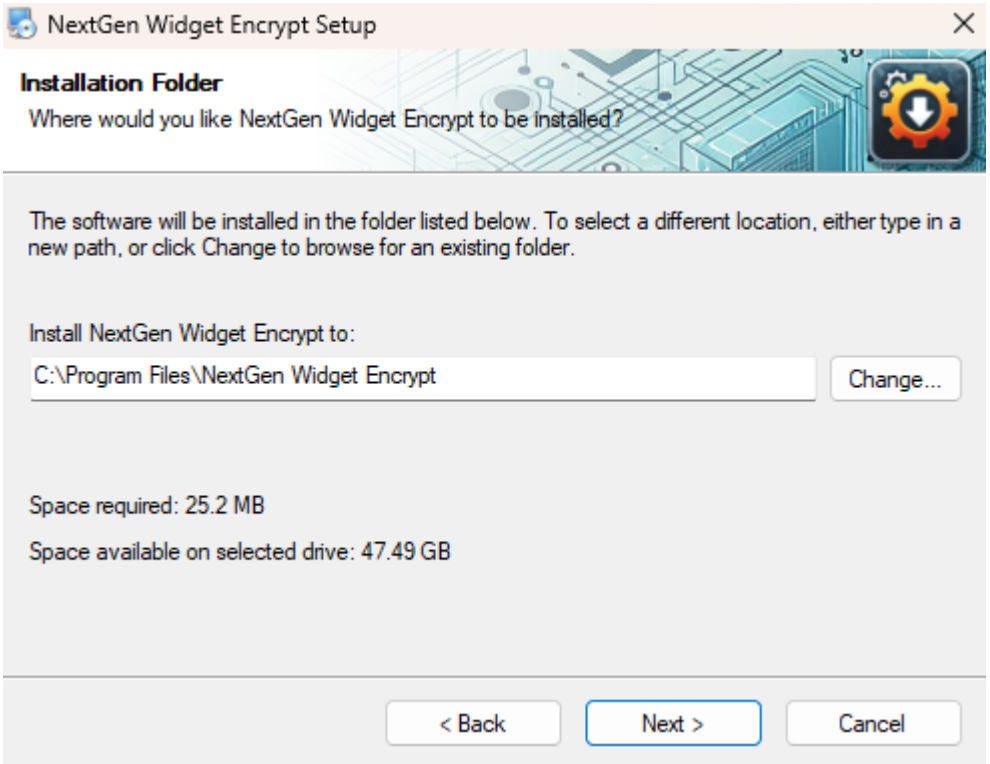
This is fine and you can install it. Just click "YES", The program comes with a built in Root CA that you can install if you so choose.

NGWEsetup_v4.3.0513.7.exe

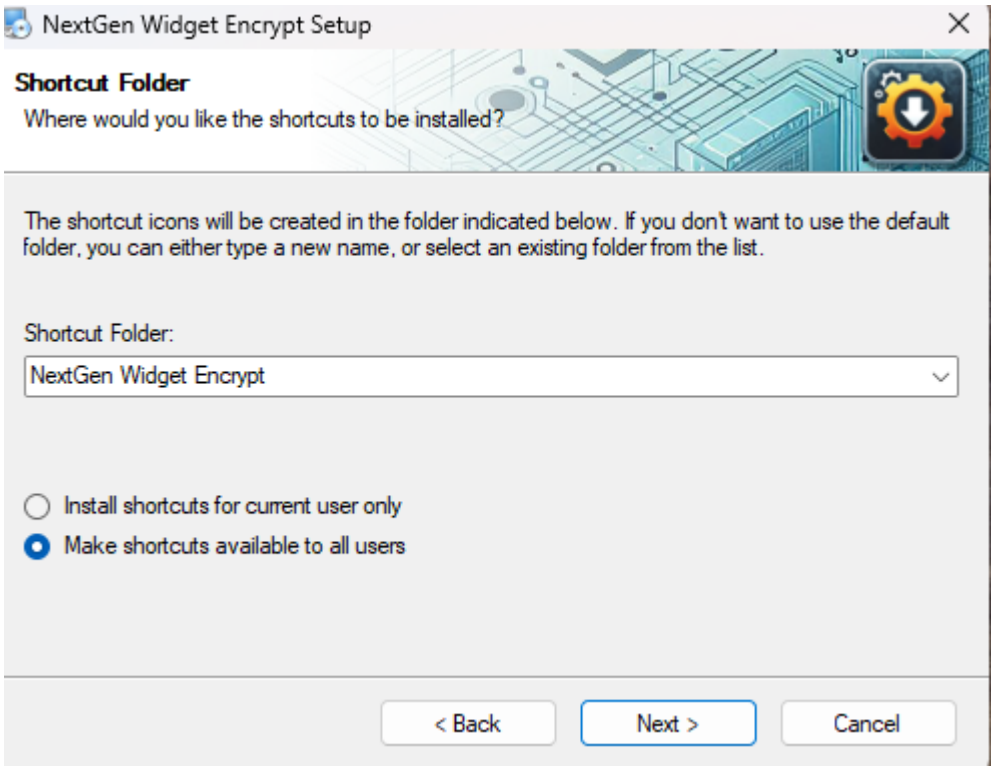
User Account Control (UAC)



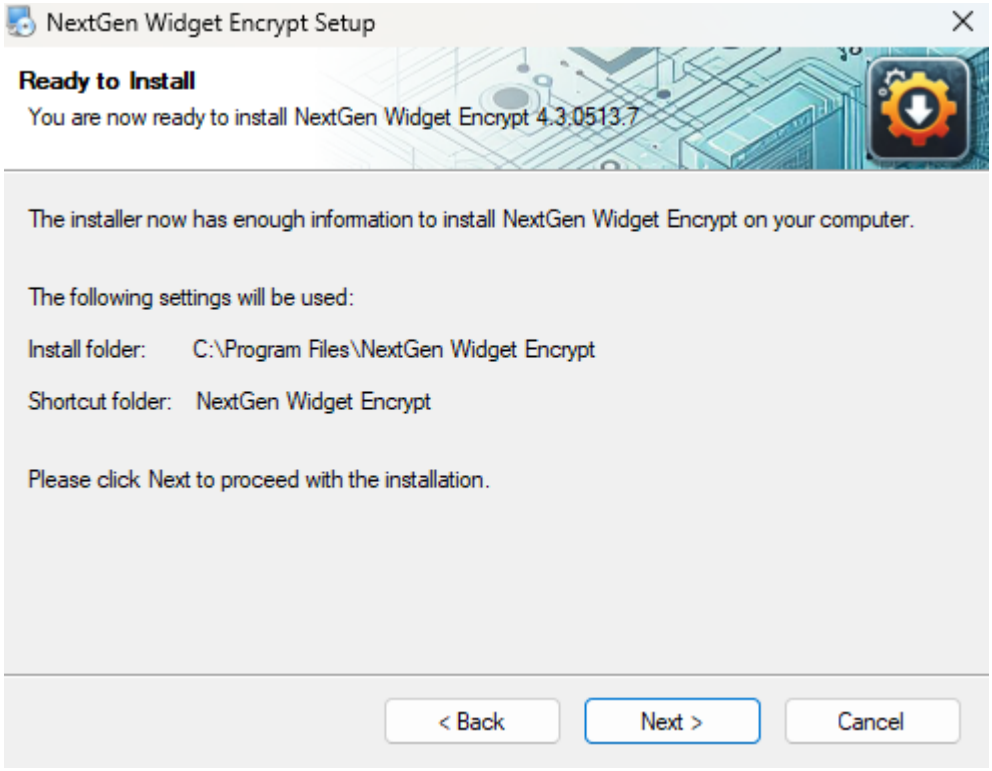
Now just click "Next" and agree to the software terms. Click "Next add user information and then select your directory if default is not adequate.



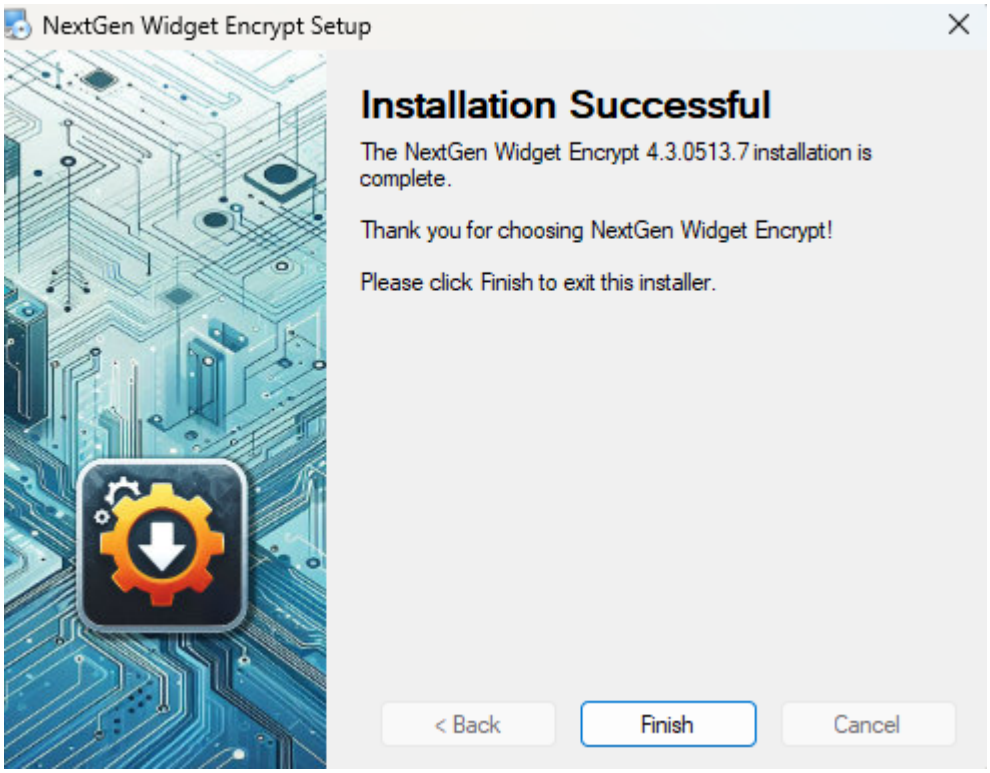
The program will create a shortcut folder and install the shortcut for the current user only. However, you can select to "Make the shortcut available to all users". Even though the application would be installed for all users. Each user has their own Key Store which is placed in "C:\Users\[YourUserName]\AppData\Roaming" folder.



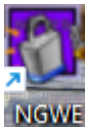
Verify the directory and shortcut and then click Next.



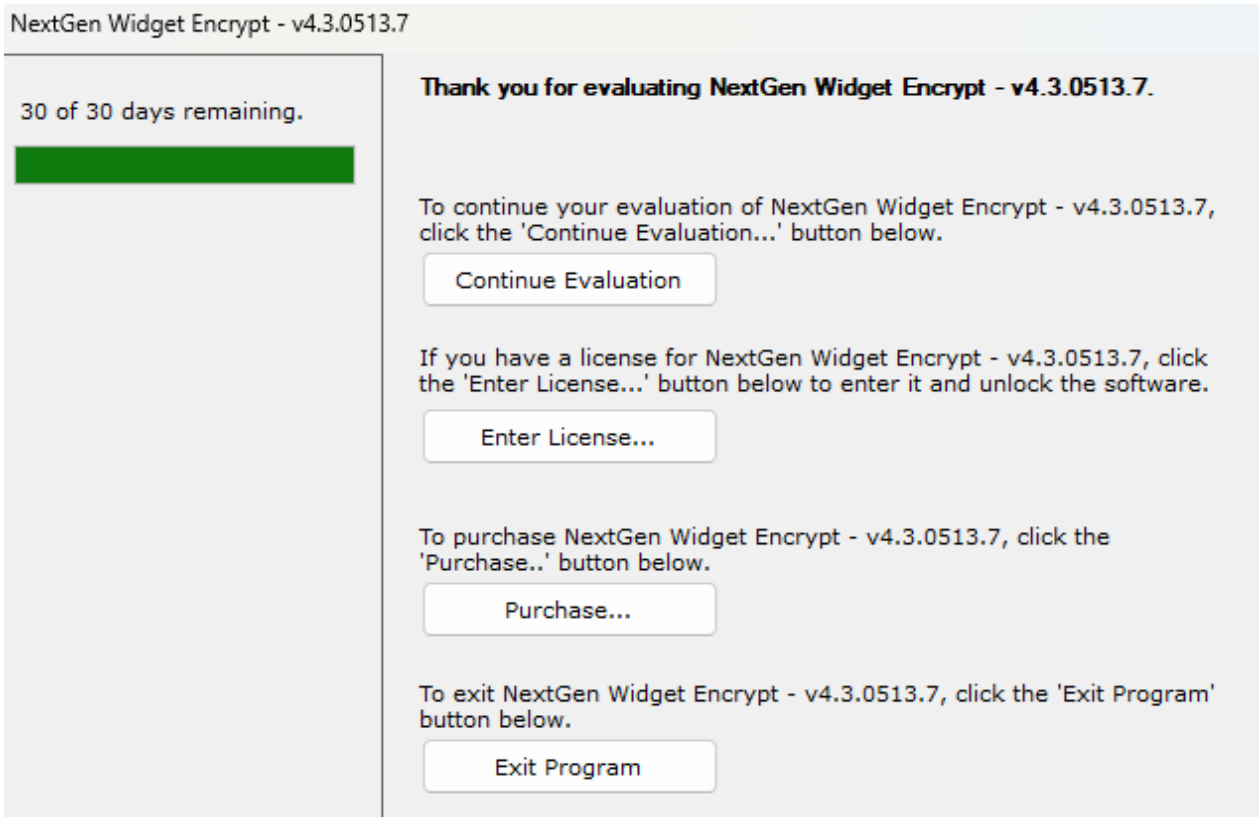
NextGen Widget Encrypt installs in the selected directory, click Finish and you're done.



Just double-click on shortcut on the desktop and the evaluation will pop up.



Just double-click on shortcut on the desktop and the evaluation will pop up with 30 Day Evaluation .



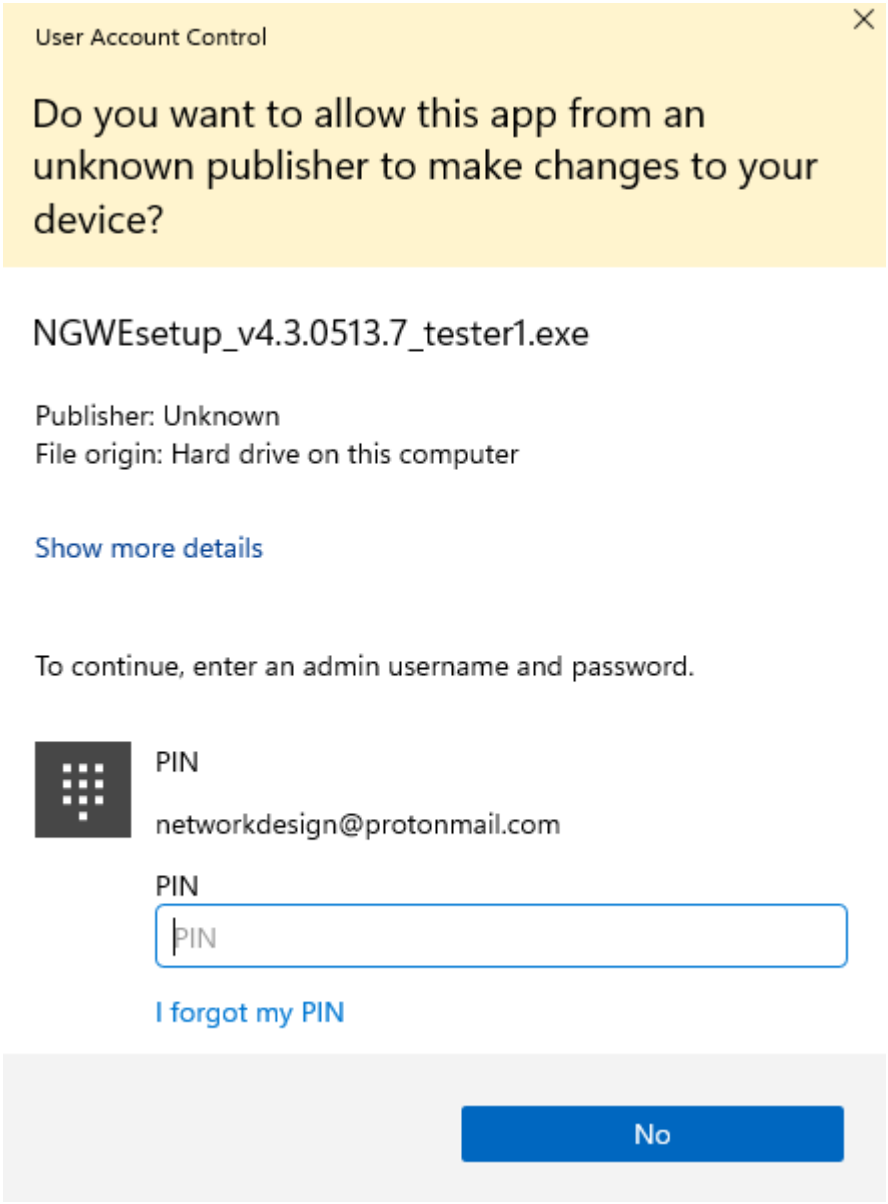
Restricted User Setup Instructions

When the "Current User" is selected and the user account is restricted (non-administrator) the shortcuts are assigned to administrator account because it is technically the currect user. Reason being is you have to receive authorization from the administrator account in order to install programs.

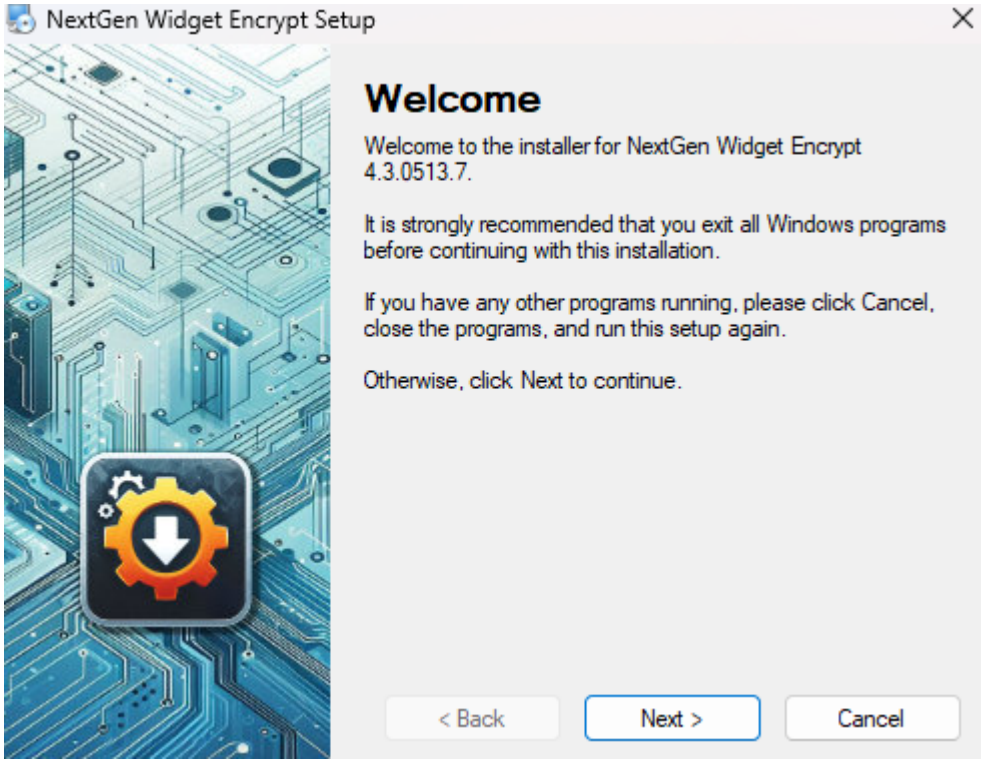
You have two options. One option is to change the restricted account permissions to administrative permissions and then install the program. When done, just change it back which is the easier way to go or option two.

Here's what you can do for option two:

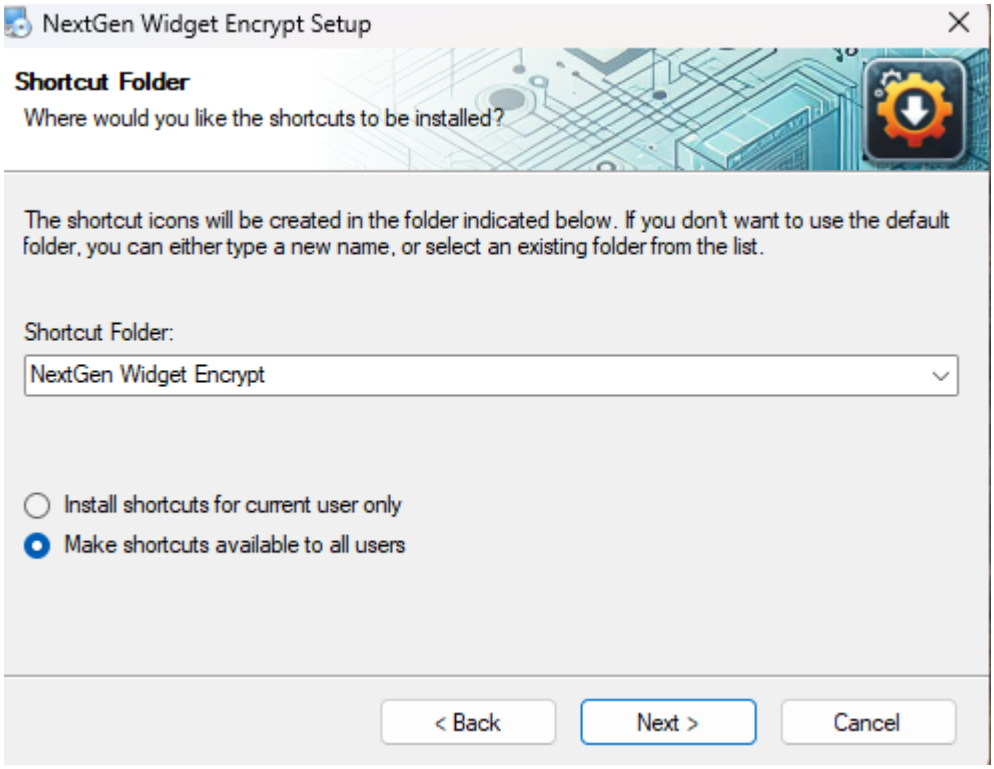
Double-click on the setup executable and then you will see the User Account Control (UAC) and the administrative password will be required.



Once you have entered the administrative password a welcome screen will pop up.



Cleck "Next>", agreed to the license agreement then click Next>. Enter a name and company if applicable and then click Next>. Choose the directory to install or leave as the default. Now, "Make shortcut available to all users". This is best left at this setting sense the administrator account is technically the one that is installing this software. If you choose "Install shortcuts for current user only" then the shortcut and Start Menu will only be installed for the administrator as well as the uninstall shortcut.



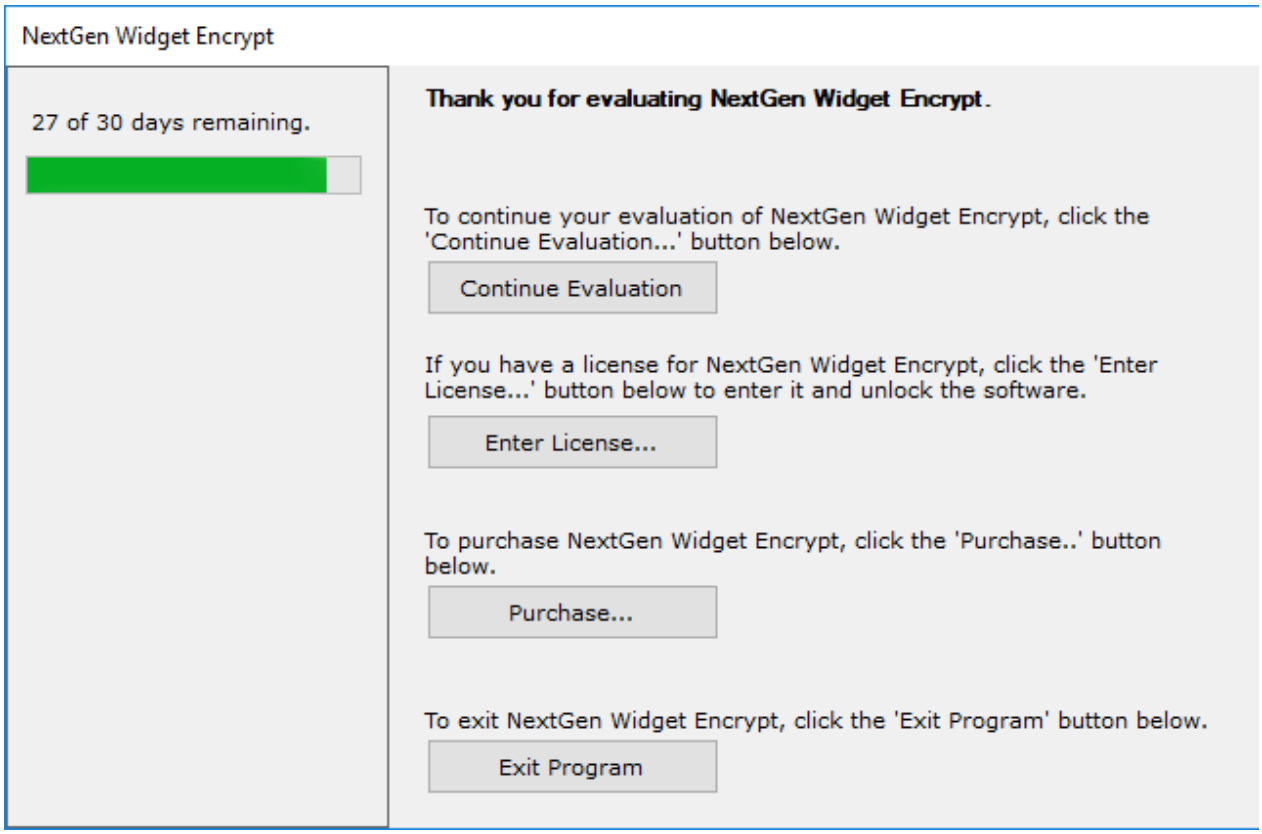
So, let's stick with "Make shortcuts available to all users", Next>, Next> the program installs and Finish.

Even though the application would be installed for all users. Each user has their own Key Store which is placed in "C:\Users\[YourUserName]\AppData\Roaming" folder.

Evaluation

The evaluation is a 30 day evaluation with the only restrictions being that the generated keys (Open PGP and X509) are limited to 30 days only. This includes the X509 generated certificates.

When you first launch the program an evaluation window will pop up. To evaluate the software simply press to "Continue Evaluation" button and the program will open right up. The "Enter License..." button is for those who purchase the software and need to enter in the permanent license they receive via email. If you decide to purchase the software simply click the "Purchase..." button which will take you to the website so that you may purchase the software. The "Exit Program" button closes everything down.



Front Door

The front door of the program is very easy to understand and simply provide you with a menu down the left side, subjects and top general options. A support link to our website contact page. The front door has a default username and password already set and needs to be changed. Once you create the name and password and press the okay button, the program will create the key store for you.

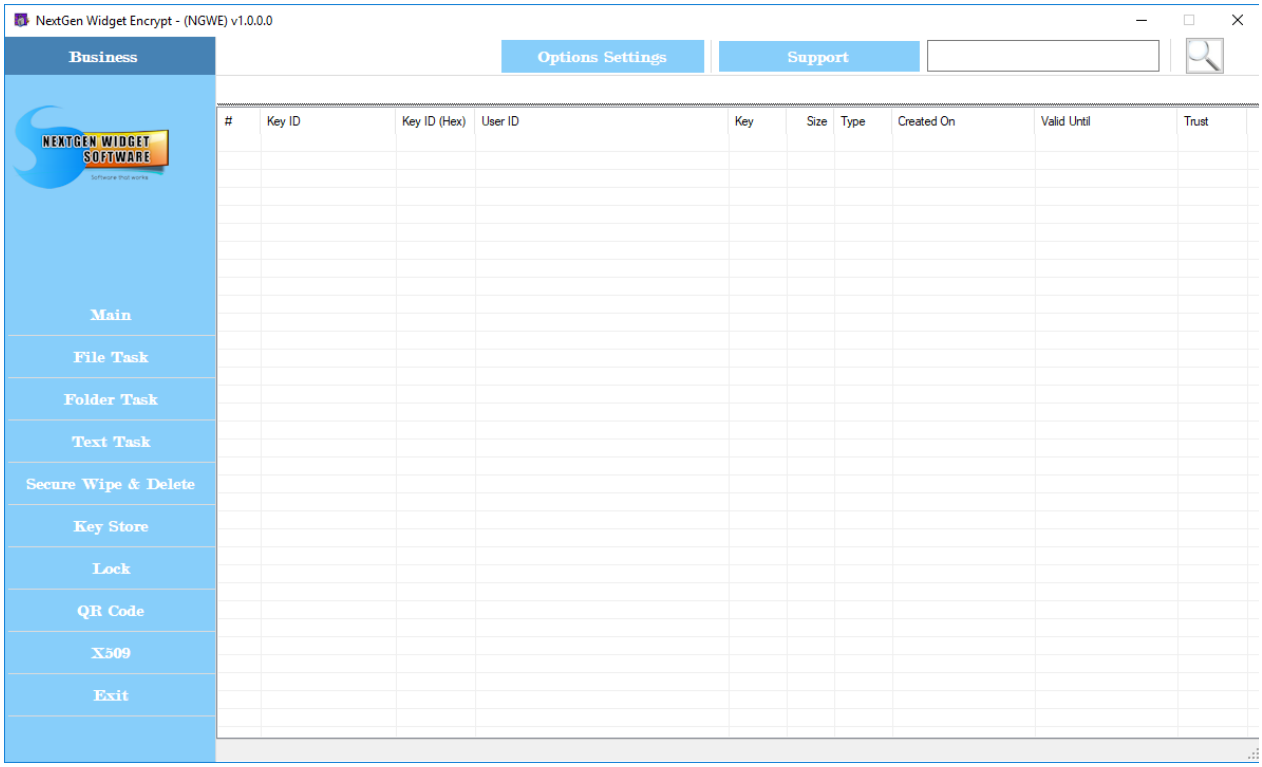
Note: *** It is recommended that you backup the Key Store and the location of where the Key Store is can be found, just click the optioned setting. You can also change the location of your Key Store file. ***

In this example I'm leaving the name the same and changing the password to something you should never do; test1234. Try to use long phrases instead of birthdates, children's names, the word password, anniversaries etc. Example: Jack and Jill went up the hill => J@ckAndJ1llW3ntUpTh3Hi##. Password and user ID are case-sensitive. With this super secure password, the strength indicator tells me that it is a weak password. If this is the case your password, that it suggested that you change it to something secure.

Note: *** If you lose your password or forget it, there is no recovery. Please secure your password and don't lose it. ***

Note: The program attempts to remember the location of your Key Store. So, it's a good idea if you want to change the location that you change it through options otherwise you may be locked out of your program and have to put the Key Store back in the original location so that you can once again access the Key Store.

Now, the new key store is generated and NextGen Widget Encrypt is open for business.

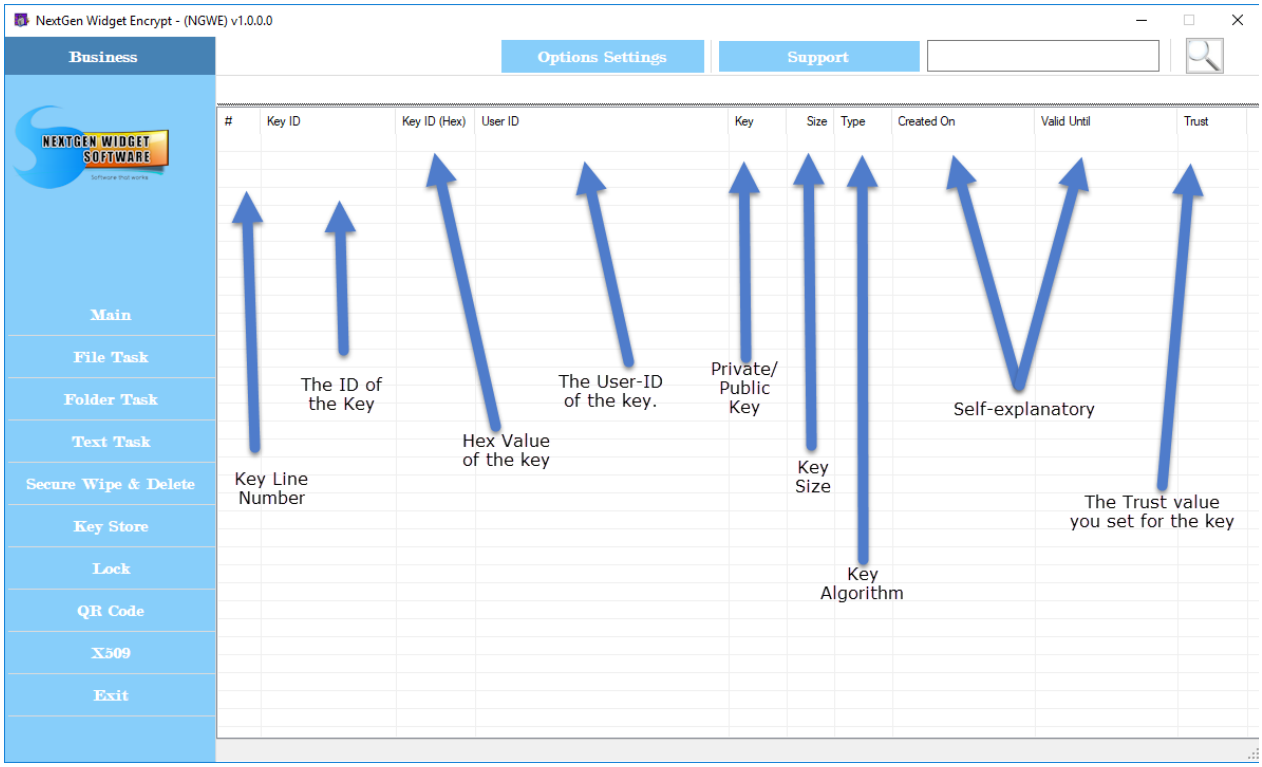


Look at the Key Store

The key store is very easy to navigate and simply has 10 columns the first column being the line number which is just that. It generates the number for each line so that you can easily see how many keys you have. The key ID is unique to each key as well as the hex ID. The user ID is something that primarily set when you generate a new OpenPGP key. The

exception to this is when you import a digital certificate. Digital certificate (X.509) user IDs are the (CN).

Almost everything is operated from the Key Store so that you become very familiar with it because it is the main functioning area.



[Manage Key Store]

Main

[PGP Key Revoke]
Here you can revoke ASC PGP keys both files are needed, the private key and the public key.

[Compose a Key]
Generate open PGP keys.

[Import]
Import OpenPGP keys for private, public and key pair in ASCII or from a in .asc, .gpg, .pkr or skr files..

[Export Public Key]
Export OpenPGP Public key in ASCII .pgp, .asc and .gpg.

Export Private Key
Export OpenPGP Private key in ASCII .pgp, .asc and .gpg.

Export Key Pair
Export OpenPGP key pair in ASCII .pkr, and .skr.

Trash Key
Left click on the selected key, press the delete button or use the right-click and delete.

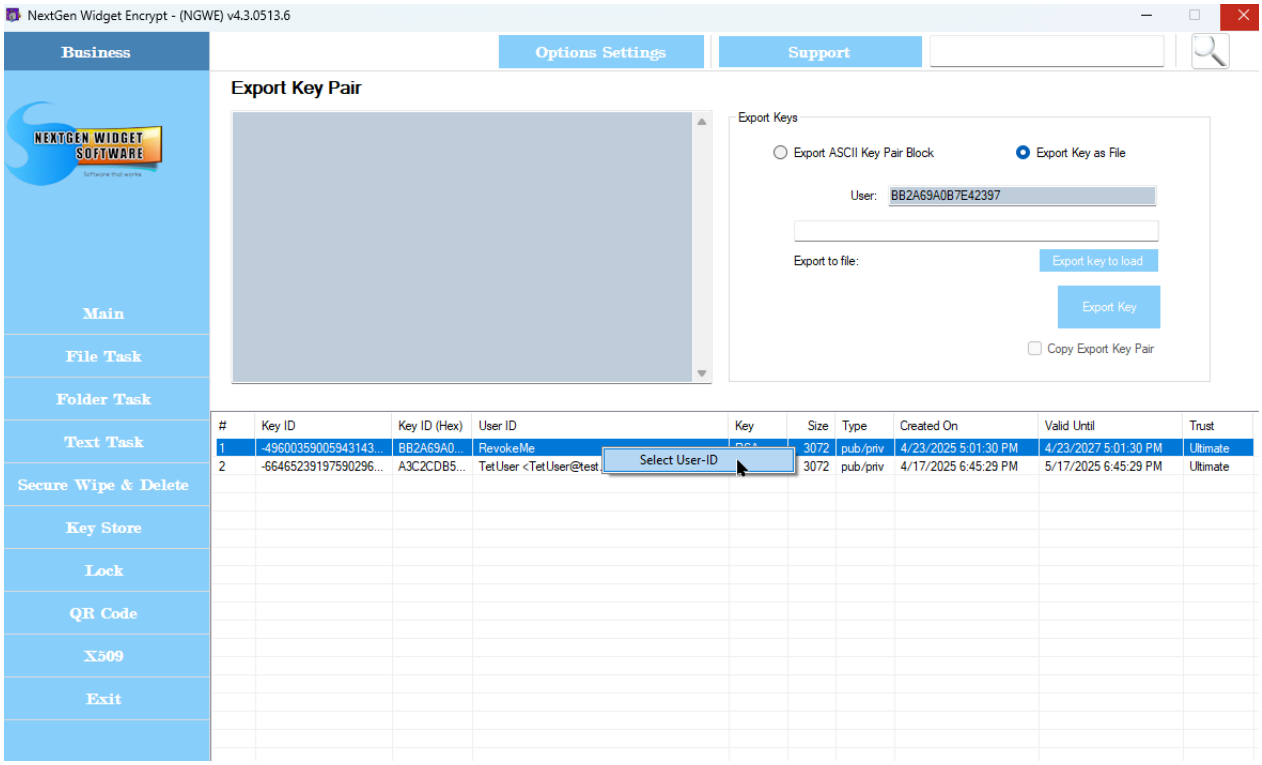
Properties
View properties such a key type, size revoked or not, expiration date and if the key has subkeys.

Change Password
Change passwords for private keys and also the Key Store.

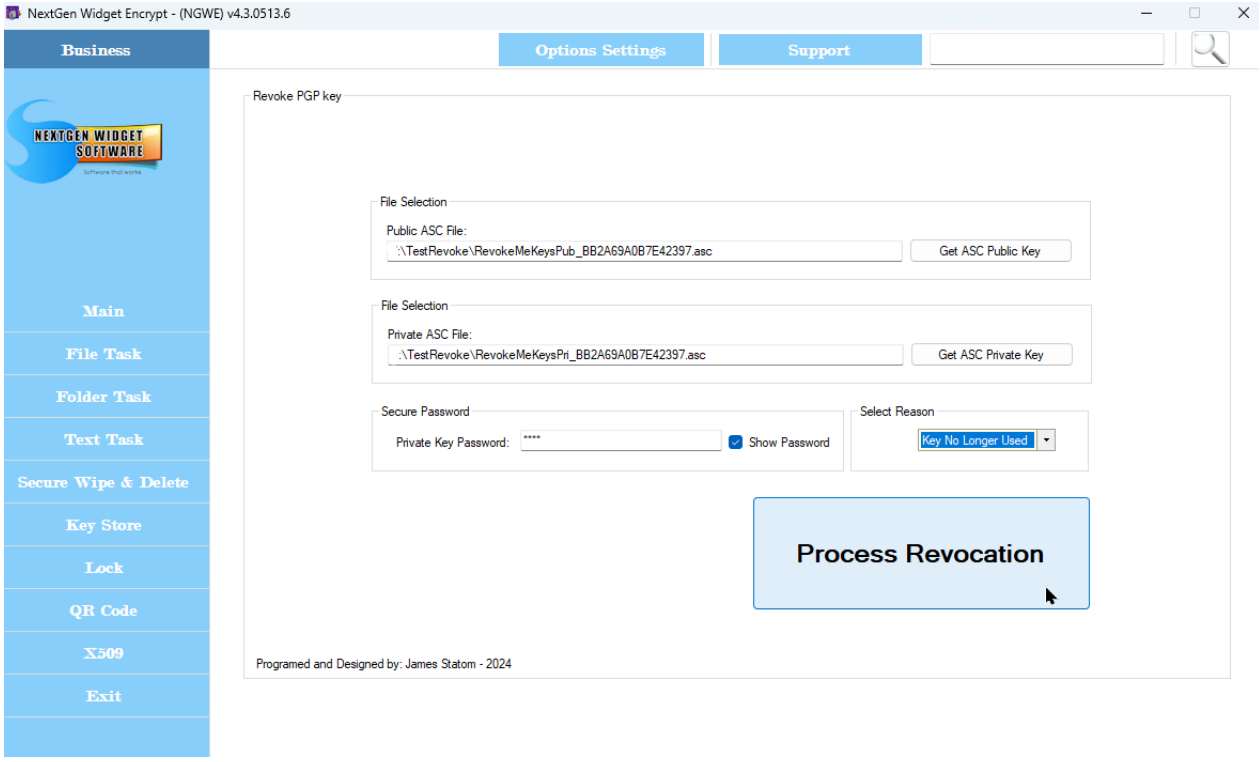
PGP Key Revoke

The OpenPGP key revocation is the process of appending a special signature to an OpenPGP public key that marks it as not usable any more.

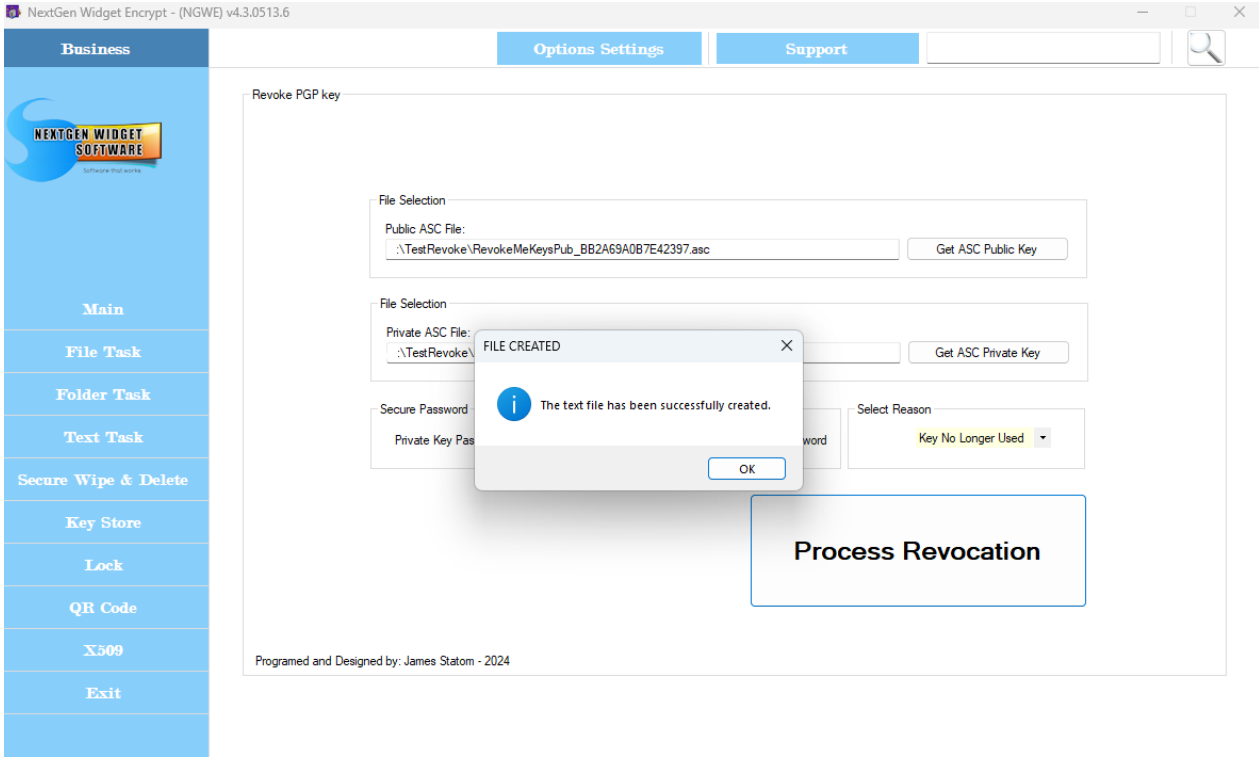
Here we can directly revoke a public key. First off we will need to create the public and private key files because this is not done inside the Key Store. So, if the keys are in the key store just export them to a.asc file.



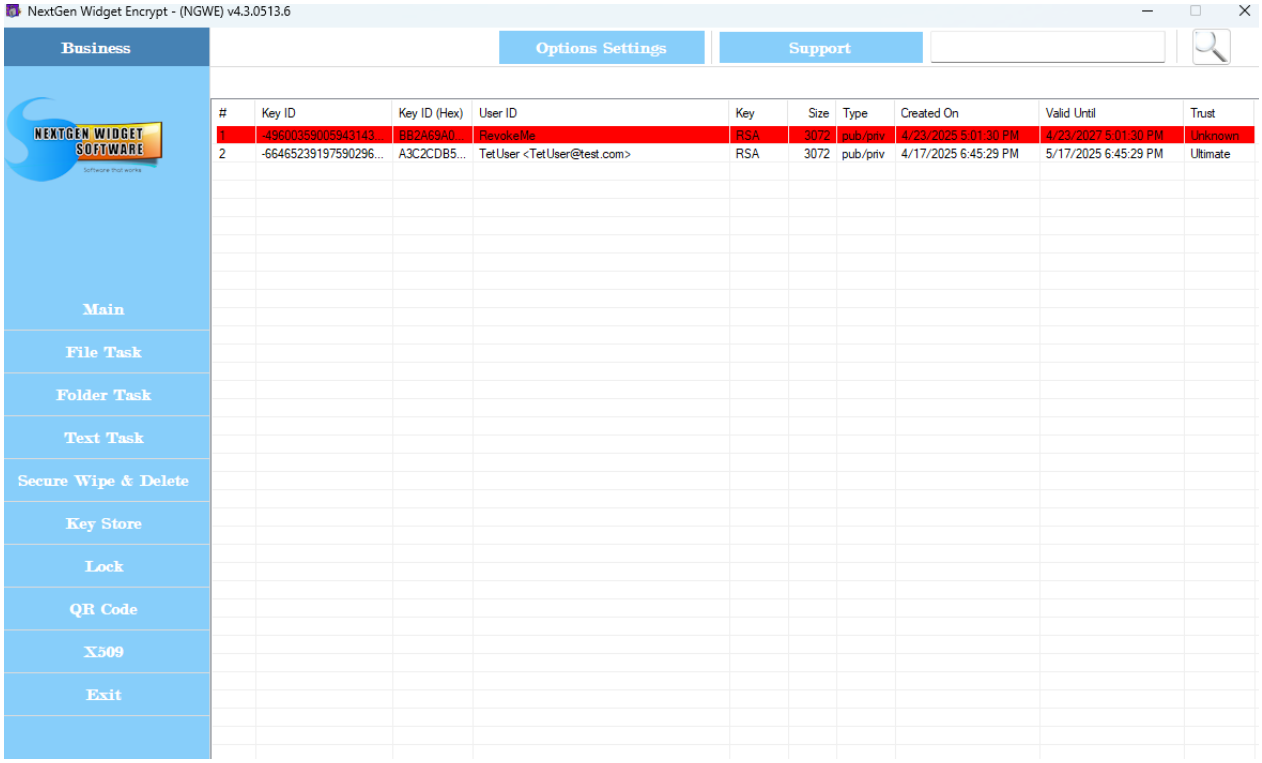
Now, locate the public key and private key. You will need to know the private key password and then select a reason.



Once you click the Process Revokes and button a save dialog box will pop up with the word "Revoked-" and the key fingerprint in eight text file. If you wish to install this revoked public-key in your key store just change the extension to .asc and import it.



Once you import the key the key located in the key store line will turn red showing that the indicated key has been revoked. If you have that key on a PGP key server, just submit the key to that server and the installed key will be revoked.

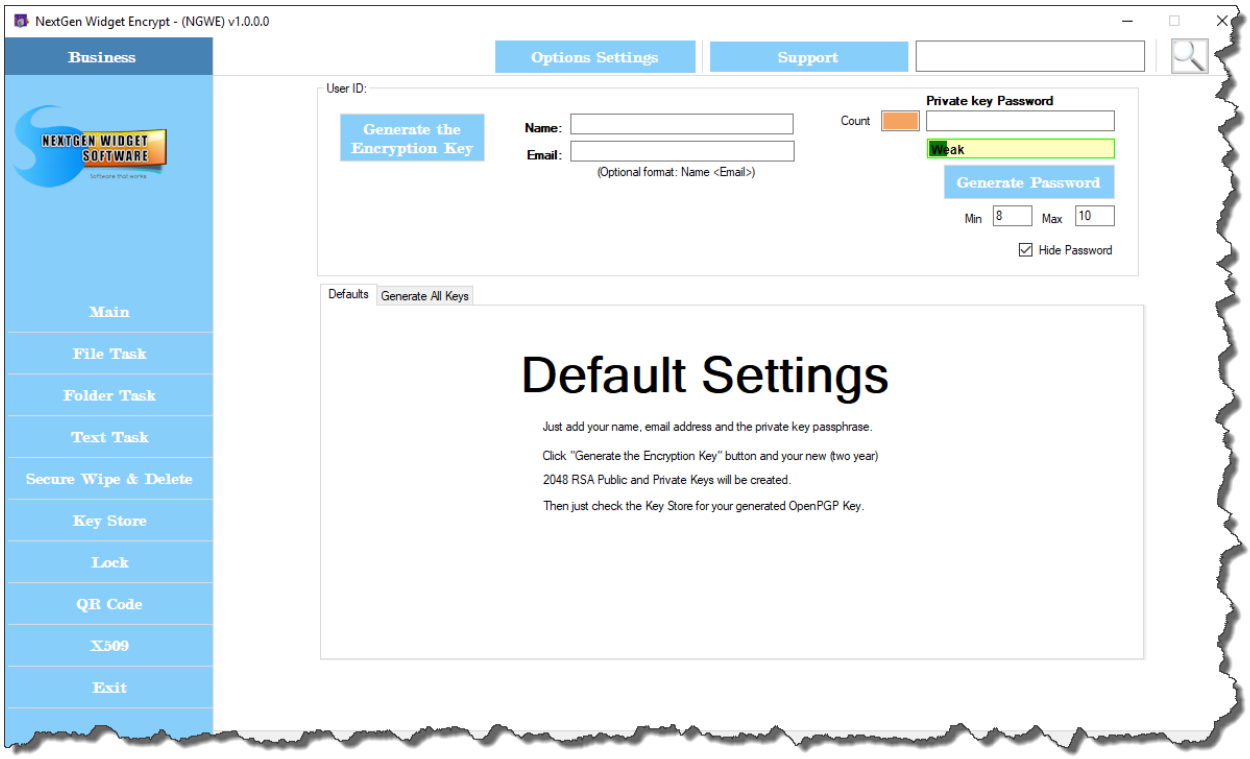


Compose a Key

The first things we need to do after entering our password and letting the program create the key store, is to compose a key. This is a relatively simple and easy process just by clicking "Main" on the menu and click "Compose key".

Now, for the composing of a key you can simply utilize the default settings and only have to enter in a user name and optional email address along with a secure password. If you don't have a secure password in generate one simply by clicking the "Generate Password" button.

