

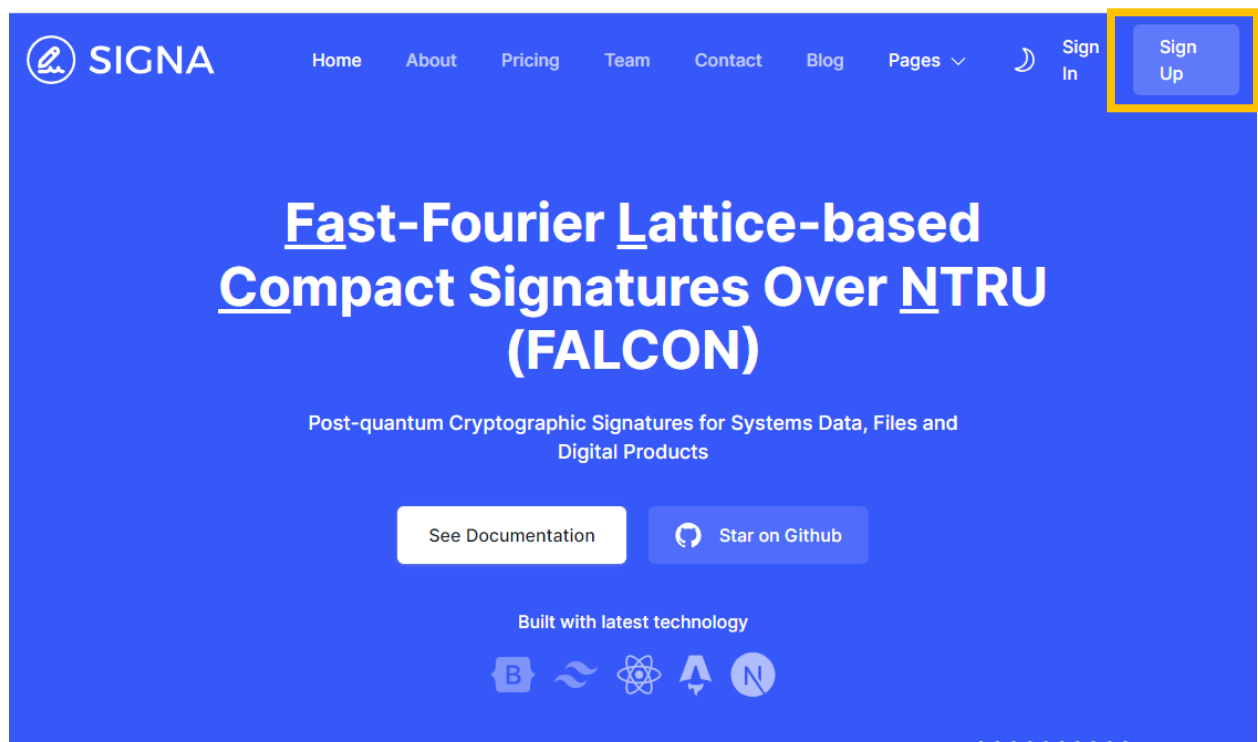
# USER GUIDE

# General Information

## Welcome to FALCON: Your Go-To for Post-Quantum Cryptographic Signatures

Welcome to the Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) user guide. Here, you'll find everything you need to know about leveraging our cutting-edge post-quantum cryptographic signatures to secure your system data, files, and digital products.

Whether you're a developer integrating FALCON into your applications, an IT professional safeguarding sensitive data, or simply someone interested in the future of cryptography, this guide will walk you through all aspects of using FALCON. We've covered everything from installation and setup to advanced configurations and best practices. First and foremost, you must create an account by clicking the Sign-Up button to get started




# Signing Up

You can begin signing up by entering your Username, Email, Password, and Confirmation Password. Ensure the Password and Confirmation Password are identical. Then click Sign Up.

## Sign Up

It's quick and easy.

[Home](#) / [Sign Up](#)



[Sign Up](#)

By creating an account you are agree with our [Privacy and Policy](#)

Already have an account? [Sign In](#)


# Signing In

After signing up, you will go to the login page. Enter your email and password to log in. Then click Sign In

## Sign In

Sign in to start your session.

[Home](#) / [Sign In](#)