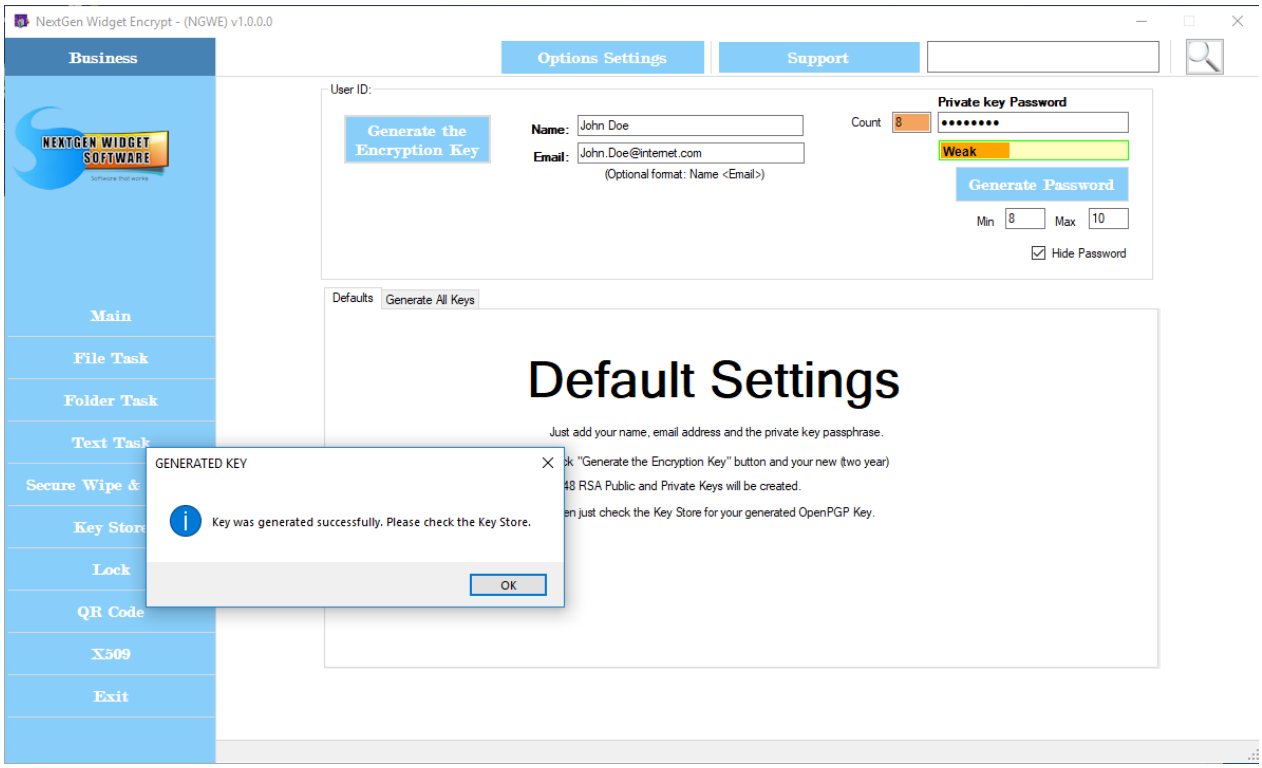

NextGen Widget Encrypt - (NGWE) v1.0.0.0
Business
NEXTGEN WIDGET SOFTWARE
Software that works
#
Key ID
Key
Main
HTTP Keyserver
File Task
Compose Key
Folder Task
Import
Text Task
Export Public Key
Secure Wipe & Delete
Export Private Key
Key Store
Export Key Pair
Lock
Trash Key
QR Code
Properties
X509
Change Password
Exit



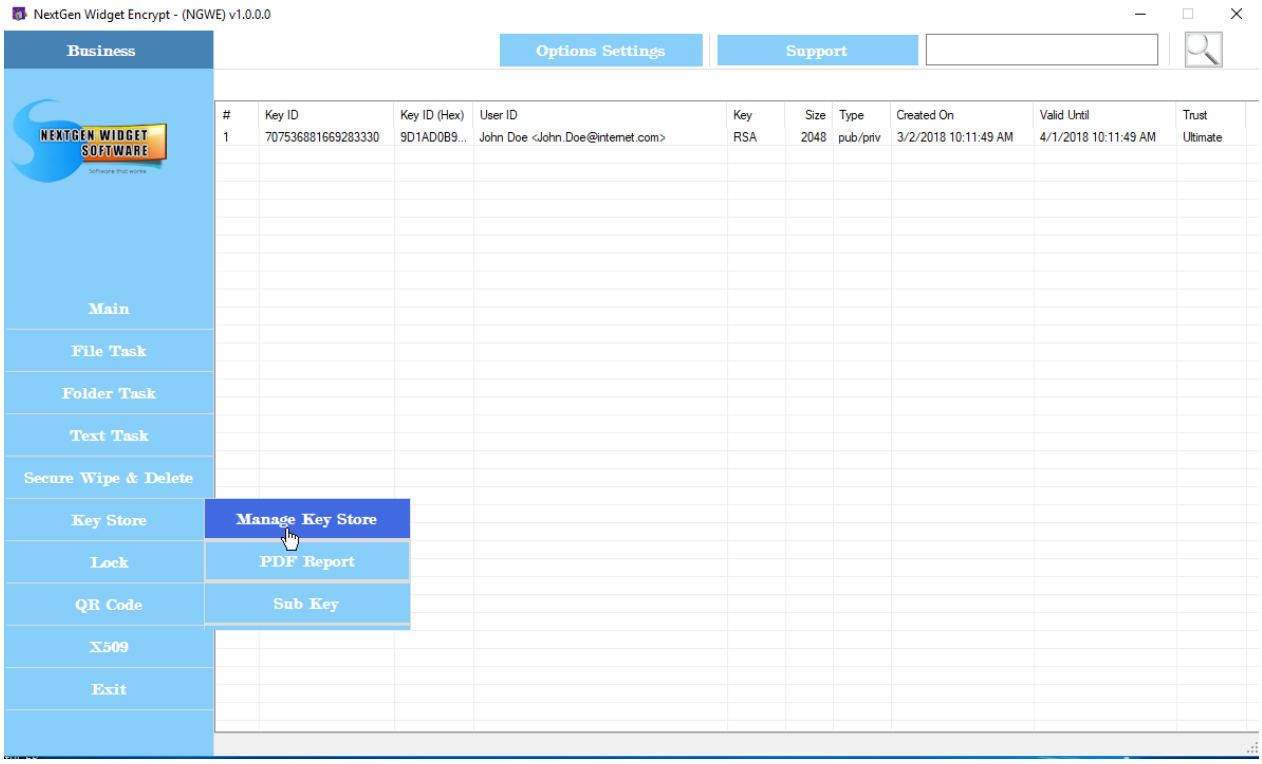
Next, I'm going to use the default settings so I only have to enter a username but I want this to be associated with my email address so I'm entering an example email address. Then, I'm entering the password for my private key. This password should be Securely secret and should be hard to guess. The best type of passwords are those that are not associated with things that are common to use such as your birthday, dogs name, children's name etc. Further, they should not be associated with dictionary terms and the best type of password is really called a passphrase.

Passphrases are easier to remember because they are a long phrase with characters changed create a secure and complexed password.

Once you have entered in these fields, simply click the "Generate the Encryption Key button and you will get a pop-up that tells you that generating a key can take a little bit of time be patient. Click the okay button and your key will be generated.

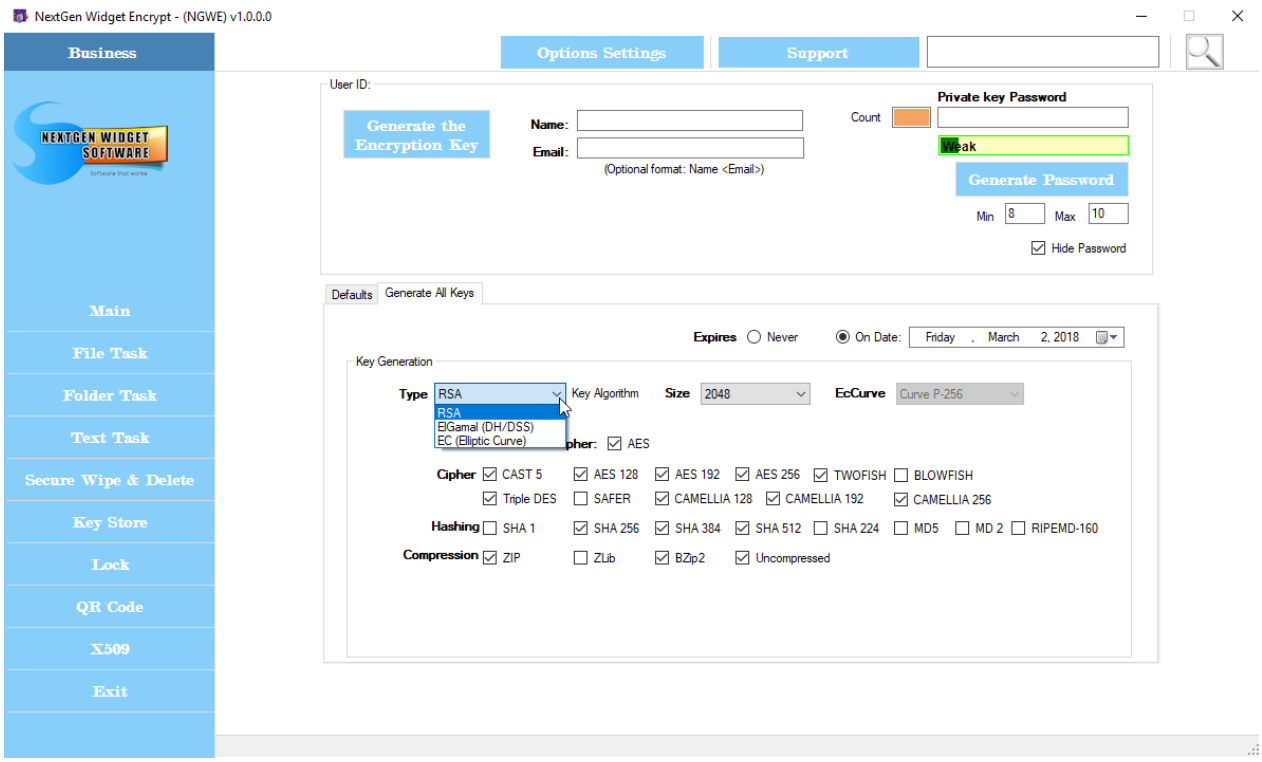


Now we need to verify that the key is located in the key store. To do this, simply click the "Key Store" menu button and then the click "Manage Key Store" button. As you can see from the below image, the key was generated successfully and is the first key located in the key store. Every key that's generated by you is considered an ultimate trust key. Simply meaning that you trust this key entirely to not be fraudulent or made by some hacker trying to steal someone's identity.

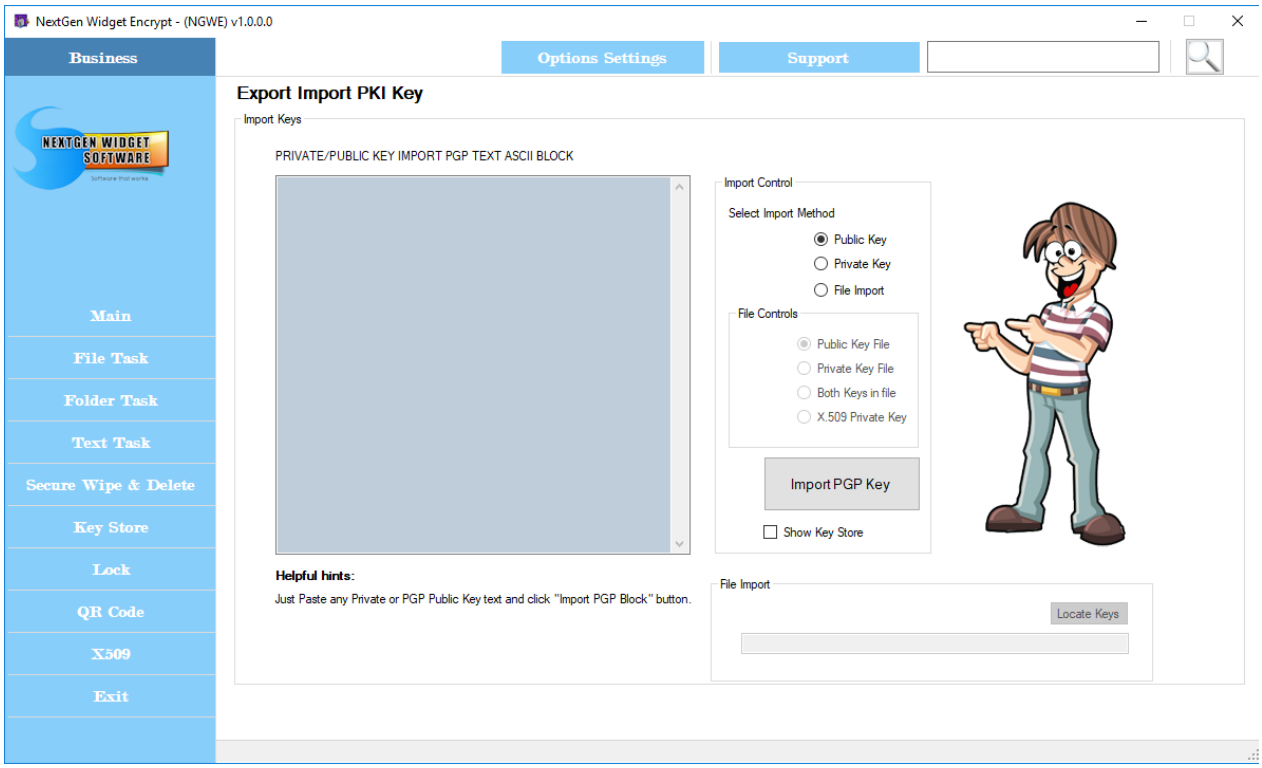


Each key is only generated for 30 days in the evaluation version. The paid version generates a two-year default key. If you wish to have something other then that, simply click

the "Generate All Keys" tab and make your choices accordingly. The program offers three key type generations which are RSA, ElGamal and Elliptic Curve.

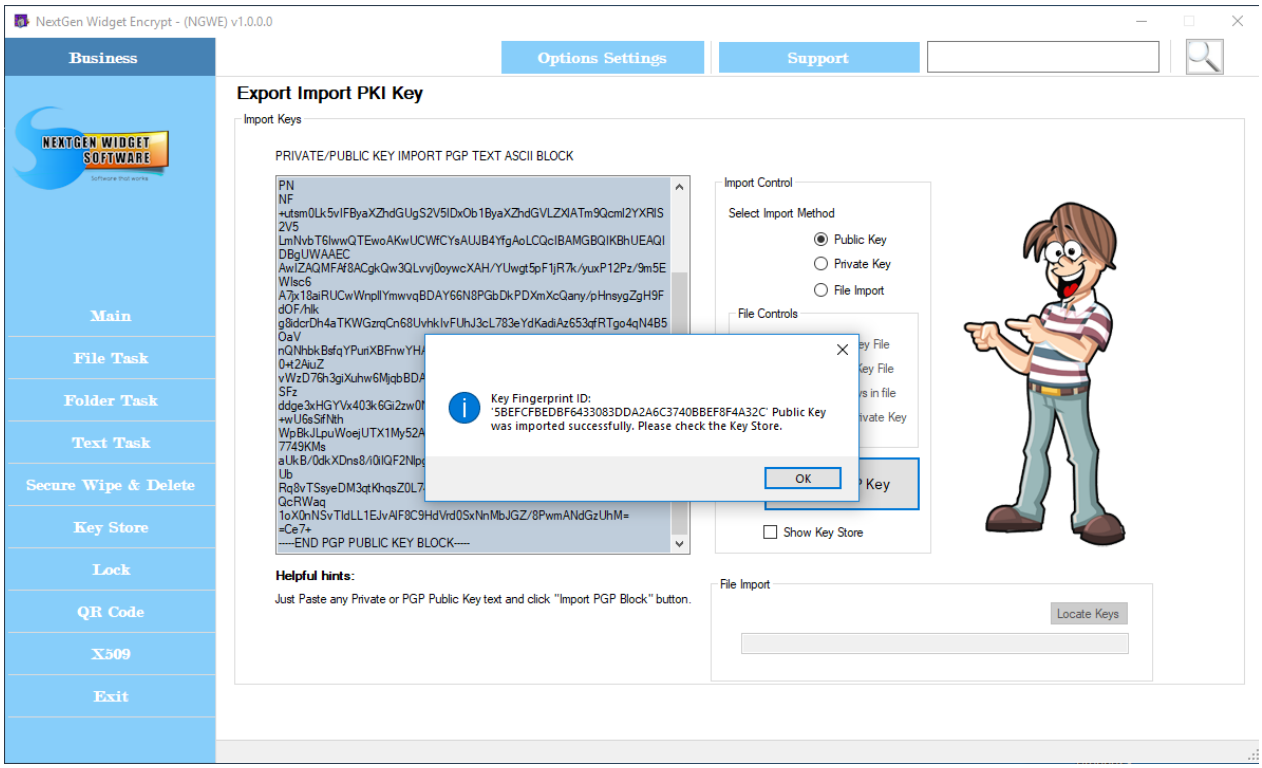


Import

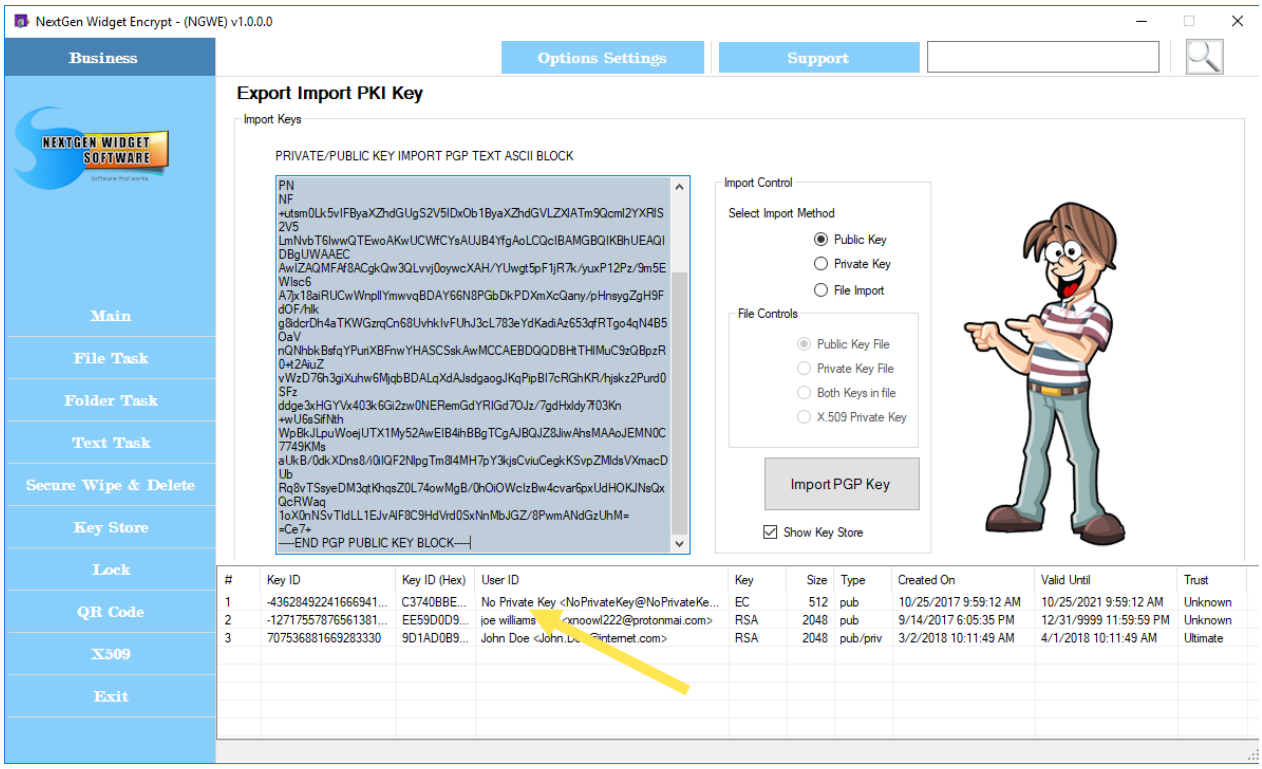


The import section imports OpenPGP keys both public and private. It also imports X.509 certificates, but for the most part OpenPGP isn't really designed for X.509. To import an ASCII text for example, just simply paste the text into the text box and click the "Import PGP

Key" button. Next you will see an acknowledgment and the fingerprint ID.



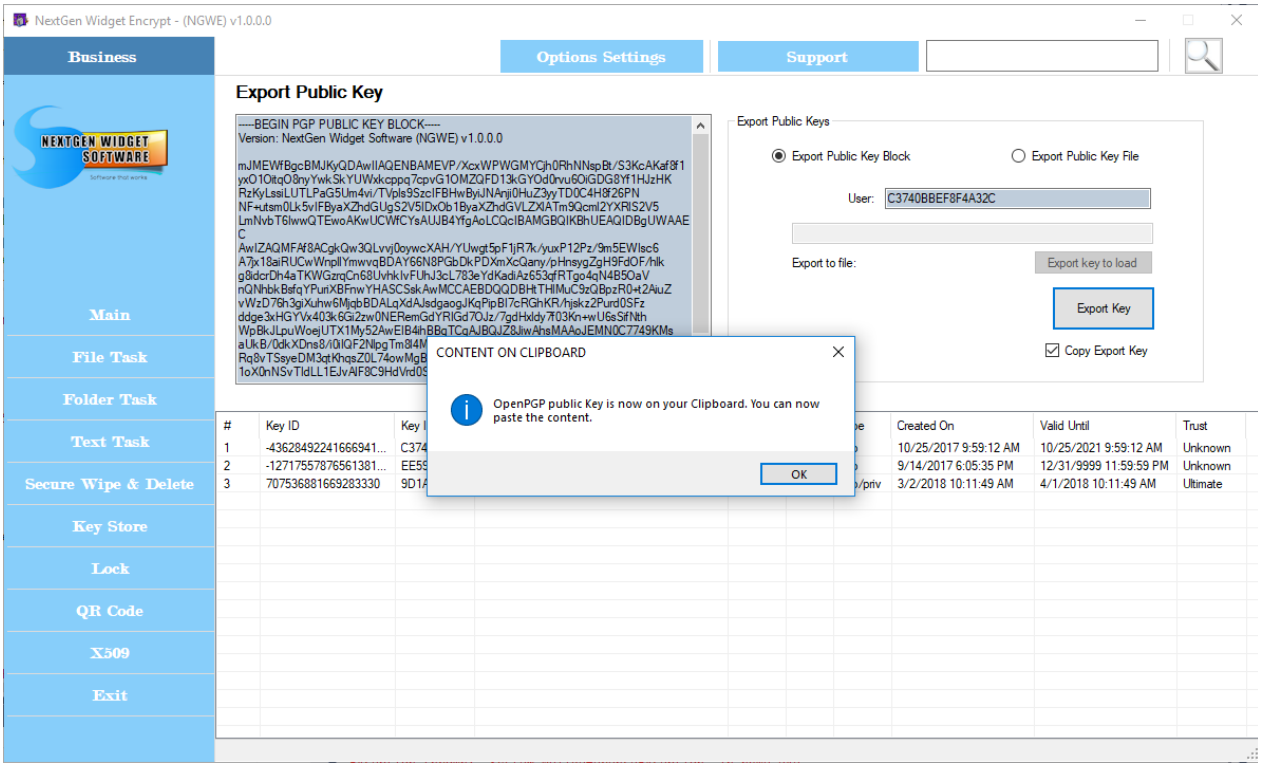
Importing a private key text works the exact same way as the public key. However, when importing a file you need to click on the file import radio button. This will enable all of the functions so that you can import a file. Select which key you want to import; public, private, both or X509 certificate. Click the locate keys button and import. Check the key store for the key and you're done.



Export Public Key

Exporting a public key as a text file is another simple process. Here you'll be able to export a public key either as a OpenPGP block or a file. Either way, you select the key by right clicking on the desired key from the Key Store and choosing "Select User-ID". You'll notice that the hex code of the key is placed in the user text area. This example shows "C3740BEF8F4A32C".Simply click the "Export Key" button and the key is exported to the OpenPGP block.

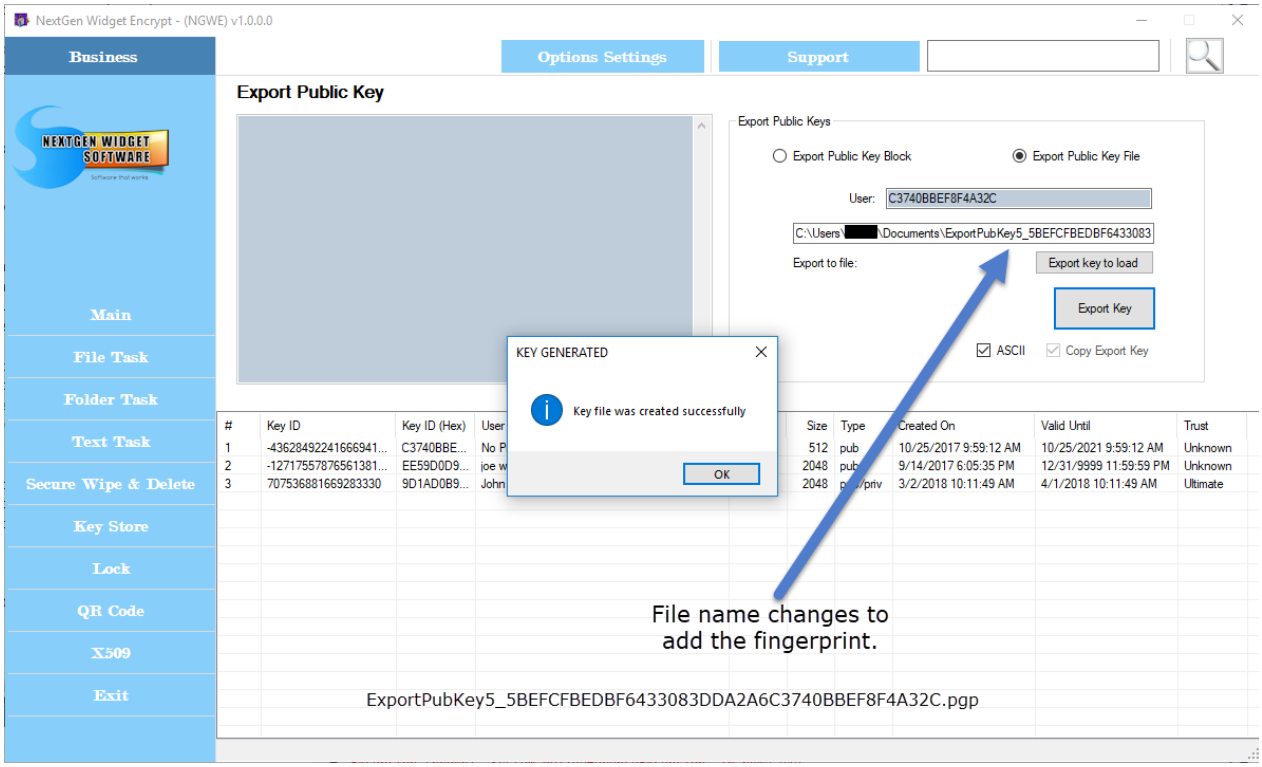
If you click the "Copy Export Key and ASCII" (clicked by default) checkbox before exporting the key, the public key will be copied to the clipboard.



To export the public key as a file simply click the "Export Public Key file"radio button, right clicking on the desired key from the Key Store and choosing "Select User-ID", click "Export key to load" and and the file name you wish to call it and save it to the desired location. In this example I'm calling the exported public key "ExportPubKey5" and saving it to my documents directory. If you do not click the "ASCII" checkbox, the output will be in binary.

Once you click the "Export Key" button the public key file is generated. When saving the file you have three file extensions in which to choose from; pgp, asc and gpg. If you click the "ASCII" checkbox before saving the file name, the extension will then be .asc. Otherwise, the extension by default will be .pgp but the file itself will be ASCII armor. Once the "Export Key" button is clicked and the file generated, the file name changes with an inserted fingerprint of the public key.

Example:
"ExportPubKey5.pgp" becomes
"ExportPubKey5_5BEFCFBEDBF6433083DDA2A6C3740BBEF8F4A32C.pgp".



Export Private Key

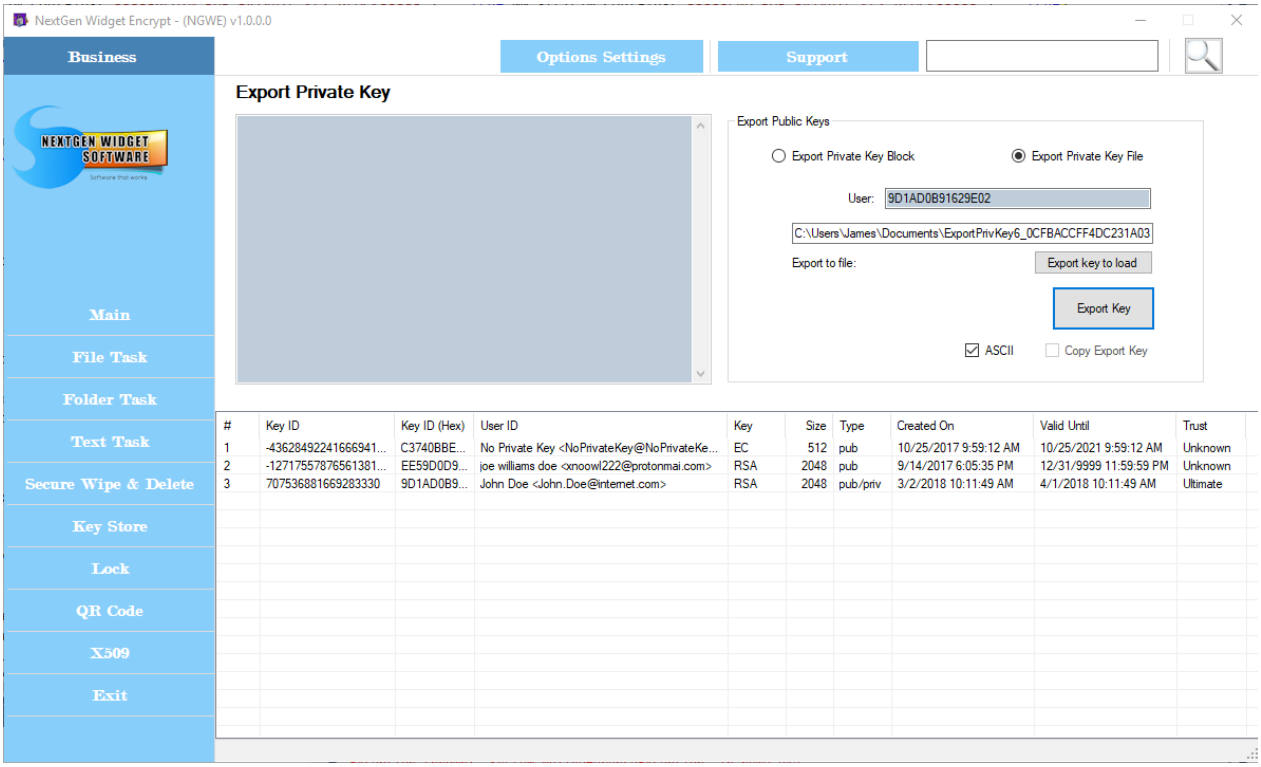
Exporting a private key woeks the same way you would export the public key. Here you'll be able to export a private key either as a OpenPGP block or a file. Either way, you select the key by right clicking on the desired key from the Key Store and choosing "Select User-ID". You'll notice that the hex code of the key is placed in the user text area. Simply click the "Export Key" button and the key is exported to the export text area.

If you click the "Copy Export Key" (clicked by default) checkbox before exporting the key, the private key will be copied to the clipboard.

To export the private key as a file simply click the "Export Public Key file"radio button, right clicking on the desired key from the Key Store and choosing "Select User-ID", click "Export key to load" and and the file name you wish to call it and save it to the desired location. In this example I'm calling the exported public key "ExportPrivKey5" and saving it to my documents directory. If you do not click the "ASCII" checkbox, the output will be in binary.

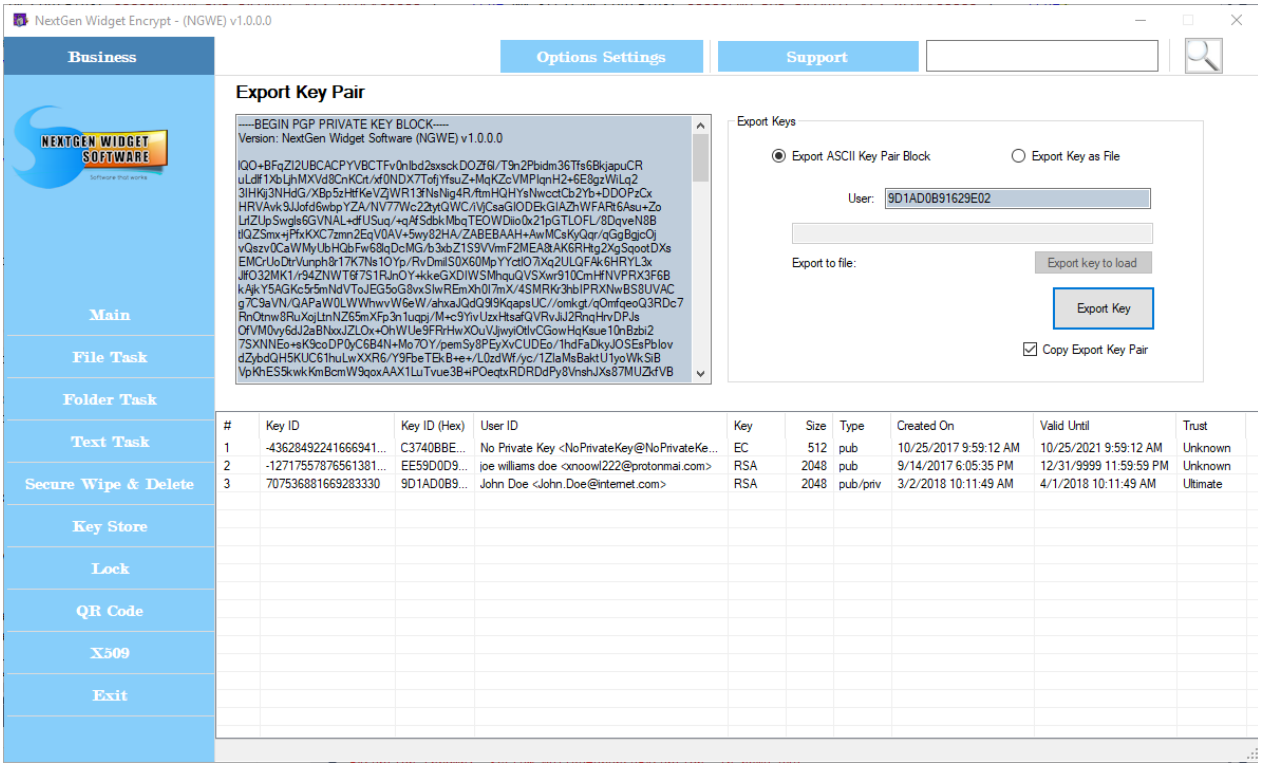
Once you click the "Export Key" button the private key file is generated. When saving the file you have three file extensions in which to choose from; pgp, asc and gpg. If you click the "ASCII" checkbox before saving the file name, the extension will then be .asc. Otherwise, the extension by default will be .pgp but the file itself will be ASCII armor. Once the "Export Key" button is clicked and the file generated, the file name changes with an inserted fingerprint of the public key.

Example:
ExportPrivKey6.pgp becomes
ExportPrivKey6_0CFBACCFF4DC231A03087A8509D1AD0B91629E02.pgp.



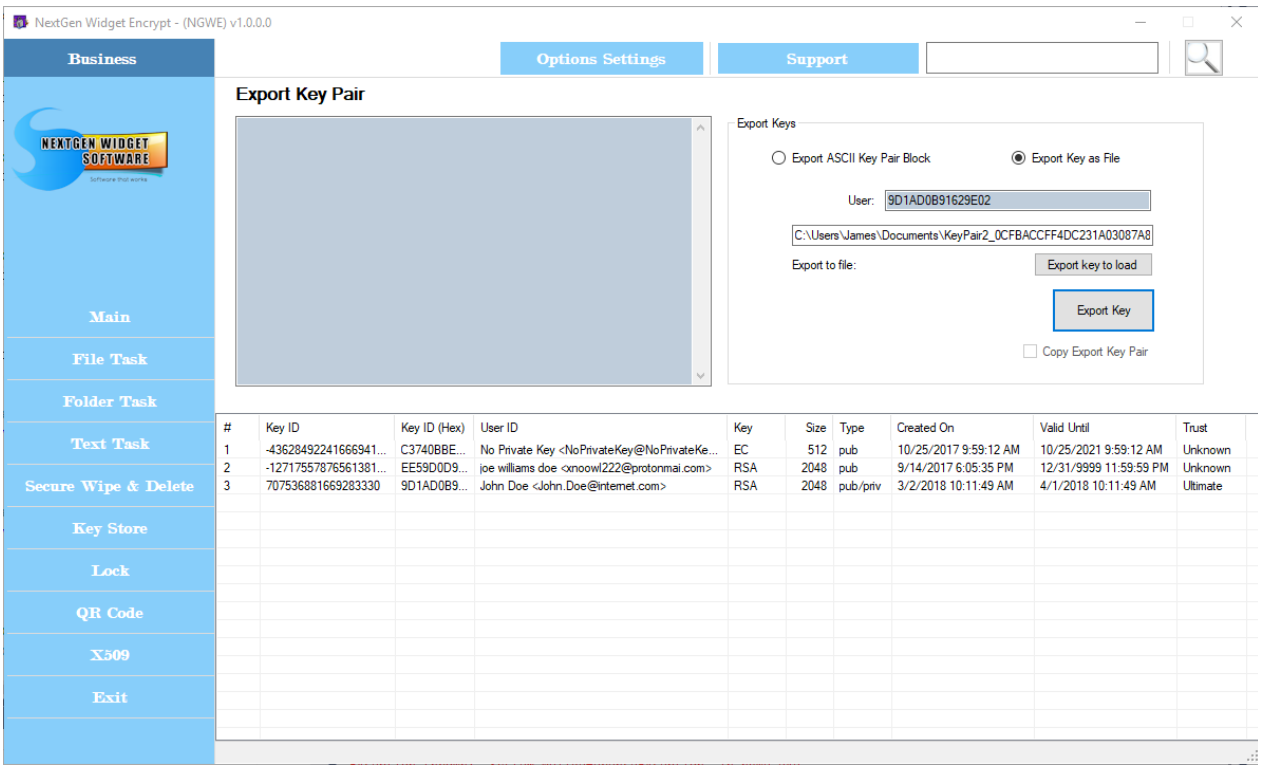
Export Key Pair

The process of exporting a key pair is exactly the same as you would for a public key or private key. Two export the key pair you must have both the private key and the public key located in the key store. Select "Export ASCII Key Pair Block", right-click and select "John Doe" in our example, then click "Export Key". Both the private and public key exported to the key pair Block.



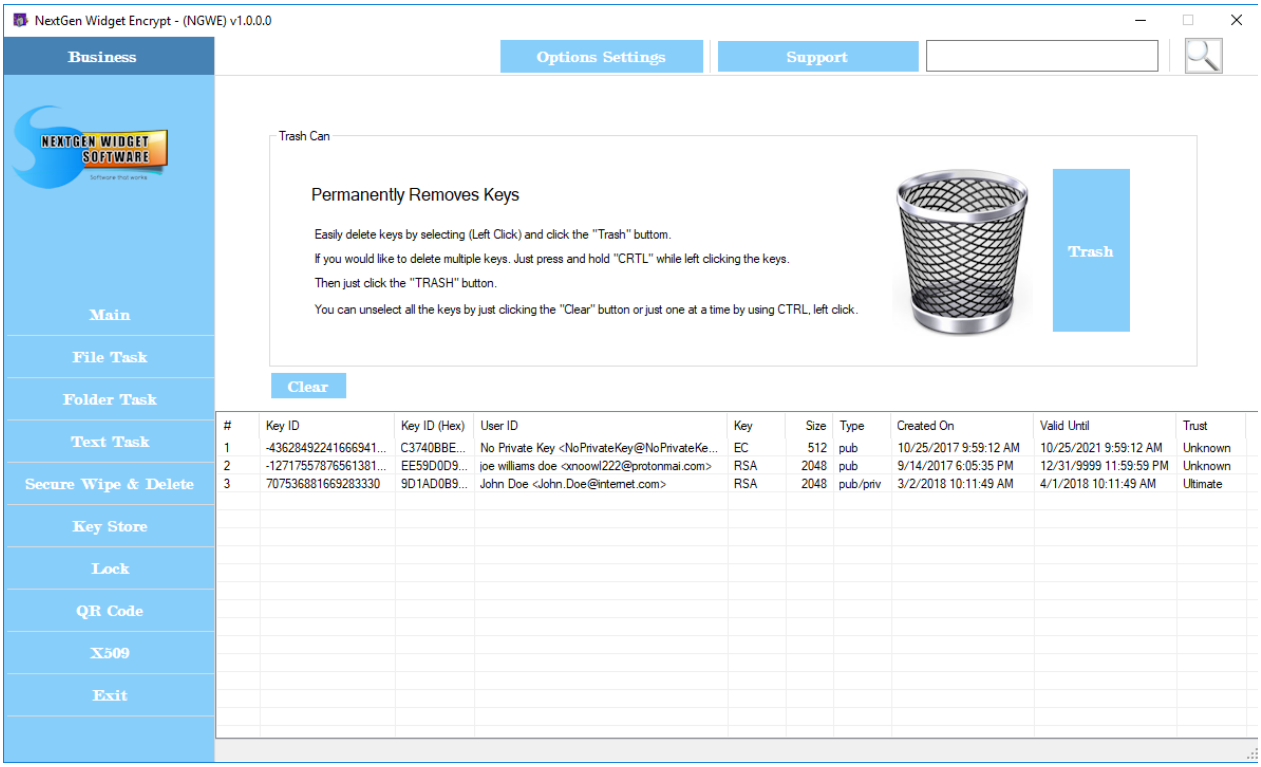
Exporting the key pair as a file is slightly different than exporting a private key or public key in a block. The only difference is that you are not able to select ASCII via a checkbox.

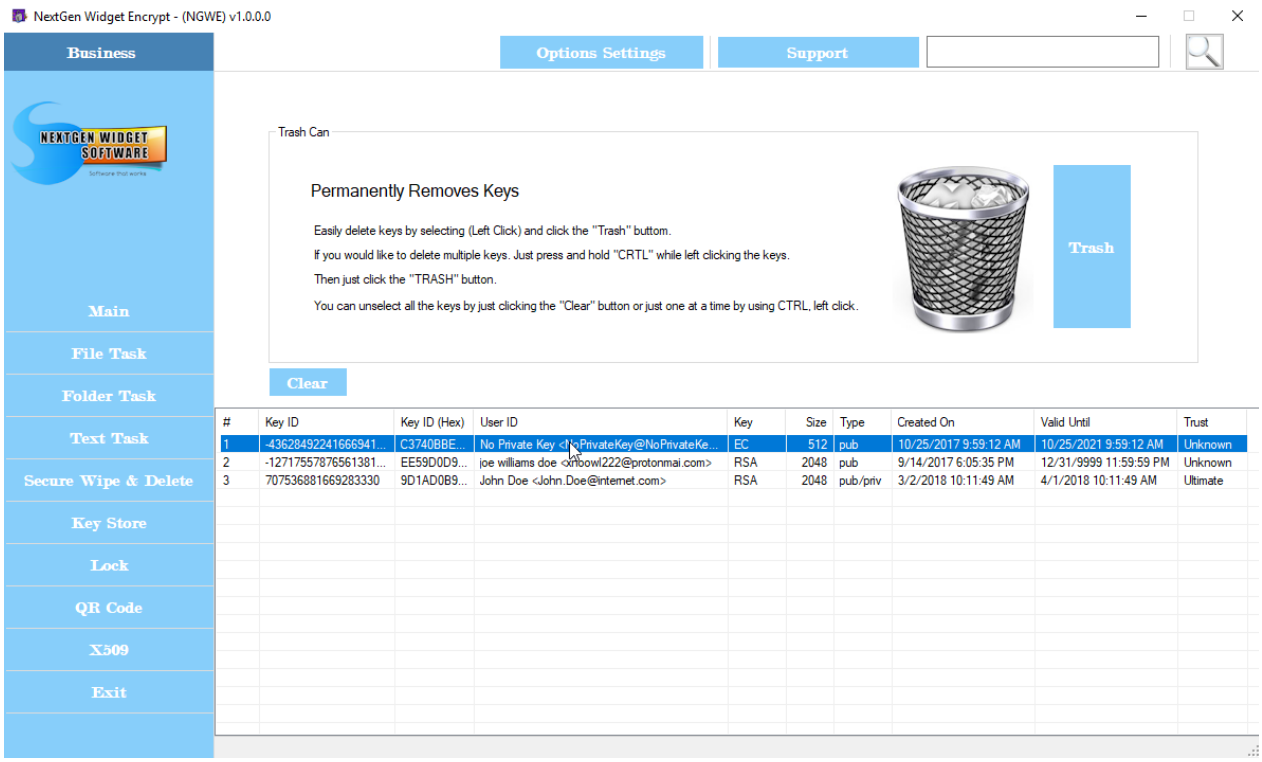
Instead, when you export the key via the "Export key to load" buttton, you are given the option to select a file type; .skr. .pkr or .asc. If you select the file extension (.asc), the output of the file will automatically be ASCII armor. The other two are exported as binary files.



Trash Key

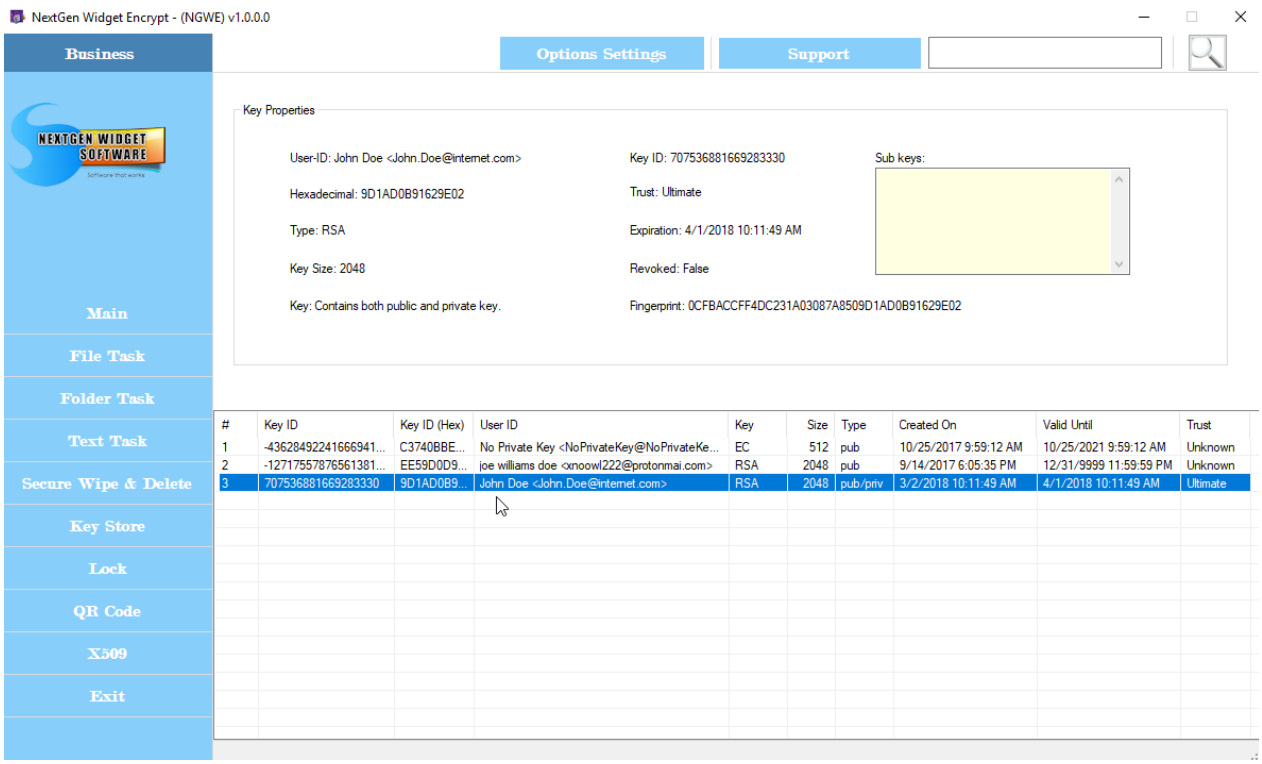
Removing keys couldn't be easier, all of the instructions are located right on the program page. However, in the Key Store you can just simply right-click on the key and select delete.





Properties

To see the properties of each key you simply click on the key and all of the details are instantly viewed.



Change Password

Change password area is for the changing the Key Store and Private Key password. You can alse change the "User ID" of keys.