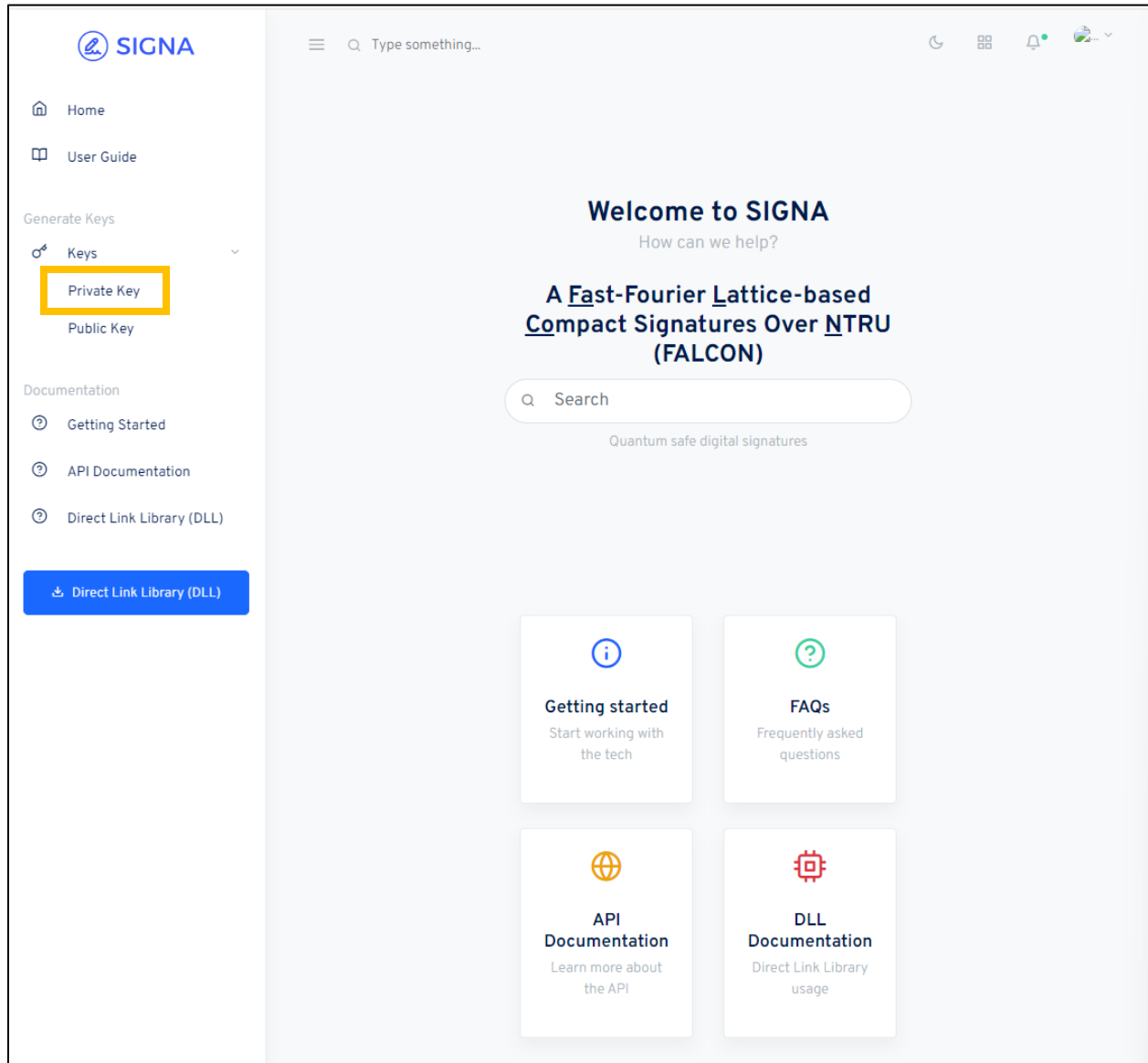
[Sign In](#)

[Forget Password?](#)

Not a member yet? [Sign Up](#)

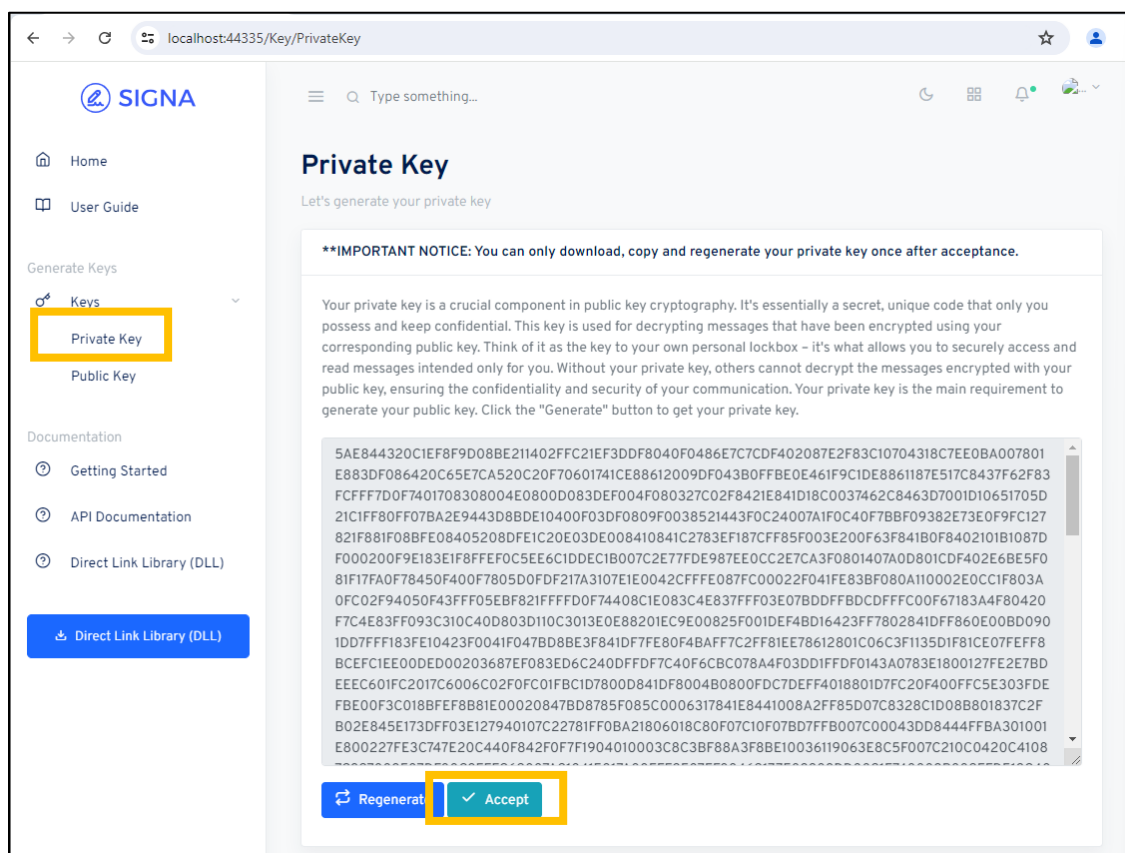
# Homepage

The homepage has info about the app. Use the navigation bar to reach other modules. Click "Private Key" to generate your private key.