[Change Private Key Password]

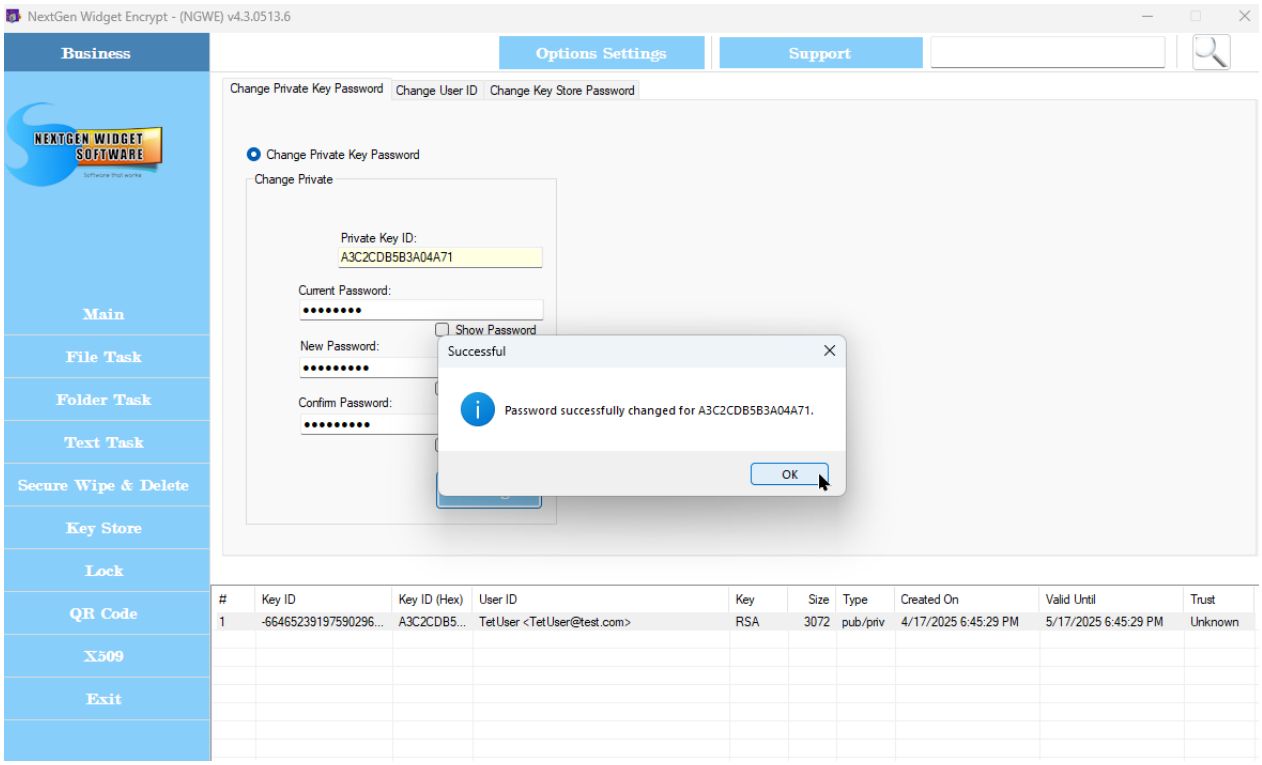
[Change Private User-ID]

[Change User ID]

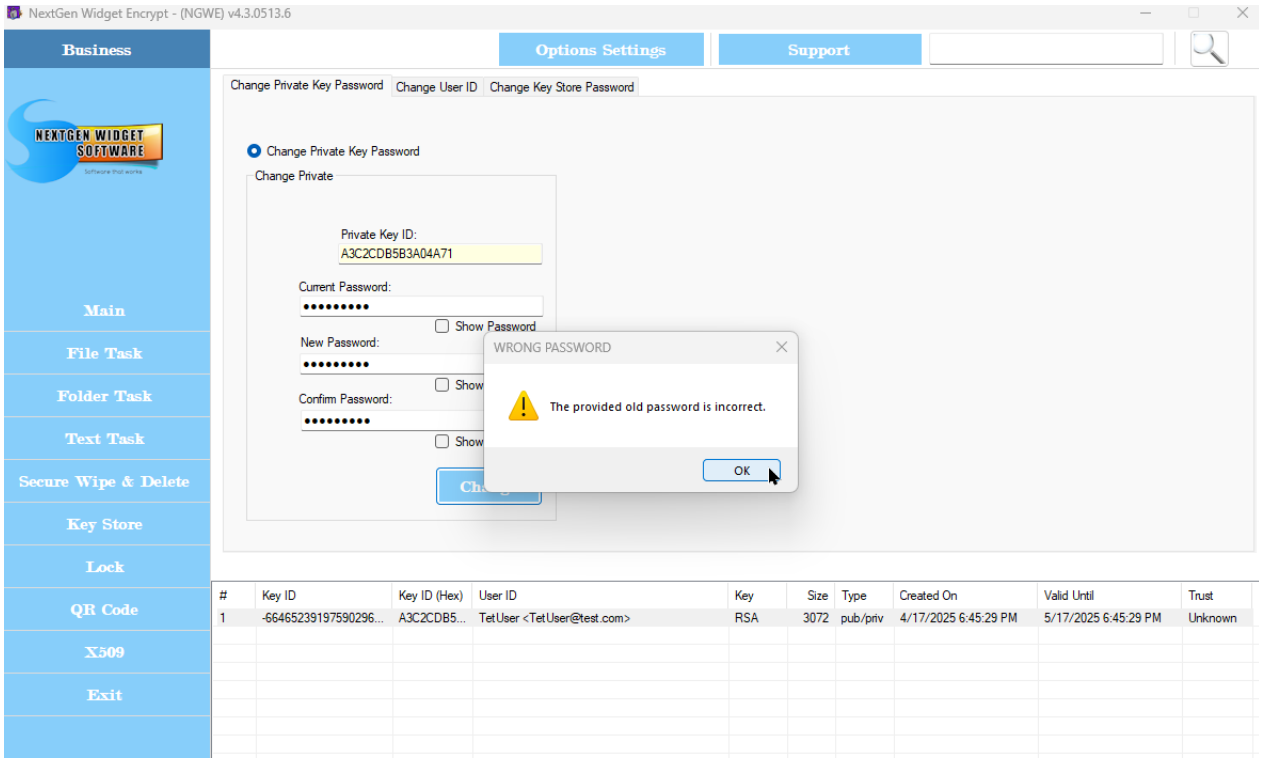
[Change Key Store Password]

Change Private Key Password

Changing a private key password is very simple. Simply right-click on the key you wish to change the private key password for. The private key must be located in the Key Store. Enter the current password, the new password and confirm the new password. Just click "Change" button and you're all done.

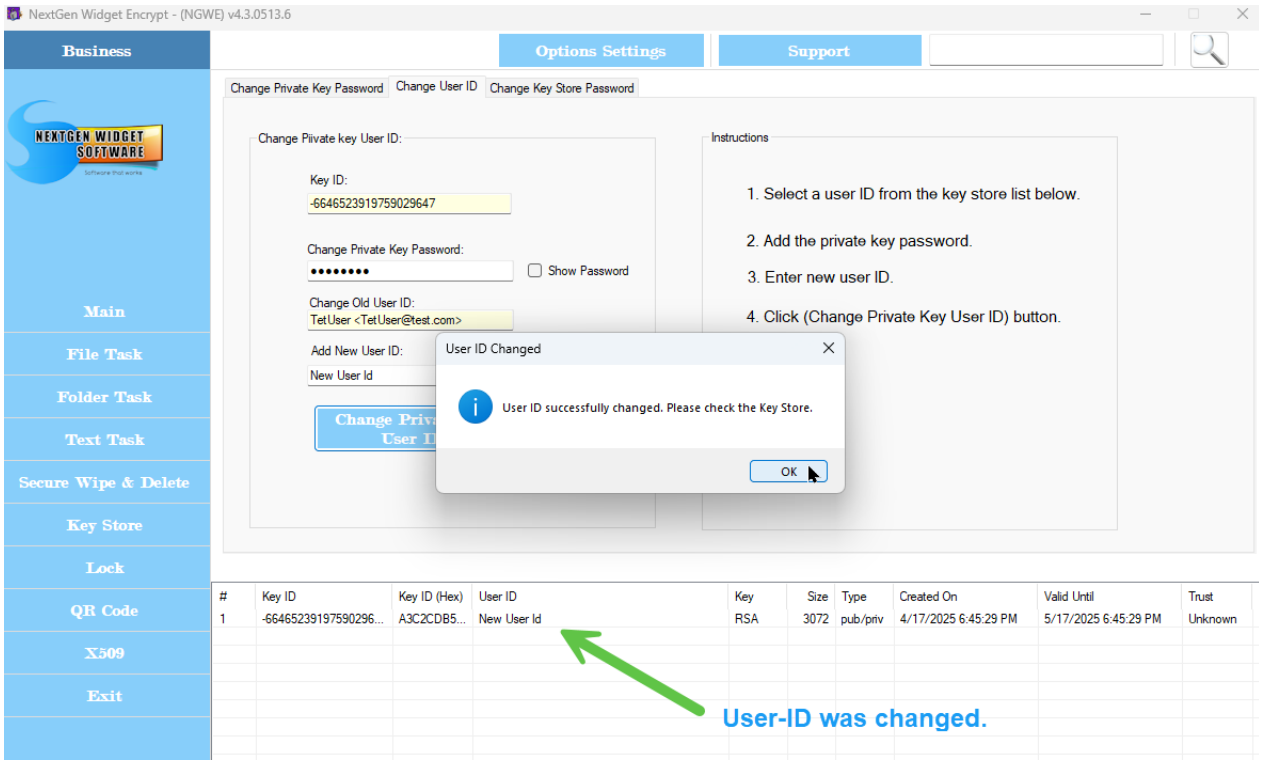


If you enter the wrong password you will be notified.



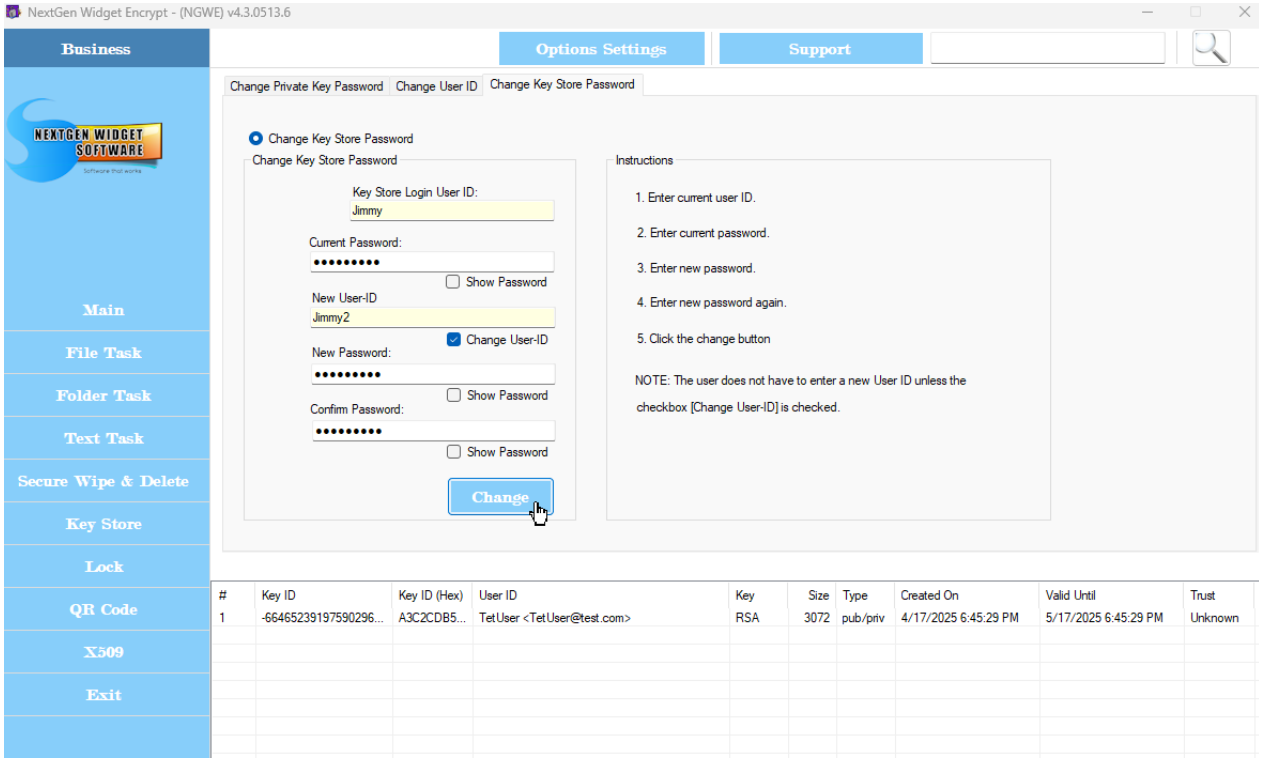
Change Private User-ID

When changing the private key User-ID the process is simple. Just right-click and select the User-ID you wished to change. The private key must be in the Key Store. The program will automatically enter the old User-ID. Just enter the new User-ID and click on the "Change Private Key User-ID" button.

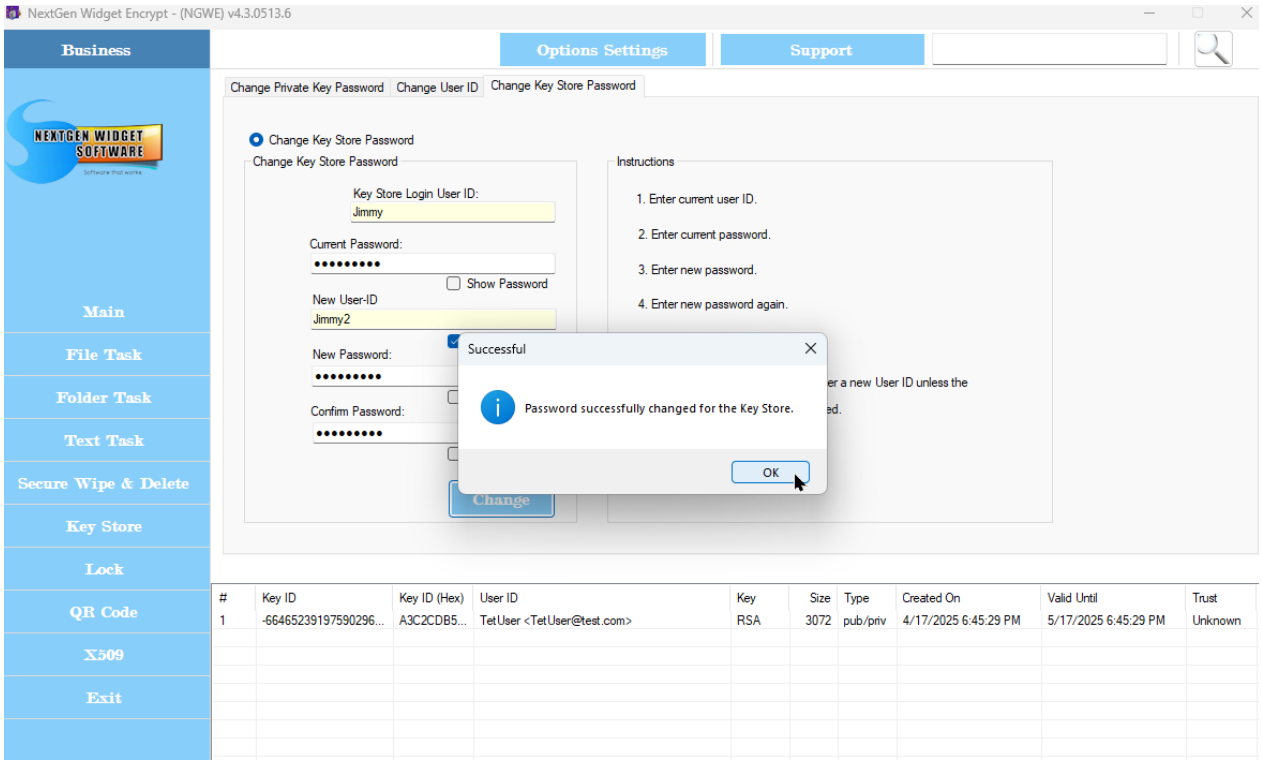


Change User ID

Changing the User ID is the same process as changing the password. You will need to enter in all of the information after clicking the [Change User-ID] check box. It can still be the same password for the current and new password if you are only interested in changing the User-ID.



User-ID changed only.



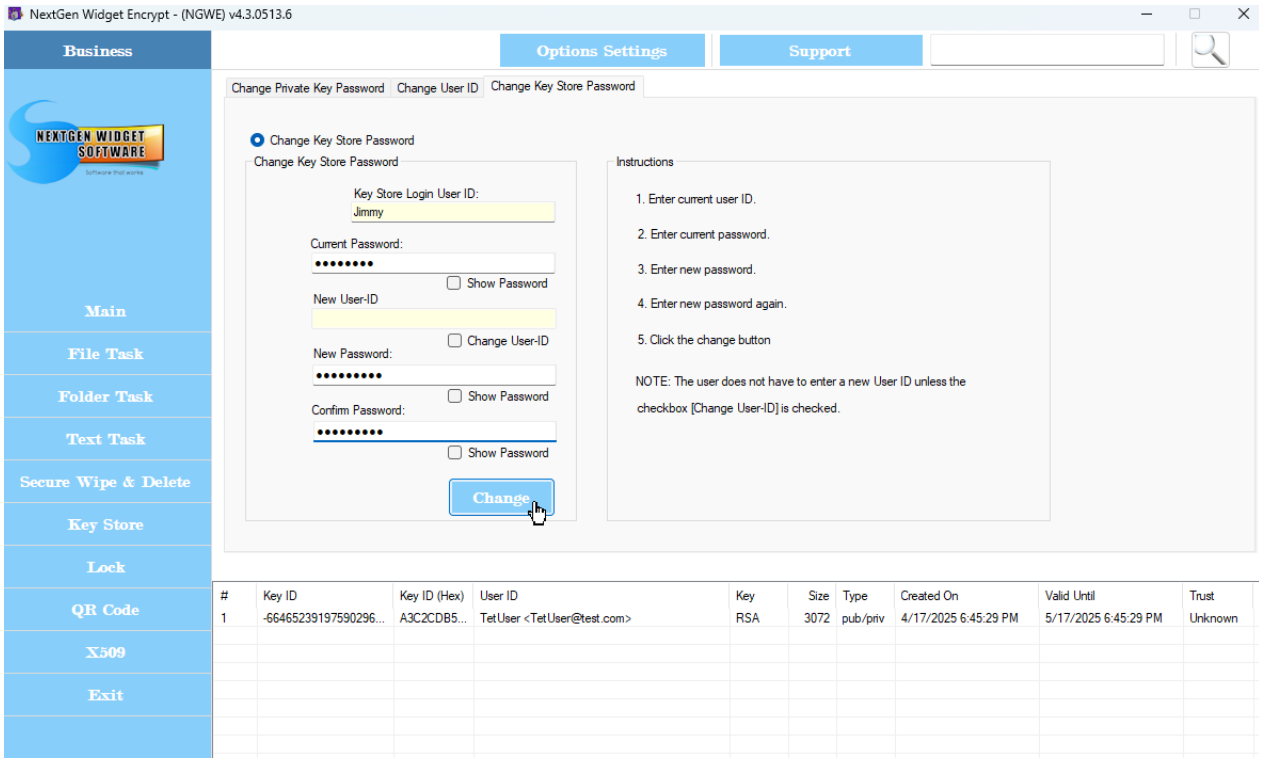
Change Key Store Password

To change the Key Store passwordand/or User-ID simply click the "Change Key Store Password" tab.

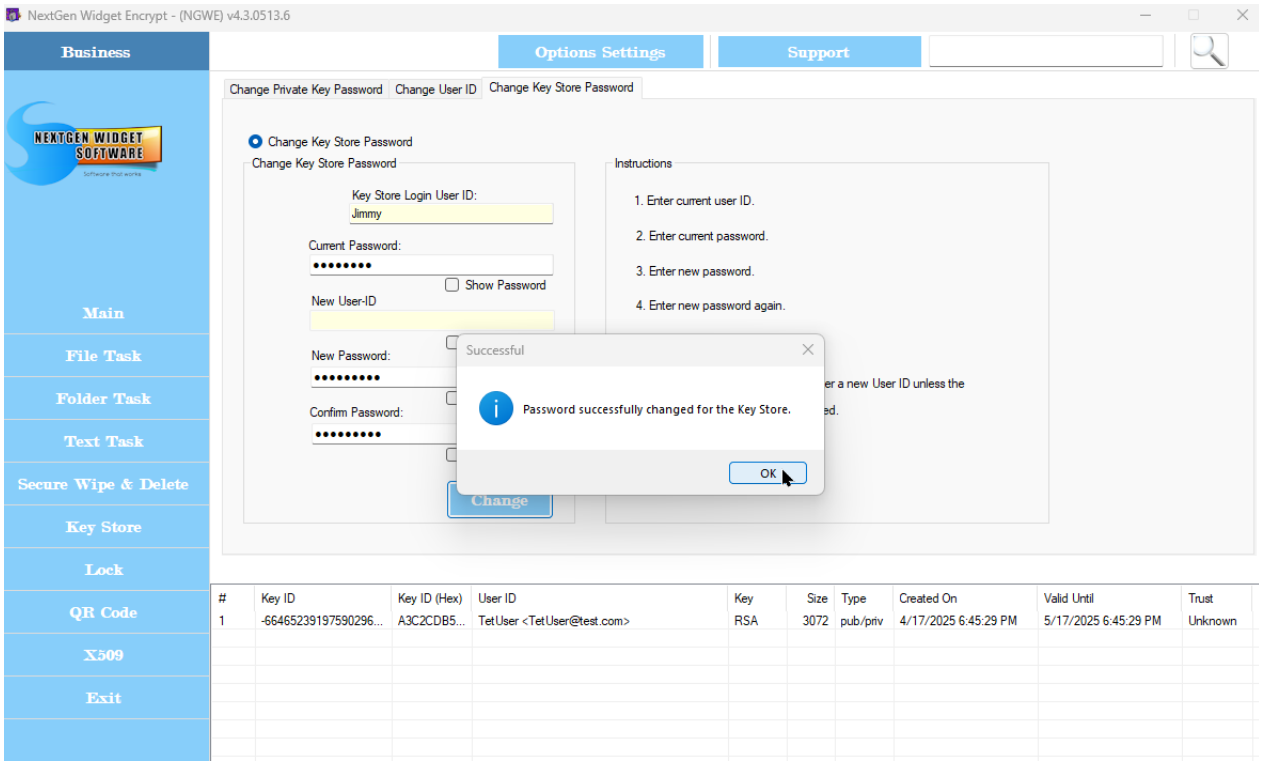
1. Enter current user ID.
2. Enter current password.
3. Enter new password.
4. Enter new password again.

5. Click the change button

NOTE: The user does not have to enter in a new User ID unless the checkbox [Change User-ID] is checked.



If the change was successful you will get a notification that the password successfully changed for the Key Store.



File Task

File Encryption
This area is used to encrypt files by file type for example .txt.

File Decryption
This area is used to decrypt files by file.

Sign & Encrypt File
Protect your encrypted data integrity by signing with your private key.

Decrypt & Verify File
Verify the authenticity of a message by verifying its signature.

File Encryption

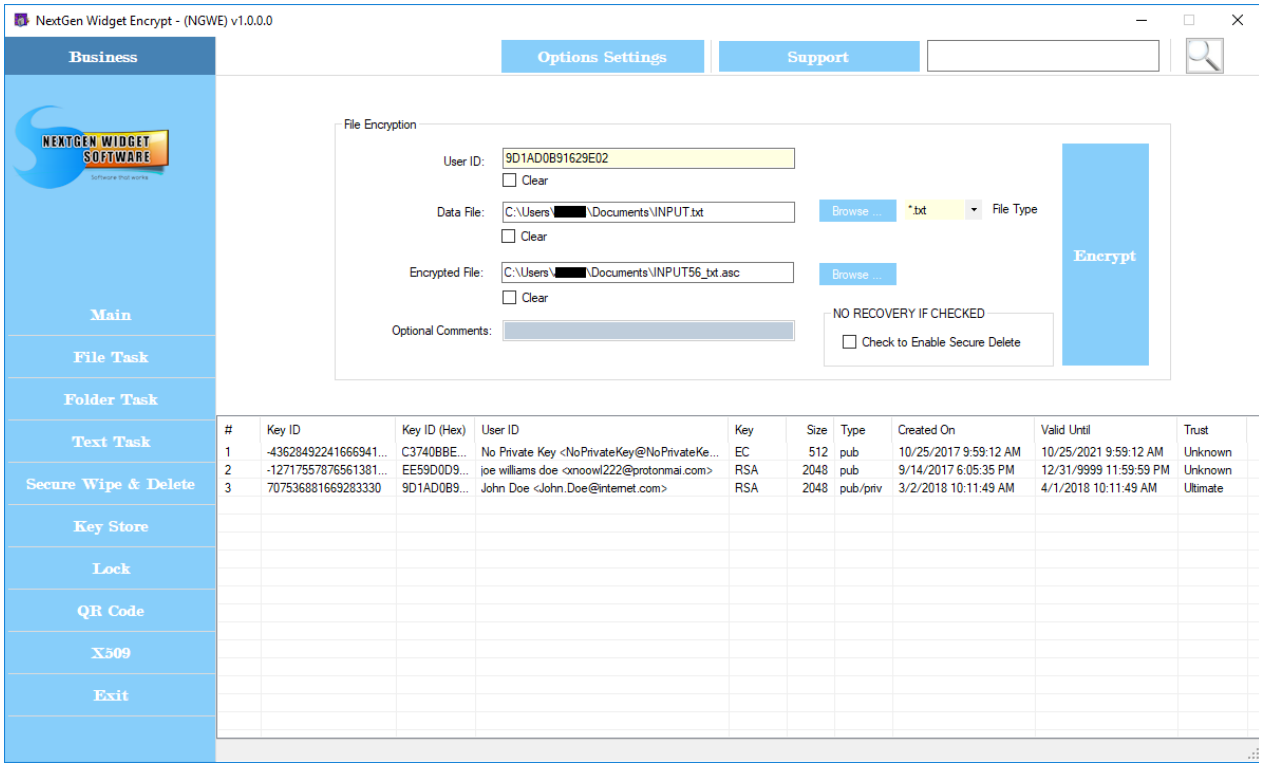
Encrypting files is an easy process. Simply, right click and select the User ID of the recipient. This enters their hex ID into the User ID field. Next you will have to select the data file. Now, just to the right of the browse button is the file type selection. You can select a file type so that if you have a directory with a lot of files in it you can scale them down to just let's say text files or doc files.

Just select the down arrow and choose your type; in my example I selected (.txt). Next just click the browse button and the only files you should see are text files. After selecting the desired file, click the second browse button so that you can save the encrypted file with the selected file extension; (.pgp, .asc, .gpg). If you select the .asc file extension, the encrypted file will automatically be in ASCII armor format. All of the file selection and save encrypted must be done vai the browse buttons.

There is a secure delete checkbox for those who wish to securely delete the original. Warning, there is no recovery for the secure delete. If you select this, after the encryption is completed and the file is generated, the original file will be securely deleted.

When the encryption is all done the program inserts the original file extension into the encrypted file name so that you will know what file type the file is for decryption and viewing.

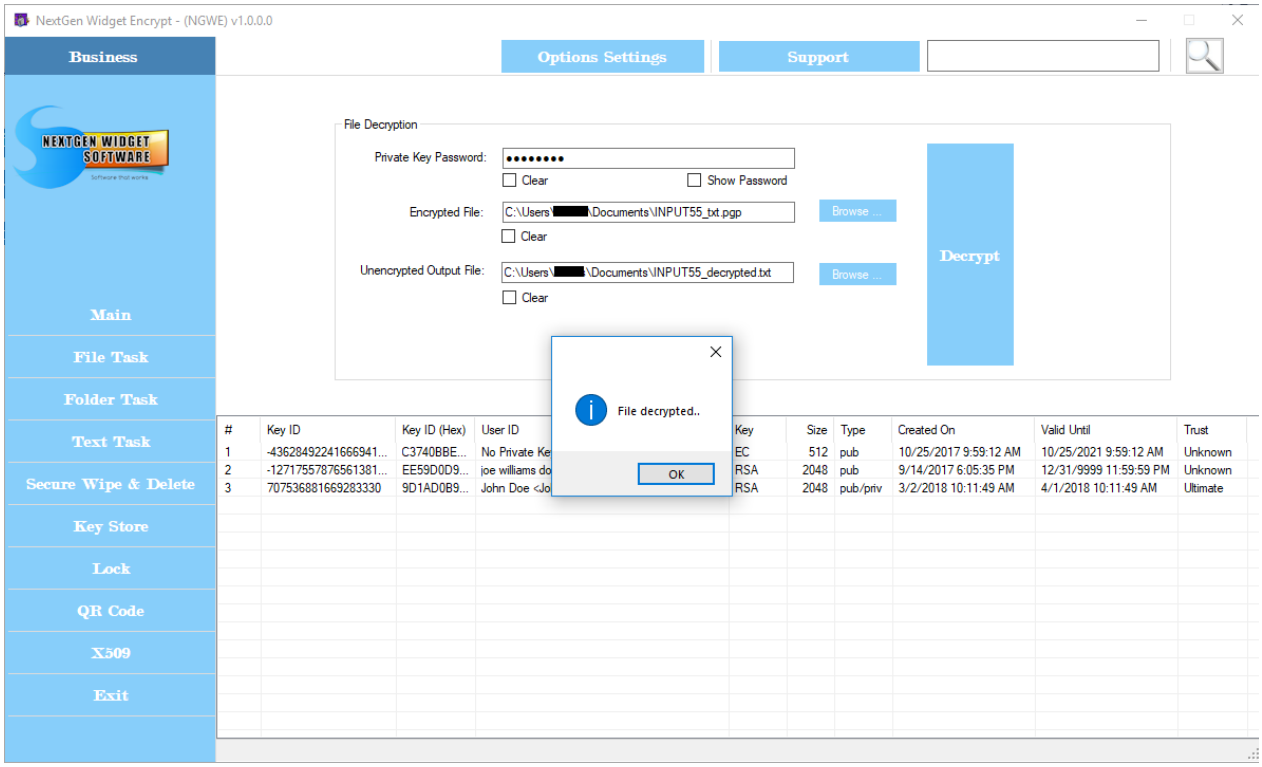
The Compatible check box makes the key compatible with earlier version of OpenPGP 2.x. However, for the most part it's not used anymore.



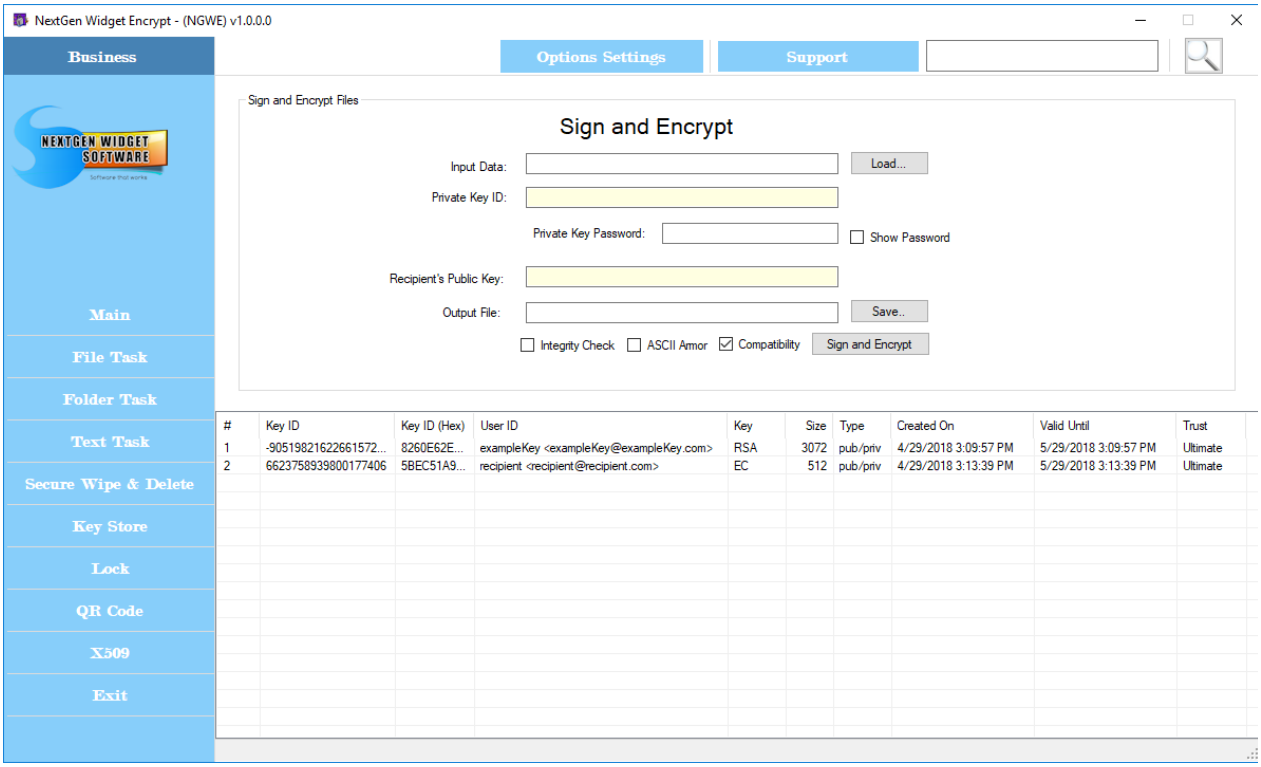
File Decryption

File decryption is relatively simple. The private key needs to be located in the Key Store and you only need to enter in the private key password, the encrypted file and your output file directory. Start by entering the private key password, then click the browse button and locate the encrypted file; you have three choices for the file extension (.pgp, .asc and .gpg). Save the file in whatever location you want to and don't forget to set the file extension.

Once you click the decrypt button, the file is decrypted and a message displayed.



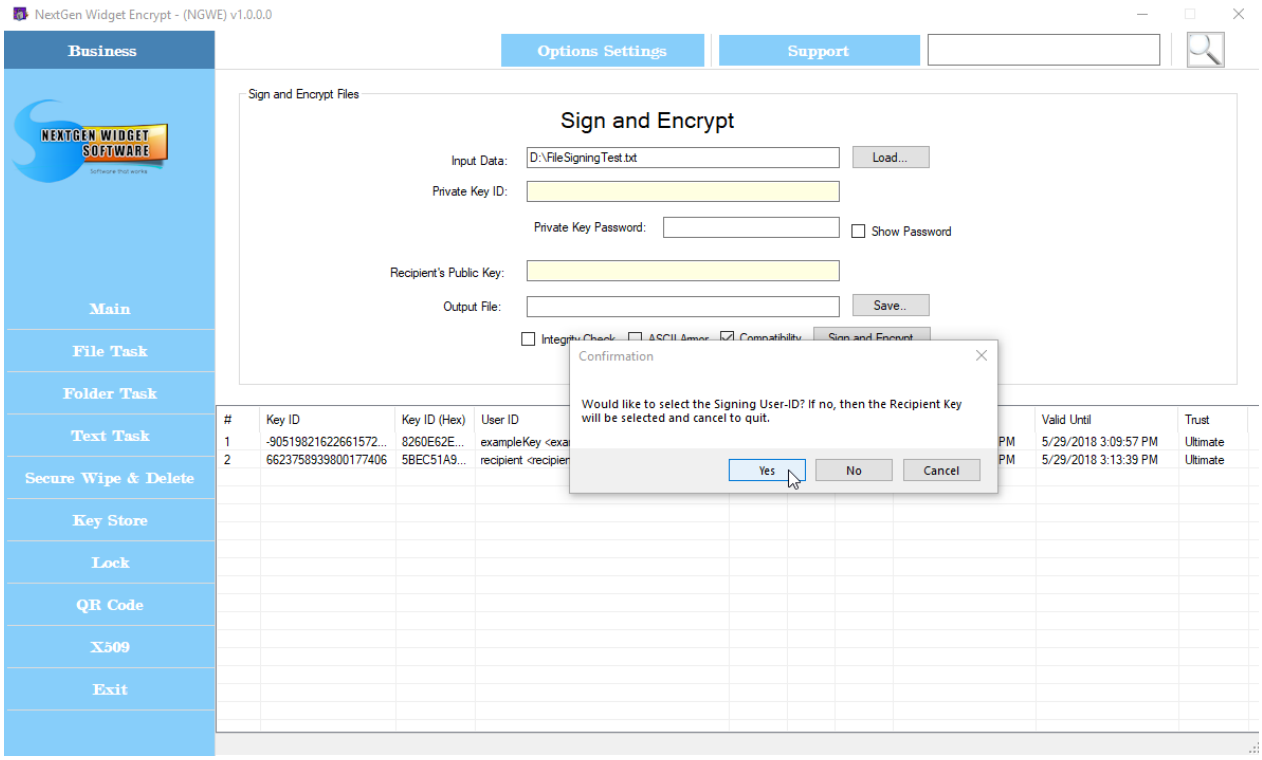
Sign & Encrypt File

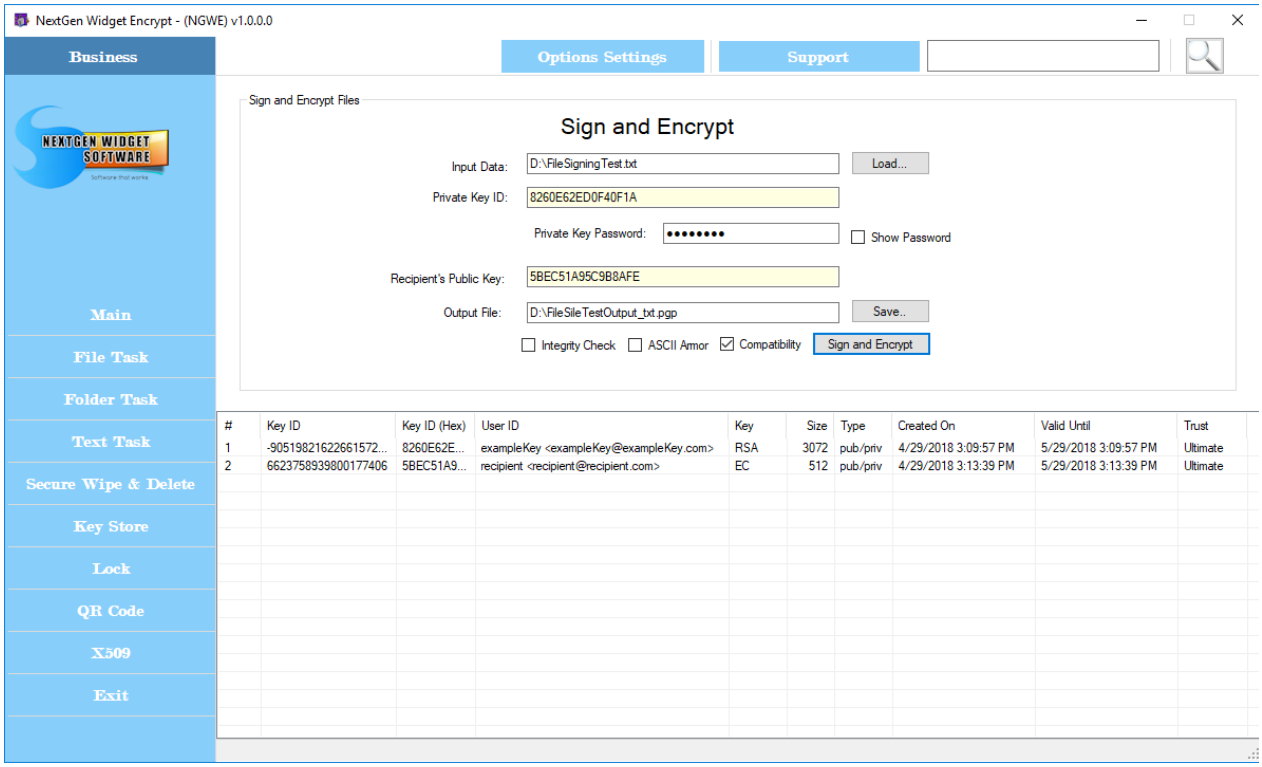


There may be times where you need to sign a file to prove that it cames from you. Simply click the load button and select the file you wish to sign. Then right-click on your private key and choose "Select User-ID" from the pop-up menu.

A window pops up that has two functions. First when it pops up it will copy the User ID into the Private Key ID field once you select yes. If you select no, then it will copy the User ID into the recipients public key field. Sense we want the private key we will select Yes and then enter the private key password. Next we will do the exact same process; right-click on the recipient key and select No.

Once we've completed that process we only need to choose the output file location by clicking the save button and give the file a name. Then click "Sign and Encrypt". The file will be encrypted and signed and the location specified. However, the file name will change adding the file extension so that you know what file type has been encrypted and so will your recipient.

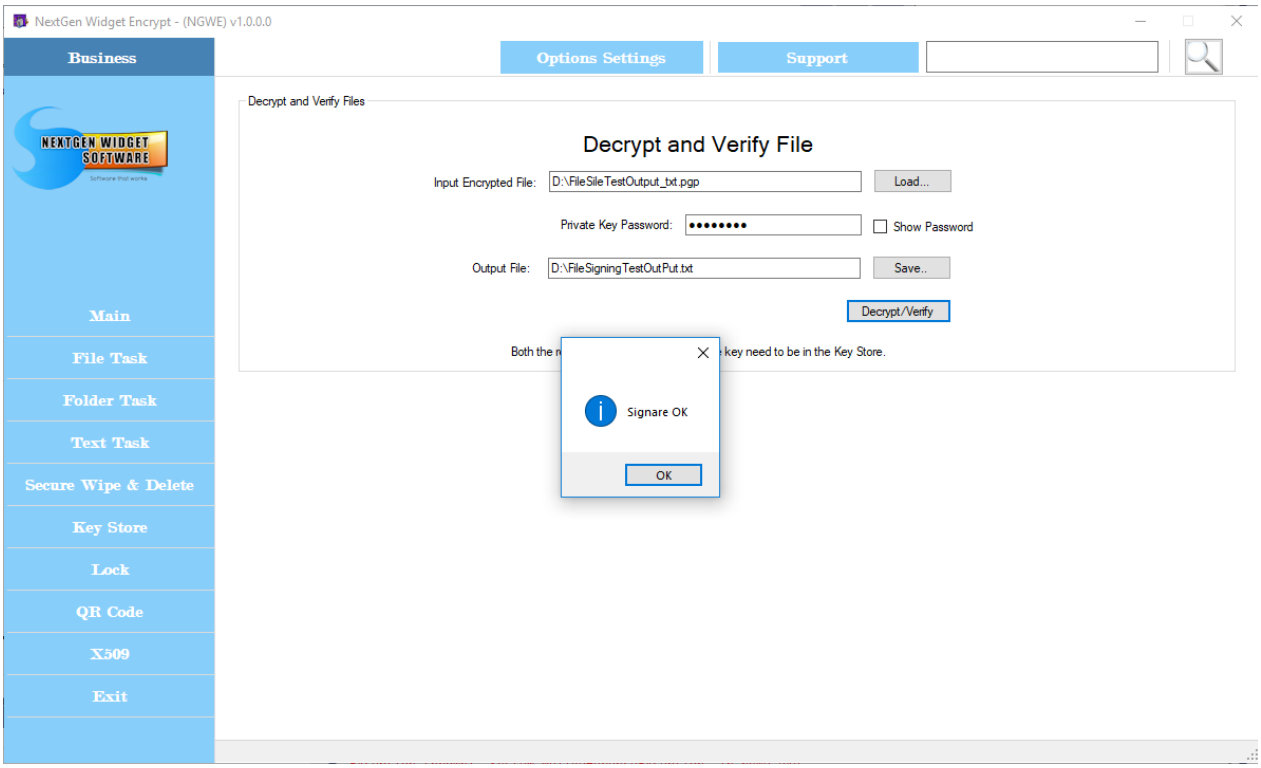




Decrypt & Verify File

Decrypt and verify a file is a very simple process. Just simply load the encrypted file, enter the private key password and the output file. You don't need to select the private key User ID for the file. The private key for the file must be in the Key Store and will be automatically detected and selected.

Click "Decrypt/Verify" button and if the file is authenticated you will see the "Signature OK" verification message and the file will be decrypted.



Folder Task

Folder Encryption
Encrypt an entire folder including all content.

Folder Decryption
Decrypt an entire folder including all content.

Folder Encryption

To encrypt a directory just enter recipients public User-ID and then select the directory to encrypt. Next, select the save file location and name it. In this example I'm using "John Doe" because he also has a private key which I will need to decrypt the directory. This technique can also be used if you have directories on your system that you wish to keep private.

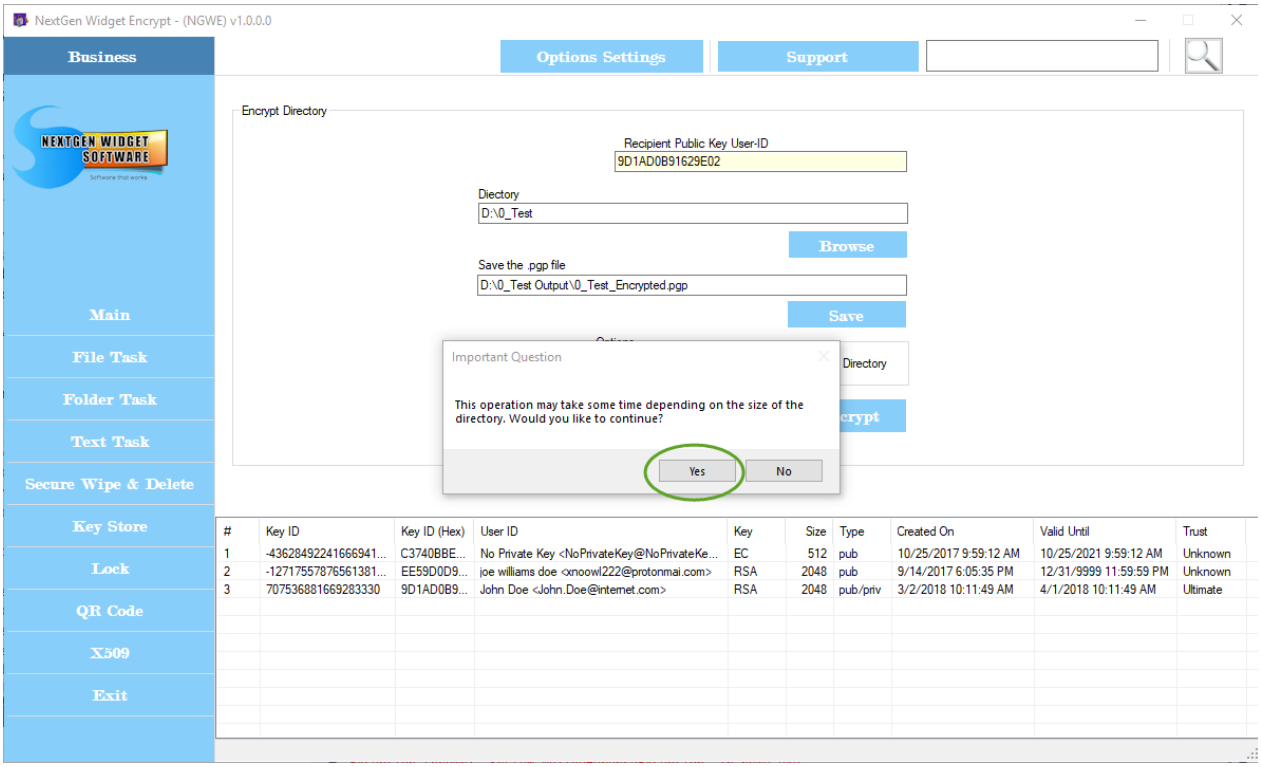
If we select the ASCII armor checkbox, the main directory and its subdirectories will all be encrypted as an ASCII text. Once you hit the "Encrypt" button, this may take a little bit of time depending on the size of the directory so you will need to be patient. During this process you will see the wait cursor although you will still be able to do other functions

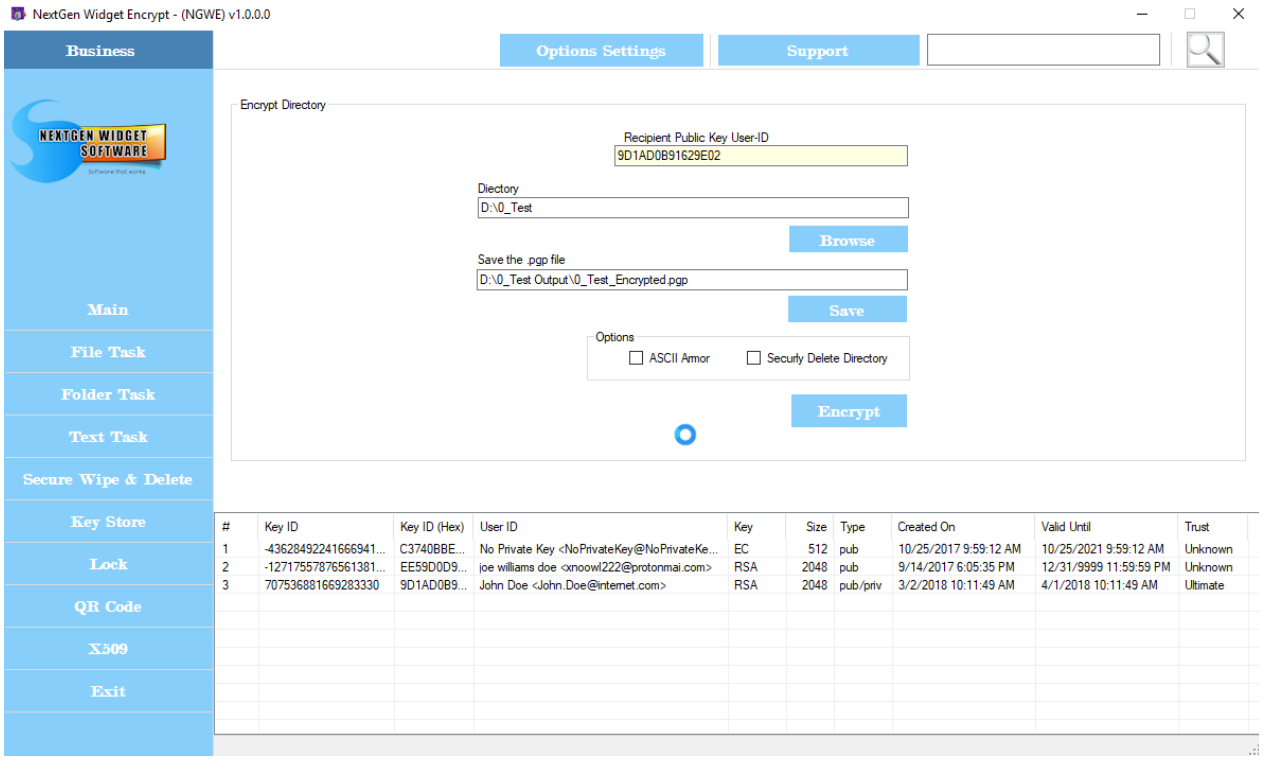
within the software. Once the encryption is completed, you'll receive a message.

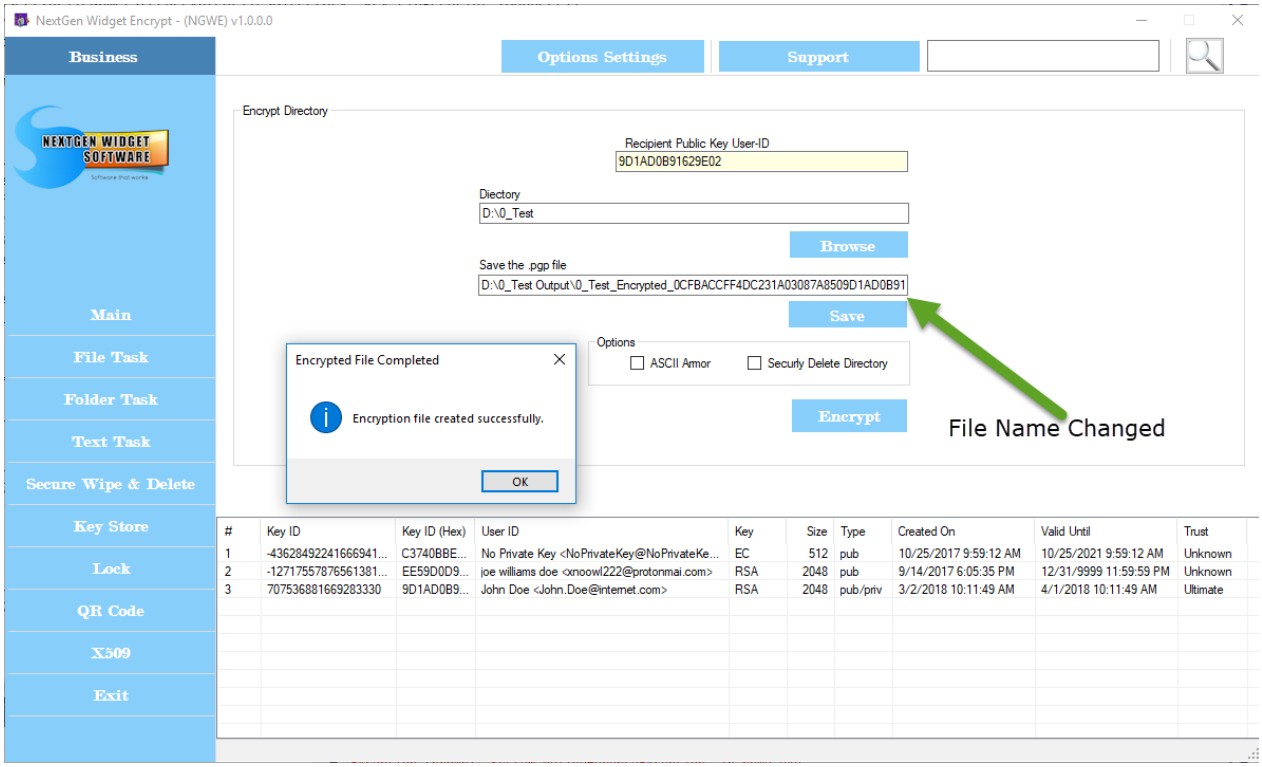
When the file has been encrypted, the file name will change and the fingerprint of the recipients public key is inserted.

If you click the securely delete directory checkbox, you will have one opportunity to cancel the operation. After which, the original folder will be securely deleted and unrecoverable. There is no back door so please be careful with this.

NOTE: Although "NextGen Widget Encrypt" software is able to encrypt large folders in ASCII armor text. Not all text editors will be able to open up large text files so our recommendation is not to use ASCII armor for large directories and leave the output file as binary which is the program's default setting.



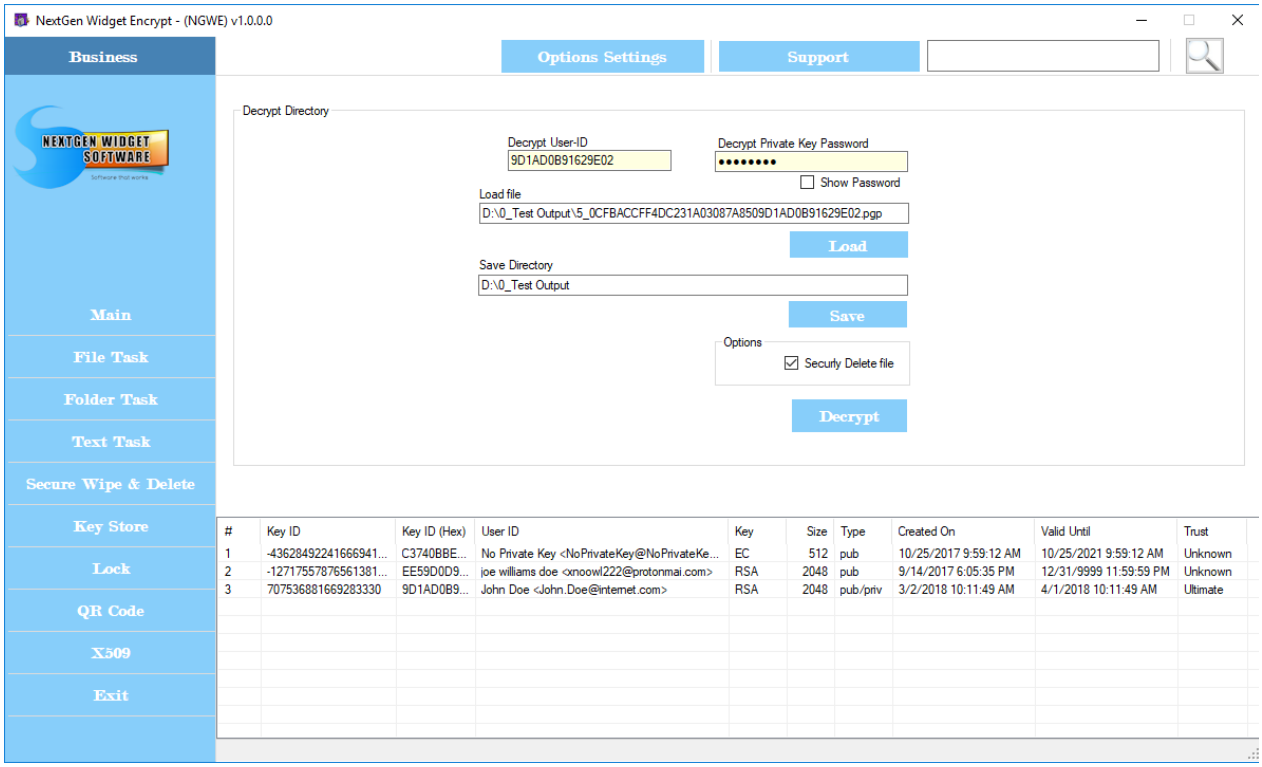




Folder Decryption

Decrypting a directory involves having the private key located in the key store. Right click and enter the user ID the decrypt user ID field and then enter the private key password. Locate the encrypted file that represents the directory that you wish to decrypt. Next, save the decrypted directory to a directory or to a drive root.

Once you click the "Decrypt" button you will receive a message letting you know that it may take some time depending on the size of the file to be decrypted and directory created. Next, if you have clicked the checkbox "Securely Delete File", after the directory is decrypted. You will receive an opportunity to decline the "Securely Delete File", once you say Yes at this point, there is no turning back and there is no recovery for the deleted original encrypted file.



Text Task

Text Encryption

Text Decryption

Sign & Encrypt Text
The OpenPGP clear text signed format is designed for text data and contains the data intact plus the signature.

Decrypt & Verify Text
When we receive OpenPGP one pass signed and encrypted message we can simply decrypt it or both decrypt the data and verify the authenticity of the sender in a single step.

Clear Text Signing

The OpenPGP clear text signed format is designed for text data and contains the data intact plus the signature. In this format the digital signature is appended after the clear text original message; this way the recipient can still read it without using special software.

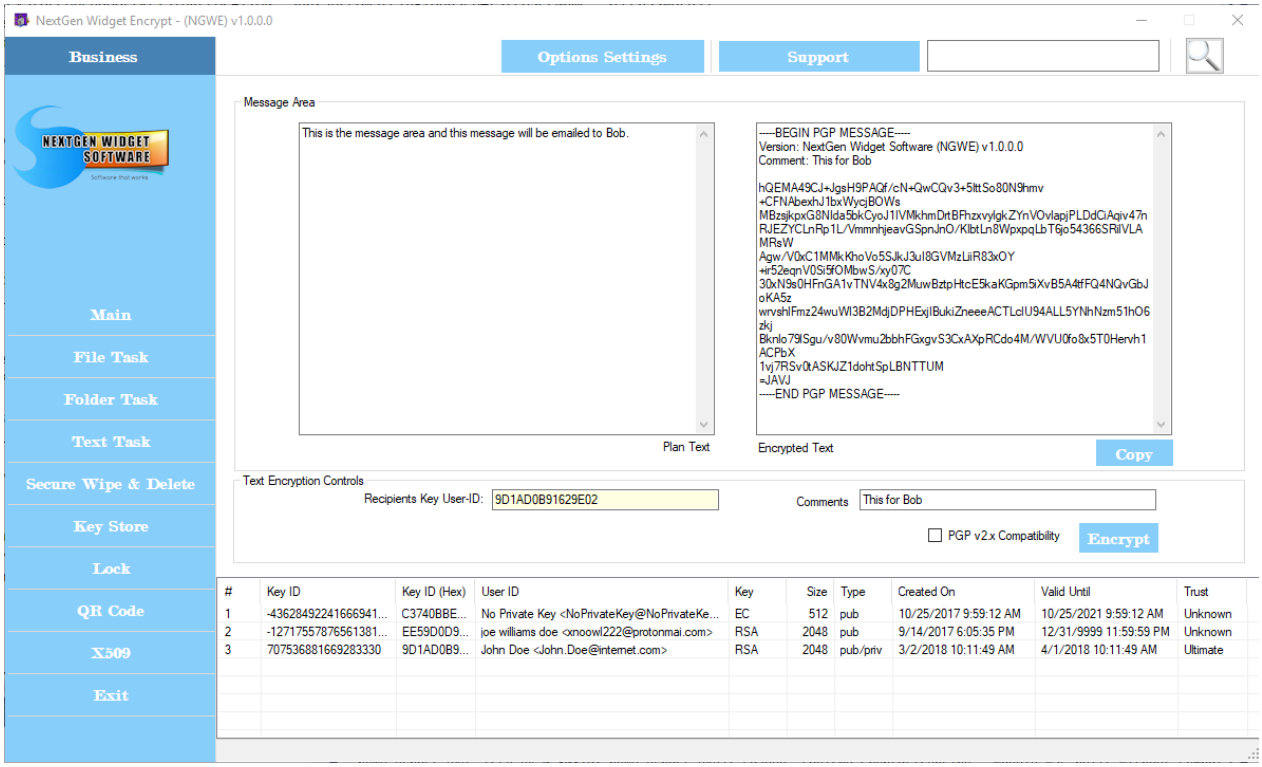
Clear Text Verify

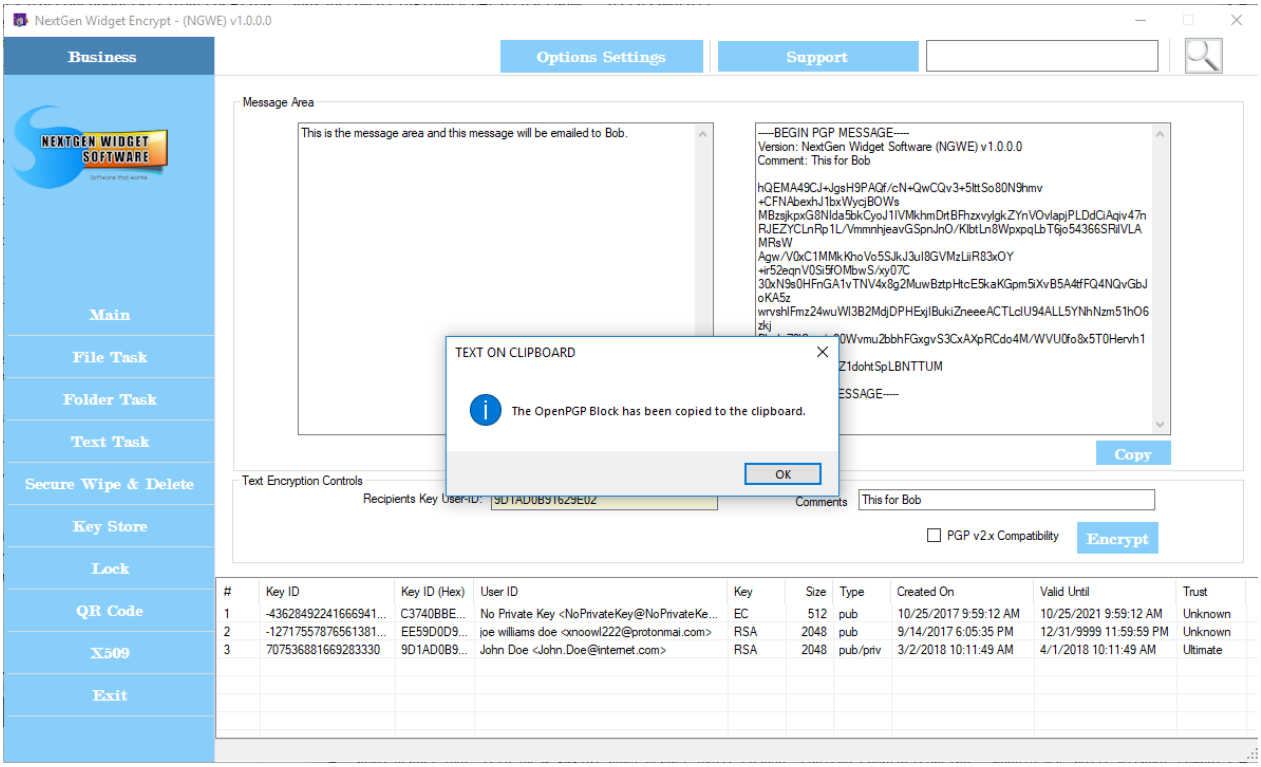
Text Encryption

The text encryption area is a nice easy area to write a message and instantly encrypted. These messages are great for emails or anywhere that you need to send by text messages. In the message area just simply type your message, right click and select the recipients User ID. If you want, you can also add a comment line to the ASCII armor text that's generated.

Some of the old versions of OpenPGP are not really compatible with the newer versions. However, if you have someone that's using an older version then OpenPGP v2.x, then you should click the compatibility checkbox. Once your message is complete just simply click the "Encrypt" button and your encrypted message instantly appears in the right hand OpenPGP block.

You also have the ability to copy that OpenPGP block to the clipboard so that you can send it in an email or add to a note, etc.

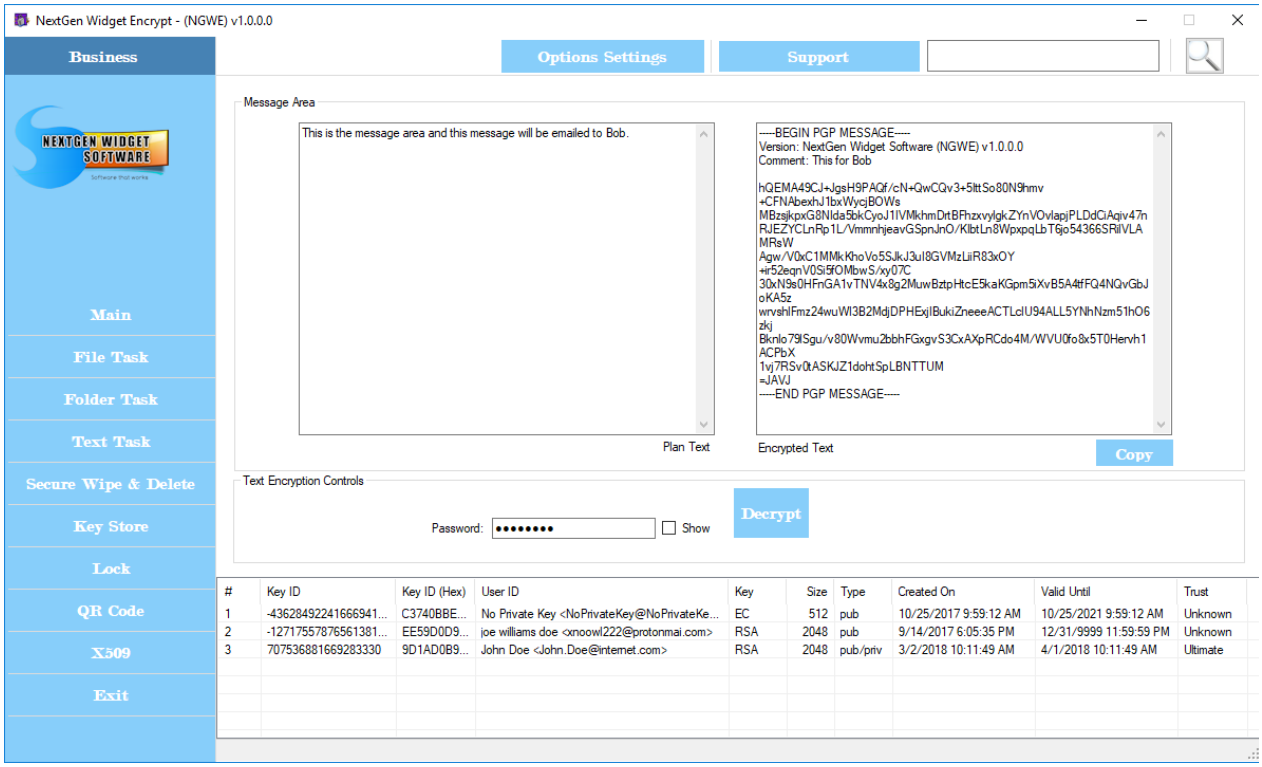





```
-----BEGIN PGP MESSAGE-----
Version: NextGen Widget Software (NGWE) v1.0.0.0
Comment: This for Bob

hQEMA49CJ+JgsH9PAQf/cN+QwCQv3+5IttSo80N9hmv+CFNAbexhJ1bxWycjBOWs
MBzsjkpxG8NIda5bkCyoJ1IVMkhmDrtBFhzxvylgkZYnVOvlapjPLDdCiAqiv47n
RJEZYCLnRp1L/VmmnhjeavGSpnJnO/KIbtLn8WpxpqLbT6jo54366SRilVLAMRsW
Agw/V0xC1MMkKhoVo5SJkJ3uI8GVMzLiiR83xOY+ir52eqnV0Si5fOMbwS/xy07C
30xN9s0HFnGA1vTNV4x8g2MuwBztpHtcE5kaKGpm5iXvB5A4tfFQ4NQvGbJoKA5z
wrvshlFmz24wuWl3B2MdjDPHExjIBukiZneeeACTLclU94ALL5YNhNzm51hO6zkj
Bknlo79lSgu/v80Wvmu2bbhFGxgvS3CxAXpRCdo4M/WVU0fo8x5T0Hervh1ACPbX
1vj7RSv0tASKJZ1dohtSpLBNTTUM
=JAVJ
-----END PGP MESSAGE-----
```

Text Decryption

Decrypting a message is very simple. Just add the encrypted message to the encrypted text block, enter the password for the private key associated with the encrypted message. The private key needs to be located in the Key Store. click "Decrypt" and you're done.

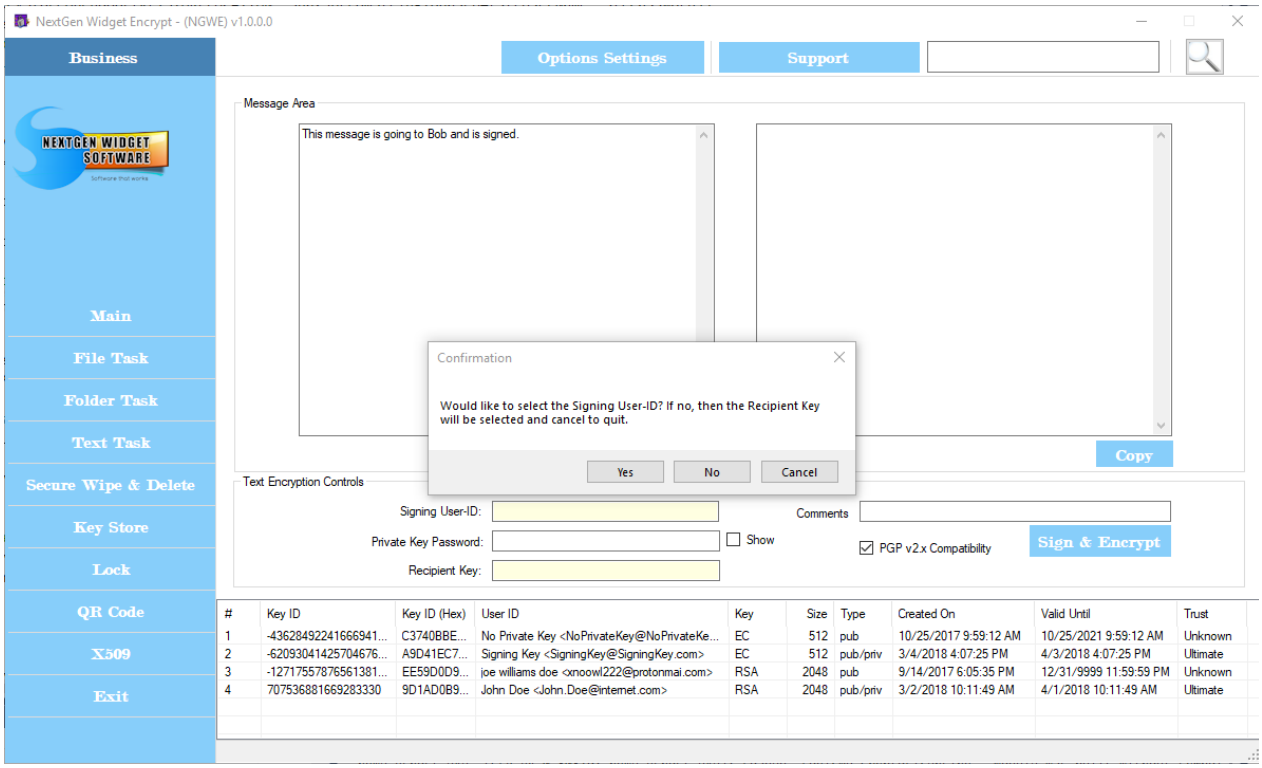


Sign & Encrypt Text

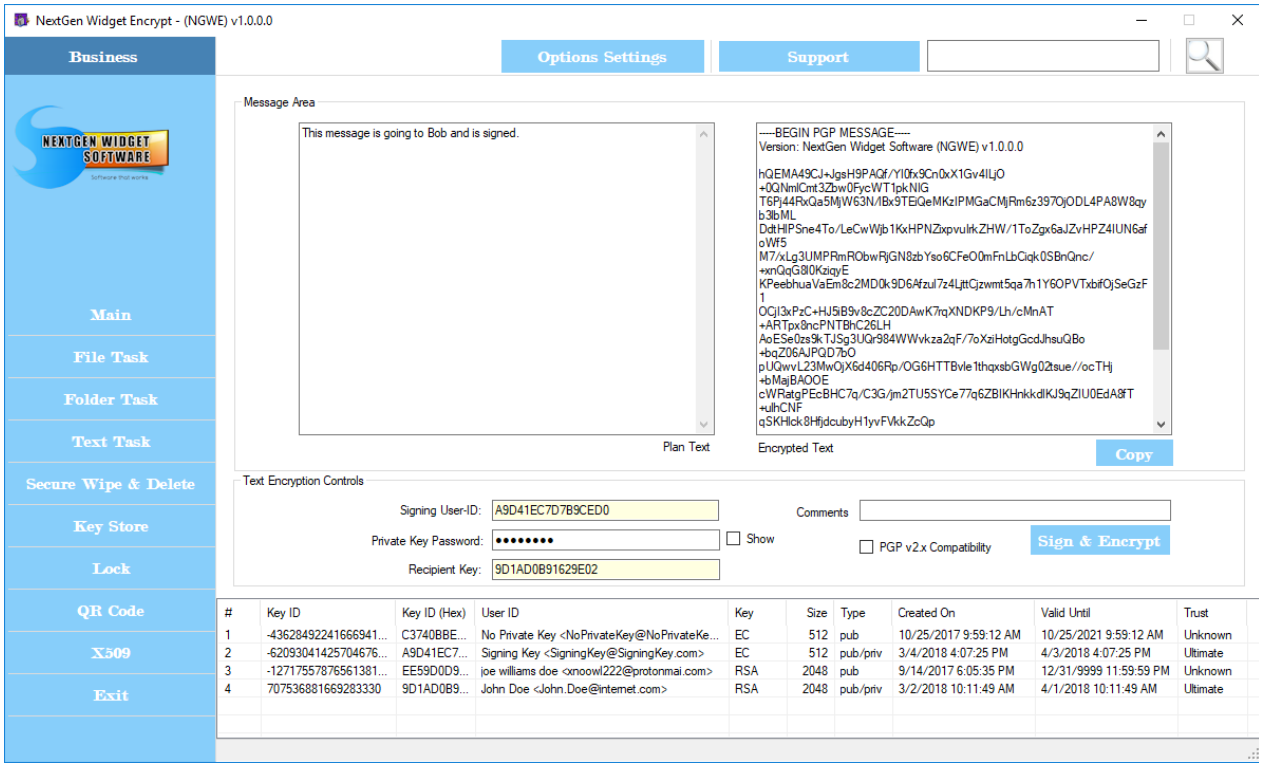
Many times you may need to prove to the sender that you are who you say you are. This is done by signing the key and it is verified on the other end with your public key. In this case we will create a message, the User ID that will sign the message, enter the private key password and select the recipients public key.

For this example I have generated another key called "Signing Key" so that I have another public and private key located in the Key Store. The "Signing Key" is going to be the creator of the email or message and the recipient is going to be "John Doe". First I'm going to select the User ID "Signing Key" and a confirmation window pops up asking you if you would like to select the signing User ID. The reason for this is because the same pop up is used to answer the recipients User ID as well.

Some of the old versions of OpenPGP are not really compatible with the newer versions. However, if you have someone that's using an older version of OpenPGP v2.x. Just clect "PGP v2x Compatiblity".



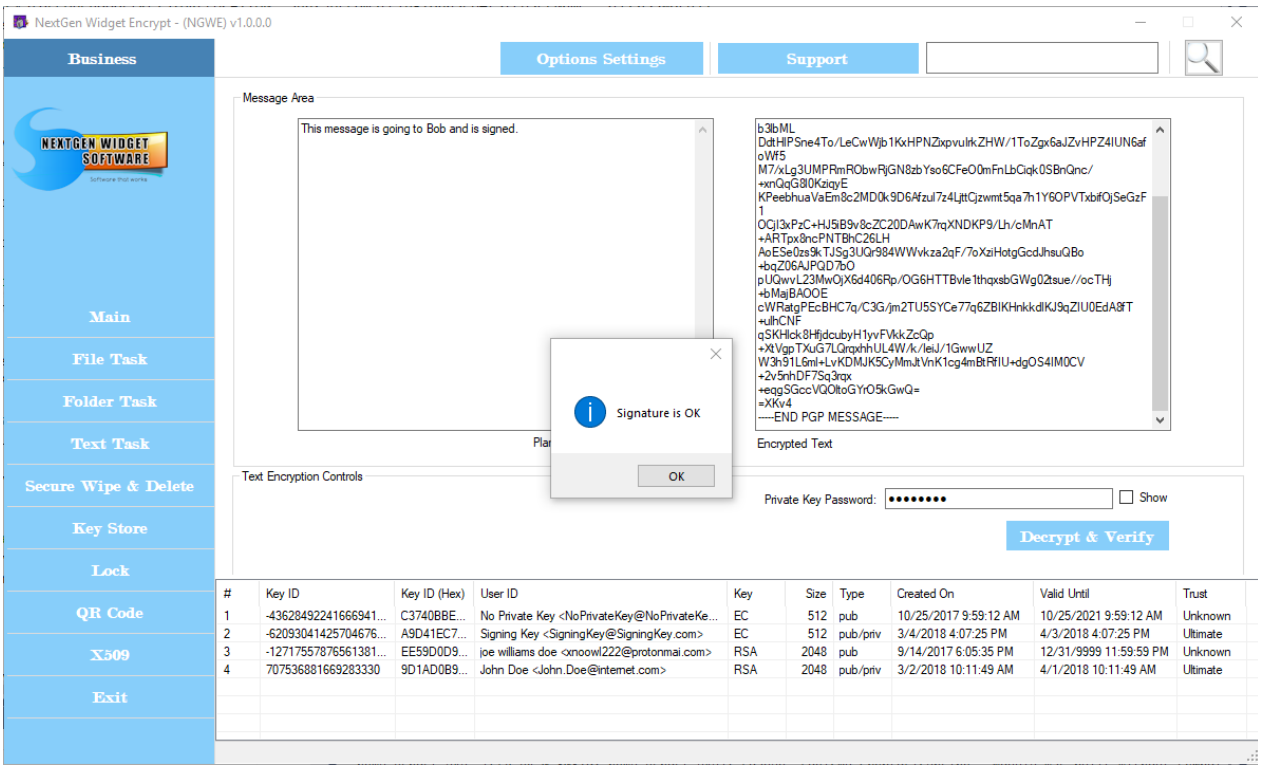
Since I'm looking to enter the signing User ID I'm going to select yes and then enter the password. Next, I repeat the same process but this time selecting "No" and the program adds the User ID to the recipient field. Now the only thing left to do if I don't want to add a comment is click the "Sign & Encrypt" button.



Decrypt & Verify Text

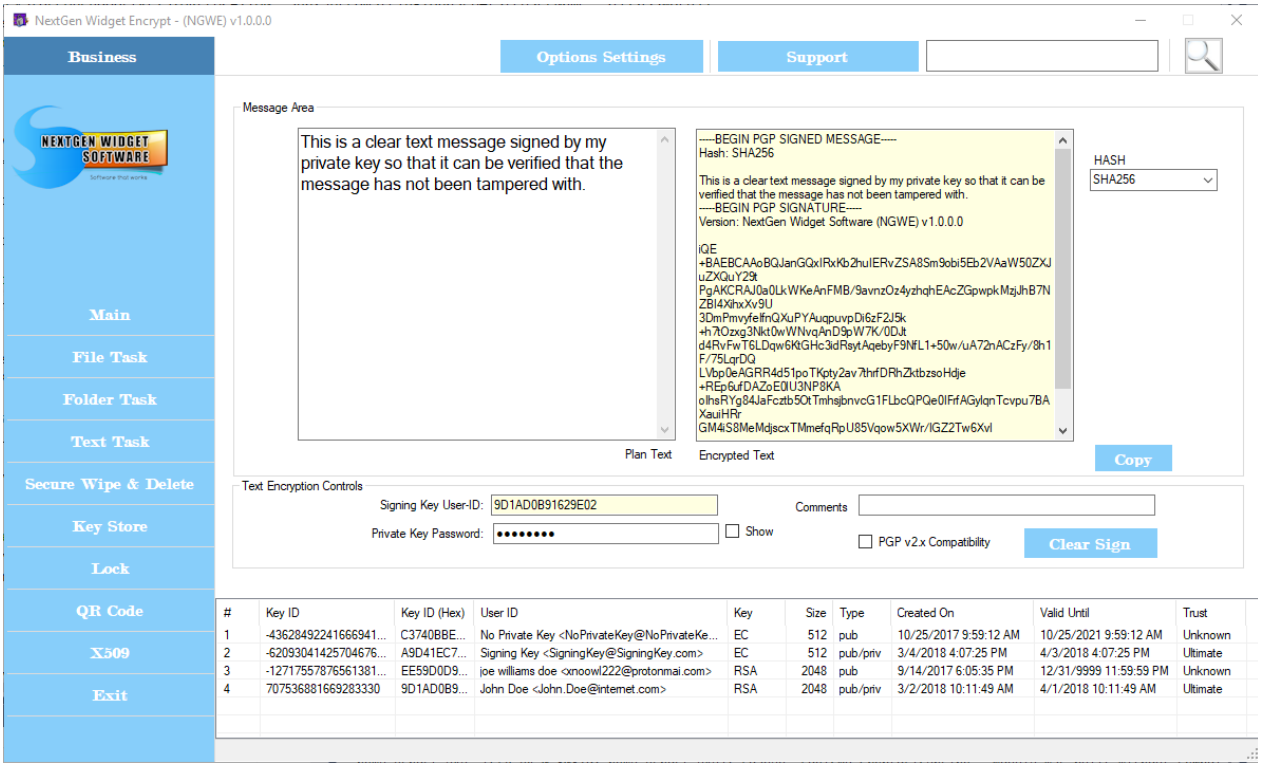
To decrypt a signed message the private key needs to be located in the Key Store. You only need to add the encrypted text to the OpenPGP block, and the private key password and click "Decrypt & Verify".

If verification is successful you will receive the message "Signature is OK" as the message is generated in the message area block.



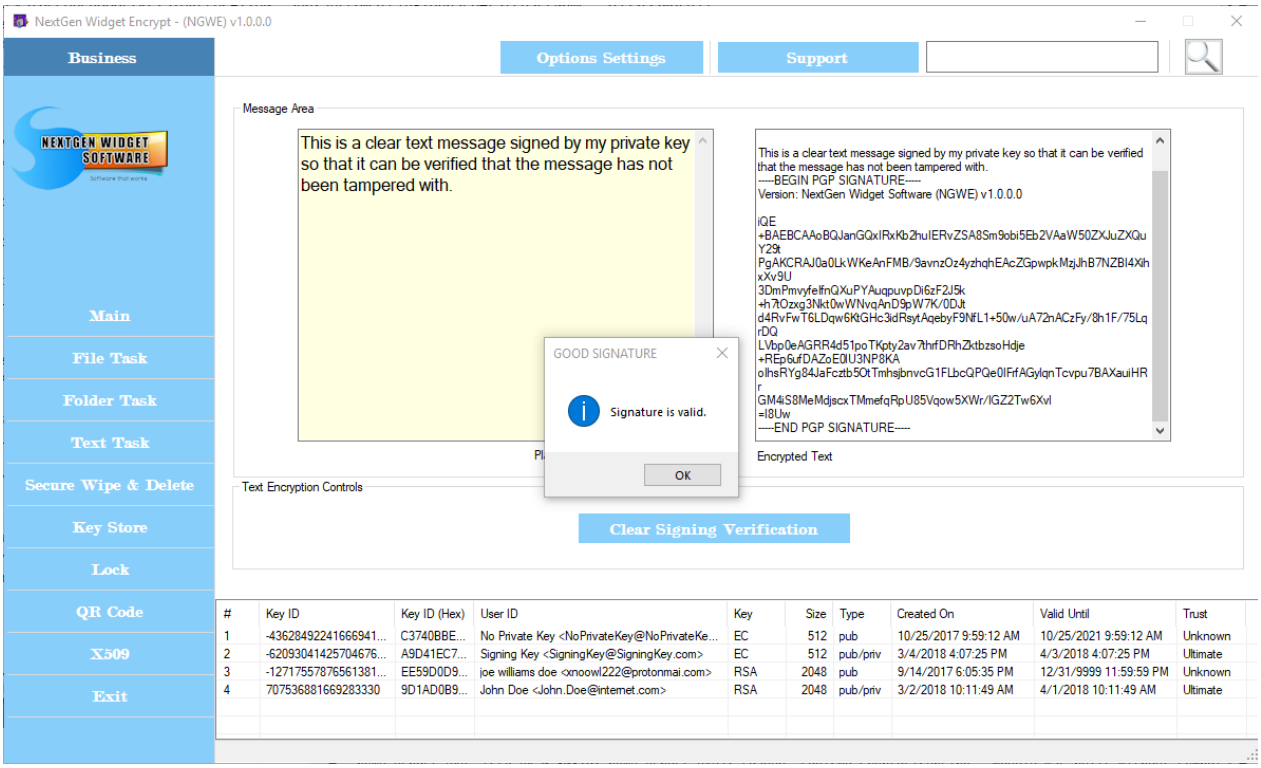
Clear Text Signing

Clear text signing is just a way to verify that your text has not been tampered with. The message is in plain text for anyone to read. With the signing message, you can choose the hashing algorithm you would like in the drop down box located to the right of the encrypted text field.



Clear Text Verify

Clear text verification you only need to enter the signature and message as it is generated. Click the clear signing verification button and that's it as long as the public key is in the Key Store.



Secure Wipe & Delete

Secure Files

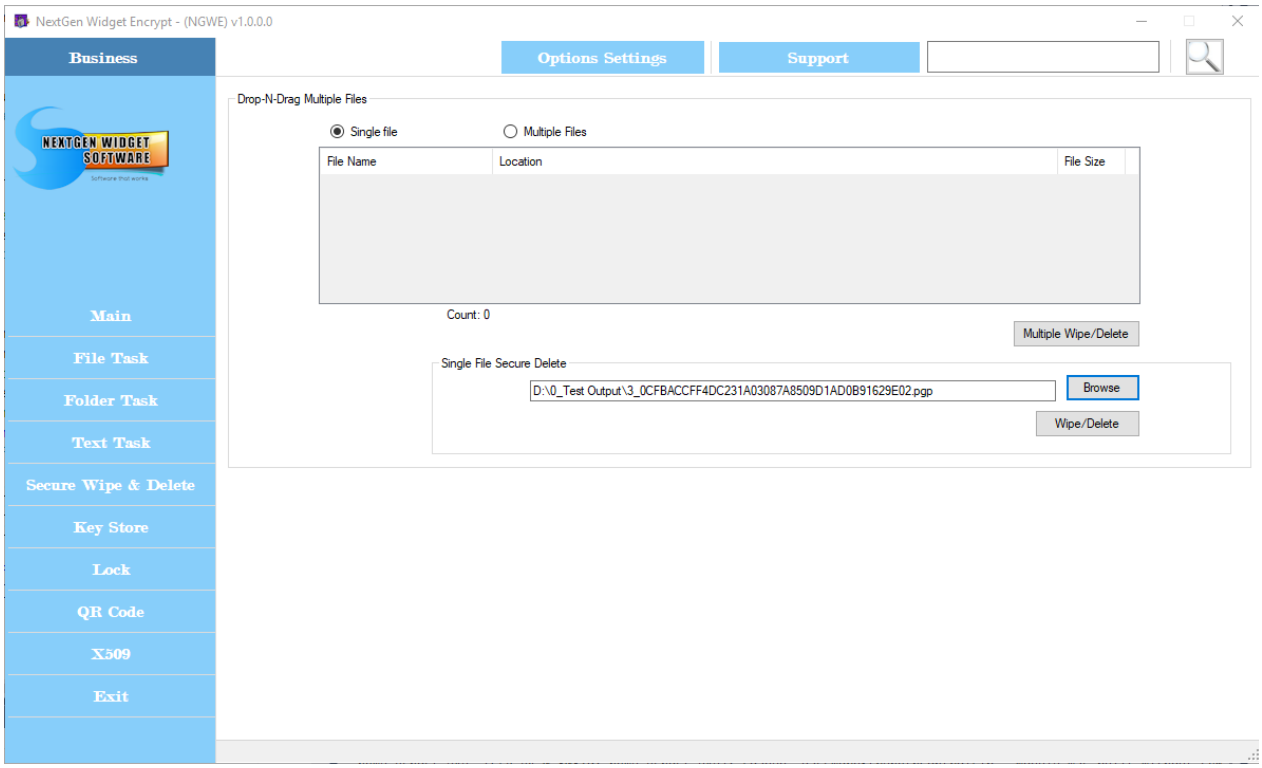
Secure Folders

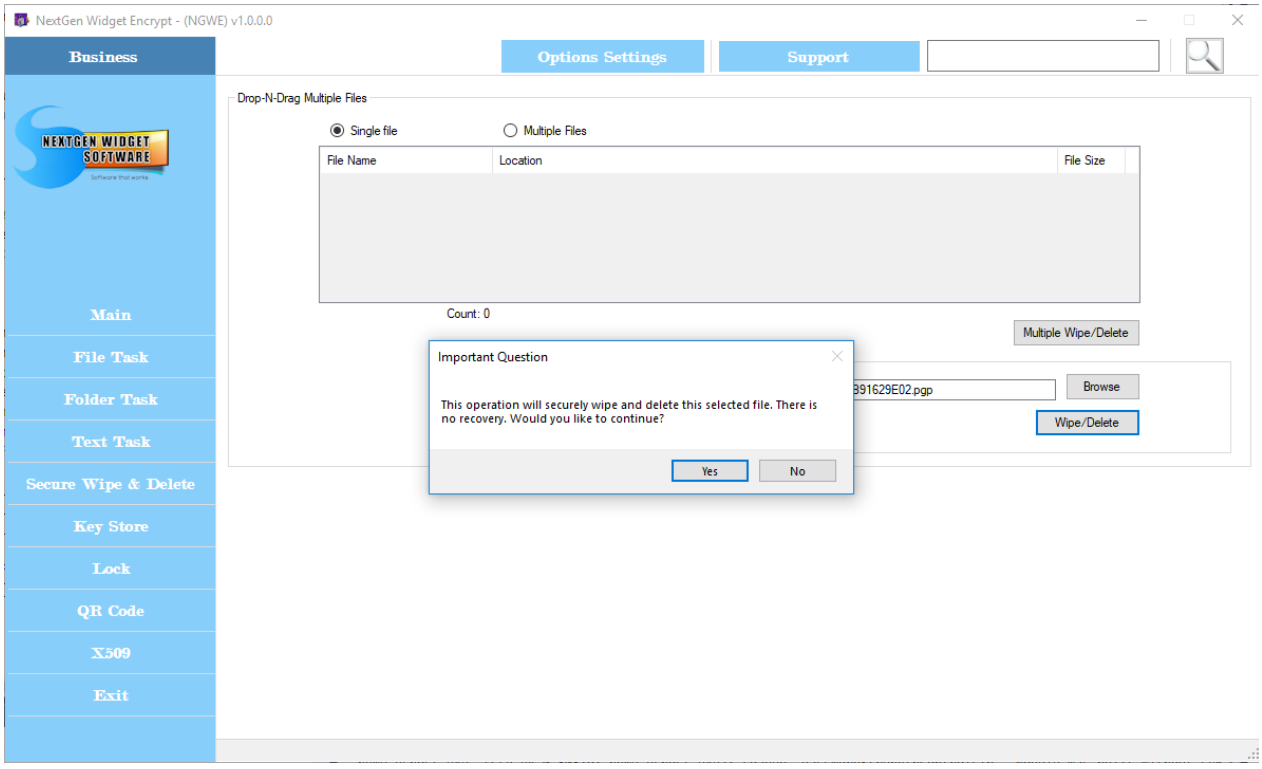
Secure Files

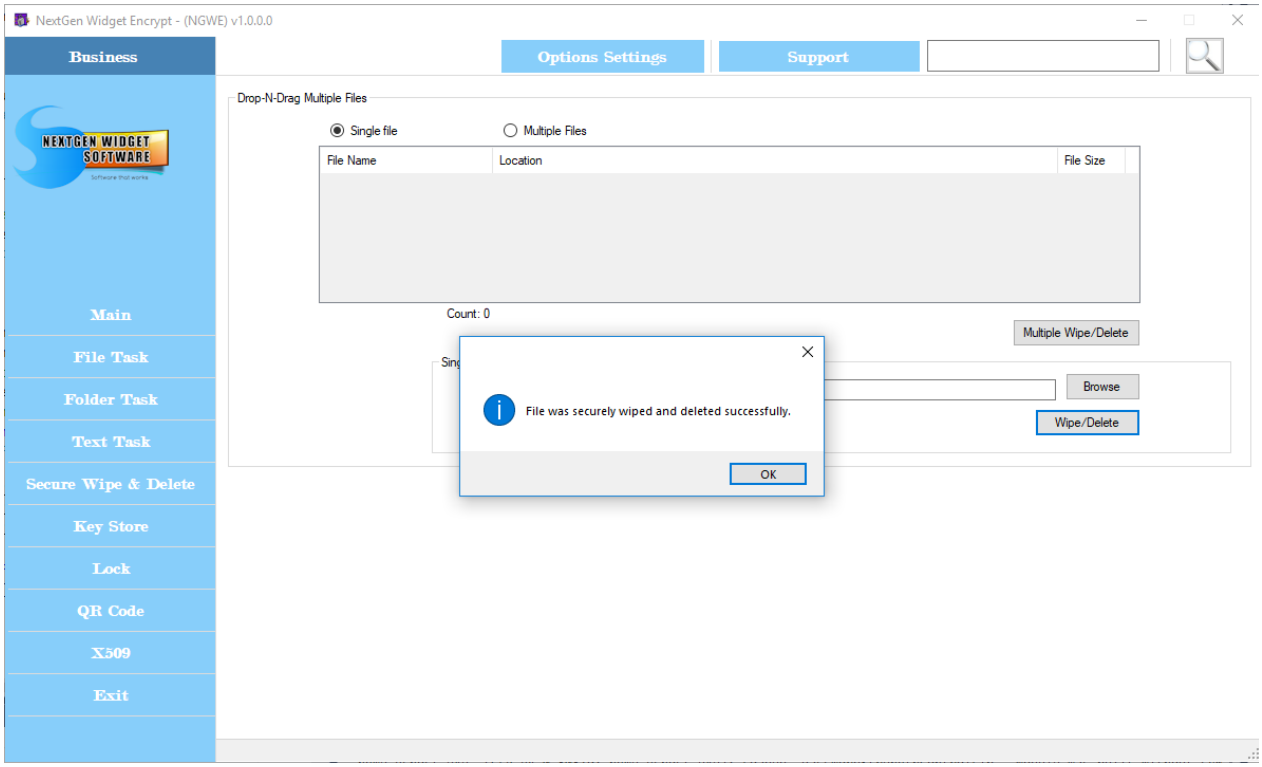
This secure wipe and delete area for file deletion works in two different ways. First, you can work with one file at a time using the single file secure delete or the multiple files. The multiple files area is a drop and drag area that you use your Windows Explorer to drag files to the view area.

Working with a single file, click the browse button and locate the file you wish to securely wipe and delete. Then click the wipe/delete button and you will get a notification letting you

know that this is a permanent deletion and there is no recovery. Once you select yes the file is wiped and securely deleted.



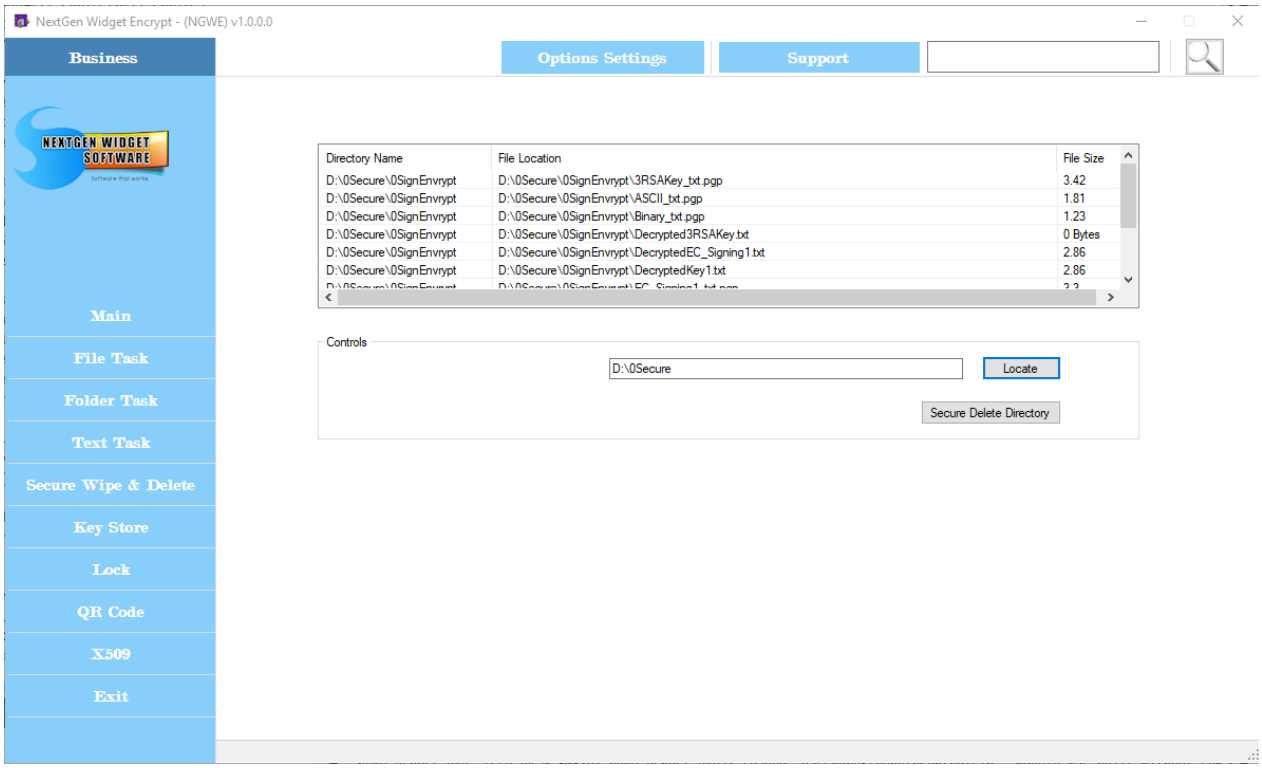




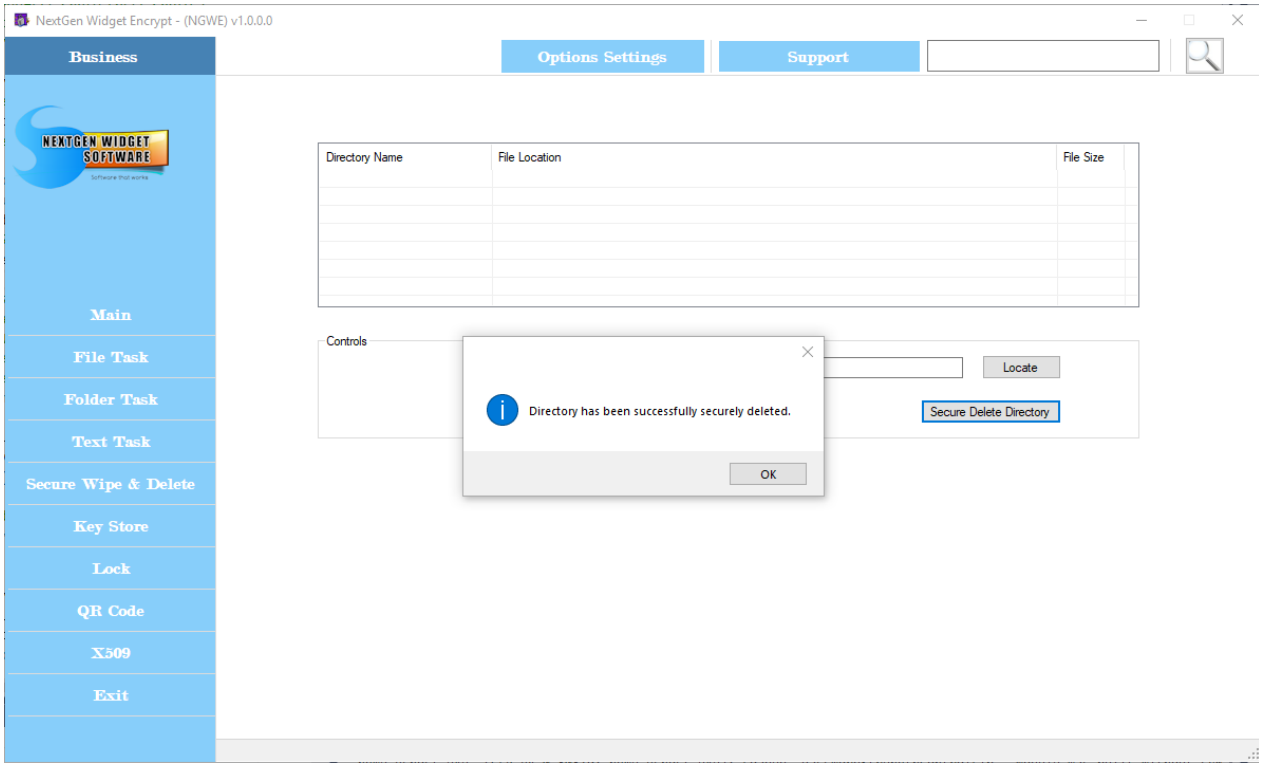
Secure Folders

Securely deleting a folder is simple and easy with NextGen Widget Encrypt. There are really only two buttons to operate this area. One, is the locate button which simply locates the folder you wish to securely delete. The other, is the process button labeled "Secure Delete Directory". The view area only lets you see which files are in the root and subdirectories.

So let's go through the process of securely deleting a folder. I've chosen the directory on my "D:\drive" and as you will notice from the list below, the files are listed along with their file sizes.



From this point you only need to click the "Secure Delete Directory" button and once all the files and directory are securely deleted, you'll receive a notification.



NOTE: There may become times when you will have to elevate the application Privileges to delete some folders. For instance, if you have a external drive that previously belongs to another computer and you connected it via a docking station. You may not have the privileges to securely delete the folder and or content. At that point you only need to right-click on the icon and launch the program as administrator.

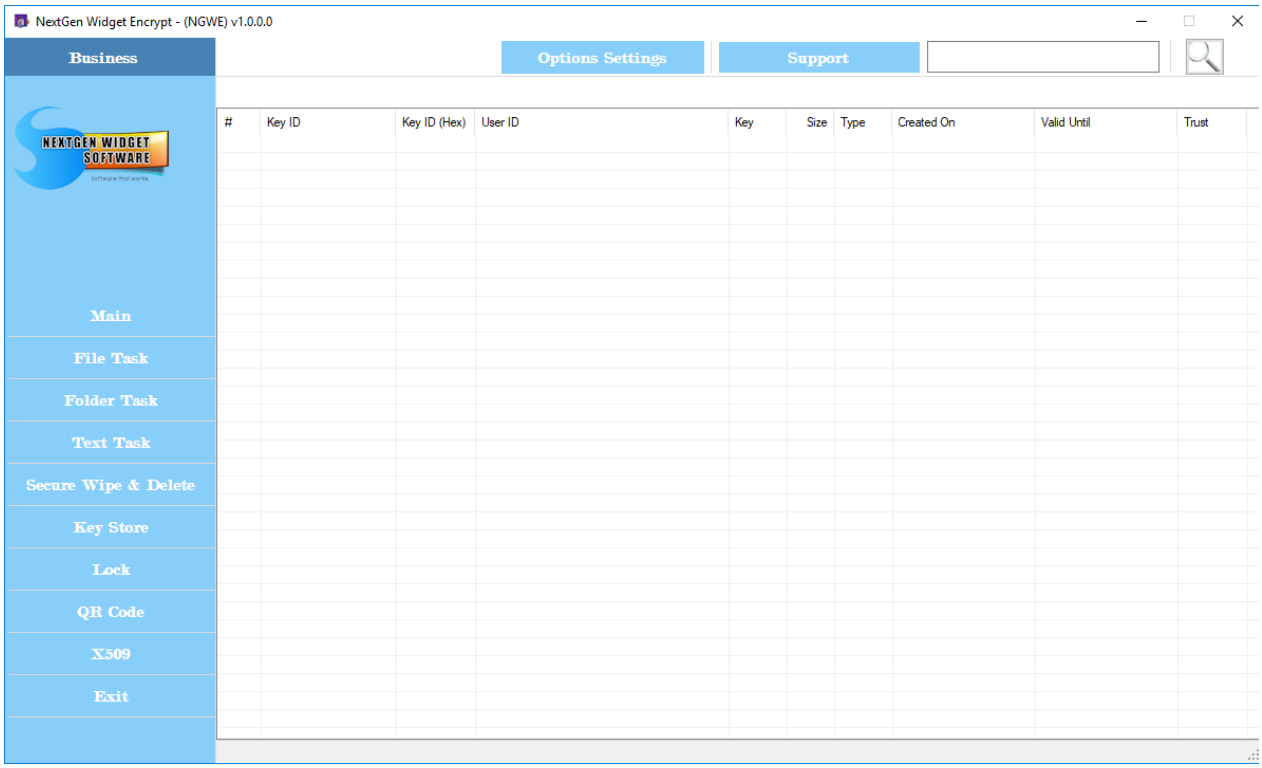
The rule of thumb here is that you have to be the owner of the directory before you can securely delete it.