# Private Key

Your private key is a crucial component in public key cryptography. It's essentially a secret, unique code that only you possess and keep confidential. This key is used for decrypting messages that have been encrypted using your corresponding public key. Think of it as the key to your own personal lockbox – it's what allows you to securely access and read messages intended only for you. Without your private key, others cannot decrypt the messages encrypted with your public key, ensuring the confidentiality and security of your communication. Your private key is the main requirement to generate your public key. Click the "Generate" button to get your private key. You can regenerate your key if necessary. A copy of your private key will be downloaded after clicking the accept button. After Acceptance of the private key, proceed to public key menu.



# Public Key

Your public key is a fundamental element in public key cryptography, serving as the counterpart to your private key. Unlike the private key, which you keep secret, your public key is freely shared with others. It's essentially a piece of information that allows anyone to encrypt messages intended for you securely. Once encrypted with your public key, only your corresponding private key can decrypt these messages, ensuring that only you can access the information. The public key serves as a digital identifier, enabling secure communication and data exchange in a variety of contexts, from email encryption to online transactions. Click the "Generate" button to get your public key. Then click Generate to generate your public key. A copy of your private key will be downloaded after clicking the accept button.

[Direct Link Library \(DLL\)](#)

Download or copy your public key here.

Your public key is a fundamental element in public key cryptography, serving as the counterpart to your private key. Unlike the private key, which you keep secret, your public key is freely shared with others. It's essentially a piece of information that allows anyone to encrypt messages intended for you securely. Once encrypted with your public key, only your corresponding private key can decrypt these messages, ensuring that only you can access the information. The public key serves as a digital identifier, enabling secure communication and data exchange in a variety of contexts, from email encryption to online transactions. Click the "Generate" button to get your public key.

### Your public key

Empty ...

# Generate

# Certification

Once your public key is accepted, a new "Certification" menu will appear in the navigation bar. Enter your personal information and click the Update Information button to update your primary information.

The screenshot shows the SIGNA web application interface. On the left is a navigation sidebar with the SIGNA logo at the top. Below the logo are links for 'Home' and 'User Guide'. A section titled 'Generate Keys' contains links for 'Keys', 'Private Key', and 'Public Key'. A 'Documentation' section includes links for 'Getting Started', 'API Documentation', and 'Direct Link Library (DLL)'. At the bottom of the sidebar is a blue button labeled 'Direct Link Library (DLL)'. The main content area is titled 'Certify' with the subtitle 'Certify your personal information here to receive a certificate'. Below this is a 'Certification form' section. It features a profile picture placeholder (a red square) and a 'Fullname' label next to a text input field. Below these are several input fields for personal information: 'First name', 'Last name', 'Middle name', 'Username', 'Email' (with a '.com' suffix), 'Mobile number', 'Address', 'Company', and 'Position'. At the bottom of the form is a blue button labeled 'Update Information', which is highlighted with a yellow rectangular border.



# Certification continued

Upload your profile picture, first valid ID, and second valid ID using the "Choose File" button. Double-check your information for accuracy, as the administrator will use it to activate your account. Click the Certify button to generate your information signature. Wait for the administrator to activate your account.

API Documentation

Direct Link Library (DLL)

Direct Link Library (DLL)

Profile picture

Choose File No file chosen

First valid ID

Choose File No file chosen

Second valid ID

Choose File No file chosen

Public Key

0A8AFA04DBEBE357A290A1F24A5DC665050186  
D0A0687D8D3D463C11958DF8A10BF71F784F15E  
0E77B84A4BF167C4A9ED7063CC9A5231B8DA35  
54630E672EA15A952AEB93D51BF558E1602AA0  
BEE8FE9B8493729066461FB931112981F168FB05  
7847AB149AA156A4ECA00D4662AF8511BB5BC88  
18051A263E499E9BAED59AAB5609A52FCA3506  
9ED38AA71A83A5F82297241580335EC2A8A9EF  
EC1995CEF84CD09225C0A6F9F3564BB3A1BCC8  
...

Private Key

5AE844320C1EF8F9D08BE211402FFC21EF3DDF8  
040F0486E7C7CDF402087E2F83C10704318C7EE  
0BA007801E883DF086420C65E7CA520C20F706  
01741CE88612009DF043B0FFBEOE461F9C1DE88  
61187E517C8437F62F83FCFFF7D0F74017083080  
04E0800D083DEF004F080327C02F8421E841D1  
8C0037462C8463D7001D10651705D21C1FF80FF0  
7BA2E9443D8BDE10400F03DF0809F003852144  
3F0C24007A1F0C40F7BBF09382E73E0F9FC1278  
...

Certificate

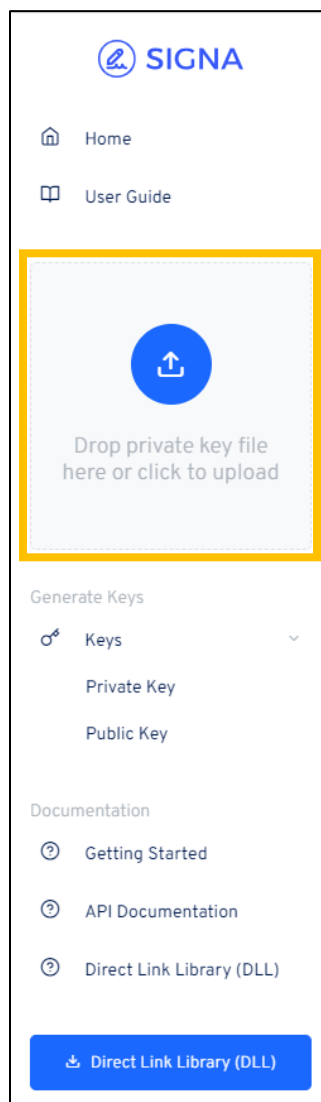
Empty ...

Certify

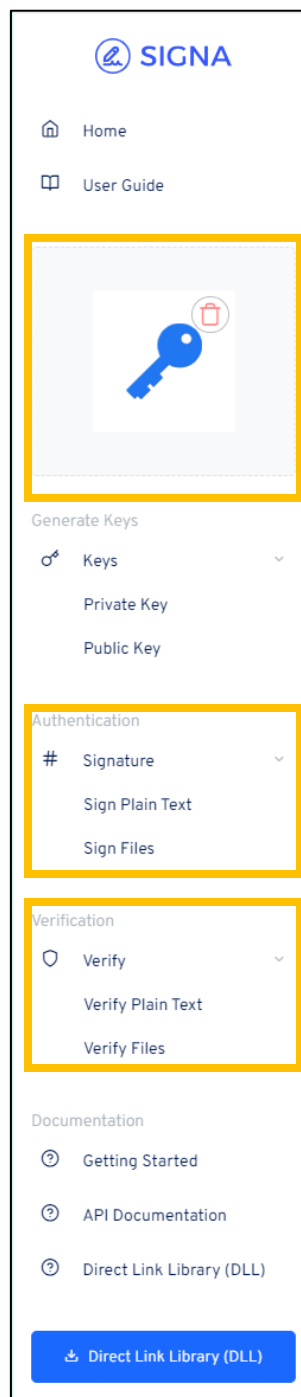
# Private Key Slot

After certification, a new menu item will appear in the navigation bar. The private key slot functions as the app's keyhole and only accepts a user's private key. It verifies the uploaded private key to ensure ownership. When your private key is accepted, the Signatory and Verification menu will be added to the navigation bar.