Key Store

Manage Key Store

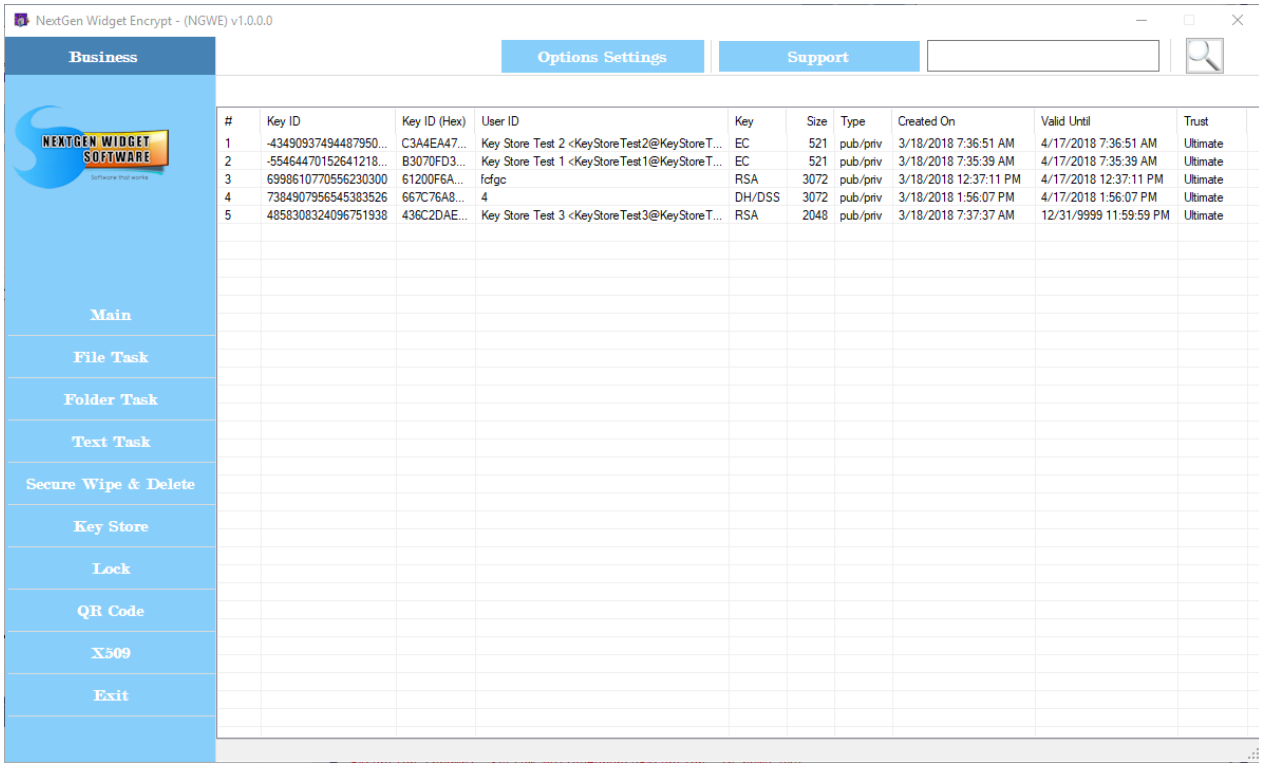
Manage Key Store

Some of this information was already discussed under the "Front door" topic. The Key Store is the viewing and quick management area for all of your OpenPGP keys. Not only can you instantly see all of your keys but, you can actually do some basic management straight from the Key Store itself with a simple right click.

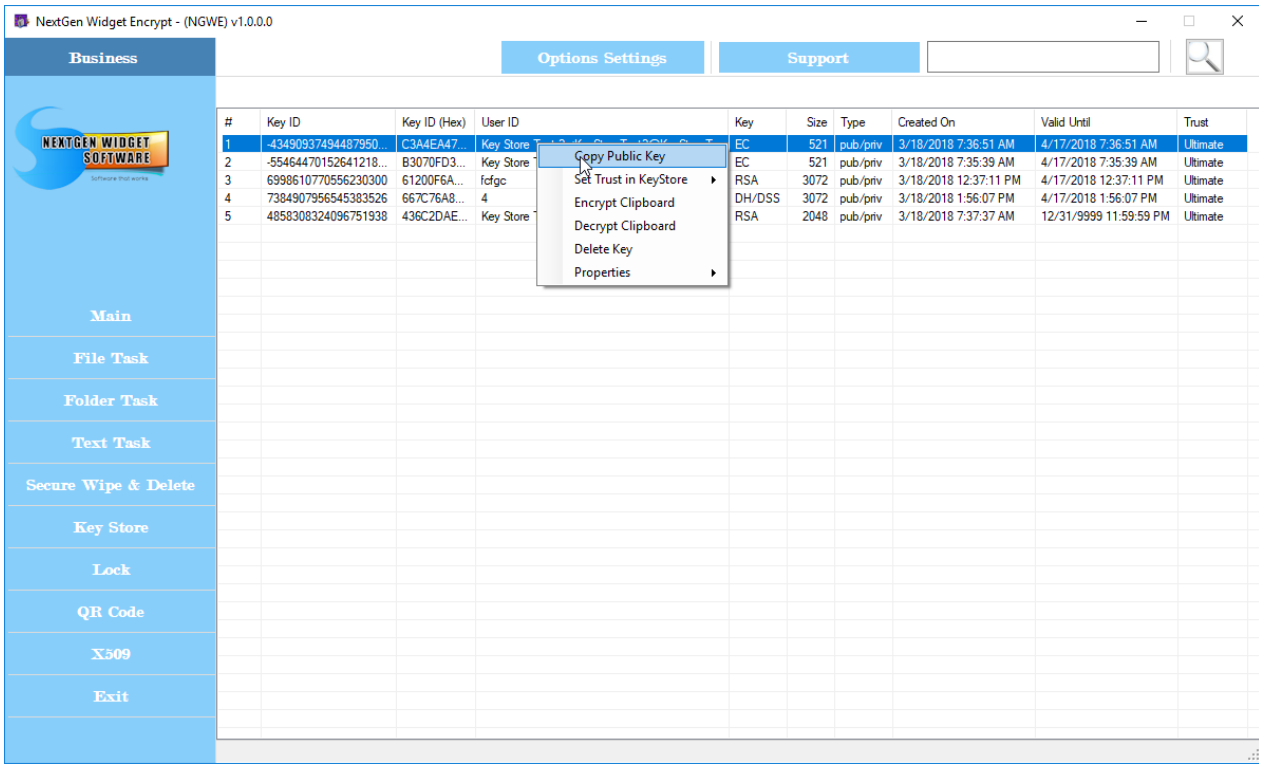


All of the columns should be self-explanatory with the exception of the last column (Trust). This column is used in the web of trust however, it could be used to show just how much trust you have for a particular key. For instance, this key is your best friends key so the trust would be ultimate; unless your best friend a hacker. :-)

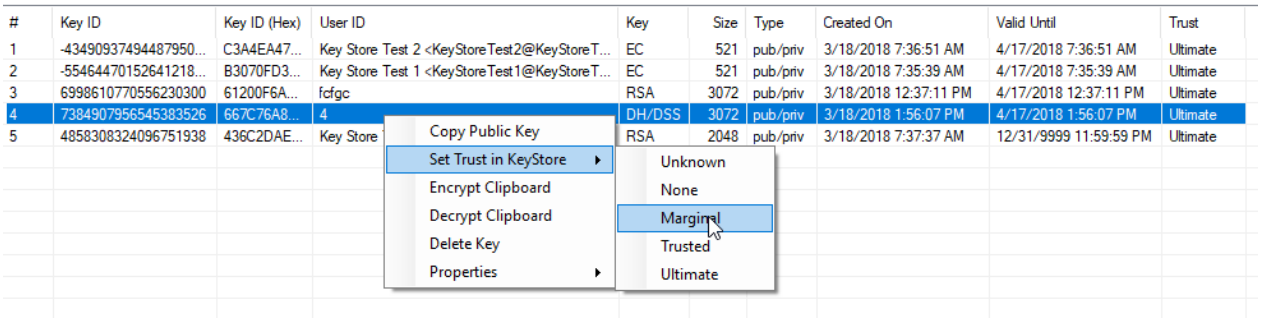
So now that we have a clean slate in our Key Store I'm going to generate a couple of keys.



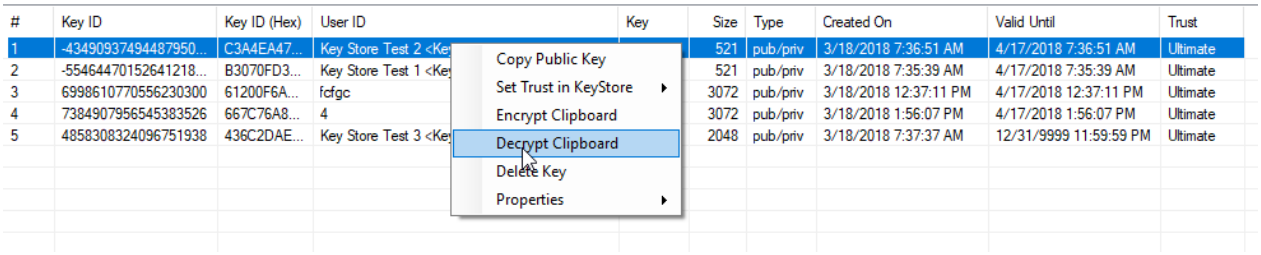
So, we generated a few keys and now we want one of the public keys.

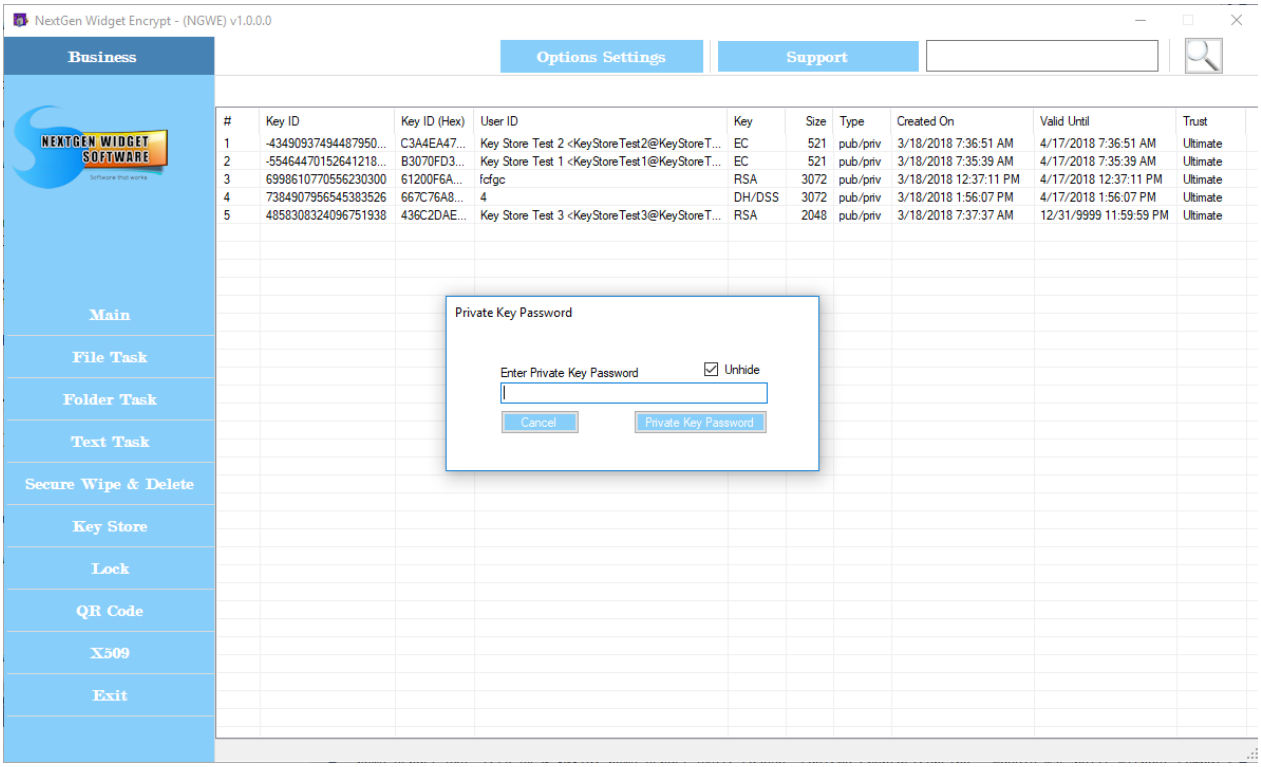


The Key Store has a right click menu that permits access to the public key, setting trust, encrypting text context on the clipboard, decrypting text on the clipboard, deleting keys and checking the fingerprint. All of the keys that you generate have a trust of ultimate. If you get a key from someone who is less trusted, you can set the trust to unknown, none, marginal, trusted and of course ultimate.

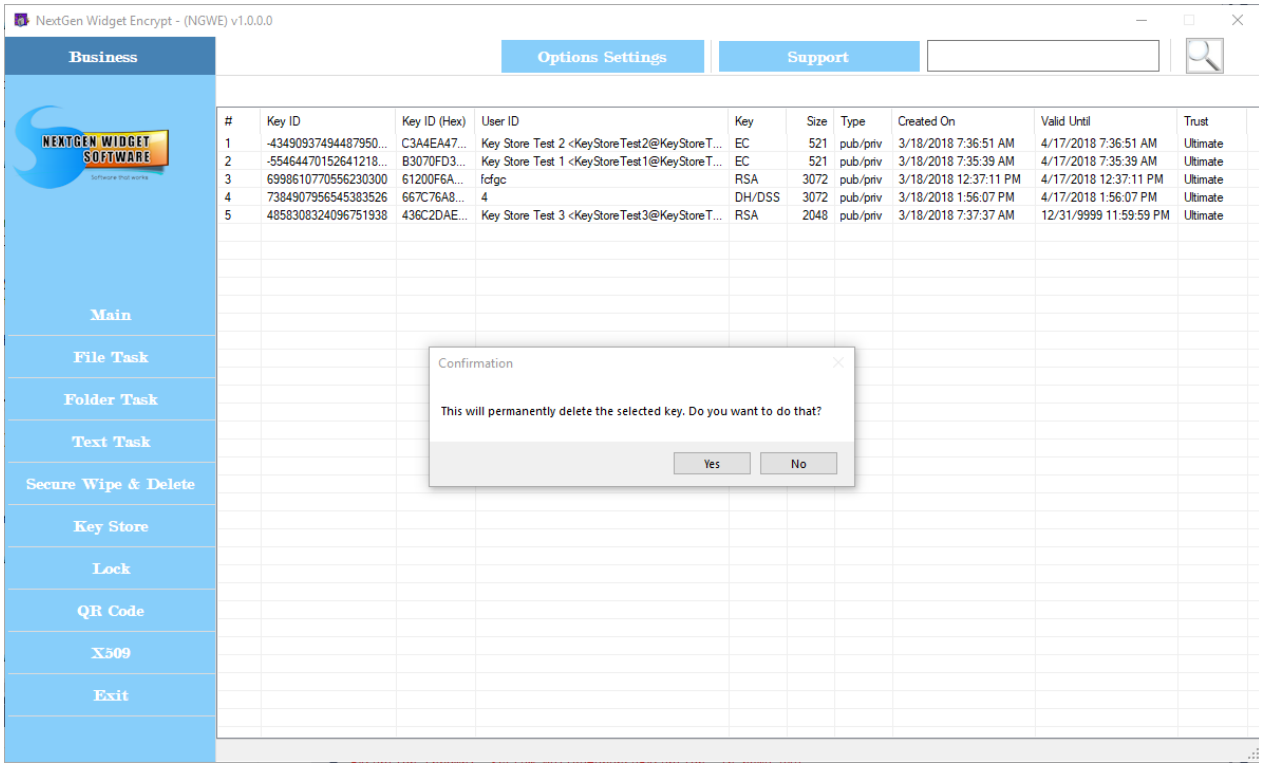


Decrypting the text is just as easy and you only need to copy the encrypted text from "-----BEGIN PGP MESSAGE-----" to "-----END PGP MESSAGE-----" with everything else in between. Select the private key that this cryptic text was meant for and right click, select "Decrypt Clipboard" and enter the private key password, then paste the unencrypted text to an email or document. Images below.



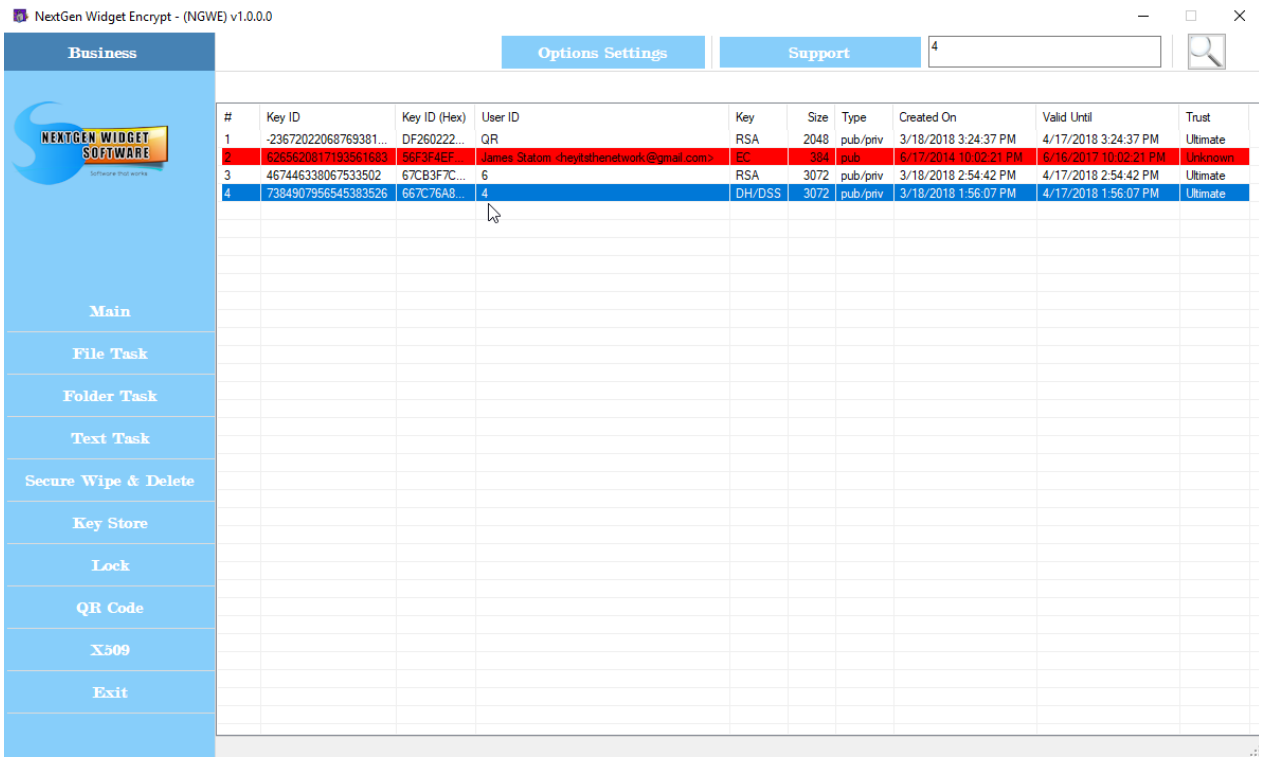


Deleting keys works pretty much the same way as the trash key area does. With the exception, you can only delete one key at a time. You'll receive a message letting you know that the key would be permanently deleted; no back door.



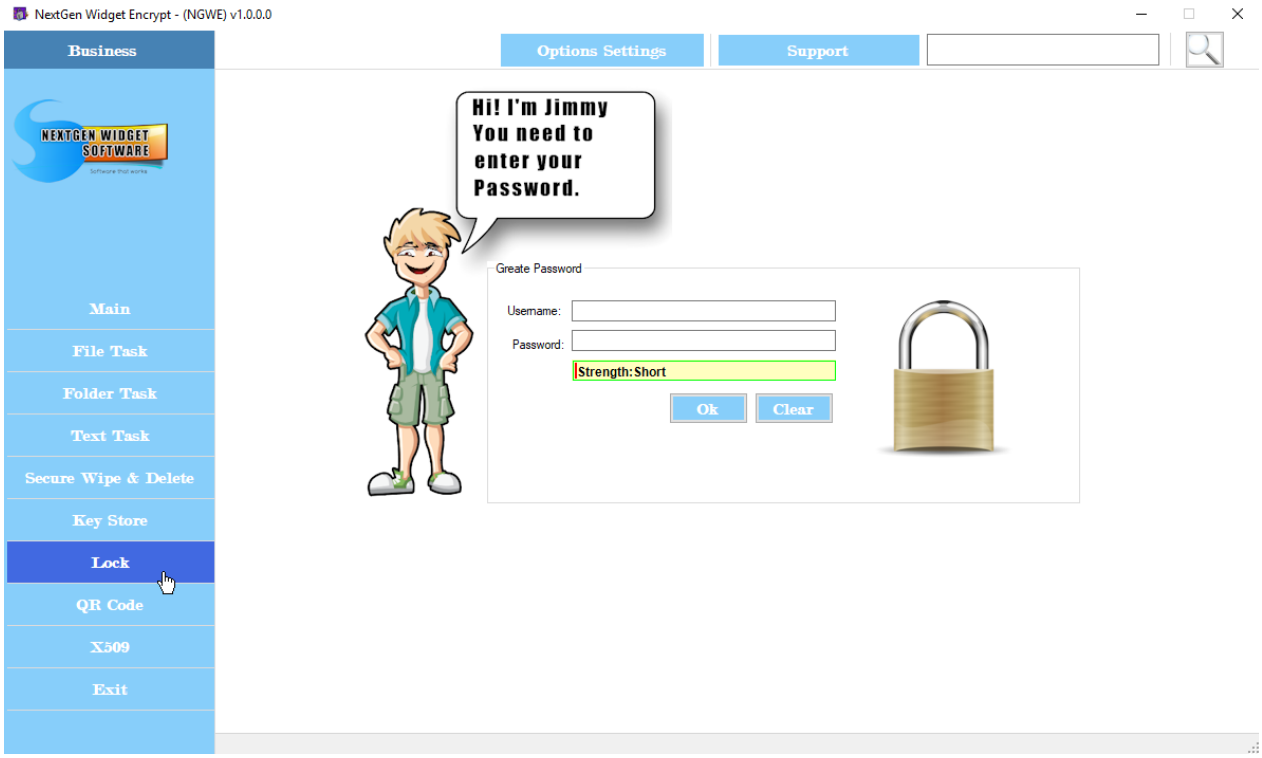
If a key becomes revoked or expired, the row that key is on will become red for revoked keys. Also, you will not be able to utilize that key for encryption. Expired keys will turn yellow but are still usable.

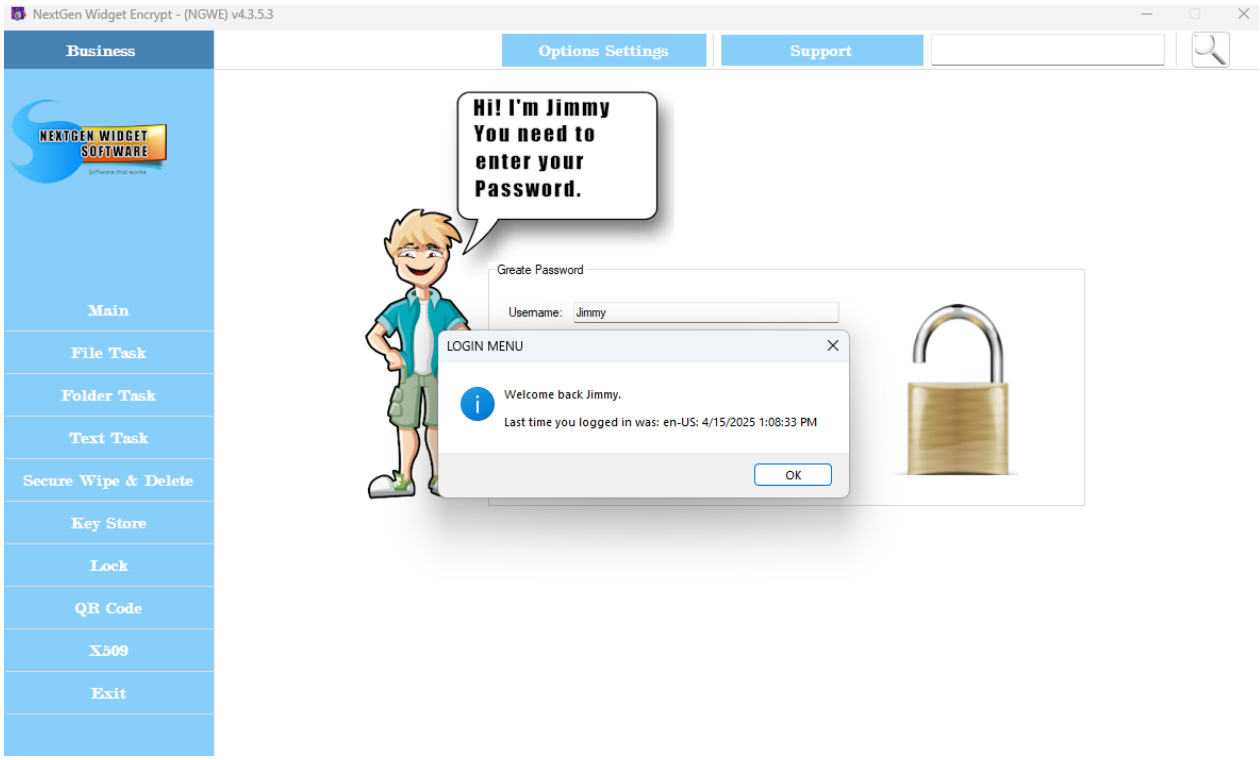
When you search for a key, you will receive a message telling you that the key has been found and the letters will turn light green and the row will be selected and blue. Searching for a key uses the "User ID" section but your description must be exact. If there are multiple User ID's with the same name, the program will select just one of them and will not rotate to the others.

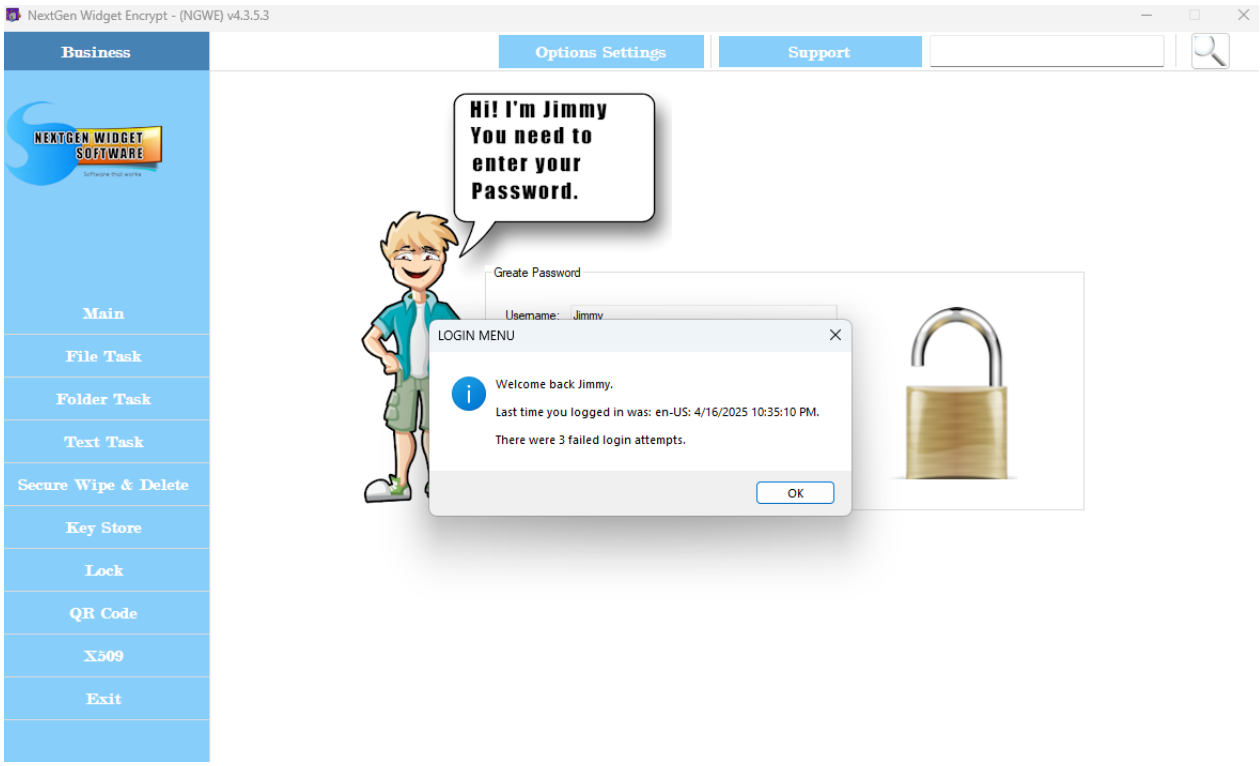


Lock

The idea of locking the program is that if you have to step away from the program you should aways close it or lock it. By closing the program you will get a count of how many tries there were utilized to try to access the program. Upon three failed attempts the program was shut down.




NextGen Widget Encrypt - (NGWE) v4.3.5.3
Business
Options Settings
Support
NEXTGEN WIDGET SOFTWARE
Main
File Task
Folder Task
Text Task
Secure Wipe & Delete
Key Store
Lock
QR Code
X509
Exit
Hi! I'm Jimmy
You need to
enter your
Password.
Greate Password
Username:
Jimmy
LOGIN MENU
Welcome back Jimmy.
Last time you logged in was: en-US: 4/15/2025 1:08:33 PM
OK

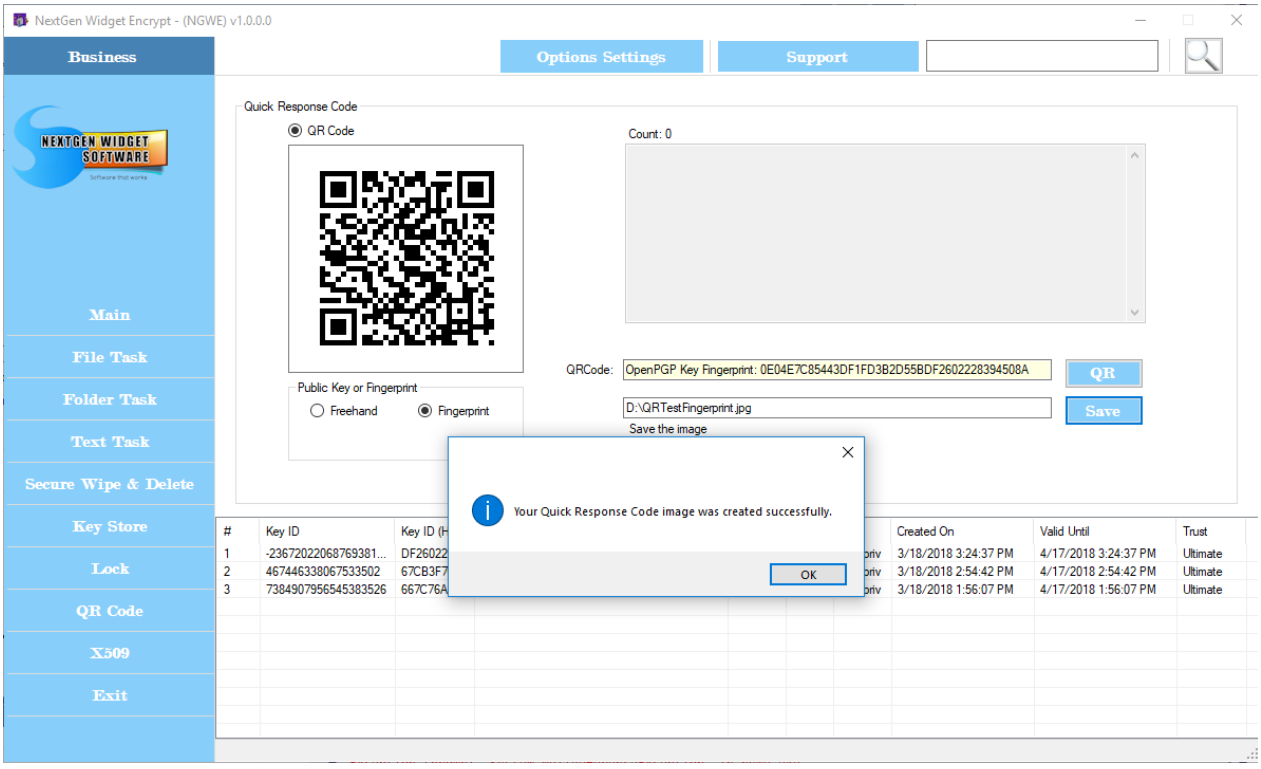

NextGen Widget Encrypt - (NGWE) v4.3.5.3
Business
Options Settings
Support
NEXTGEN WIDGET SOFTWARE
Main
File Task
Folder Task
Text Task
Secure Wipe & Delete
Key Store
Lock
QR Code
X509
Exit
Hi! I'm Jimmy
You need to
enter your
Password.
Greate Password
Username:
Jimmy
LOGIN MENU
Welcome back Jimmy.
Last time you logged in was: en-US: 4/16/2025 10:35:10 PM.
There were 3 failed login attempts.
OK

QR Code

QR Code
Create QR codes for your public key and/or private message.

QR Code

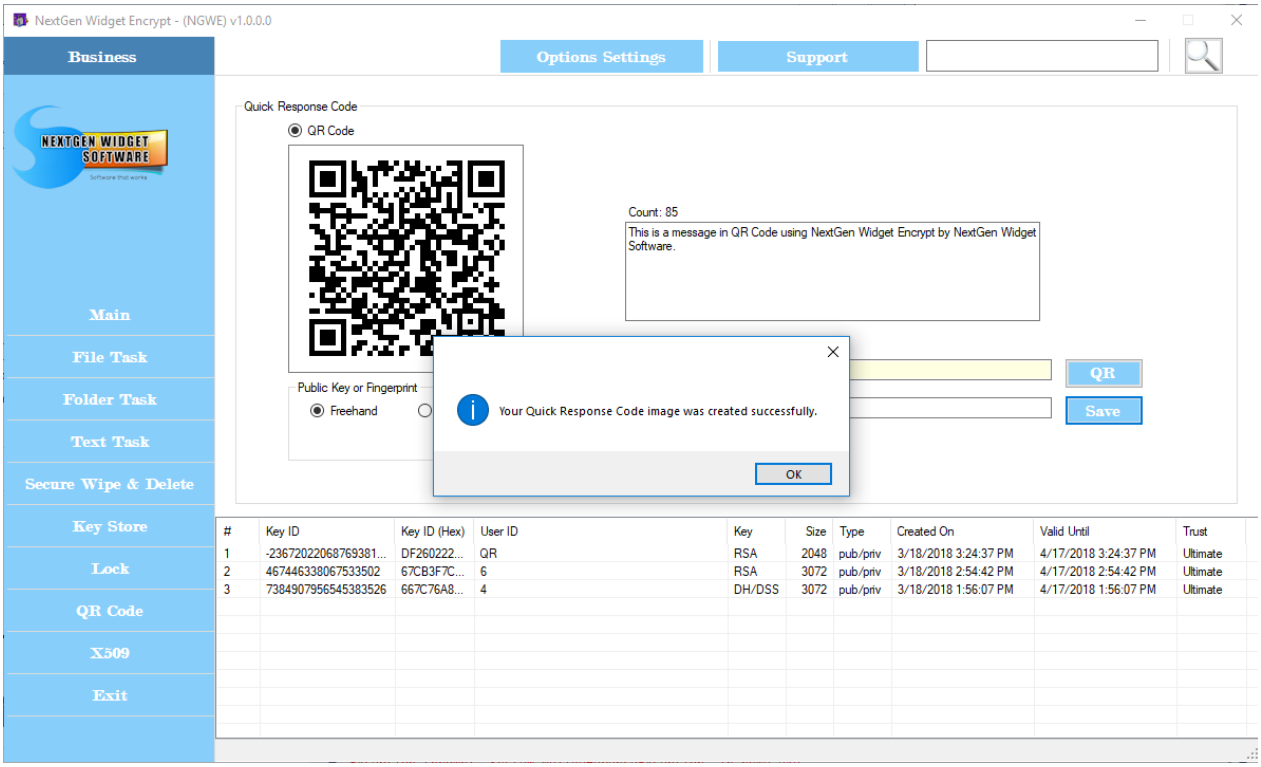
The "QR" area creates QR code for use with smart phones. The QR code can embed a public key fingerprint and the ability to add your own text to the QR code. First, let's add a fingerprint to our QR code. Right click on the key that you would like to embed in the QR code and click "Select User-ID". You'll notice that the fingerprint is generated to the QR code text area. Click the "QR" button which generates the image in the QR square and from this point, simply click the "Save" button, locate the directory you wish to save the file to, name it and click save.



You now have a saved image of your QR code. Use your smart phone to verify the fingerprint. QR code freehand gives you the ability to enter your own text. It works the same way as the fingerprint, simply type your message, click the QR button, click the save button, locate the folder you wish to save the image to, name it, click save. You're done.

The QR code image can be saved in four different formats; PNG, JPEG, BMP and GIF and

freehand as a character limitation of 196.



X509

X.509 (International Telecommunication Union (ITU) standard) is primarily used to bind the identity to a person, organization or service and to an public-key which uses a digital signature. Although this program offers X.509 it is not primarily a feature of OpenPGP.It is just an added feature to the NexGen widget encryption software for user convenience.

However, OpenPGP is able to use the certificate but it may not look the way you want it to look in the OpenPGP Key Store but it will still work. Once again, is just an added feature that you can use but it is not part of the OpenPGP project so this is as is, I will make every attempt to remedy any issues that may be found but no guaranty.

X509 Generator

X509 Encryption

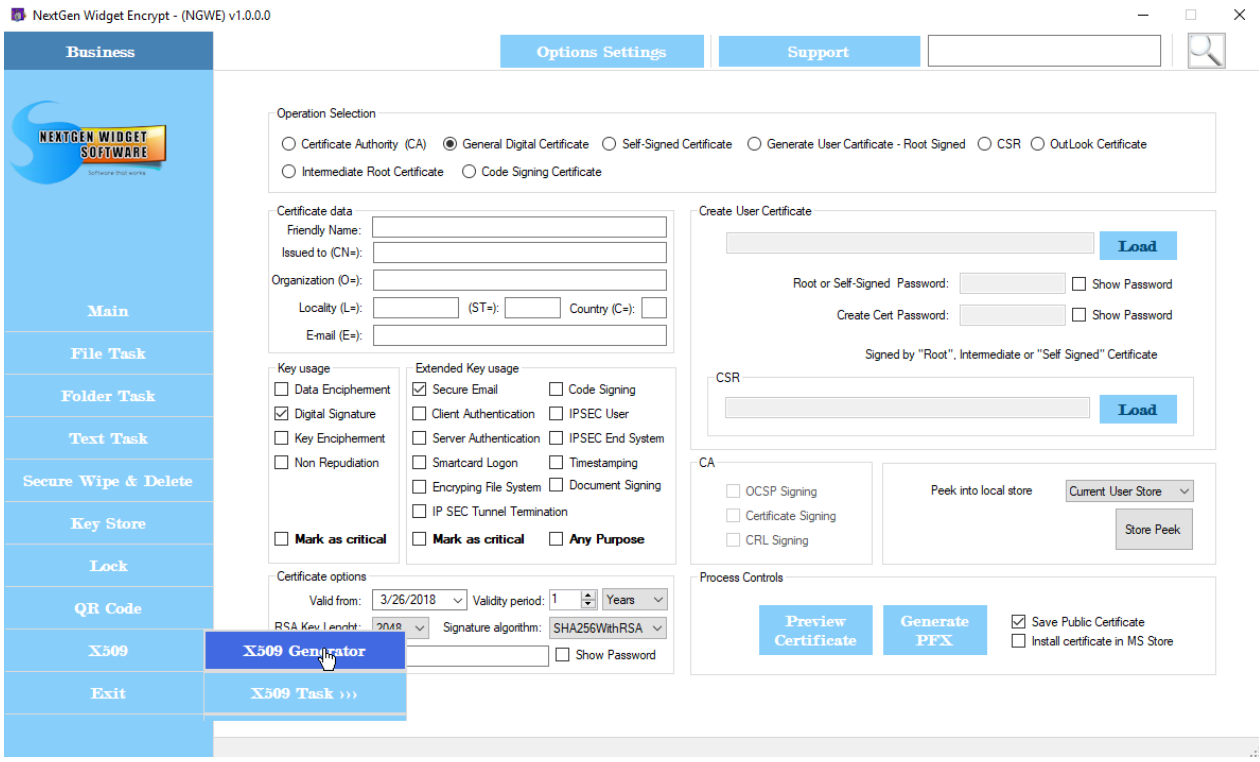
X509 Decryption

X509 Generator

The X.509 area has many functionalities and the ability to create a certificate authority, general digital certificate, self signed certificate, using certificate signed by the root, intermediate root certificate, Outlook certificate and code signing certificate. Also, you can generate a CSR and create a certificate from that.

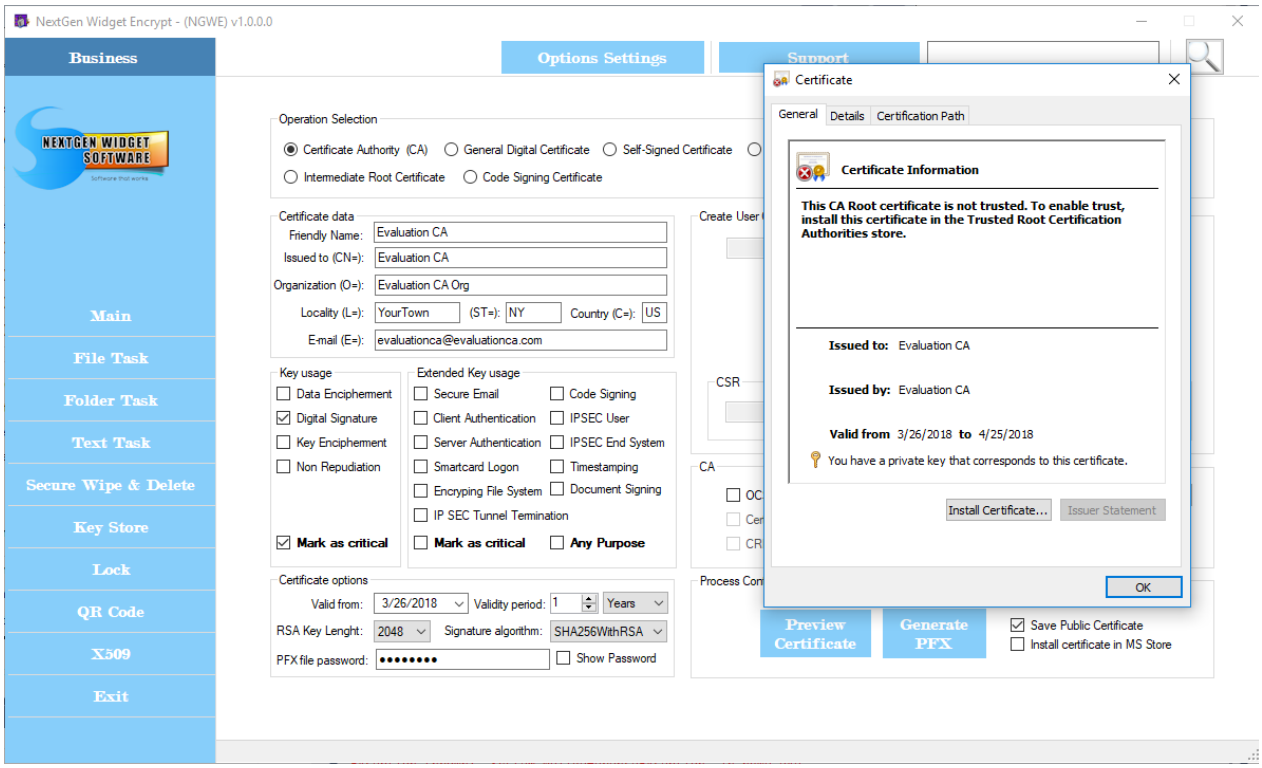
Each time you select a radio box, default key usage is automatically selected. Of course, you can select additional key usage or just create a certificate for any purpose. The only restriction to the certificate is that any key generated in the evaluation version is limited to 30 days.

NOTE: By the way, the root certificate for NextGen Widget Software is embedded in the program. If you don't want to see notices that may keep popping up saying the program is unknown etc. Just install NextGen Widget Software certificate into your root certificate store.

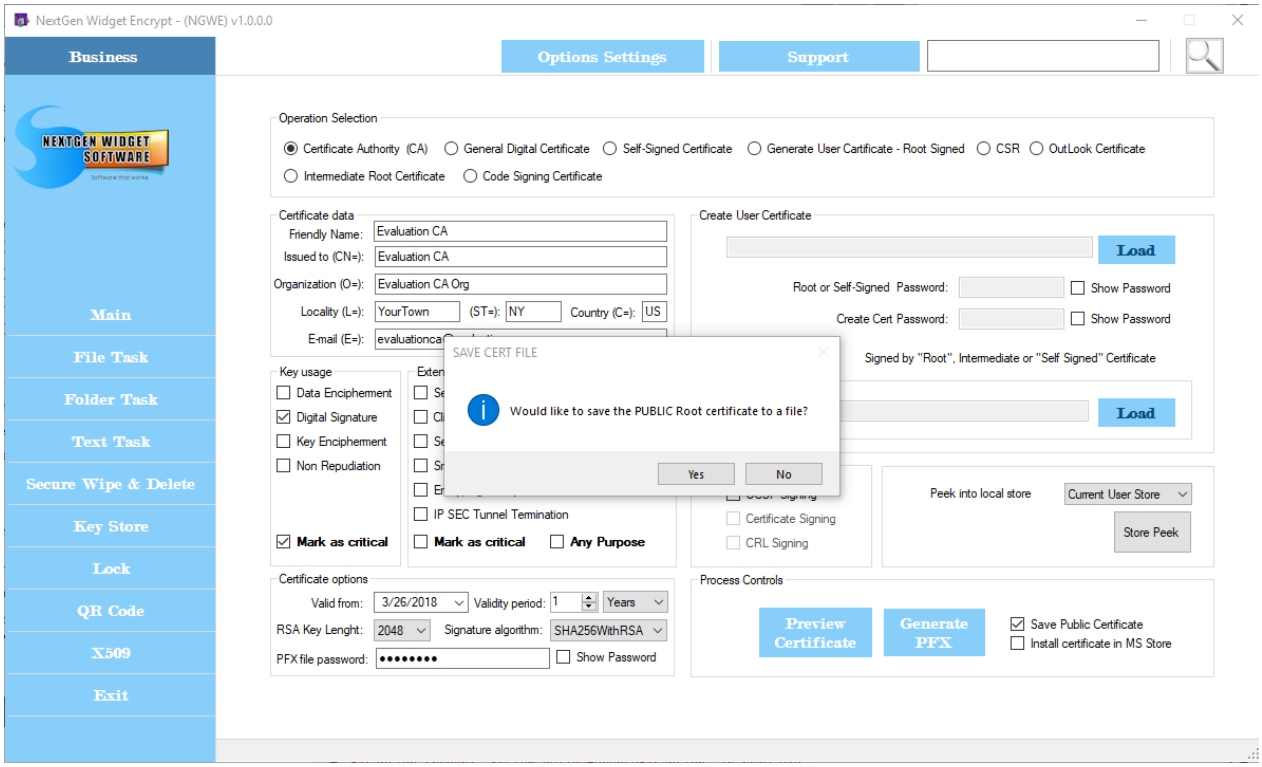


Let's go ahead and start by generating a certificate authority. Select Certificate Authority (CA) radio button and the usage automatically selects the digital signature and marks the key as critical. Now, the mandatory field is the (CN), but I'm going to fill out most everything here and I'm going to leave the certificate options as default. Now I'm going to enter a password. This should be a very complex passphrase and you will need to secure your certificate.

Once you've entered all of the necessary information you can choose to view the certificate before generating it by clicking the "View Certificate" button.



Since the certificate looks good, I'm going to click the "Generate PFX" button and I'm making sure that the "Save Public Certificate" checkbox is checked. After you click the "Generate PFX" button a browser pops up so you can save the certificate to whatever location you desire. Then, you are given the opportunity to save the public key as well.