## Empty Private Key Slot

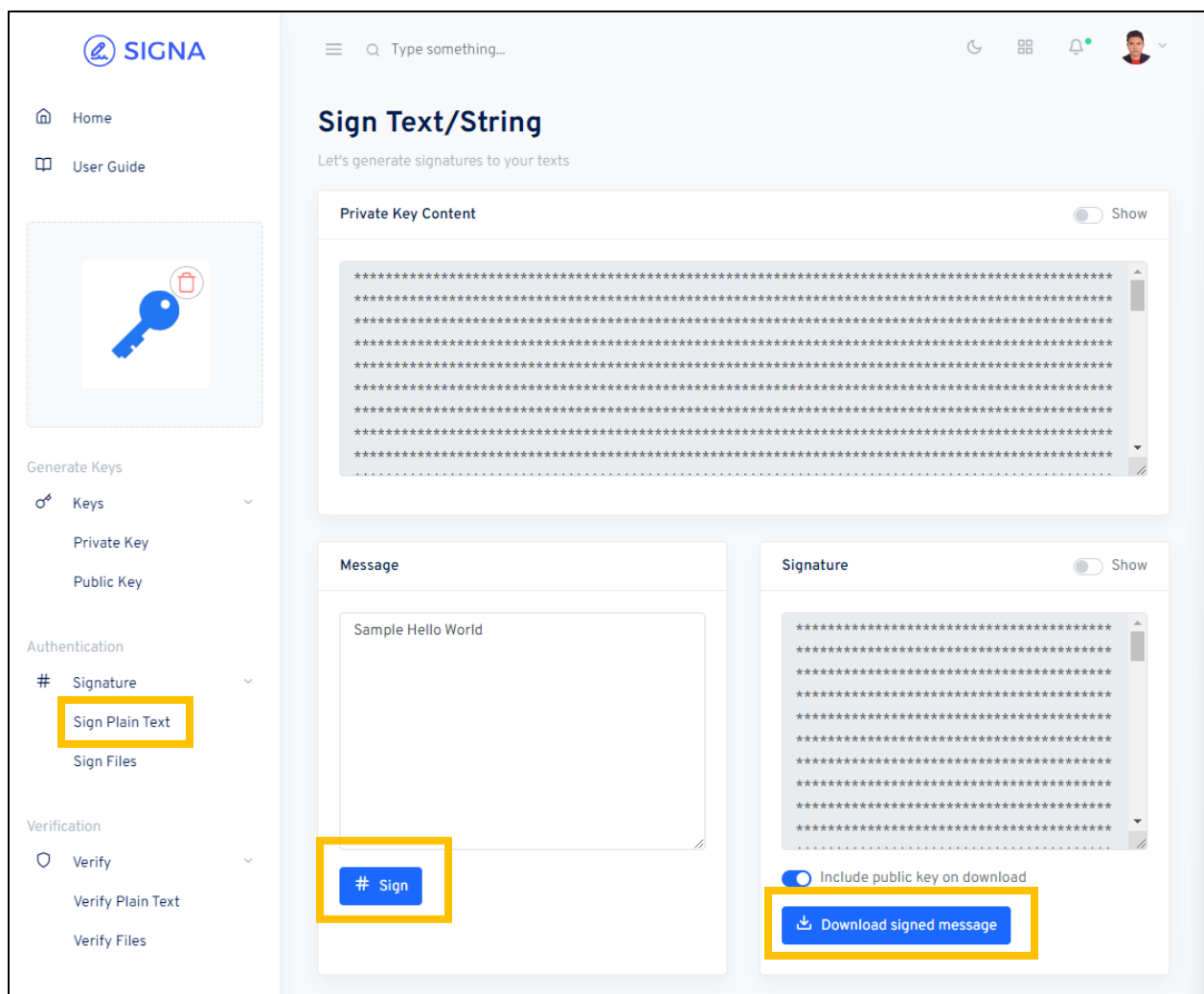


## Private Key Slot with accepted private key



# Signature – Sign Plain Text

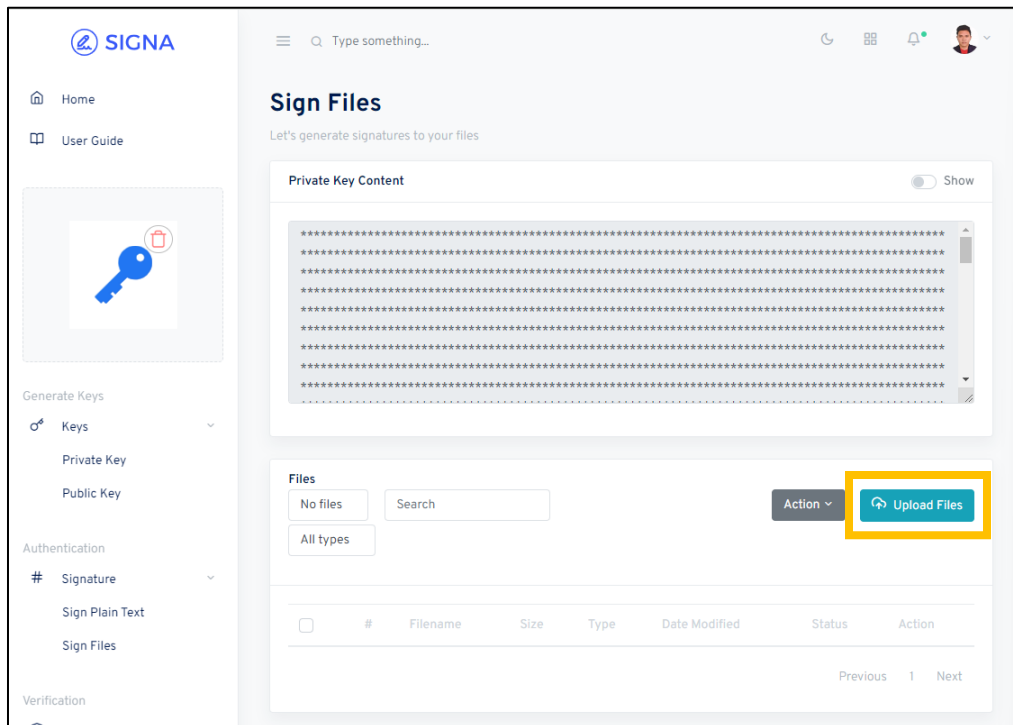
The "Sign a Plain Text" module allows you to sign any plain text. Enter your message in the Message section and click Sign. This generates a signature using your private key stored in the private key slot and the provided plain text message. You can download the zipped file of the signed message via the Download Signed Message button. You also show the contents of your private key and signature for further checking.



# Signature – Sign Files

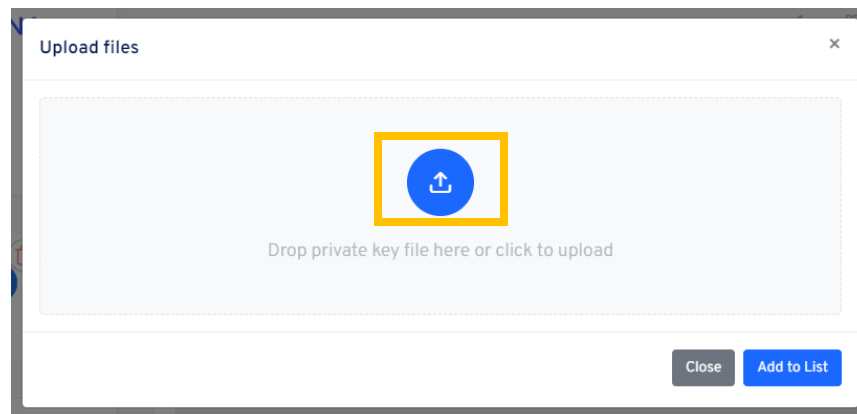
Sign files let you generate signatures of your files. First, you must click the Upload files button to show the file upload pop-up modal.

## Upload Files Button



## Empty Upload Files Pop-up modal

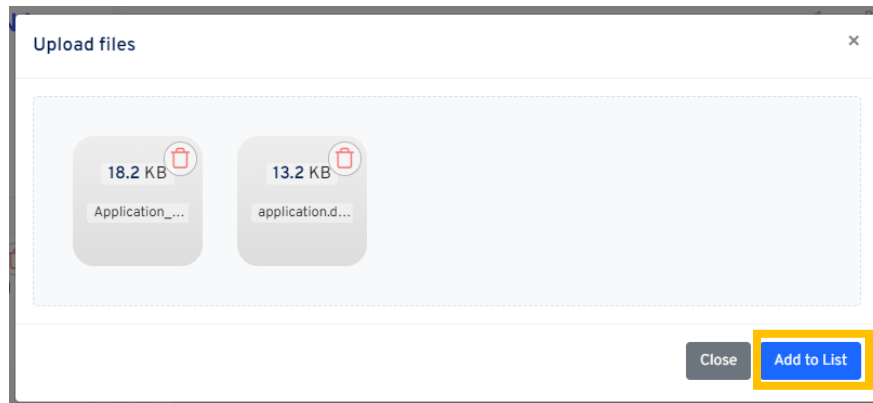
Click the circle upload button and choose your file to sign. The pop-up modal accepts any file type.



# Signature – Sign Files continued

## Upload Files Pop-up modal with uploaded files

You can add multiple files in the pop-up modal as many as you want. After choosing your files, click the Add to List button.



After clicking the Add to List button, all files in the pop-up modal will be transferred to the table below the private key section.

Files

10

Search

Action ▾

Upload Files

☒ Include public key on download

<input type="checkbox"/>	#	Filename	Size	Type	Date Modified	Status	Action
<input type="checkbox"/>	1	Application_Letter.docx	0.02 MB	docx	6/14/24 1:46 PM	UNSIGNED	# Sign  Remove
<input type="checkbox"/>	2	application.docx	0.01 MB	docx	6/14/24 1:33 PM	UNSIGNED	# Sign  Remove

Previous 1 Next

# Signature – Sign Files continued

You can sign or remove all your added files at once by clicking the Action dropdown button. You can also individually sign or remove files using the individual Sign and Remove button. The default status of your file will be unsigned.

## Action Dropdown Button and individual Sign and Remove button

Files

10

Search

All types

Action ▾

Upload Files

# Sign all

Remove all

☒ Include public key on download

<input type="checkbox"/>	#	Filename	Size	Type	Date Modified	Status	Action
<input type="checkbox"/>	1	Application_Letter.docx	0.02 MB	docx	6/14/24 1:46 PM	UNSIGNED	# Sign Remove
<input type="checkbox"/>	2	application.docx	0.01 MB	docx	6/14/24 1:33 PM	UNSIGNED	# Sign Remove

Previous 1 Next

## Signature – Sign Files continued

After clicking the sign buttons, the status will be changed to signed and the Download Signature will replace the Sign button. If you wish to download the signature of the signed file click the Download Signature button to download the zipped file of your original file and its corresponding signature.

### Status and Download Signature button

Files

10

Search

Action ▾

Upload Files

All types

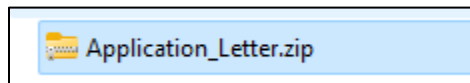
Include public key on download

<input type="checkbox"/>	#	Filename	Size	Type	Date Modified	Status	Action
<input type="checkbox"/>	1	Application_Letter.docx	0.02 MB	docx	6/14/24 1:46 PM	SIGNED	<div><div>Download Signature</div><div>Remove</div></div>
<input type="checkbox"/>	2	application.docx	0.01 MB	docx	6/14/24 1:33 PM	UNSIGNED	<div># Sign Remove</div>




Previous 1 Next

# Sample Contents of the downloaded zipped signature for files

The filename of the downloaded zipped file is the same as the filename of the signed file



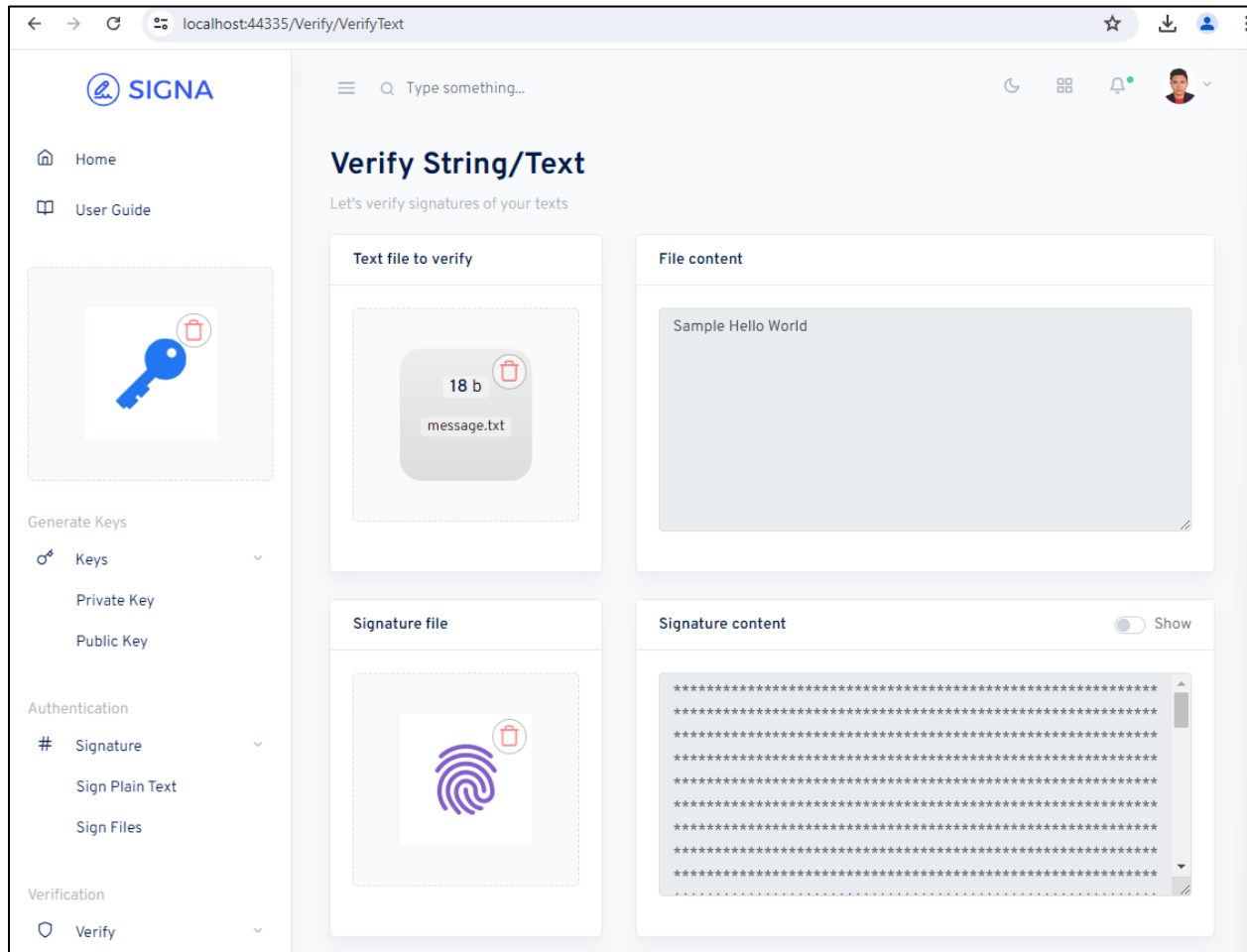
The contents of the zipped file will be the original file that is signed, the signature file (.sig), and the public key (.key) of the user with the username as the filename.