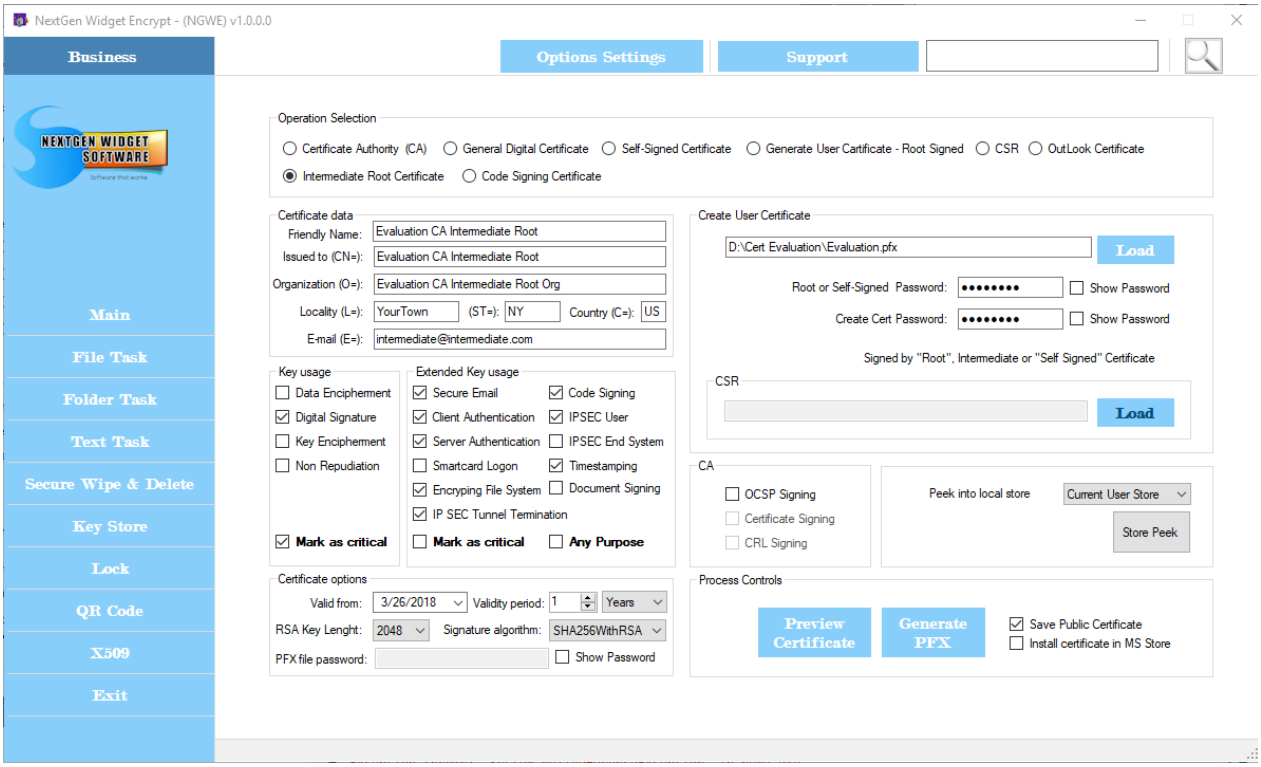


I'm selecting yes because I want a public root certificate. Once you select yes, another browser pops up so that you can save the certificate to a designated location. Now, you'll have both certificates saved in a particular area. What you'll need to do from this point is install the public root certificate into your key store or install the public search into your

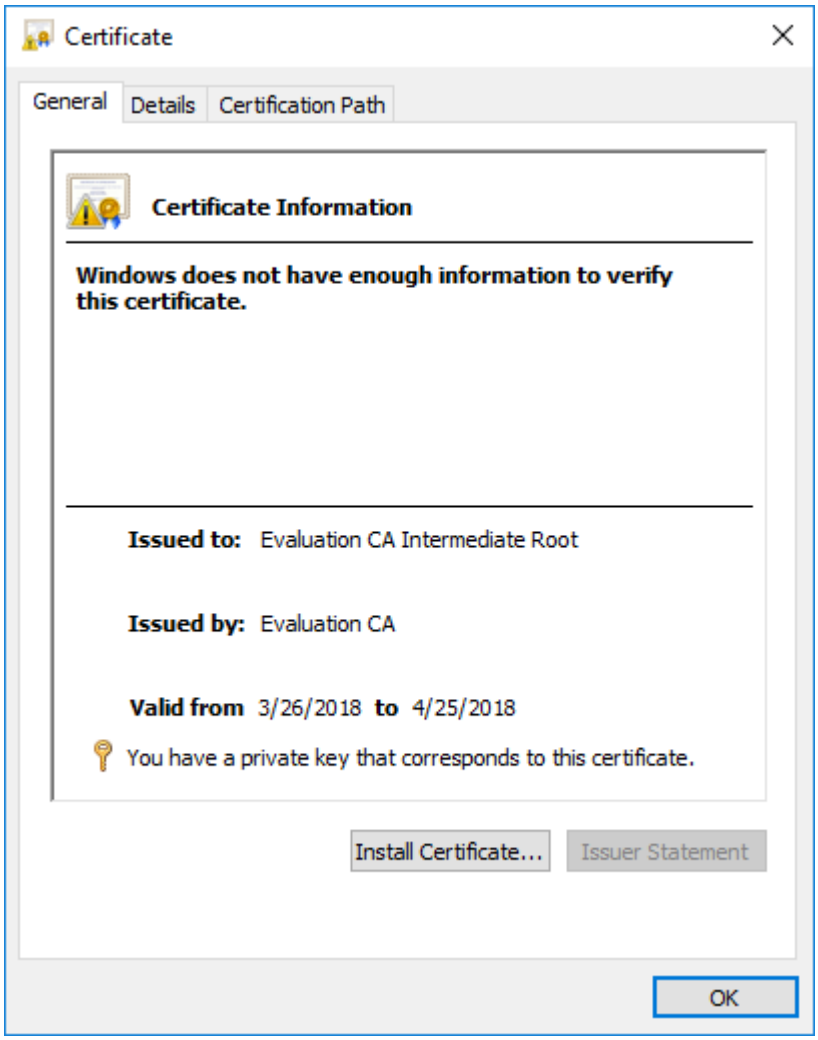
users key store.

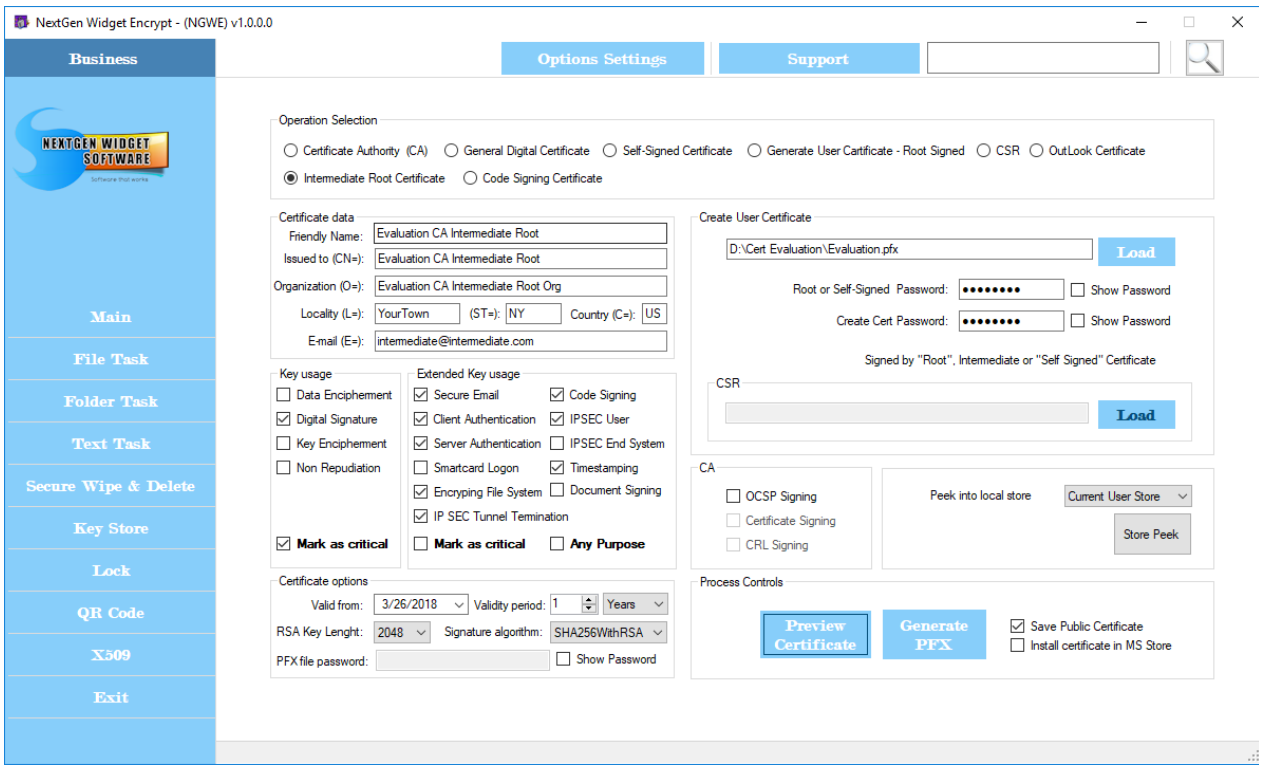
Some certificate authorities using an intermediate root certificate. This way, they can simply put the master root certificate away in a lockbox secure location and utilize the intermediate root certificate. Let's click on the "Intermediate Root Certificate" radio button and you'll notice that the key usage changes. Now, once you've entered the certificate data you will now utilize the right side of the program in the create user certificate area. You'll notice that the load button becomes active and the password text boxes also become active.

Now, click the load button and locate the private key for the root certificate that we just created. Enter that passphrase and also the passphrase for the new intermediate certificate we are about to create.

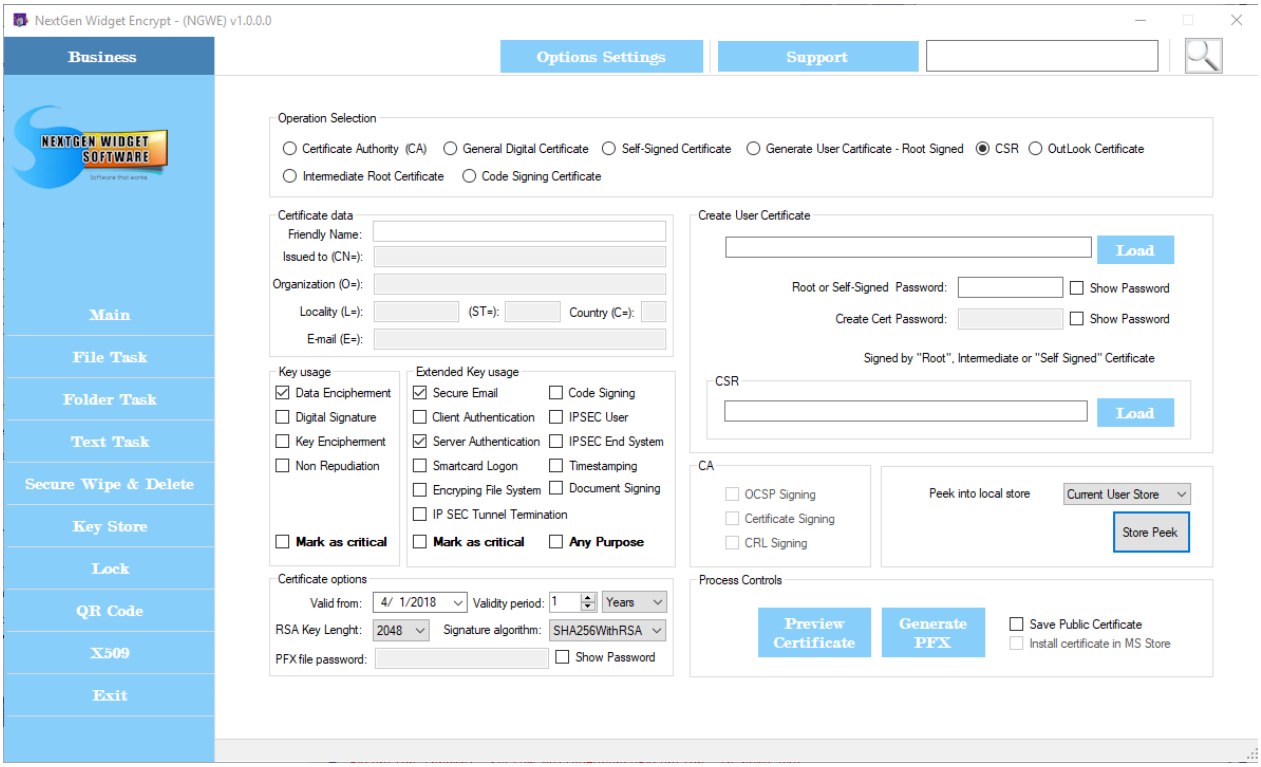


Click the "Generate PFX" and once again make sure that "Save Public Certificate" checkbox is checked. If you view the certificate first you will notice that the issued by is your root certificate and the issued to is the intermediate root.





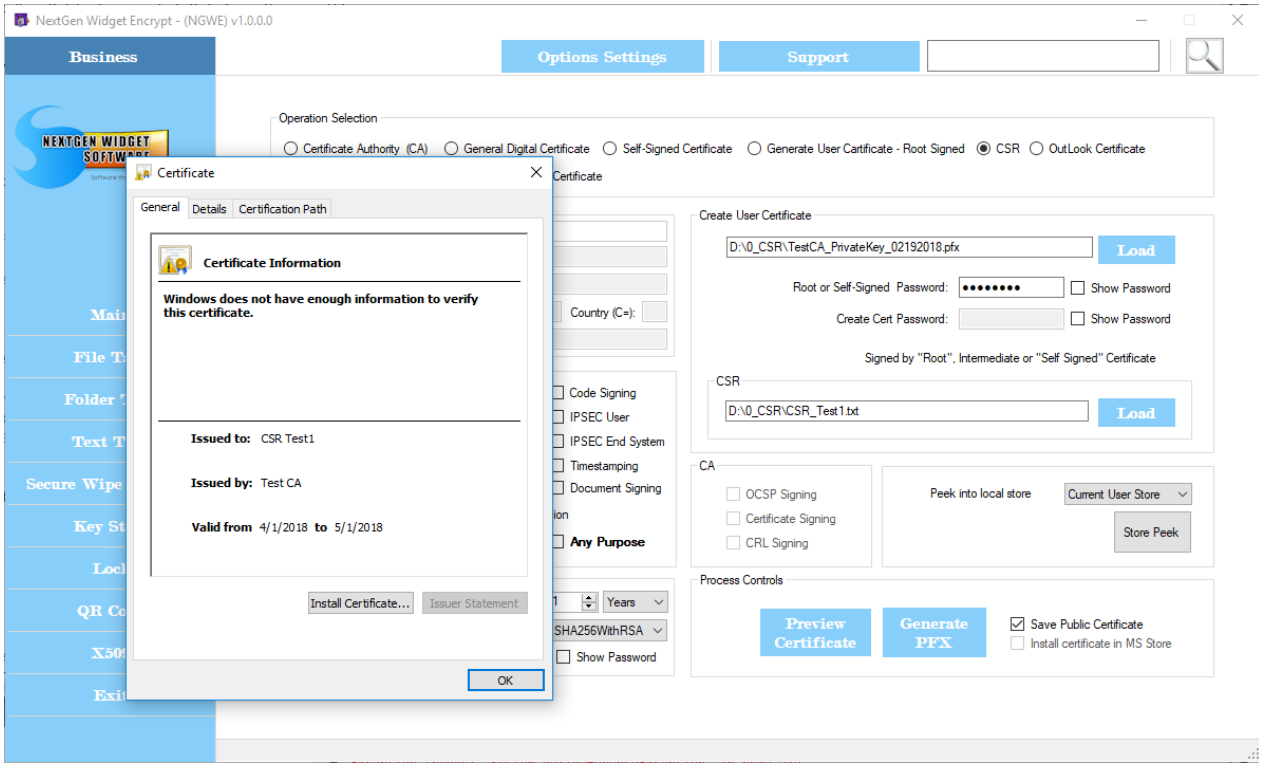
NextGen Widget Encrypt is a great program for creating certificates from a certificate signing request (CSR).



NextGen Widget Encrypt is a great program for creating certificates from a certificate signing request (CSR). Generate the certificate signing requests from your device or server and save it as a text file. Press the "Load" button and locate the certificate signing request text file.

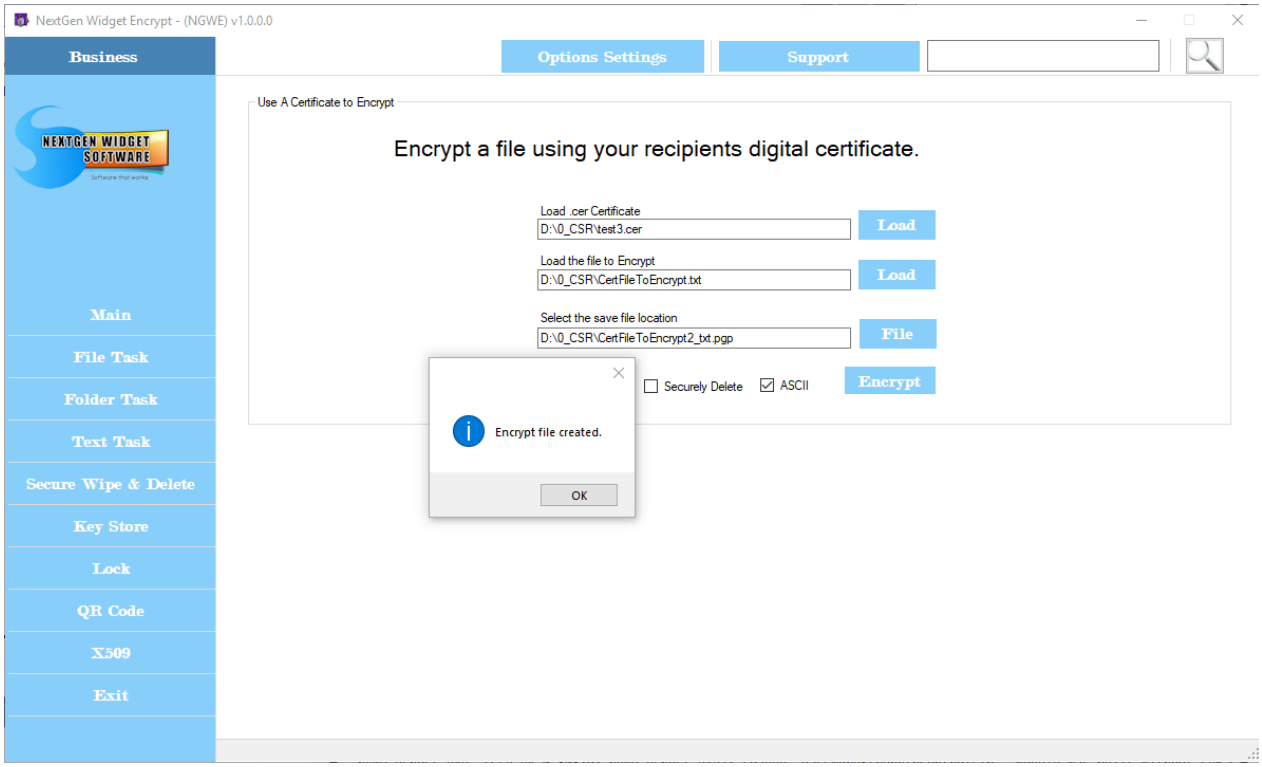
Next, simply load the roots signing certificate and enter the password for the root certificate. Now, click the key usage checkboxes that apply and click the "Save Public Certificate" checkbox.

Lastly, click the "Generate PFX" button and save the private key to a folder as well as the public key.



X509 Encryption

NextGen Widget Encrypt can easily be used to encrypt files using an X.509 certificate. Simply load the certificate, file to encrypt and save to a location. In our example ASCII is selected by default so that's what we'll use. After I click the "Encrypt" button, the file is encrypted and the extension is added to the file name so that you know what type of extension the file was before encryption.

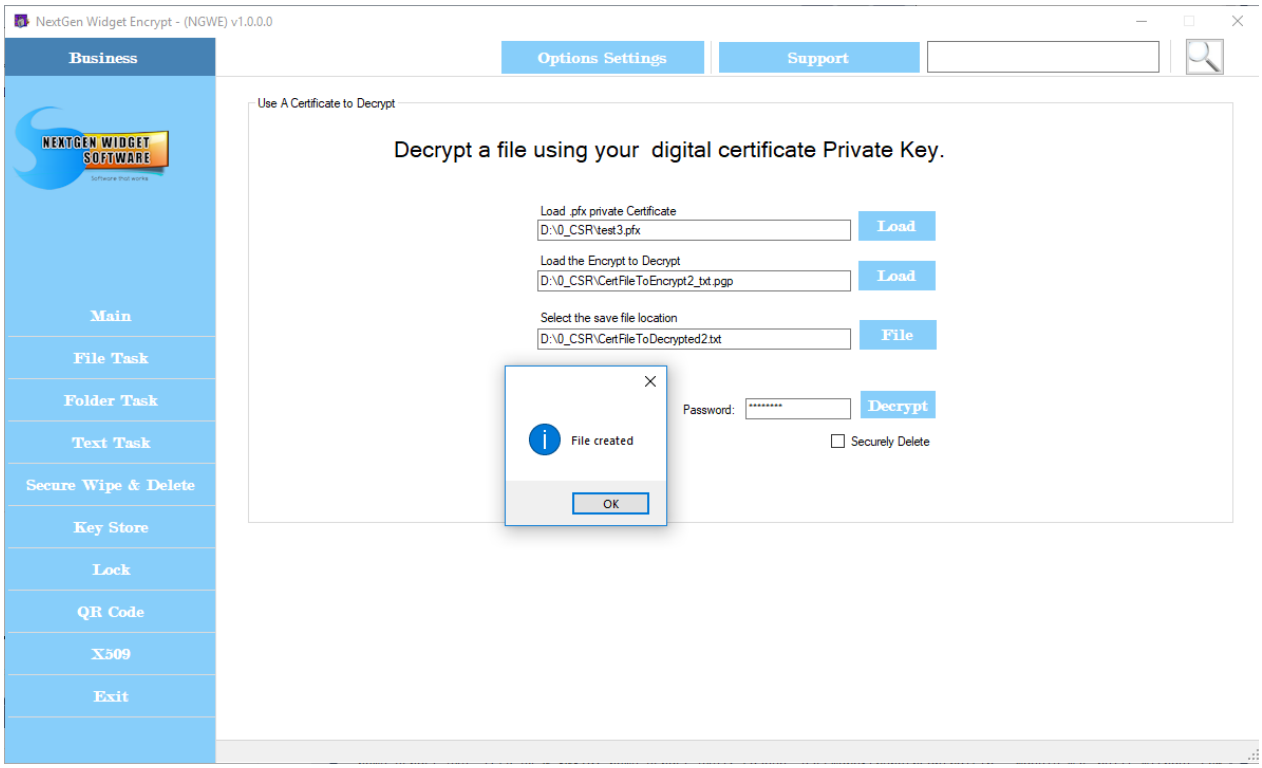



```
-----BEGIN PGP MESSAGE-----
Version: NextGen Widget Software (NGWE) v1.0.0.0

hQEMAx4rGrW958oIAQgAjngHa2sEDk6ZrFxoHIDG3Dfp3ONWM5yBwAM+74M/ukun
VhZ801N1zIqsSoUuyTB0HyzzqCaXCvsBTMKp3+LAboKLWX1QXESBi/xhAJHhU0TV
hz4suGeqCOOoe/4IFp7gU3ij/zbUtdBgE4he/pNiSVlBbej2Xw1kh856+PkKwRhO
GFHyciAT37bLW0v9oKg3F30K+Sv5NWUuy8NIX+a+R/VGNG94YKDog6oZr0583HRs
Ta+x/d5/dT49hi6kAYpi/Zsg9Qzsm67TGqa0/YCd1DXngf+VL5bAuWKzrvVf5tQ7
jYxI8HLeQpDRiipx82WNHEb0MRrIr/7ge1H7r537Kck3hOi2auDQc72W1V/RmmGj
N6AA5RGRpqeNTvepgbUvB3FTDd9lpVBPEZc1H0IVPXhW7SbhxOc0XQ==
=ibeX
-----END PGP MESSAGE-----
```

X509 Decryption

NextGen Widget Encrypt can easily be used in the decryption of files using an X.509 certificate. Load the private key (PFX), the encrypted file and select the save file location; name your file and give it the proper extension. Now we simply need to enter the private key password. Also, you can choose to securely delete the encrypted file if need be.

Once you're ready, click the "Decrypt" button and were all done.



Settings

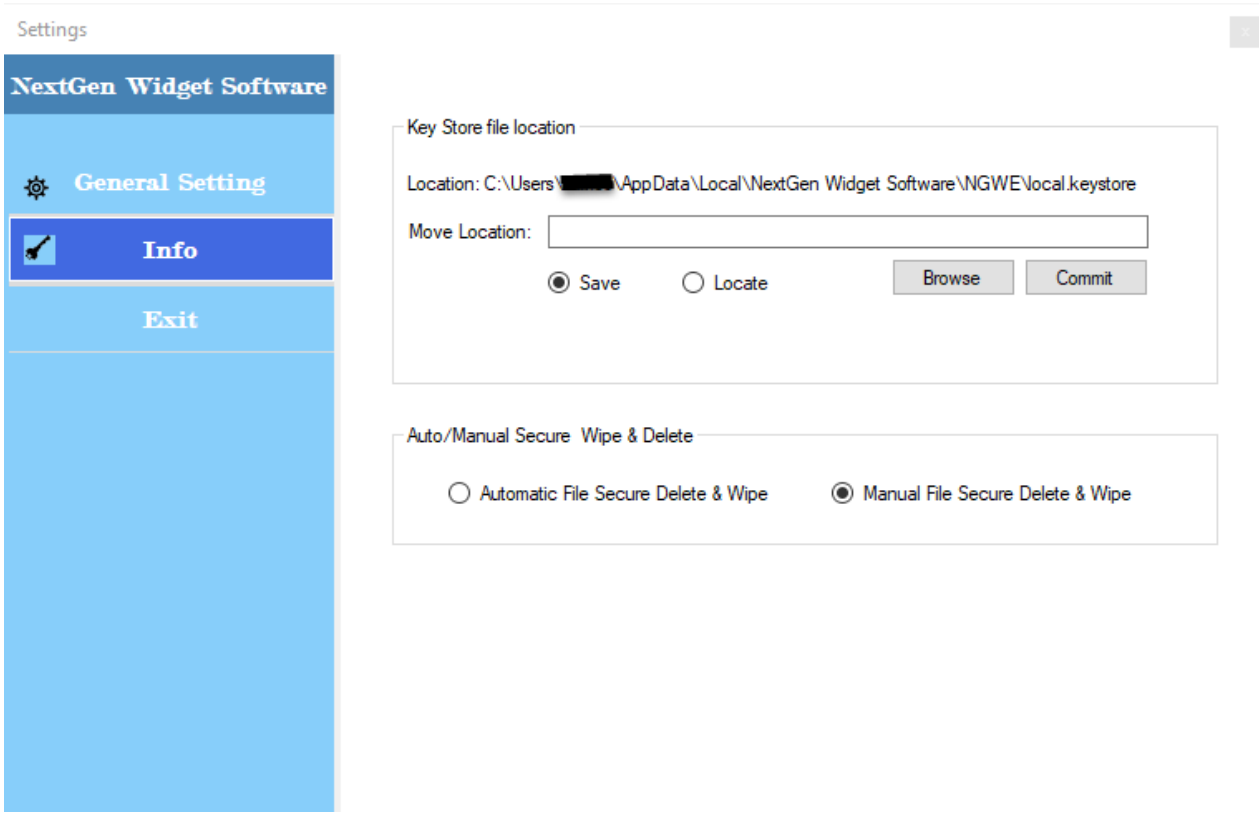
[General Setting]

[Info]

General Setting

The general settings area is very simple and accessible by the options settings button. General settings gives you the ability to move your key store from one location to the another. This move is relatively simple just click which operation you want to do. The save radio button gives you the ability to save your key store in a different location. It moves the key store from one location to the other and does not save it in the previous location.

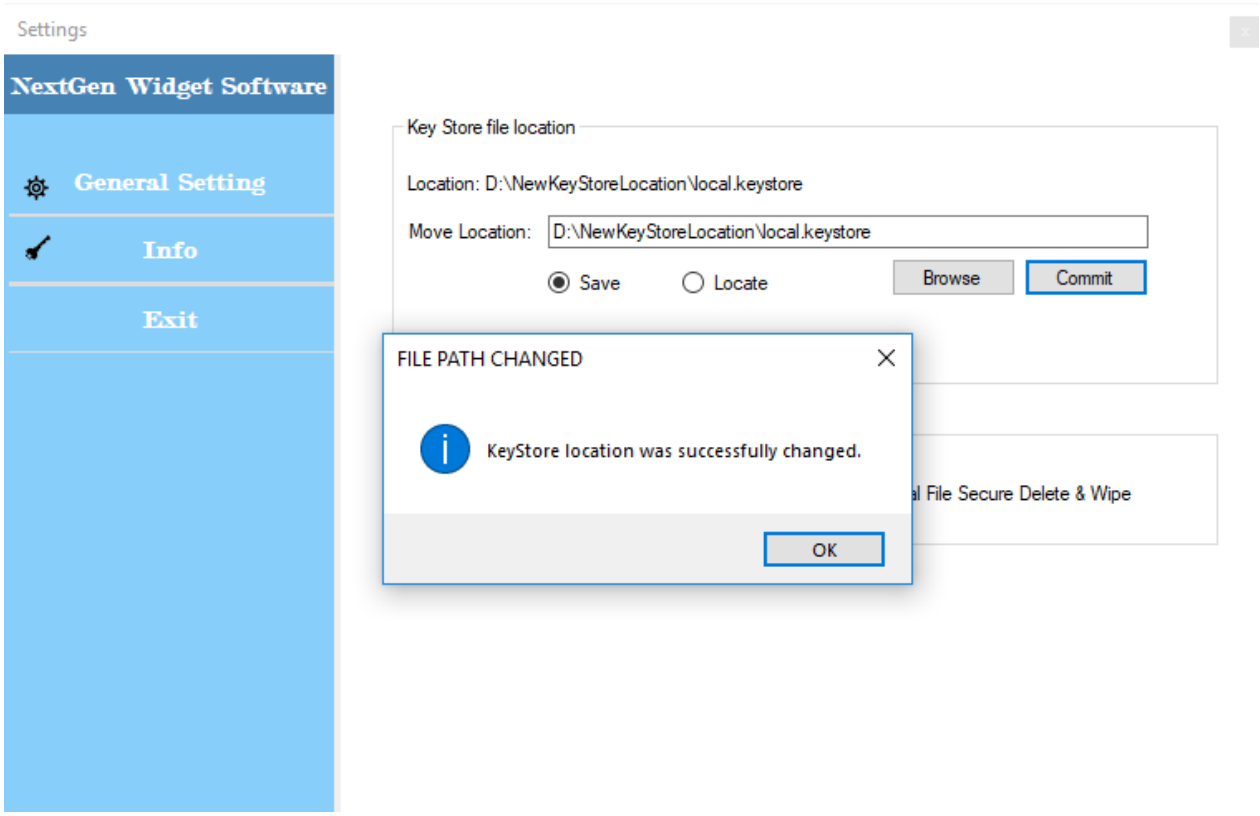
The locate radio button gives you the ability to locate your key store and save the current location. For instance, if you moved your key store you will need to locate it and commit the changes. The default location for "NextGen Widget Encrypt" is your local application data directory. This directory is created upon install of the program.



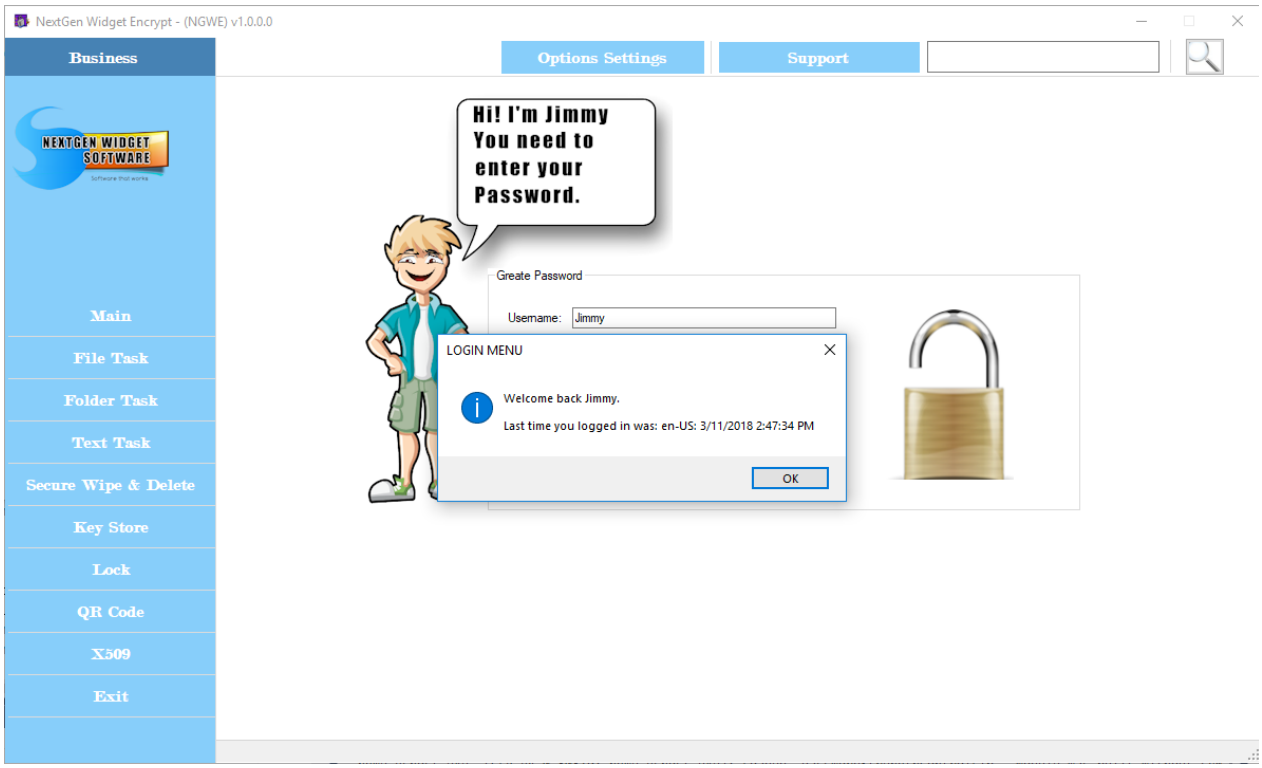
There is one of the function currently that the general settings has. That's the ability to automatically securely delete the original files once you've encrypted them. Not really recommended and should be done on a case-by-case basis in the function included with each file encryption or decryption.

Decryption you have the option to securely delete the encrypted file once the original is created from the encrypted file.

Moving the file to a different location:



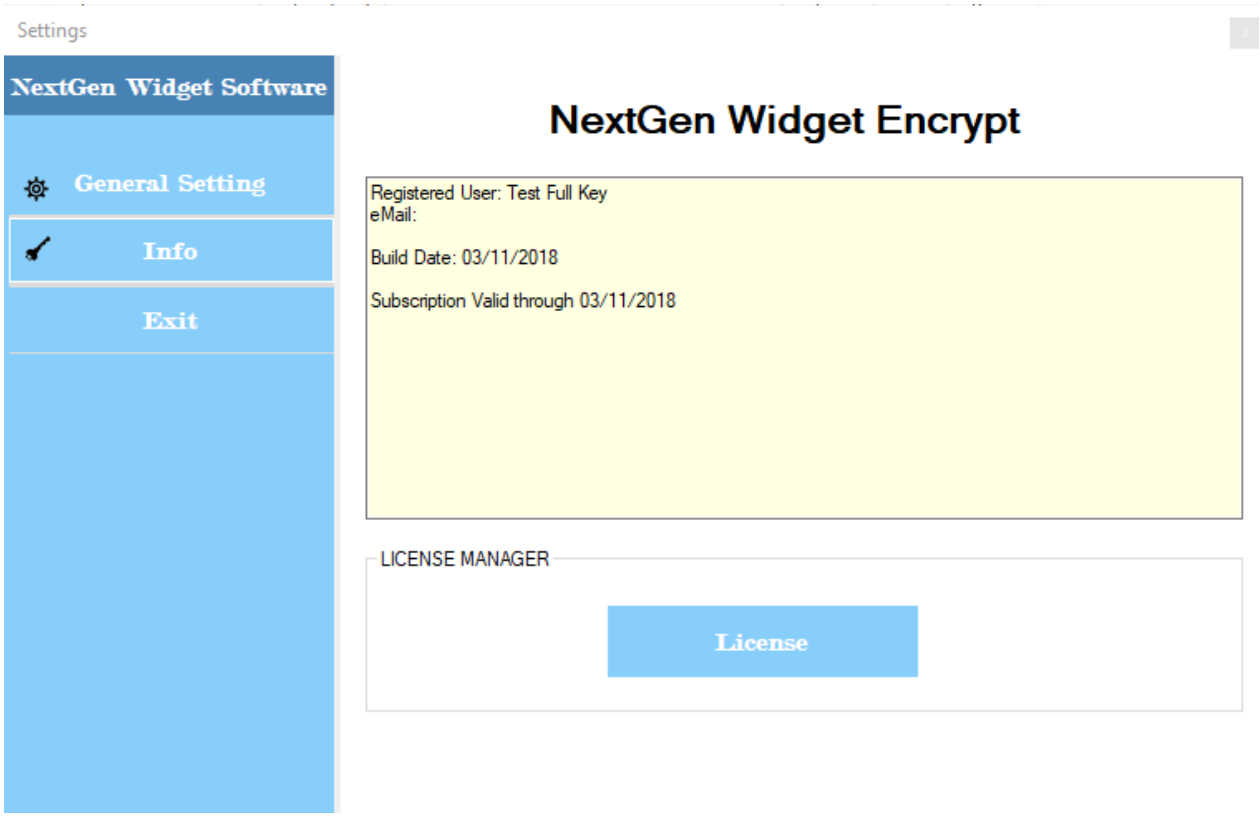
Make sure the save radio button is checked. Click browse, select your new location, click Commit and you're done. No location will be listed in the label and you will get a notice that the change was successful. Close and you can test by locking the program from the program menu click on "Lock" and log back in.



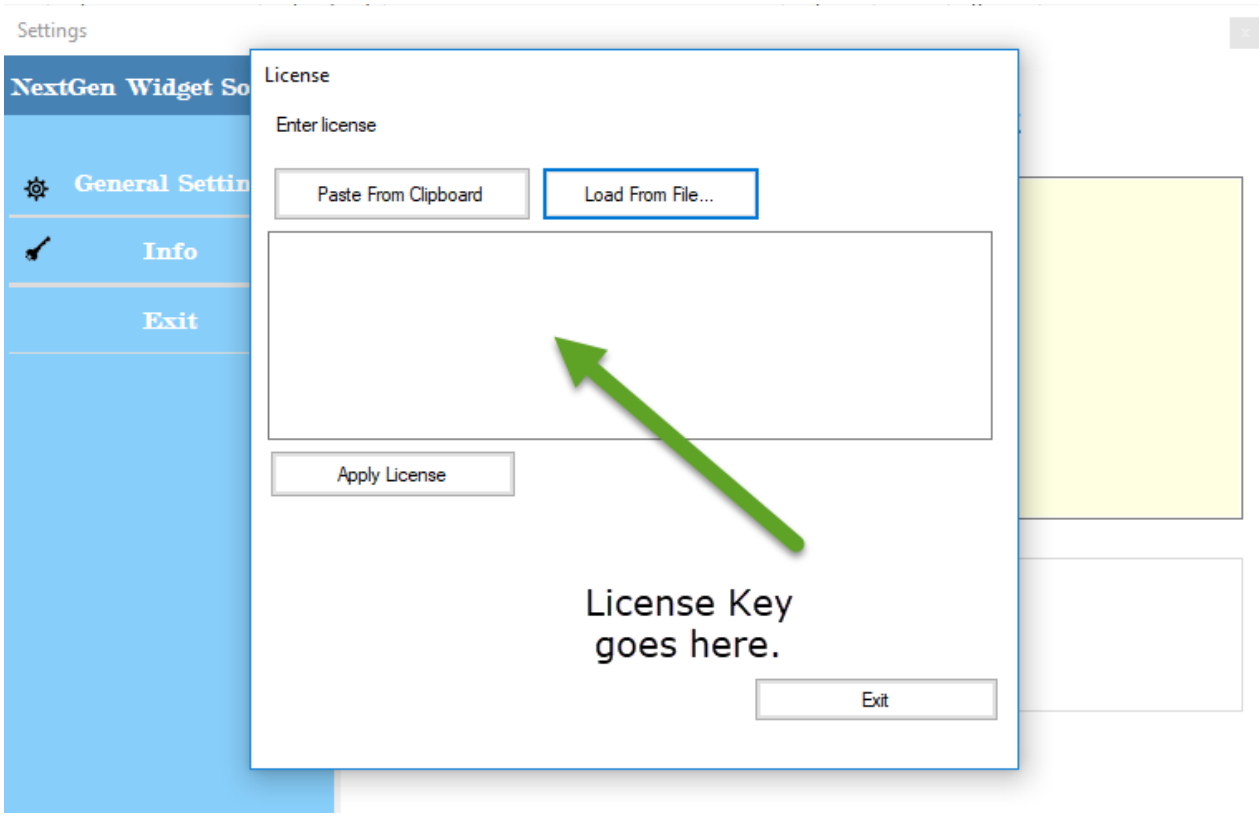
Info

Info gives you your subscription validation date and information about the license. Also,

there is a License button to enter your paid description license or your general license key.



Enter license key you simply copy the key from the email you'll receive, click "Paste From Clipboard" and click "Apply License". The program will give you an acknowledgment and attempt to restart.



Troubleshooting

Moved Key Store

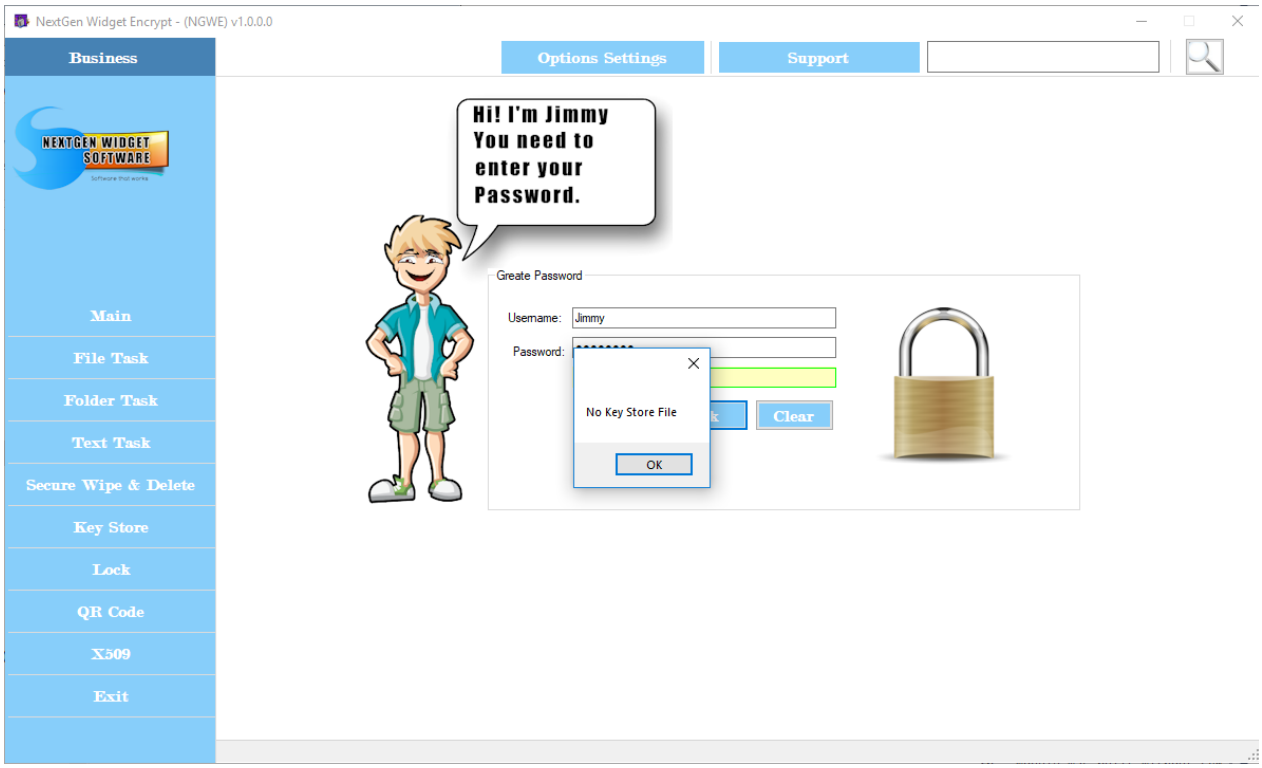
X.509

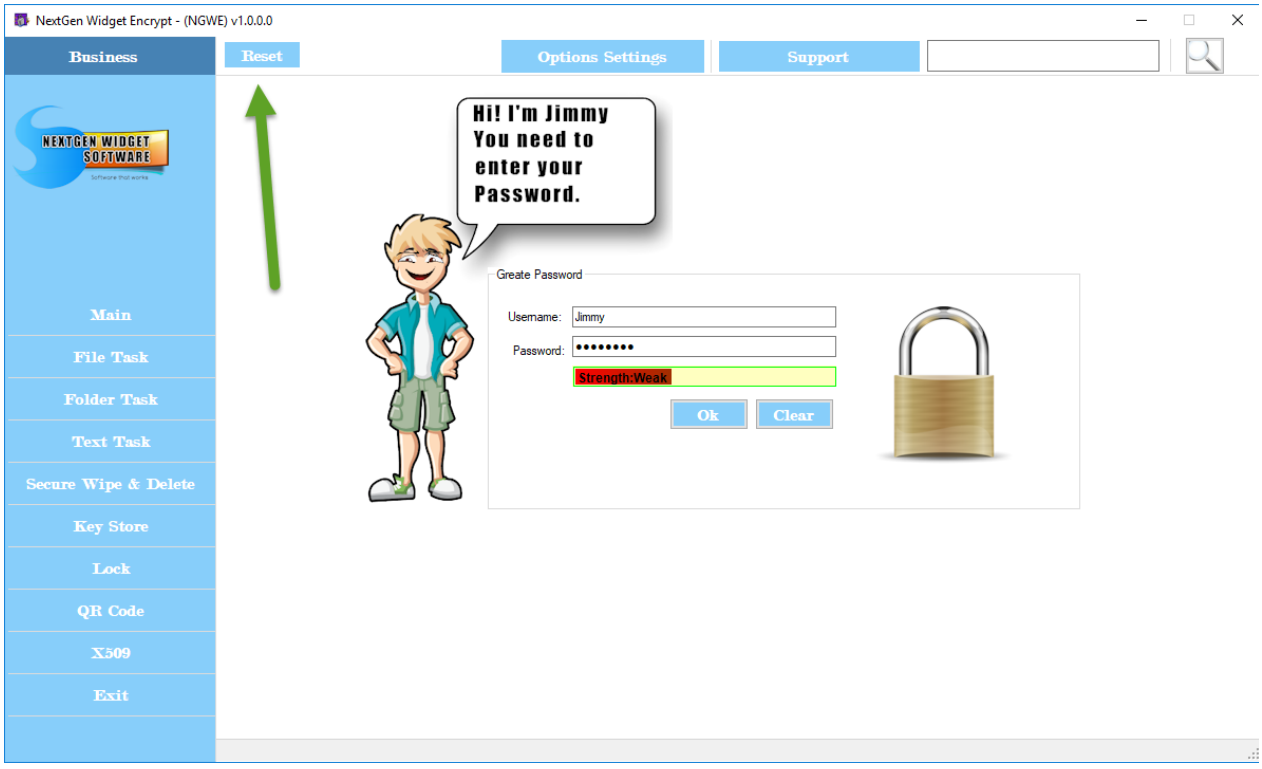
Moved Key Store

If you move the key store outside of the program, you may have difficulty logging back in because the program will not know where the key store is located. For example, I currently have the Key Store located in "D:\NewKeyStoreLocation" directory. Now, if I use the file manager and move the Key Store to an alternate location "D:\NewKeyStoreLocation2". When I log back in (after restarting) I will have the default information "Jimmy" because the program does not know where the key store is located.

Also, if I do not exit the Key Store and just just lock it, I will receive a message telling me the Key Store could not be found. The easiest fix is to put the Key Store back in the previous location and restart the program. Then, move the Key Store via the application "Options Settings", General Setting.

So, let's walk through the process. I've started the program but did not login and decided I wanted to move the Key Store to a network drive. So I'm using the file manager to move the Key Store to the new location "D:\NewKeyStoreLocation2". Now I'm going to try to login.

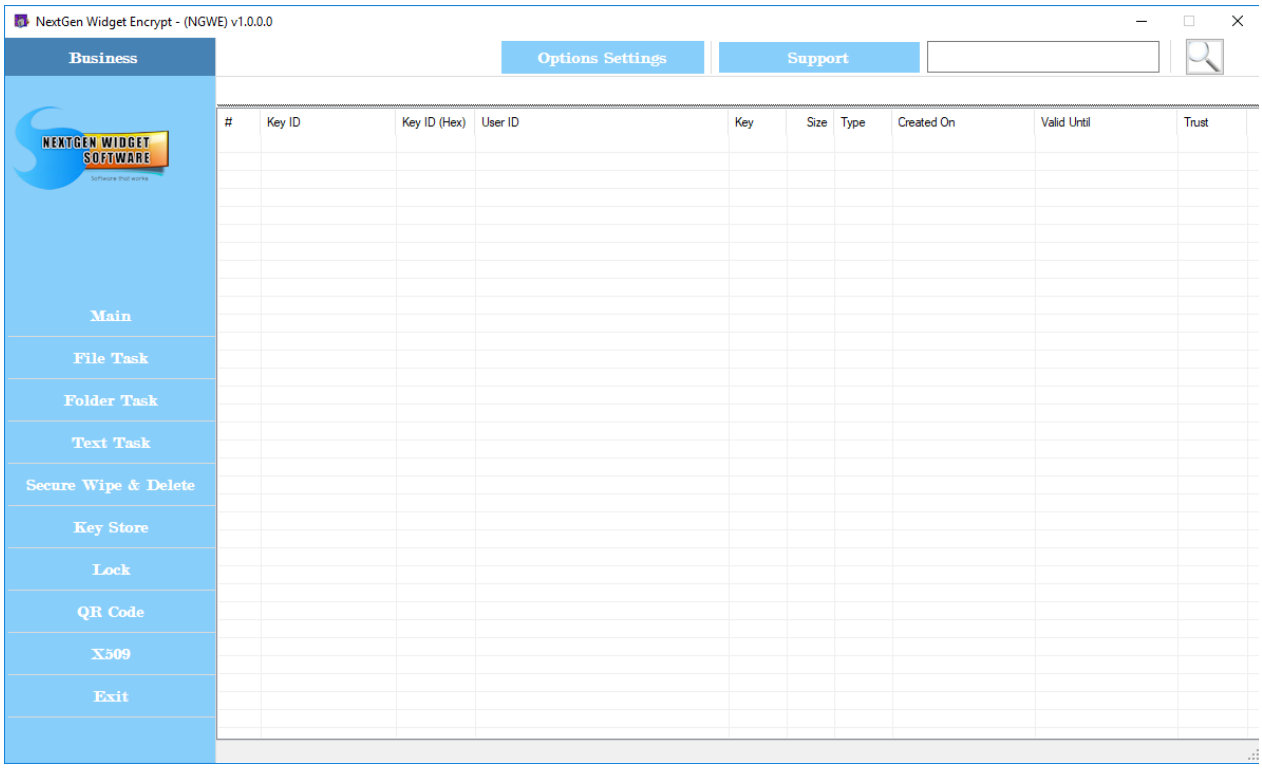




As we can see from the above image I got the message "No Key Store File". As I said, the best solution is to put the file back and move it via the program.

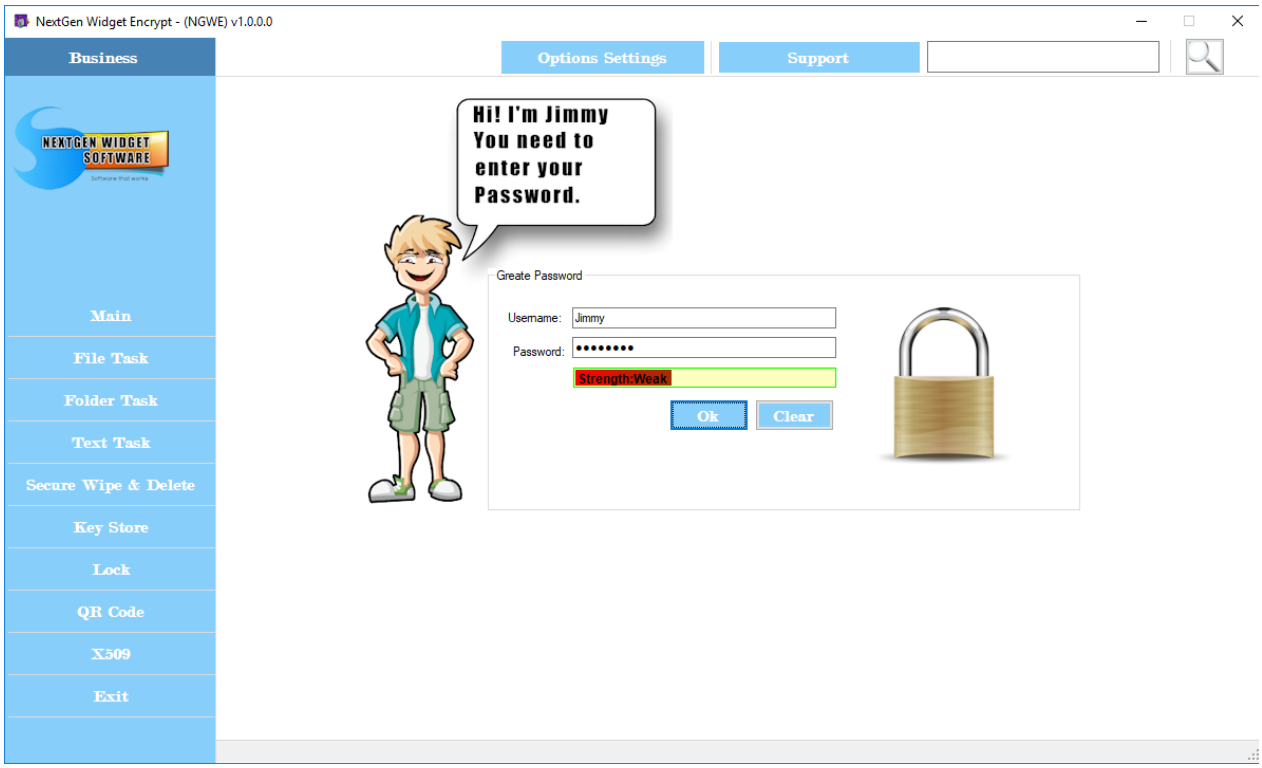
But let's say there were some unforeseen circumstances in case this was moved some other way or perhaps by an administrator. First I'm going to go ahead and click the "OK" button and place the cursor in the username field. Then, I'm going to hold down "CRTL+ALT+Shift+R" and you will notice a "Reset" button appears in the top left-hand part of the application (green arrow above). Simply click that "Reset" button and you will get a

notification that the application configuration was reset.