Name	Type	Compressed size
 Application_Letter.docx	Microsoft Word Document	18 KB
 Application_Letter.sig	SIG File	3 KB
 weigle.key	KEY File	4 KB



# Verify – Verify Plain Text

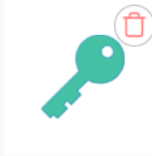
In the "Verify Plain Text" module, you can upload a .txt file in the "Text file to verify" section to open its contents. Additionally, upload a .sig file in the "Signature file" section to read the signature's contents.



## Verify – Verify Plain Text continued

Below the "Text file to verify" and "Signature file" sections, is the "Public key file section" You can choose to upload the public key by enabling the "Upload public key switch" and then choose the public key file of the signer. Otherwise, use the select box to select public keys stored in the app during public key generation.

### The Public Key file section Upload Public key switch Enabled

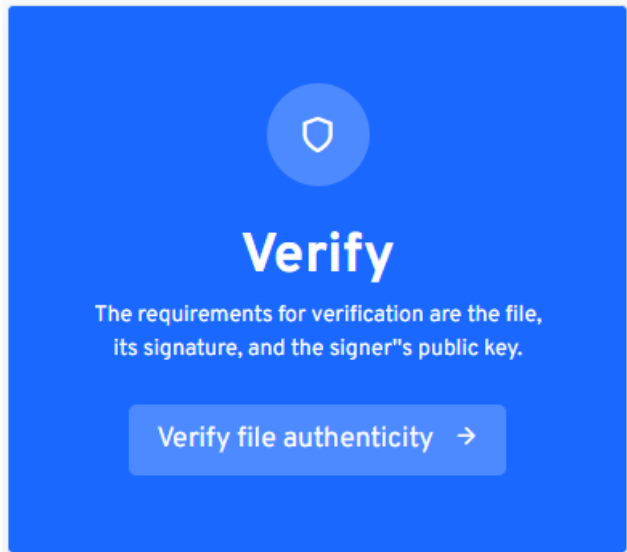
Public key file	Public key content
<p>Toggle upload signer public key</p> <p><input checked="" type="checkbox"/> Upload public key</p> <div></div>	<p>Owner: [REDACTED]</p> <p>Status: <span>Active</span></p> <pre>0A8AFA04DBEBE357A290A1F24A5DC665050186D0A0687D8D3D4 63C11958DF8A10BF71F784F15E0E77B84A4BF167C4A9ED7063CC9A 5231B8DA3554630E672EA15A952AEB93D51BF558E1602AA0BEE8 FE9B8493729066461FB931112981F168FB057847AB149AA156A4ECA 00D4662AF8511BB5BC8818051A263E499E9BAED59AAB5609A52F CA35069ED38AA71A83A5F82297241580335EC2A8A9EFEC1995CE F84CD09225C0A6F9F3564BB3A1BCC893D09166CIDA492BEDC98 856FCA214DC018681FD4830E141404D5B6671A2BB10A853C4472A B020A50408611E14AEC0FD10C7C5351835299044503785186D51A 00D4662AF8511BB5BC8818051A263E499E9BAED59AAB5609A52F CA35069ED38AA71A83A5F82297241580335EC2A8A9EFEC1995CE F84CD09225C0A6F9F3564BB3A1BCC893D09166CIDA492BEDC98 856FCA214DC018681FD4830E141404D5B6671A2BB10A853C4472A B020A50408611E14AEC0FD10C7C5351835299044503785186D51A</pre>

### The Public Key file section using the select box

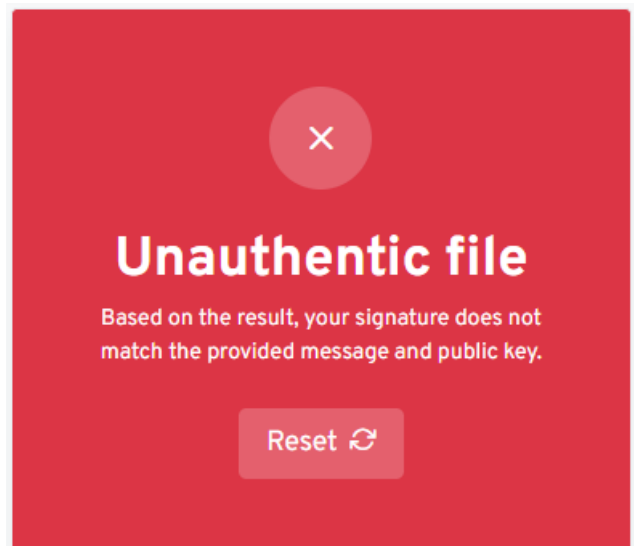
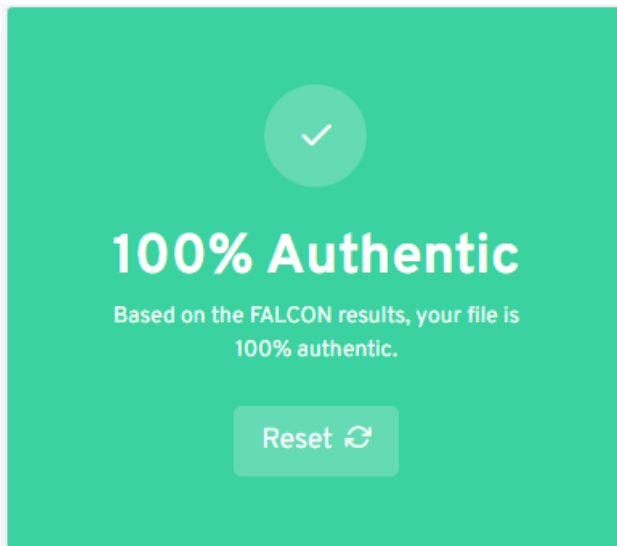
Public key file	Public key content
<p>Toggle upload signer public key</p> <p><input type="checkbox"/> Upload public key</p>	<p>Search signer's name or username here. Use @ when searching for username.</p> <p>@ [REDACTED] an</p> <pre>0A8AFA04DBEBE357A290A1F24A5DC665050186D0A0687D8D3D4 63C11958DF8A10BF71F784F15E0E77B84A4BF167C4A9ED7063CC9A 5231B8DA3554630E672EA15A952AEB93D51BF558E1602AA0BEE8 FE9B8493729066461FB931112981F168FB057847AB149AA156A4ECA 00D4662AF8511BB5BC8818051A263E499E9BAED59AAB5609A52F CA35069ED38AA71A83A5F82297241580335EC2A8A9EFEC1995CE F84CD09225C0A6F9F3564BB3A1BCC893D09166CIDA492BEDC98 856FCA214DC018681FD4830E141404D5B6671A2BB10A853C4472A B020A50408611E14AEC0FD10C7C5351835299044503785186D51A 00D4662AF8511BB5BC8818051A263E499E9BAED59AAB5609A52F CA35069ED38AA71A83A5F82297241580335EC2A8A9EFEC1995CE F84CD09225C0A6F9F3564BB3A1BCC893D09166CIDA492BEDC98 856FCA214DC018681FD4830E141404D5B6671A2BB10A853C4472A B020A50408611E14AEC0FD10C7C5351835299044503785186D51A</pre>