Now, you can enter any username and password you like. It can be any type of gibberish you want because were not going to keep this Key Store. The program will save the information back to the default location and allow you access to the program.

Once you have access to the program, we now need to navigate to "Option Settings", "General Setting" and click the "Locate" radio button and then the browse button. Select the location of the original Key Store, click "Open" and then "Commit" and "Exit". Now you can use the original Key Store as long as you have the username and password.



X.509

The code signing certificate can be used for just that, code signing. However, adding the code signing certificate to the signing area in Visual Studio's generally doesn't work. Unfortunately, Visual Studio's is a little finicky and you will need to create a (.snk) keys that is actually used for strong name which in effect is different than code signing. Most people get this a little bit confused and I have to admit I was actually one of them. :-)

Verify Signature

Topics:

OpenPGP_Detached_Signature

OpenPGP_Detached_File

OpenPGP_Verifies_Signature_Key_Store

OpenPGP_Verified_Detached_Signed_File

OpenPGP_Message_Detached_Signing

OpenPGP_Verify_Detached_Signed_Message

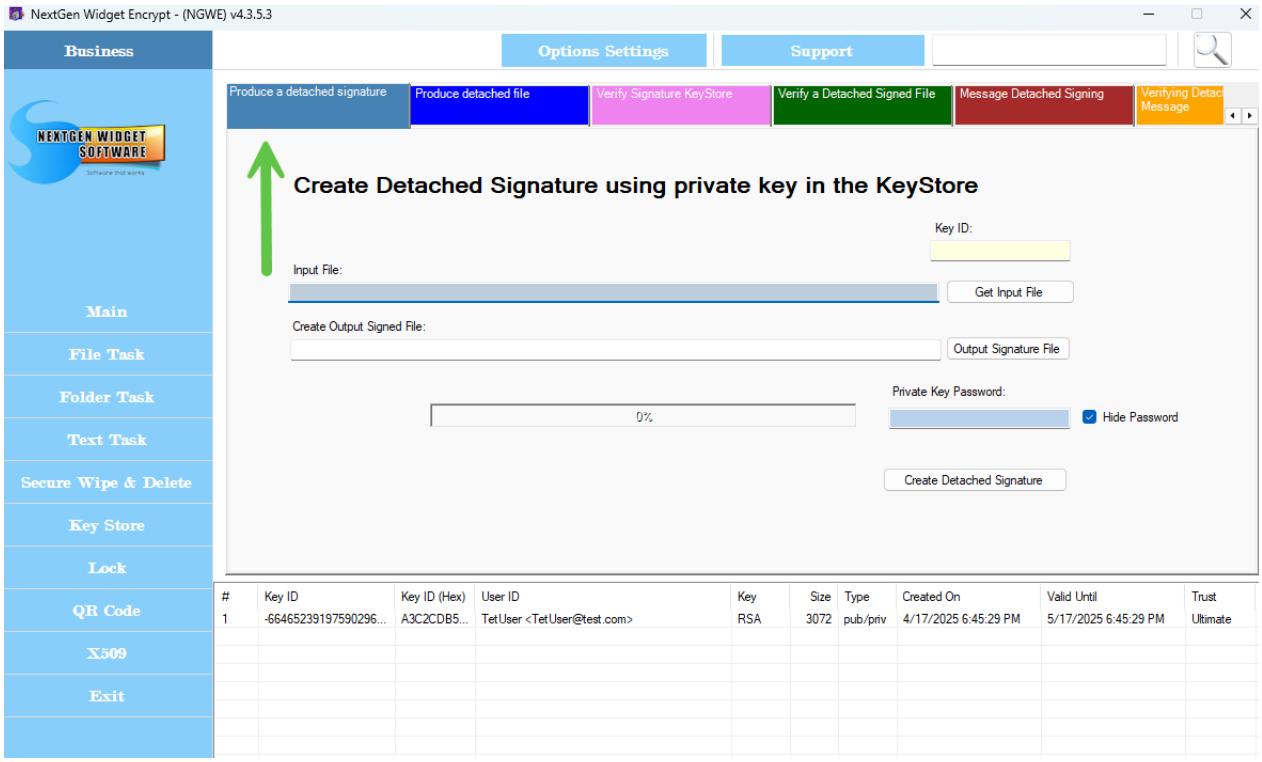
Description: A detached signature is produced by calculating an OpenPGP signature over the data intended for signing. The original data remains unchanged, and the OpenPGP signature is stored separately, e.g. as a standalone file. A detached signature file can be distributed alongside or independent of the original data. The authenticity and integrity of the original data file can be verified by using the detached signature file.

This signature format is especially useful for signing software releases and other files where it is imperative that the content remains unaltered during the signing process.

OpenPGP Descriptions taken from "The Notes on OpenPGP project". https://openpgp.dev/book/

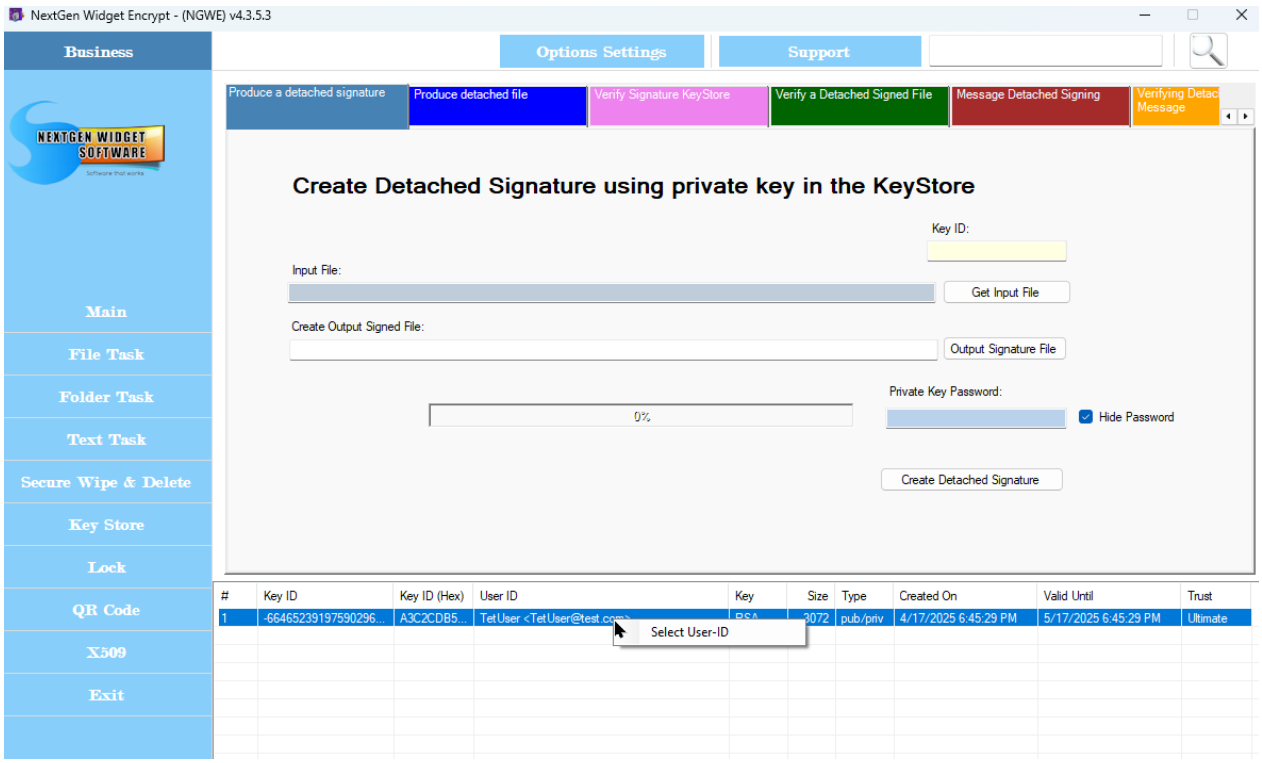
Detached Signature

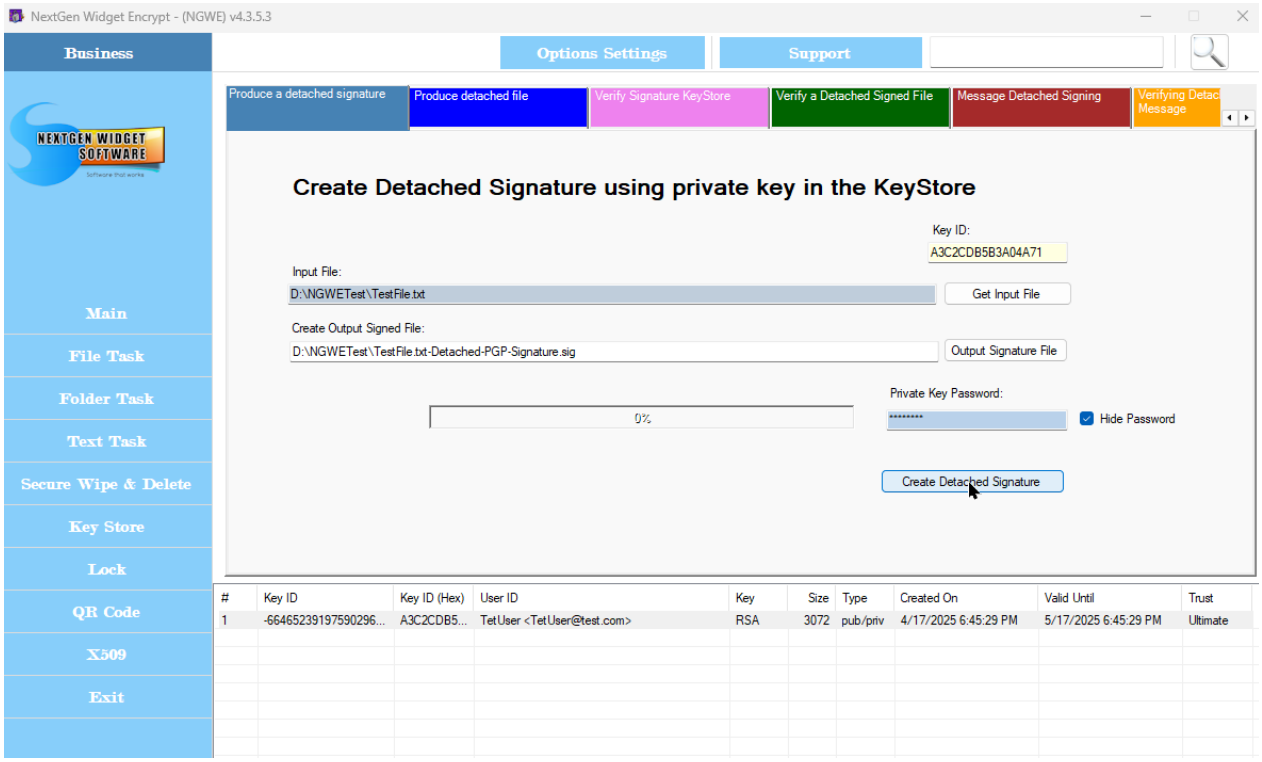
The area tab "Produce a detached signature" is for creating a detached signature using your private key which must also be in the Key Store.



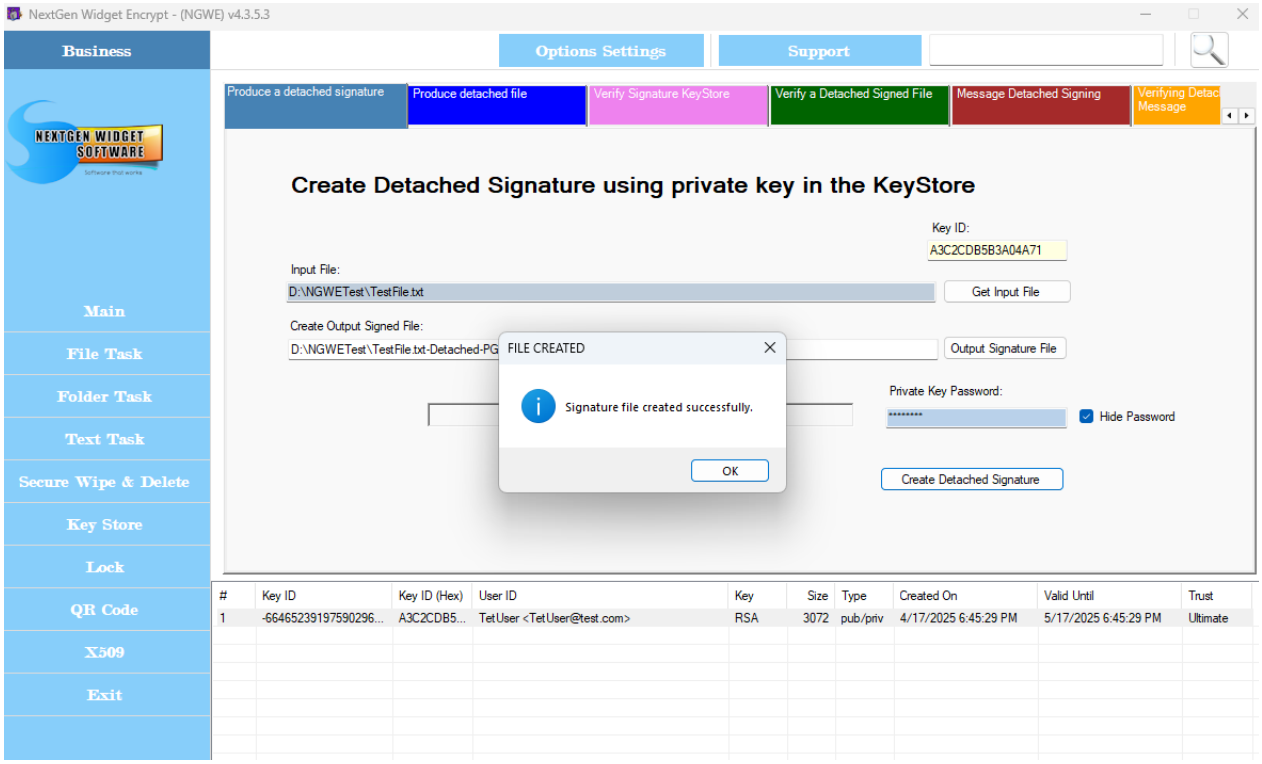
Right-click on the users name and left click to insert the Key ID in the Key ID area. Next, click "Get Input File" to locate a file. Now select the output location of the signed file. When the signed file location dialog box pops up it will add "Detached-PGP-Signature.sig" to the file. In my example will be as follows (TestFile.txt-Detached-PGP-Signature.sig).

Now, enter the password for the private key of the user you selected and click "Create Detached Signature" button.

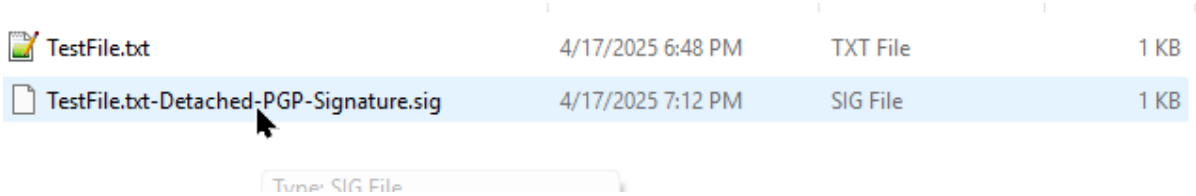




If everything went well you should see a message (Signature file created successfully.)



The test file and the signature file will be located in the directory you selected.



Now, let's take a look inside the signature file. The signature files have the userid and the fingerprint in the comment area. All done.

```
-----BEGIN PGP SIGNATURE-----
Version: NextGen Widget Software (NGWE) v4.3.5.3
Comment: TetUser <TetUser@test.com>
Comment: Fingerprint: A23FAA9FB03C727957EFA4E4A3C2CDB5B3A04A71

iQG4BAABCAAiBQJoAZjnGxxUZXRVc2VyIDxUZXRVc2VyQHRlc3QuY29tPgAKCRCj
ws2ls6BKcSYMDACvDNOjhDhBHLzf7d4ZDTDL2T2kLtSCbhOEYcylkRCZSDHEkCc0
iZdoBCeOX/J9jXpFpIpSjHBQ3K5Lfd8KoDbnnG5rfuq6Tw3i+jfn0GLTbgjBuUE+
h5FlNHxPMN7K6kVVvohTdFF2wdFyRxBwsk3ExyUo/3NvzTJblW0uon4iXEl4YQII
8bIlwV6AAujOcgevJuvLRJ9lFx4jXdFCKul2JhslBNi9JD0YccV8HWDW7HLaNZFz
bpKwPTpRKCdMQMMCpvB6LeYf7aIjsWdXka5Jlp40smQSXt3+Ae3UBGlT7lTojY47
482aMZzourC2s2a97EzANwQp8Guqi8brgHkT2YRrJ9jEWOiNcachpdGB2mZzkNdy
hDKlm3Zugqx6H2FOCXazJvvladQwdMYUuLpEqexs/SBu2lR519aTl0lx5eNFuko0
myi/kvoPL2aIBifxsXeHtZxgDsKrlo373uem8k5wsMpsRH3IHhK+Kl68q4rBFbA6
ztKI2nDbvcprs90=
=hbk6
-----END PGP SIGNATURE-----
```

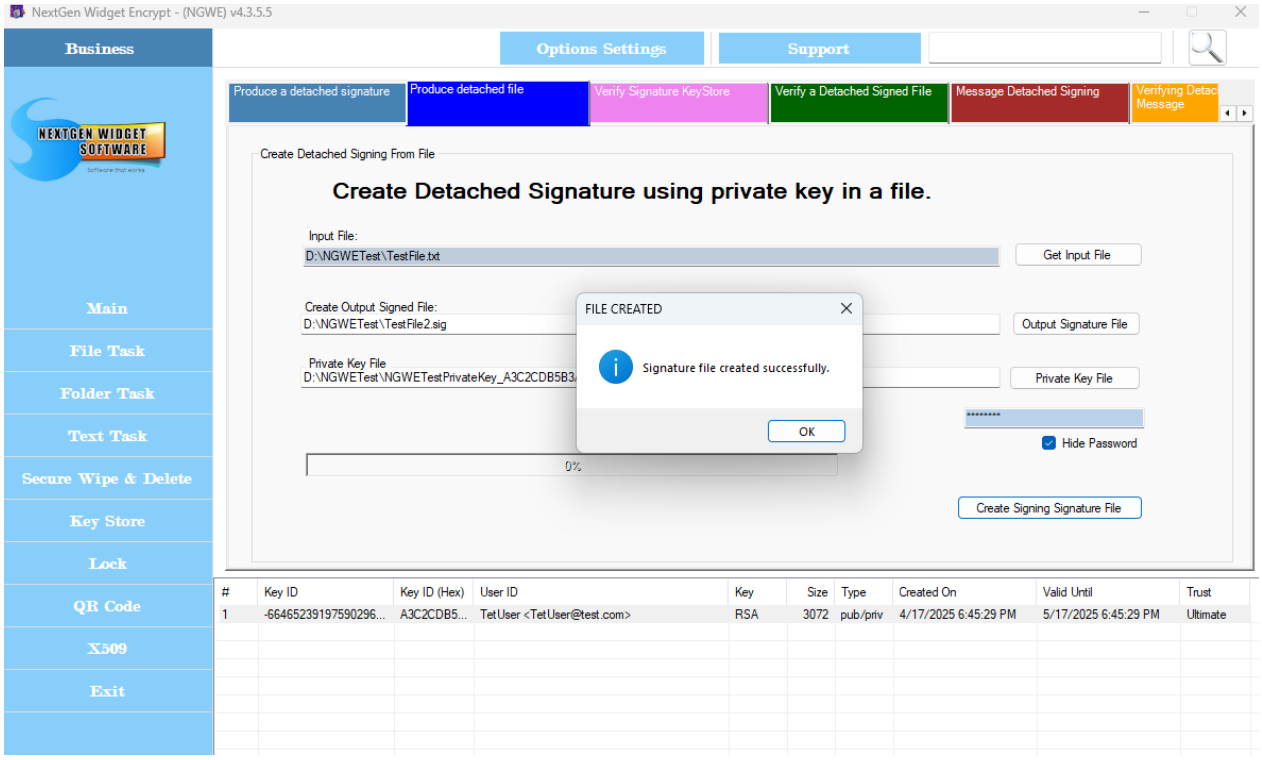
Now, let's go over to Verify Signature Key Store.

Detached File

The detached signature works pretty much the same way as the detached signature using a private key in the Key Store. However, the only real difference is the private key isn't located in the key store. Your private key would be in a file .asc.

So, let's get the file we want to create this signature against, select our output signature file Acacian and locate the private key from a (asc) file.

Now, let's enter the password and click the "Create Signing Signature File" button.

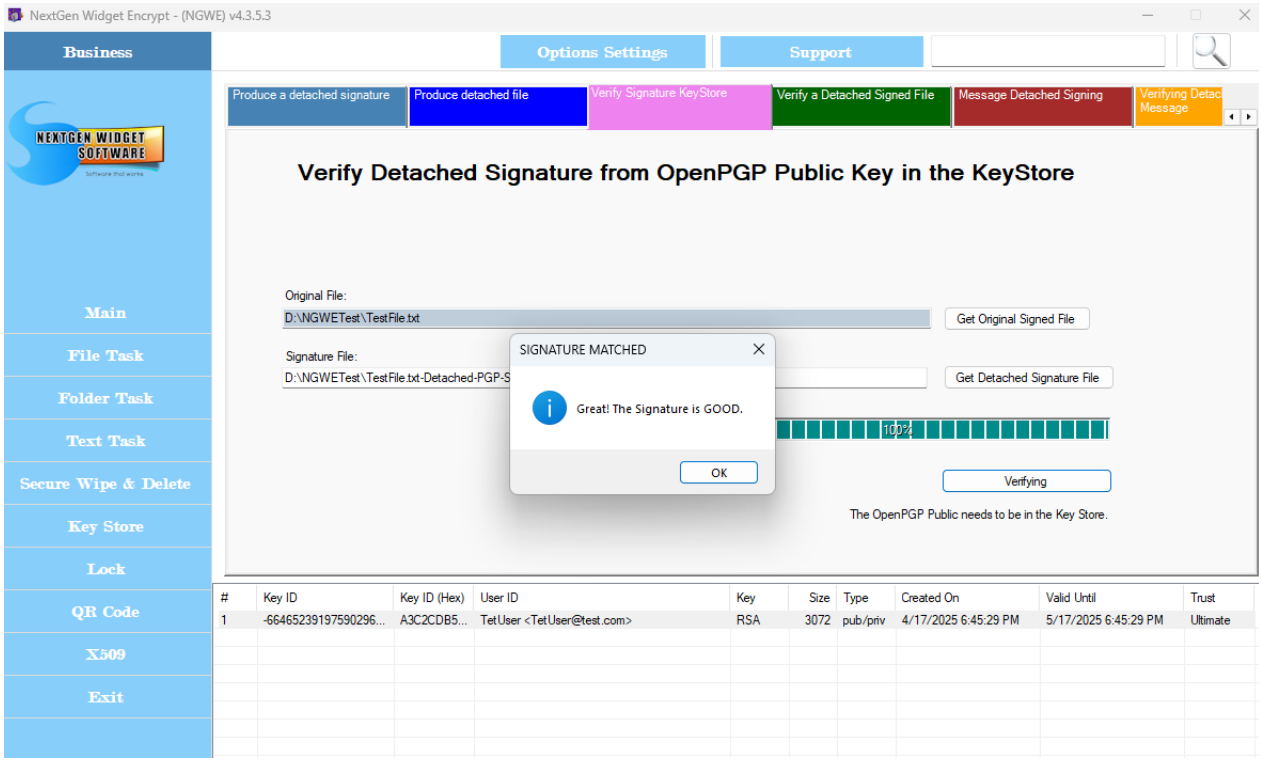


Let's open up to signature file and take a look at the signature block. All done.

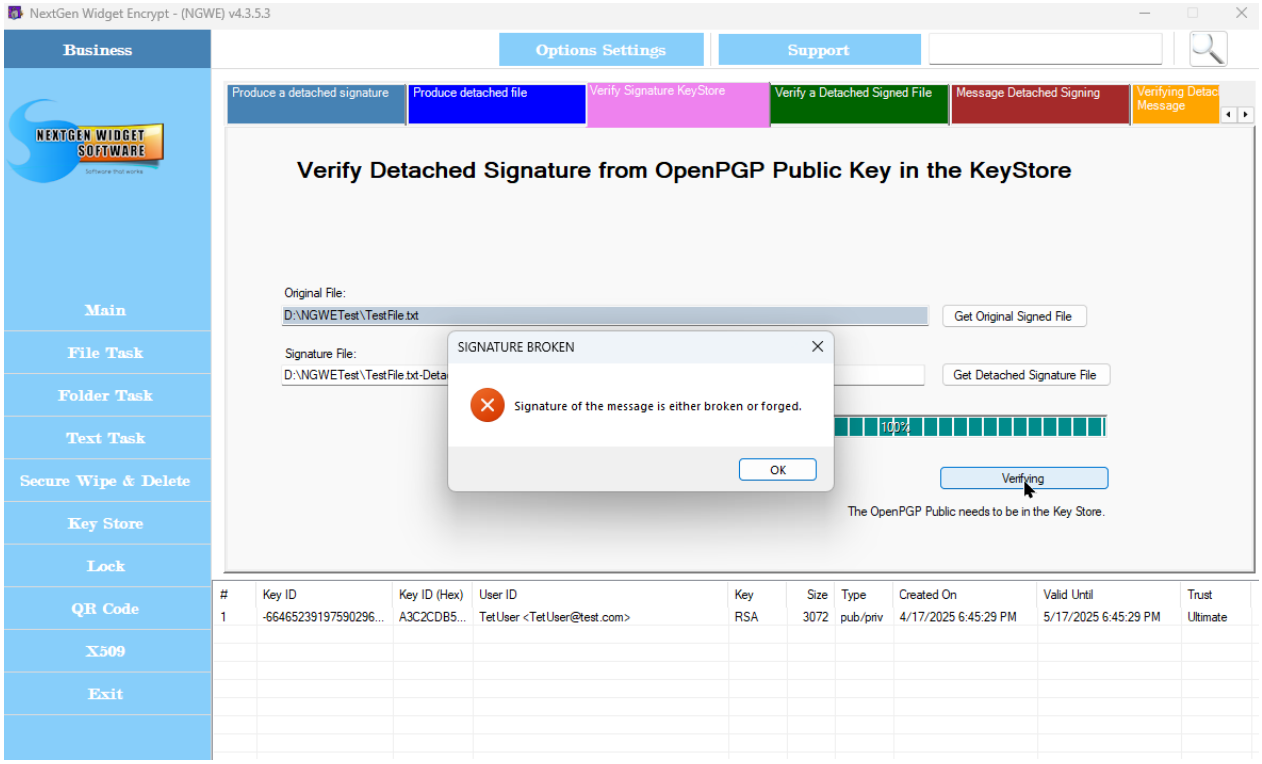
```
-----BEGIN PGP SIGNATURE-----
Version: NextGen Widget Software (NGWE) v4.3.5.5
Comment: TetUser <TetUser@test.com>
Comment: Fingerprint: A23FAA9FB03C727957EFA4E4A3C2CDB5B3A04A71

iQG4BAABCAAiBQJoAtJyGxxUZXRVc2VyIDxUZXRVc2VyQHRlc3QuY29tPgAKCRCj
ws2ls6BKcWnqC/95McmhT3yxXEZkBlz8TDWzRerjPrvoV0oziknvYA6kkrBBC/O9
NDu9BOktqtOKcAMy8QaCeAkJSg3xo6lvI8yu6AIeV7m/9v7R5QWq7nvKoca96As7
C8bjTIu3s0n8gN2T/H2i3OhvLEXc4ilYWDN95+BuhlbiiWakR0lITw399ZnK50wb
sgdIoYMtNoibv5O8G4o3dm5lVOF9Rk4d5mvD/UZIaVWVYQTUllo+VbdnbVNIYQxu
iZP6l+Wcsw7pmK7GOa6Sp5UNGo4agWvV3h4ARrlWzPlE0tpI0uJsRSsZlMTtVqNq
OW9eoPWIfYI/5PPVL2twn8cePtrnUMwvO4OimbUUNOZihxcLpfy3rrQ9bXcHqG//
VzBWC4rkMXuBxEPnID/4b+7NX3lVlo3lcwS3wzJDAH6wZxzsemaNHyGxbzhLRejK
HdmyC91019gSFzDh9to4yk9fJmEqLVtQlxGM+/Nu/e6PN3jtHvsHZikksNl8k8ON
R0Kfl8N2ME8hbIg=
=e04o
-----END PGP SIGNATURE-----
```

Verify Signature Key Store

Now, let's get the originally signed file (TestFile.txt) and the detached signature file (TestFile.txt-Detached-PGP-Signature.sig). As long as the public key is located in the Key Store we just need to click the "Verifying" button. If everything works out you'll see the message "Great! The Signature is Good".



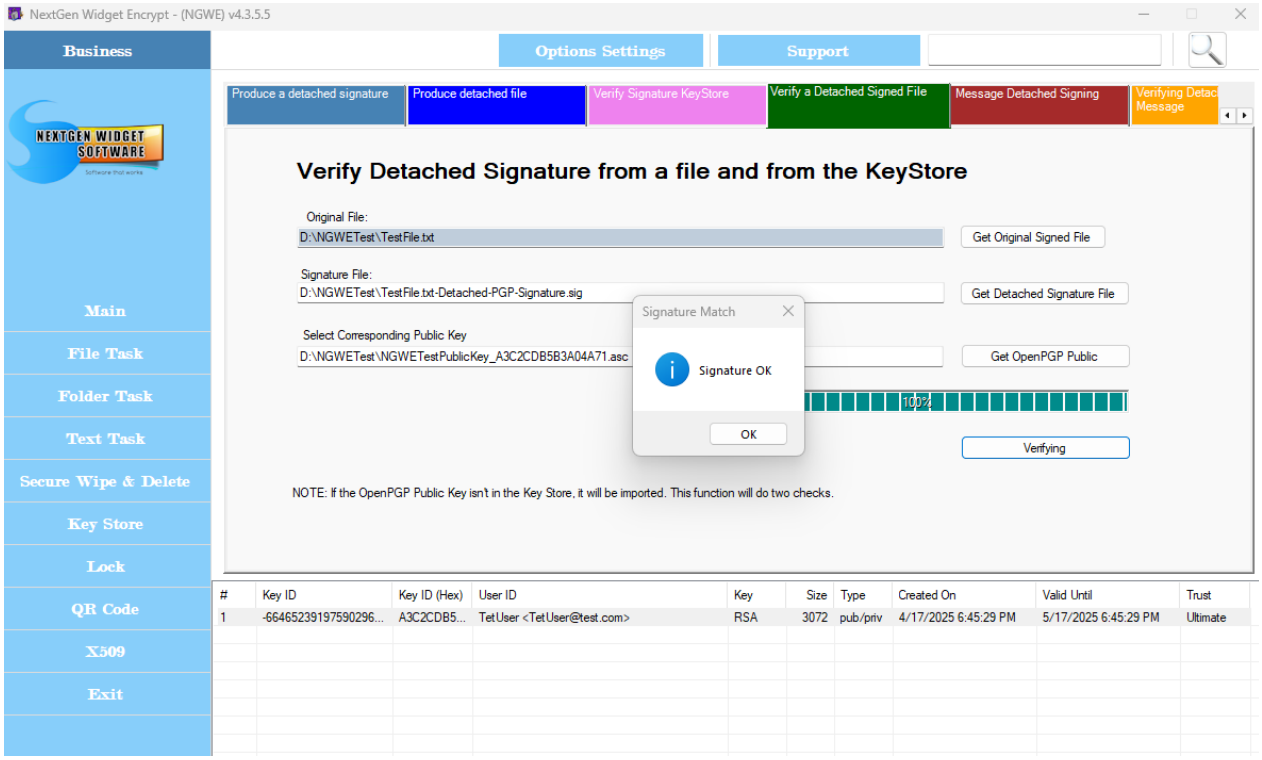
Now, if even a period is out of place or an additional character entered the signature will fail.



Verified Detached Signed file

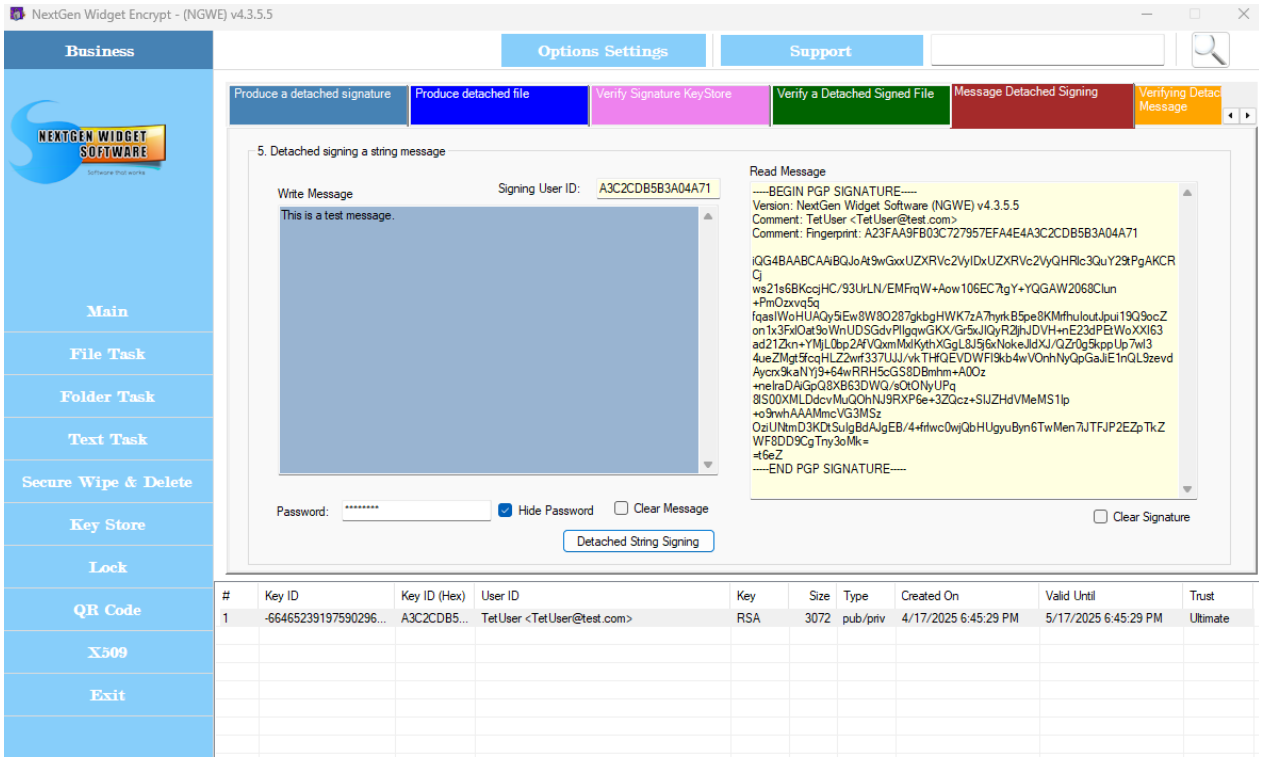
Verifying the detached signature from a file and from the Key Store. This one may be a little awkward but it requires the public key to be in a file as well as in the Key Store. On the program there is a little note that basically tells you if the public key isn't in the Key Store that it will be imported into the Key Store. This function does two checks.

So now, select the User Id by right clicking on the user, locate the original signed file, the signature file and the corresponding public key file. Click the "Verifying" button and presto... Signature OK.



Message Detached Signing

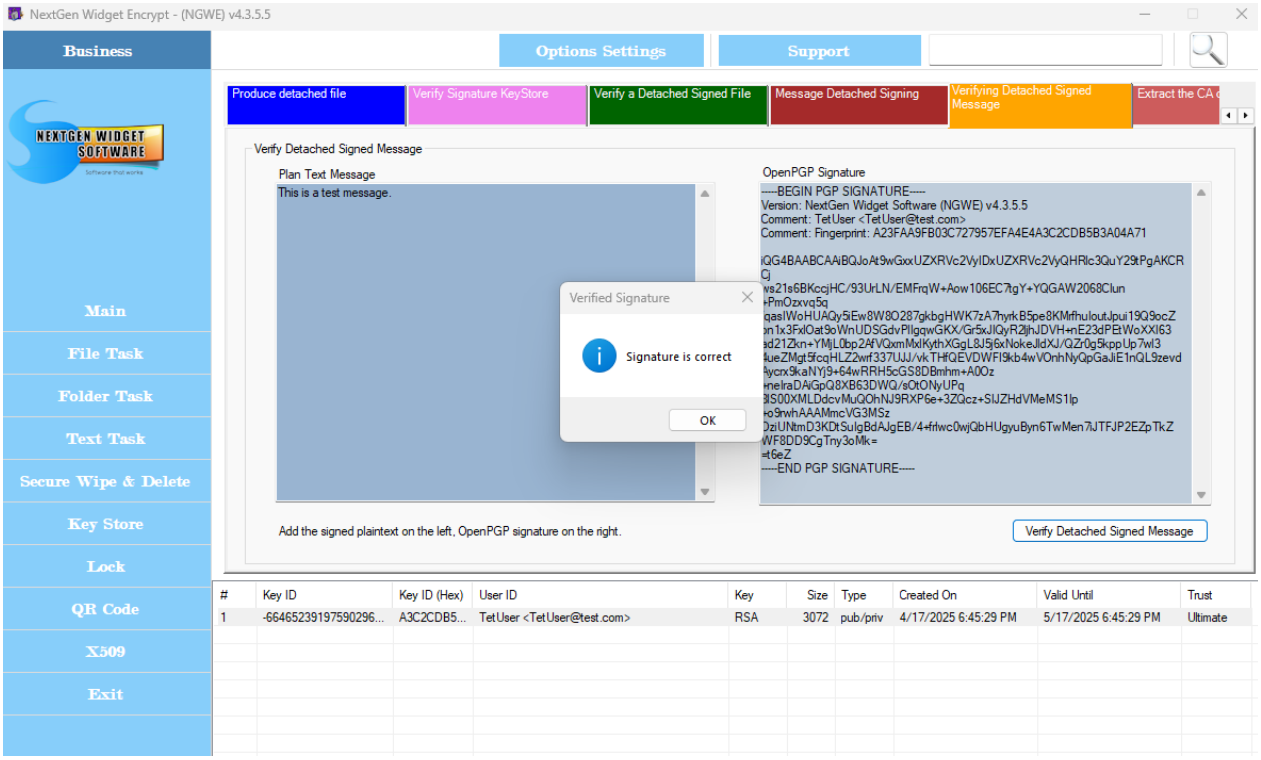
Message detached signature will create a signature for written text that can be used in in email. So, first right-click on your User ID which contains your private key, type your message, enter the private key password and click the "Detached String Signing " button. The signing block appears on the right-hand side. You can copy this block and send it along with your message.



Verified Detached Signed Message

Verifying the detached signed text message is pretty simple. Just enter the plain text in the

box on the left-hand side in the signature block on the right-hand side. The public key must be located in the Key Store. Just click the "Verified Detached Signed Message" button. That's it.



Extract NGWE CA Certificate

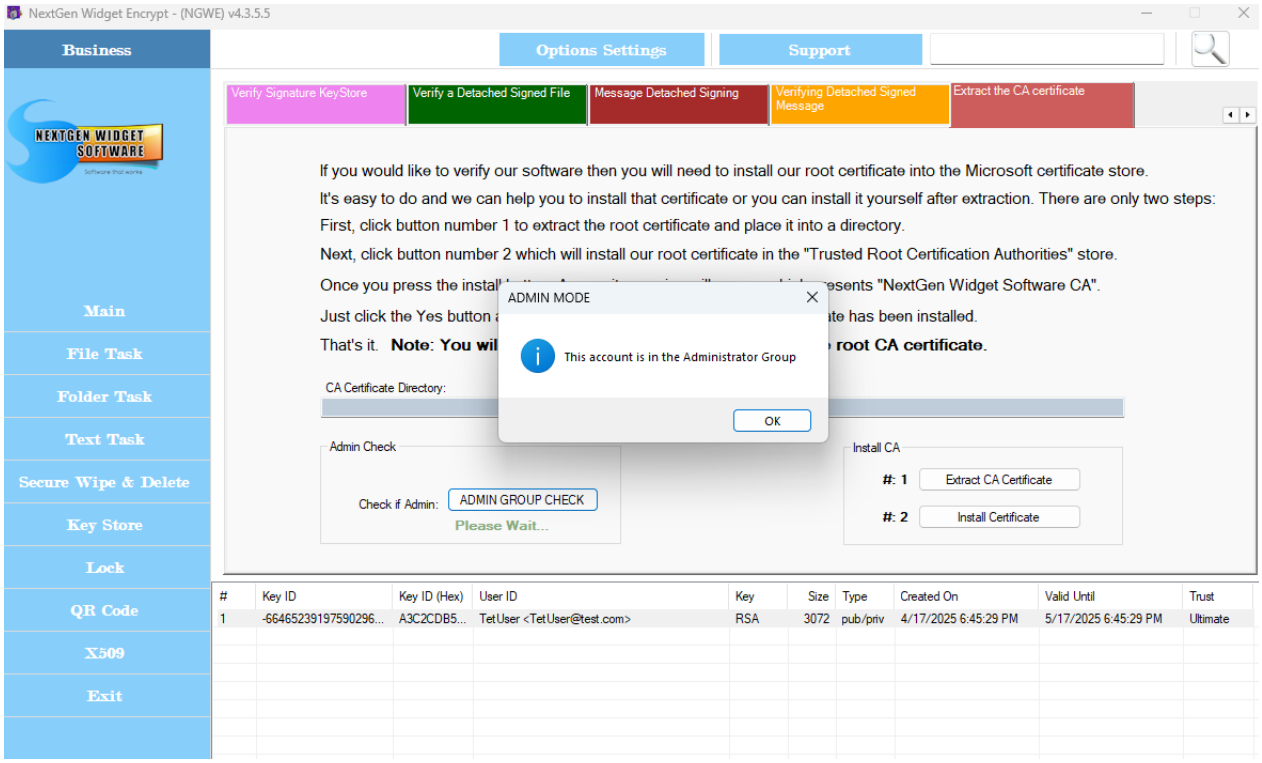
Install our Root CA
Fix Unknown Publisher Security Warning.

Install NGWE Root CA

There is times when Microsoft will say that it is unfamiliar with the software vendor and an annoying pop-up that shows up, Unknown Publisher Warning. This happens because the signing certificate or there is no root certificate recognized by the Windows 11 operating system.

To remedy this you can simply install our root certificate in the Microsoft Trusted Root Certificate Authority store. To do this you will need administrative privileges. Our CA is embedded in the software and can be extracted to a file location or installed in the Microsoft Trusted Root Certificate Authority store.

The admin check button verifies if you are in the administrative group. If you are in the administrative group there are just two buttons on the right-hand side (install CA). One is to extract the CA certificate and the other is to install it.



Troubleshooting

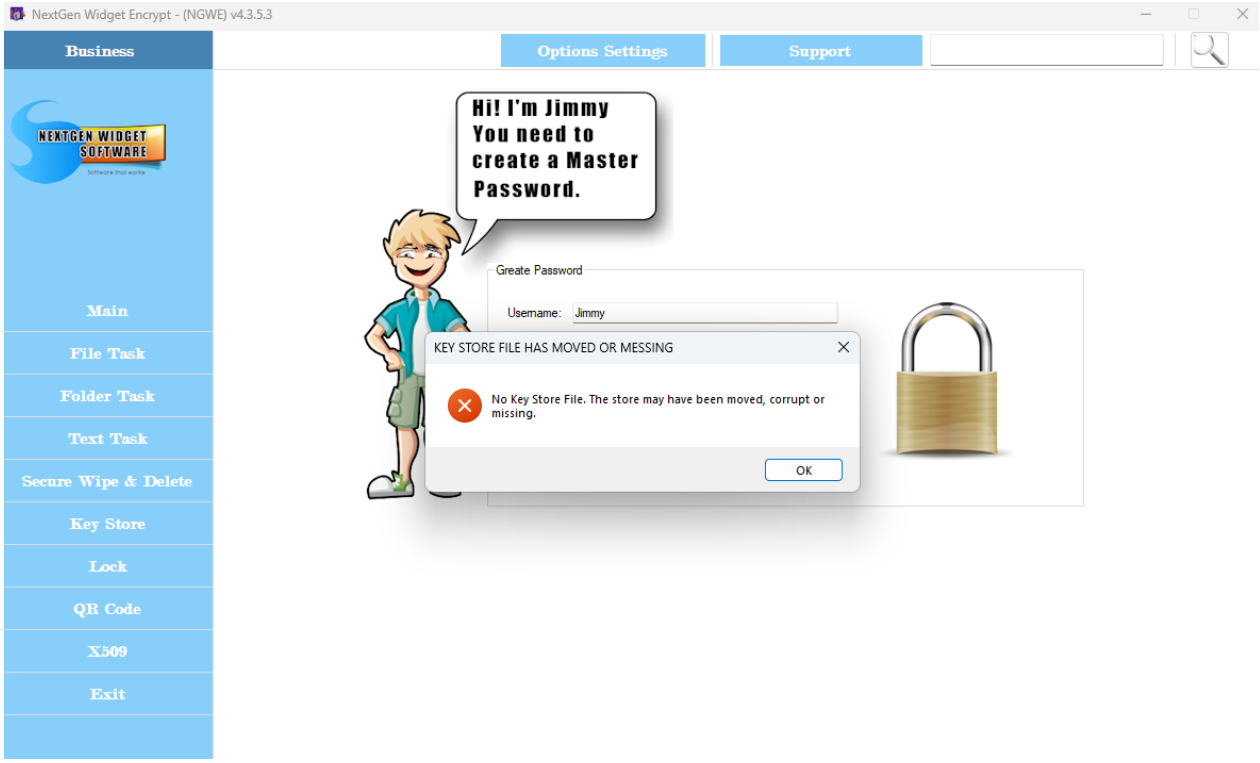
[No Key Store file]
Key Store moved, missing or reset.

[Software Upgrade Issue]
Potential issues on upgrade.

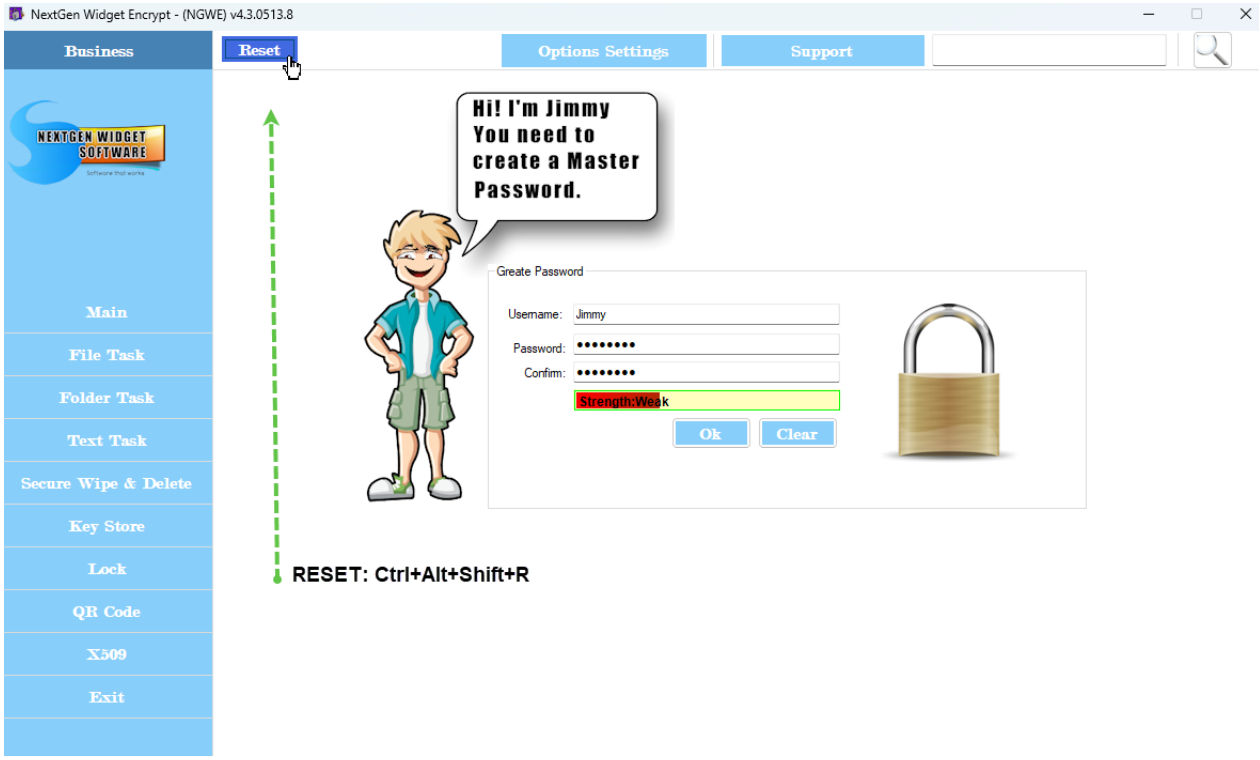
No Key Store file

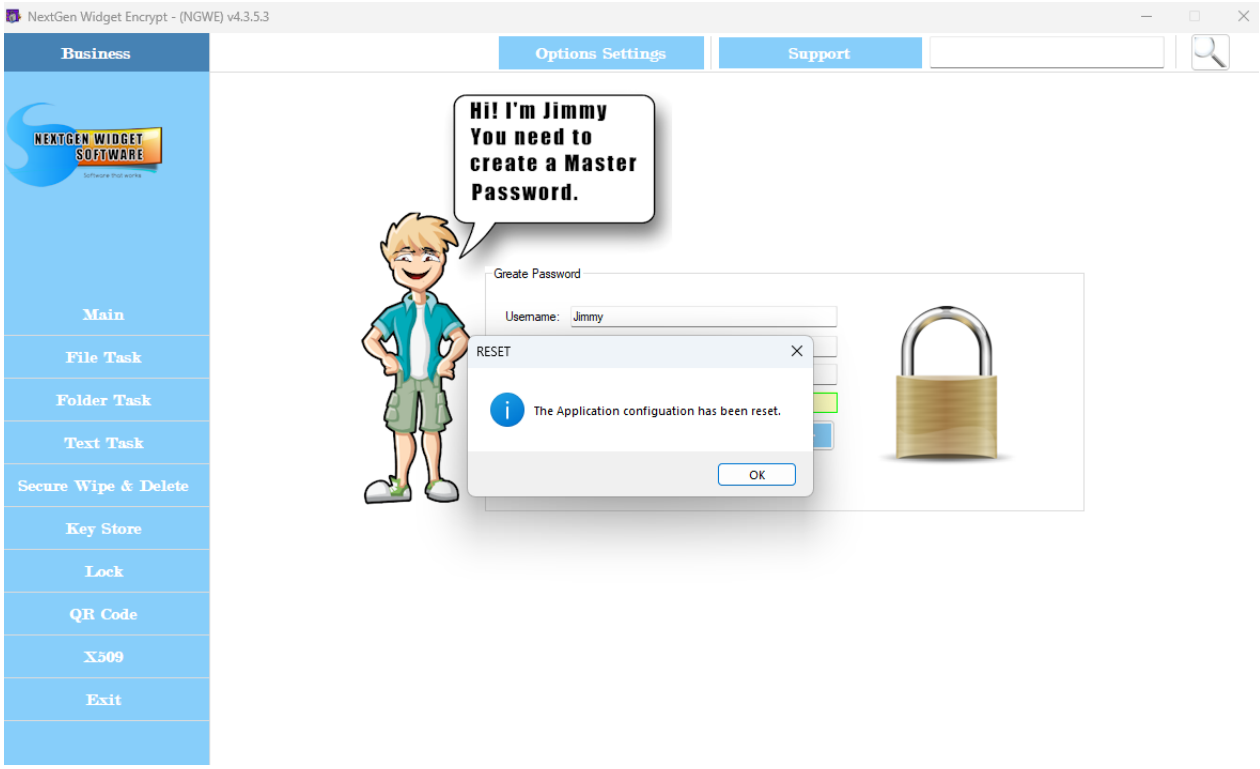
If the Key Store has moved, corrupted or not in the saved location. You will see a message (No Key Store File. The store may have been moved, corrupt or missing.) If this message shows up you are essentially locked out of the system and it will not function. If you have the Key Store file just put it back in the same location and it can be moved via the program under the option settings. So, at this point if we have lost the Key Store or its corrupted and you don't have a backup. You must start over because there is no recovery.

So let's reset the program in this example.



Click the "OK" button and place the cursor in the user name text box and press "Ctrl+Alt+Shift+R". A "Reset" button will appear in the top left-hand corner.





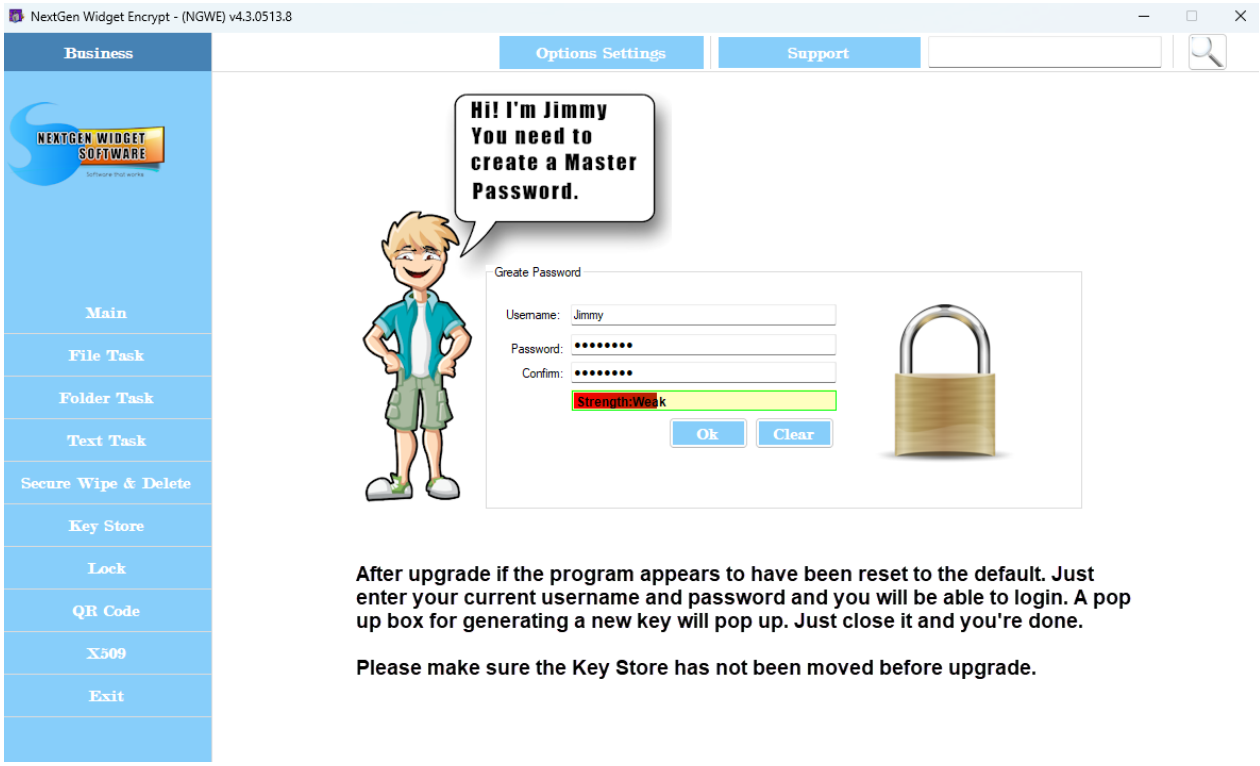
Click the "OK" button, change the user and password. From this point you will be let back into a clean new key store and the create a new key pair dialog box will pop up.

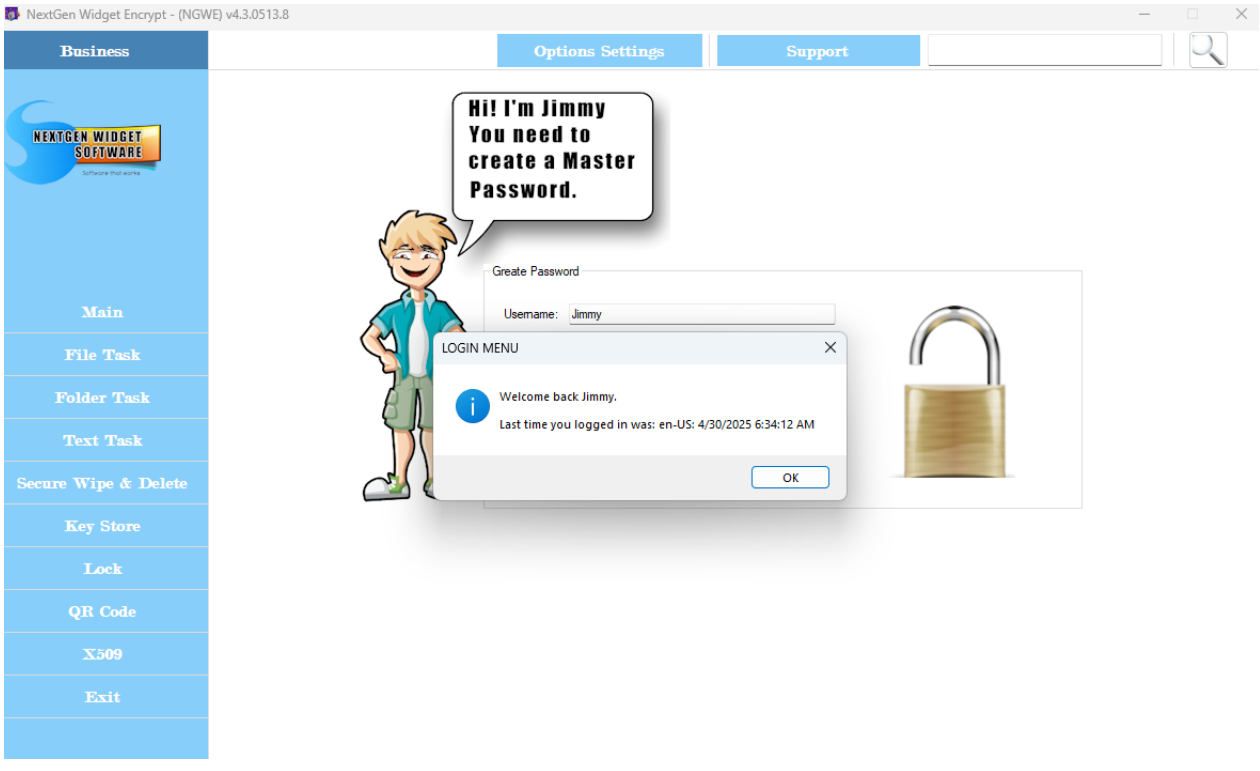
From this point if you have located your original key store, close the application and put the original Key Store file in the original location. You can Copy and Paste over the current one. Now, if you wish to move the Key Store go to the "Options Settings" and you will see the area where it says "Key Store file location". You can move it using this area and the application will remember the new location.

Software Upgrade Issue

When upgrading you may run into a small issue. So, after upgrade and use start the program it may appear as if everything got reset to default. You will see the original login screen for changing your password and username.

However, just simply enter the same username and password and click "OK" and you'll be able to log right in providing, your key store has not moved. If your key store has moved you will either need to put it back in the original directory before the upgrade or reset the program.

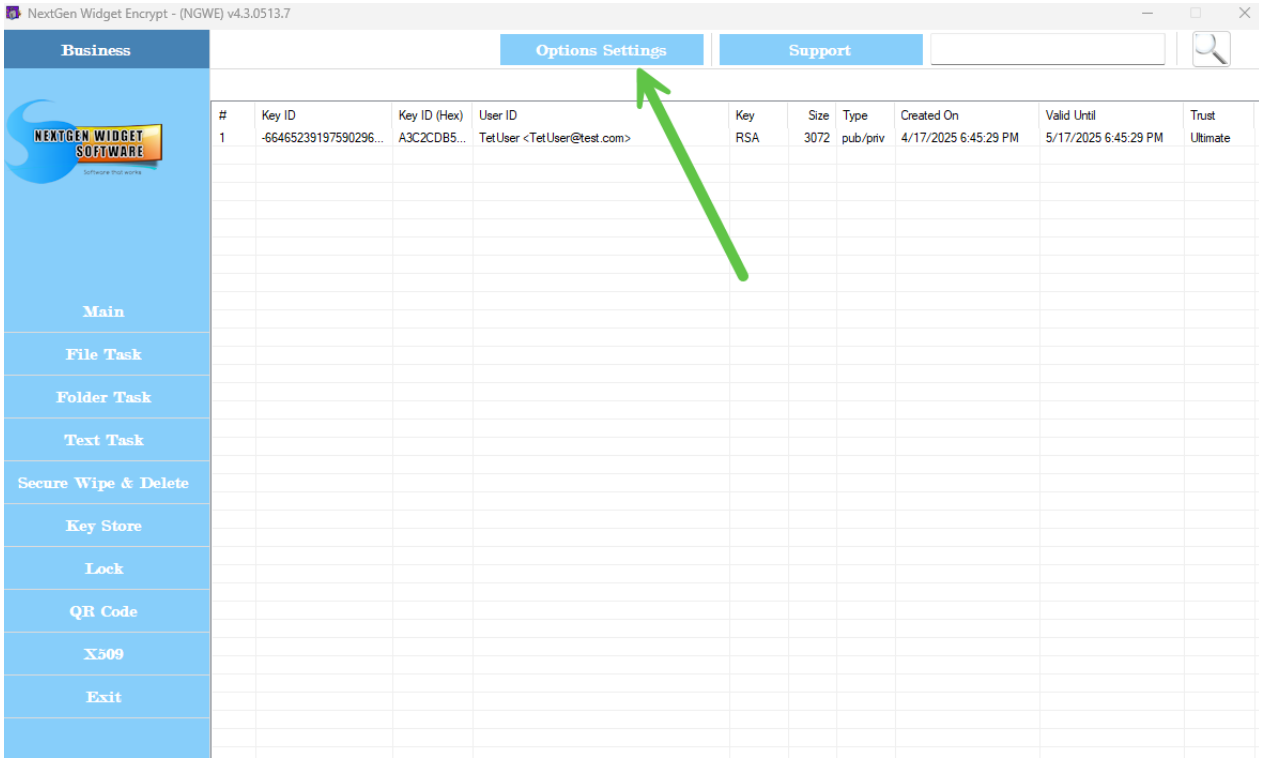


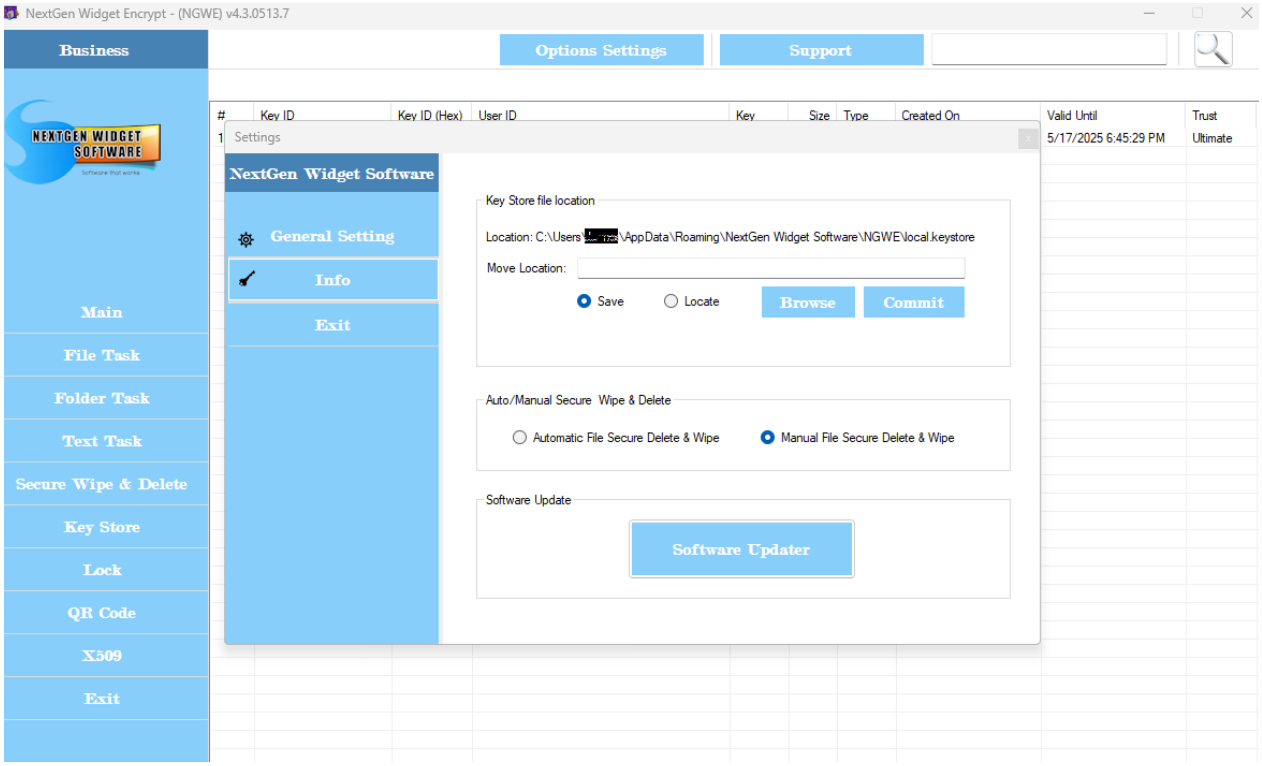


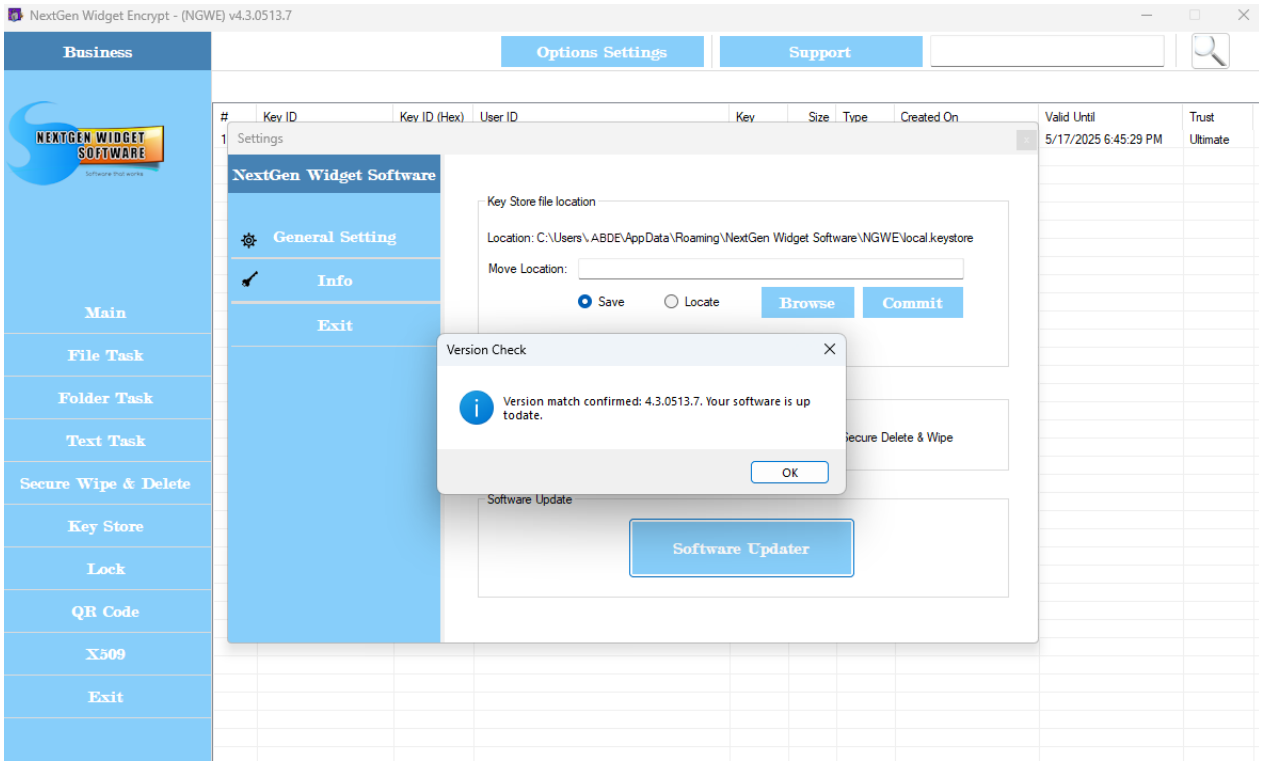
Software Upgrade

Checking for updates is a manual process and requires the user to check on their own periodically to see if there are any updates. To do this you log into your software and click the "Options Settings" button. A new form pops up and on the bottom of the form (General Settings) you should see a button that says "Software Updater". Just click that button and the software will check the website to see if there is a new version.

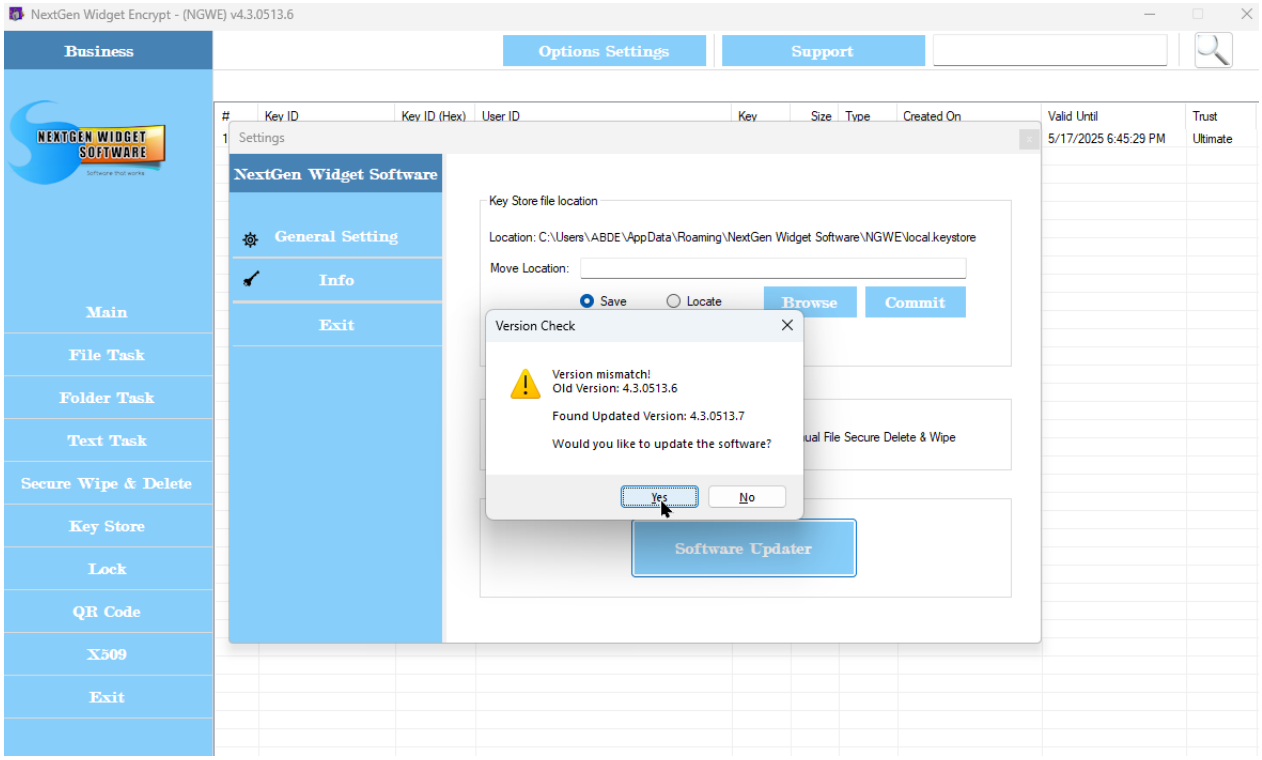
Internet access is required.







If there is an update available you will have the option to go to the website to get it or do nothing.



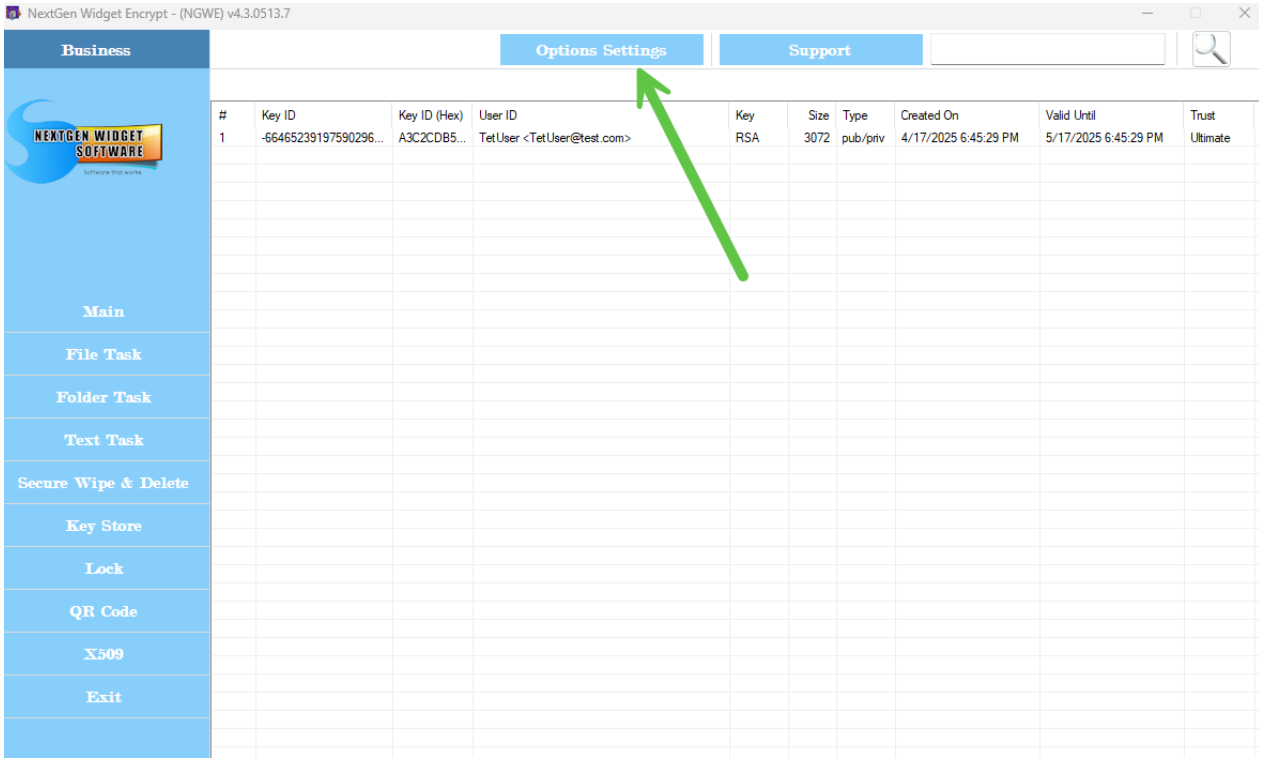
Once you locate the new version just simply download the "NGWEsetup.exe" file in run the setup application. The setup will install the application and create a desktop icon along with an uninstall shortcut in the program menu. Just overwrite the existing program it will not affect your key store which is located in a different directory.

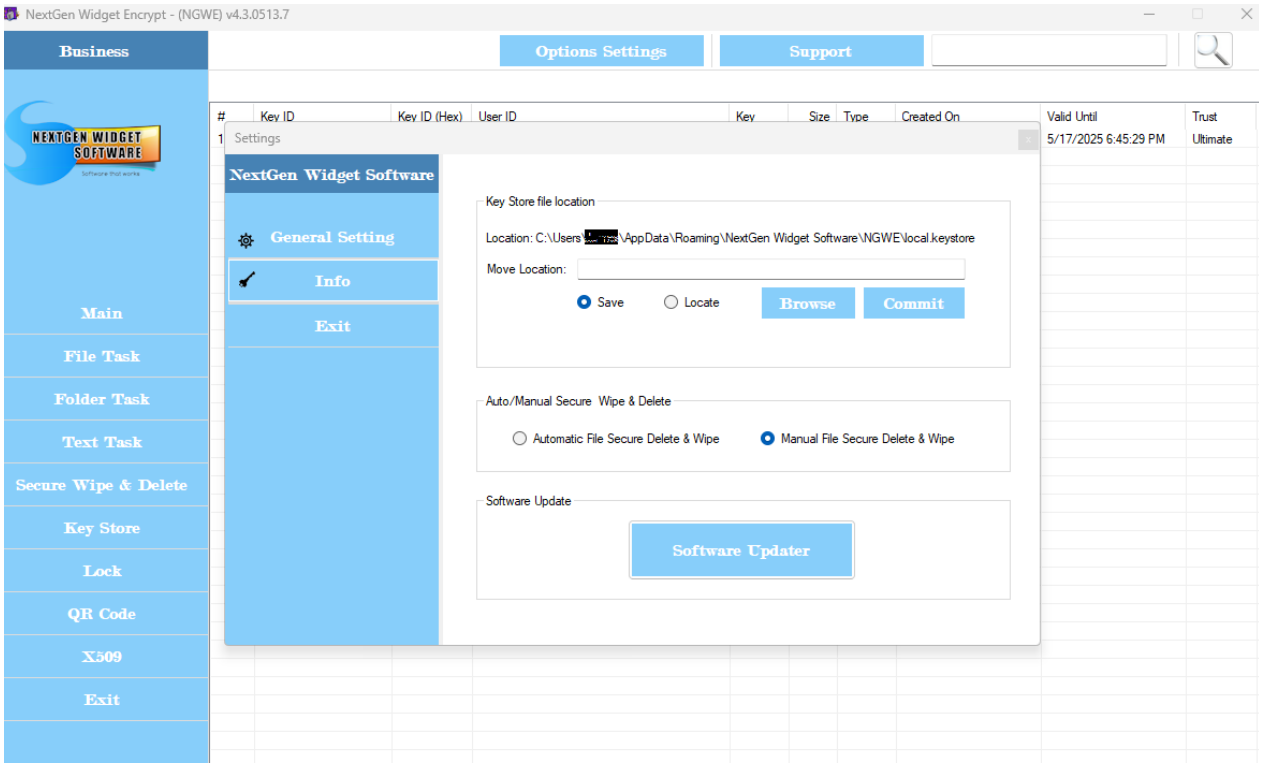
When you want to uninstall the program two files will remain. The log file and your Key Store. The Key Store isn't created with the setup program. This created by NextGen Widget Encrypt. However, you can delete the directory "AppData\Roaming\NextGen Widget Software" on your own using your file manager.

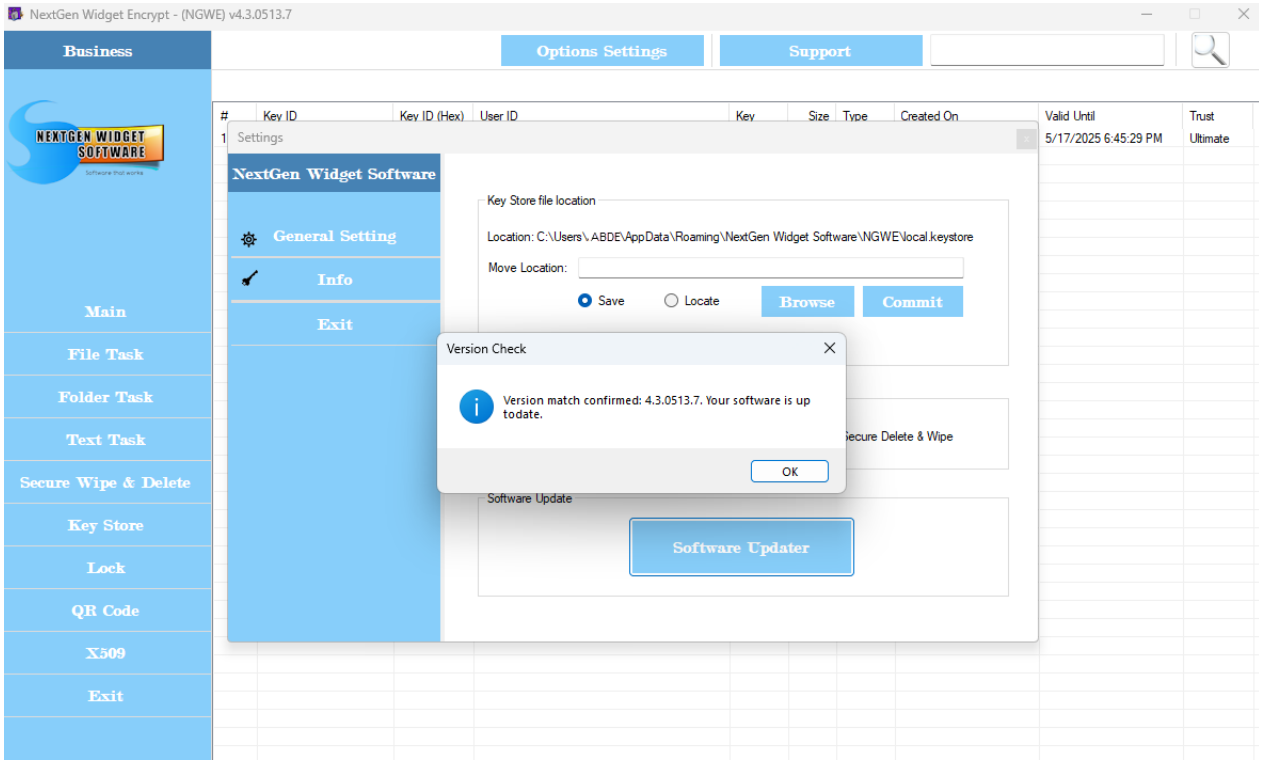
Software Upgrade

Checking for updates is a manual process and requires the user to check on their own periodically to see if there are any updates. To do this you log into your software and click the "Options Settings" button. A new form pops up and on the bottom of the form (General Settings) you should see a button that says "Software Updater". Just click that button and the software will check the website to see if there is a new version.

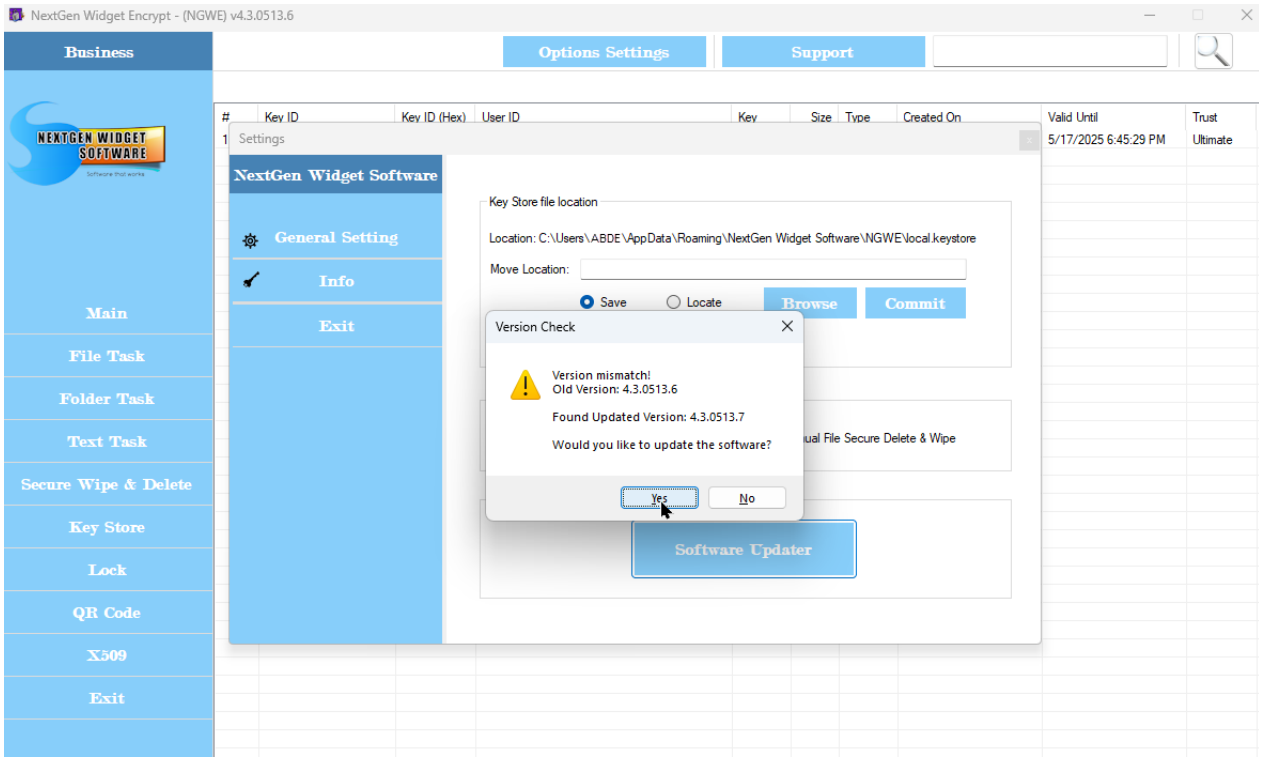
Internet access is required.


NextGen Widget Encrypt - (NGWE) v4.3.0513.7
Business
Options Settings
Support
Key ID Key ID (Hex) User ID Key Size Type Created On Valid Until Trust
1 -66465239197590296... A3C2CDB5... TetUser <TetUser@test.com> RSA 3072 pub/priv 4/17/2025 6:45:29 PM 5/17/2025 6:45:29 PM Ultimate
Main
File Task
Folder Task
Text Task
Secure Wipe & Delete
Key Store
Lock
QR Code
X509
Exit

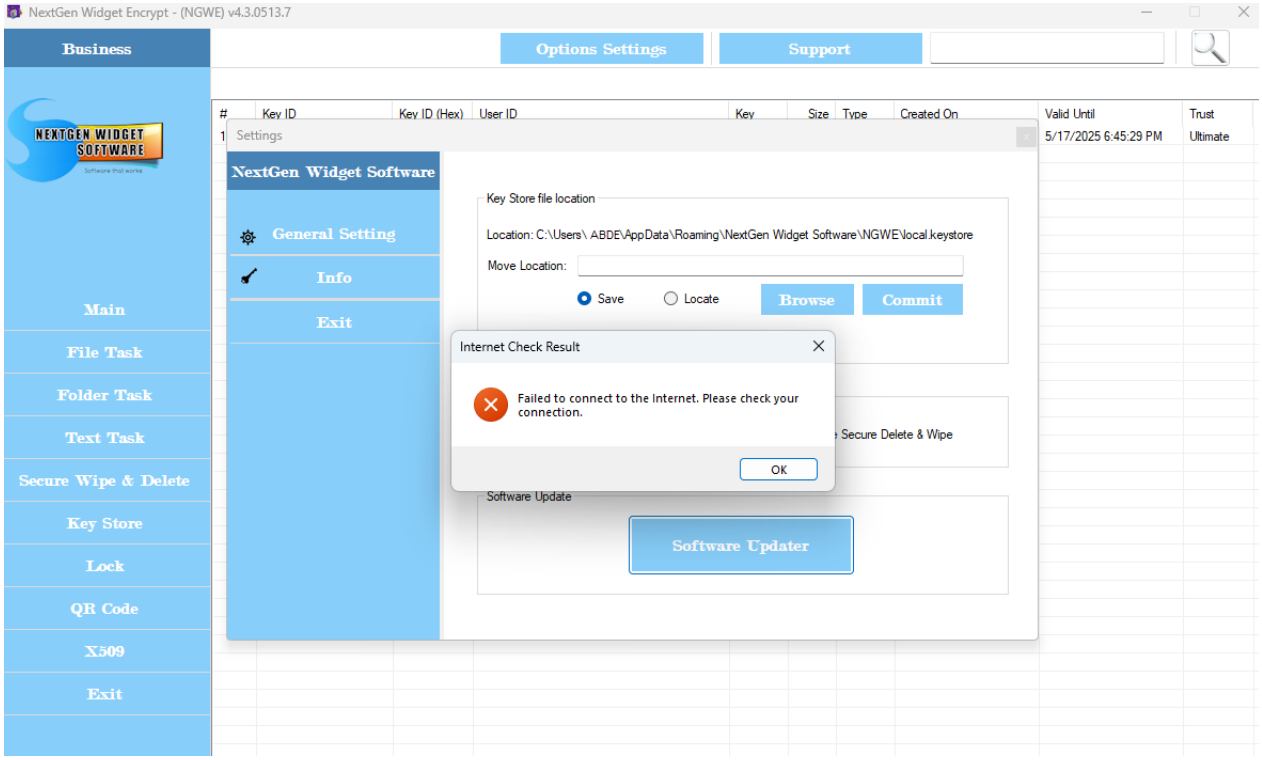

NextGen Widget Encrypt - (NGWE) v4.3.0513.7
Business
Options Settings
Support
Settings
NextGen Widget Software
General Setting
Info
Exit
Key Store file location
Location: C:\Users [redacted]\AppData\Roaming\NextGen Widget Software\NGWE\local.keystore
Move Location:
Save
Locate
Browse
Commit
Auto/Manual Secure Wipe & Delete
Automatic File Secure Delete & Wipe
Manual File Secure Delete & Wipe
Software Update
Software Updater
Valid Until Trust
5/17/2025 6:45:29 PM Ultimate
Main
File Task
Folder Task
Text Task
Secure Wipe & Delete
Key Store
Lock
QR Code
X509
Exit



If there is an update available you will have the option to go to the website to get it or do nothing.



If there is no Internet access the software will take about 12 seconds to notify you. That's because it tries to check a couple of times.

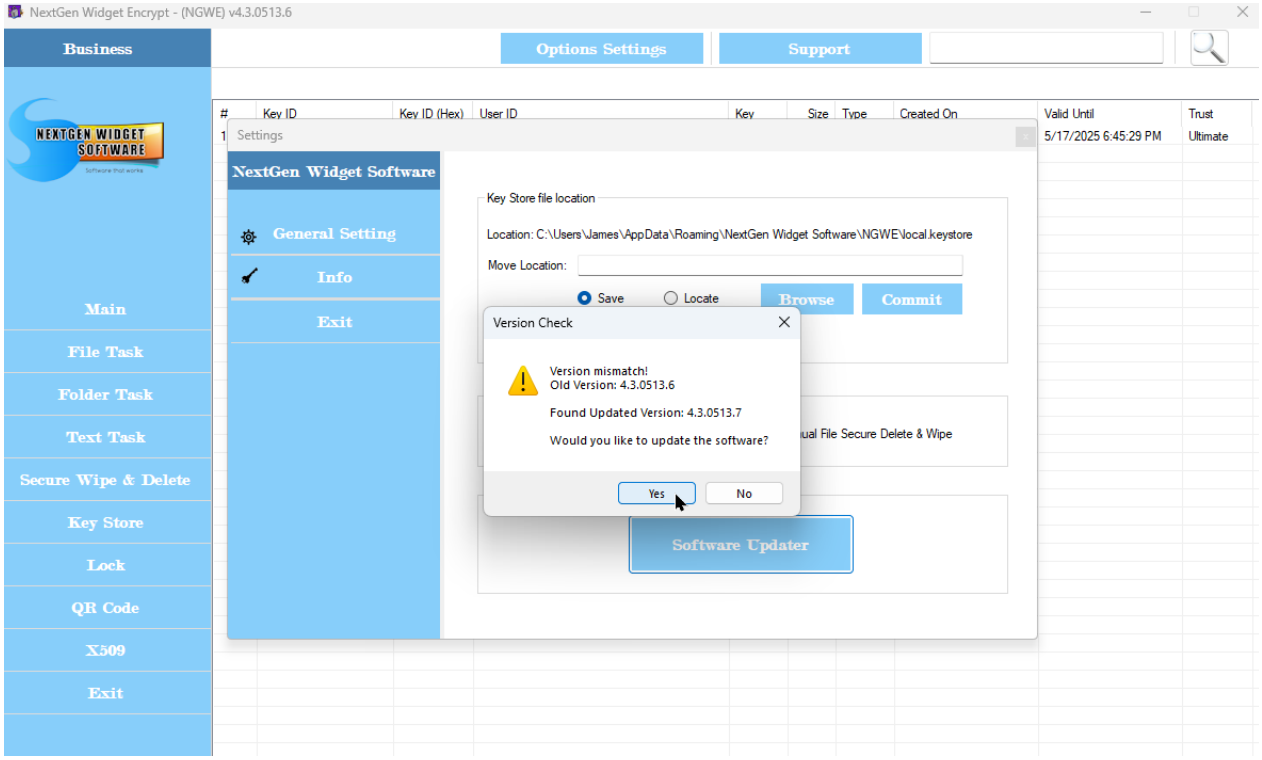


Subscription

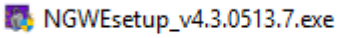
Renewing Subscription
Renewing your subscription.

Renewing Subscription

Subscriptions are for one year which include updates, both major, minor or bug fixes. First you will need to check for a software update. Sign into NextGen Widget Encrypt, click on Options Settings, Software Updater. Click on yes it will take you to the website to be able to download the updated version. Place the installer and any directory you wish but remember the directory.



Next, close NextGen Widget Encrypt and double-click on the installer. In this example it's "NGWEsetup_v4.3.0513.7.exe". Follow the directions of the installer and you're done



The installer will install NextGen Widget Encrypt in the program files directory unless you you choose a different location.

It will create a desktop shortcut and in the program start up it creates a shortcut to the uninstall program. Uninstalling the program is just as easy as installing it. However, the uninstaller will not remove your Key Store file. This file is created by NextGen Widget Encrypt and as a result the installer is not aware of it.

You can choose to keep this file or delete it.

System requirements

- Windows 10, 11
- .Net Framework 4.8

- PC Administrative Privileges
- Do not use in software development environment or debugging environment.

Getting help

Getting help is easy. Simply go to our support ticket system (https://www.ngwidgetsoftware.com/helpdesk/), click "Sign In", Create an account. Enter your eMail address, your name, phone number, time zone, create a secure password and click Register.

You will receive an welcome email from us with a confirm your account link. Just click the link and you'll automatically be logged in. Then click open a new ticket, your help topic, enter the issue summary and your message. Click "Create Ticket.

Once you create your ticket you will see the ticket status and support ticket number. You will also receive an email from us with the ticket number and a link to view the ticket progress.

Although we will acknowledge emails this is the best way to contact us so that we can make sure that any questions or issues you may have are taking care of immediately.

DISCLAIMER OF WARRANTIES

DISCLAIMER OF WARRANTIES

YOU ACKNOWLEDGE AND AGREE THAT THE SOFTWARE NEXTGEN WIDGET ENCRYPT IS PROVIDED TO YOU ON AN "AS IS" BASIS. THE LICENSOR NEXTGEN WIDGET ENCRYPT DISCLAIMS ANY AND ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY, OR HARDWARE OR SOFTWARE COMPATIBILITY, OR FITNESS FOR A PARTICULAR PURPOSE OR USE, INCLUDING YOUR PARTICULAR BUSINESS OR INTENDED USE, OR OF THE SOFTWARE'S RELIABILITY, PERFORMANCE OR CONTINUED AVAILABILITY. THE LICENSOR DOES NOT REPRESENT OR WARRANT THAT THE SOFTWARE OR CALCULATIONS OR PRINTS OR EXPORT DATA MADE THEREOF

WILL BE FREE FROM VIRUSES, MALWARE, TROJAN HORSES OR ANY OTHER DEFECTS OR ERRORS AND THAT ANY SUCH EFFECTS OR ERRORS WILL BE CORRECTED, OR THAT IT WILL OPERATE WITHOUT INTERRUPTION. HOWEVER, THE LICENSOR DOES NOT PUT VIRUSES, MALWARE OR TROJANS IN THE SOFTWARE. YOU AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR ALL COSTS AND EXPENSES ASSOCIATED WITH RECTIFICATION, REPAIR OR DAMAGE CAUSED BY SUCH DEFECTS, ERRORS OR INTERRUPTIONS. FURTHER, THE LICENSOR DOES NOT REPRESENT AND WARRANT THAT THE SOFTWARE DOES NOT INFRINGE THE INTELLECTUAL PROPERTY RIGHT OF ANY OTHER PERSON. YOU ACCEPT RESPONSIBILITY TO VERIFY THAT THE SOFTWARE MEETS YOUR SPECIFIC REQUIREMENTS.

LIMITATION OF LIABILITY

IN NO EVENT SHALL THE LICENSOR BE LIABLE TO YOU OR ANY THIRD PARTY UNDER THIS AGREEMENT OR OTHERWISE, WHETHER BY WAY OF INDEMNIFICATION OR OTHERWISE, UNDER ANY THEORY OF LIABILITY WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, NEGLIGENCE AND STRICT LIABILITY) FOR ANY DIRECT OR INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES OR REVENUE, LOST PROFITS OR EXPECTED BENEFIT NOT ACHIEVED, WHETHER FORESEEABLE OR NOT, WHETHER IN AN ACTION IN CONTRACT, TORT, PRODUCT LIABILITY OR STATUTE OR OTHERWISE, EVEN IF THE LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, RELATING TO THE SOFTWARE OR YOUR USE THEREOF, OR INABILITY TO USE THE SOFTWARE WHETHER OR EVEN IF THE LICENSOR HAS BEEN ADVISED, KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES AND WITHOUT REGARD AS TO WHETHER SUCH LOSS OR DAMAGE WAS FORESEEABLE OR NOT. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, THE LICENSOR HAS NO OBLIGATION TO PROVIDE AND YOU SHALL HAVE NO RIGHT TO SEEK ANY REMEDY FOR ANY DEFECT, ERROR OR FAILURE OF THE SOFTWARE.

NOTHING IN THIS AGREEMENT SHALL EXCLUDE OR LIMIT EITHER PARTY'S LIABILITY FOR DEATH OR PERSONAL INJURY CAUSED BY THEIR NEGLIGENCE OR FOR FRAUDULENT MISREPRESENTATION.

THE LICENSOR SHALL NOT HAVE ANY LIABILITY TO YOU OR THIRD PARTIES FOR THE LOSS OF INFORMATION OR OTHER LOSS RELATING TO THE SOFTWARE OR THE USE THEREOF OR FOR THE INTERPRETATION OF THE DESIGN NORMS OR DESIGN STANDARDS AND THEIR NATIONAL ANNEXES OR NATIONAL NON-CONTRADICTORY COMPLEMENTARY INFORMATION (NCCI) DOCUMENTS. THE INTERPRETATION OF THE TYPE APPROVALS OR CERTIFICATES OF PRODUCTS INCLUDED IN THE SOFTWARE, THE CALCULATIONS OR PRINTS OR DESIGNS OR EXPORT DATA OUTPUT FROM THE SOFTWARE, OR OTHERWISE OF THE ACCURACY, RELIABILITY, CONTINUED AVAILABILITY OF THE SOFTWARE. THE LICENSOR SHALL HAVE NO DUTY TO VERIFY, CORRECT, COMPLETE OR UPDATE THE SOFTWARE.

THE LIMITATIONS OF LIABILITY UNDER THIS AGREEMENT ARE VALID TO THE EXTENT AS PERMITTED BY THE APPLICABLE MANDATORY LAW. YOU ACKNOWLEDGE THAT YOU UNDERSTAND AND AGREE TO THE DISCLAIMERS OF WARRANTIES AND THE LIMITATIONS ON LIABILITY AND REMEDIES CONTAINED IN THIS AGREEMENT. YOU FURTHER ACKNOWLEDGE THAT THE SOFTWARE IS BEING PROVIDED TO YOU WITHOUT A FEE OR WITH A REASONABLE FEE, THAT THE DISCLAIMERS AND LIMITATIONS ARE MATERIAL PROVISIONS OF THIS AGREEMENT AND THAT THE LICENSOR WOULD NOT MAKE THE SOFTWARE AVAILABLE TO YOU IF SUCH DISCLAIMERS AND LIMITATIONS WERE DELETED OR MODIFIED TO BE MORE FAVORABLE TO YOU.

YOUR USE OF THE SOFTWARE

YOU AGREE THAT THE SOFTWARE IS PROVIDED TO YOU ENTIRELY FOR USE AT YOUR OWN RISK, ALTHOUGH THE LICENSOR HAS USED COMMERCIALLY REASONABLE EFFORTS TO CONTROL AND UPDATE THE SOFTWARE AND TO VERIFY THAT THE SOFTWARE CALCULATES ACCORDING TO THE VALID TIMBER DESIGN STANDARDS, THEIR NATIONAL ANNEXES AND NATIONAL NONCONTRADICTORY COMPLEMENTARY INFORMATION (NCCI) DOCUMENTS. AT ALL TIMES YOU SHALL USE THE LATEST UPDATED VERSION OF THE SOFTWARE. YOU MAY NOT USE THE SOFTWARE FOR ANY MISSION CRITICAL OR REAL TIME APPLICATIONS AND IT IS AN EXPRESS REQUIREMENT OF THIS AGREEMENT THAT ANY OUTPUT FROM THE SOFTWARE IS THOROUGHLY CHECKED PRIOR TO IMPLEMENTATION. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT THE

USE OF THE SOFTWARE DOES NOT ELIMINATE THE NEED TO CARRY OUT AN EXPERT CONTROL OF THE DESIGN.

REFUND POLICY

WE HAVE A "NO REFUND" POLICY ON TRY-BEFORE-YOU-BUY SO PLEASE EVALUATE THE SOFTWARE BEFORE PURCHASE.

AFTER PAYMENT APPROVAL WE WILL SEND YOU AN ACTIVATION KEY TO UNLOCK OUR SOFTWARE. THIS KEY CAN BE USED INDEFINITELY AND ONLY REQUIRES THE PURCHASE OF AN ADDITIONAL LICENSE KEY IF YOU CHOOSE TO FOR MAINTENANCE (MAJOR, MINOR, BUG FIX AND UPDATES) AFTER THE YEAR. ONCE THE KEY IS EMAILED THERE WILL BE NO REFUNDS. THIS POLICY MUST BE STRICTLY ENFORCED TO ENSURE THE INTEGRITY OF OUR SOFTWARE. IT IS IMPOSSIBLE FOR YOU TO RETURN YOUR REGISTERED VERSION OF OUR SOFTWARE.

THIS IS WHY WE STRONGLY RECOMMEND THAT ALL USERS DOWNLOAD, INSTALL AND TEST THOROUGHLY THE TRIAL VERSION TO MAKE SURE IT IS SUITABLE FOR YOUR PURPOSES BEFORE YOU PURCHASE.