## Verify – Verify Plain Text continued

After uploading the text, signature and public key file, a Verify sections show below. Click the “Verify file authenticity” to verify your files.



The system shows a green result section if the file and signature is authentic otherwise a red result section if it is unauthentic.



# Verify – Verify Files

The "Verify Files" module verifies signed files using the signer's public key. For the public key, follow the same attachment process as shown in the Plain Text verification module, located above the Verify Files module.


## Verify Files

Let's verify signatures of your files

### Public key file

Toggle upload signer public key

☒ Upload public key



### Public key content

Owner:

Status: Active

```
0A8AFA04DBEBE357A290A1F24A5DC665050186D0A0687D8D3D4
63C11958DF8A10BF71F784F15E0E77B84A4BF167C4A9ED7063CC9A
5231B8DA3554630E672EA15A952AEB93D51BF558E1602AA0BEE8
FE9B8493729066461FB931112981F168FB057847AB149AA156A4ECA
00D4662AF8511BB5BC8818051A263E499E9BAED59AAB5609A52F
CA35069ED38AA71A83A5F82297241580335EC2A8A9EFEC1995CE
F84CD09225C0A6F9F3564BB3A1BCC893D09166CIDA492BEDC98
856FCA214DC018681FD4830E141404D5B6671A2BB10A853C4472A
B020A50408611E14AEC0FD10C7C5351835299044503785186D51A
...
```

The same process of file uploading process of files is shown in the verification module.

### Upload files

3.2 MB

Final-Defens...

24.7 KB

Application\_...

Close

Add to List

# Verify – Verify Files continued

Just click the verify button to verify the signed files using the signature and the public key files.

Files to verify

10

Search

Upload zip files

Upload raw files

All types

Action

Filename	Signature	Size	Type	Date Modified	Status	Action
Application_Letter.docx	Application_Letter.sig	0.02 MB	docx	6/21/24 11:41 PM	UNVERIFIED	<a href="#"># Verify</a> <a href="#">Remove</a>
Final-Defense_Minutes_Otacan.docx	Final-Defense_Minutes_Otacan.sig	3.06 MB	docx	6/21/24 11:41 PM	UNVERIFIED	<a href="#"># Verify</a> <a href="#">Remove</a>

Previous 1 Next

Authentic status shows on files that are verified authentic using the signature and the public key files.

Files to verify

10

Search

Upload zip files

Upload raw files

All types

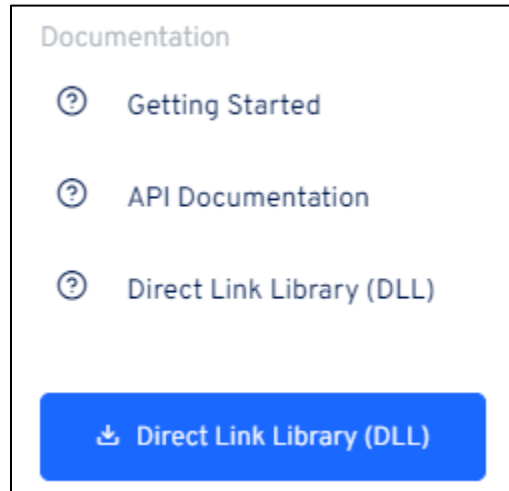
Action

Filename	Signature	Size	Type	Date Modified	Status	Action
Application_Letter.docx	Application_Letter.sig	0.02 MB	docx	6/21/24 11:41 PM	AUTHENTIC	<a href="#"># Verify</a> <a href="#">Remove</a>
Final-Defense_Minutes_Otacan.docx	Final-Defense_Minutes_Otacan.sig	3.06 MB	docx	6/21/24 11:41 PM	UNVERIFIED	<a href="#"># Verify</a> <a href="#">Remove</a>

Previous 1 Next

## Other Modules

Other modules include the Getting Started module, API Documentation, and DLL Documentation.



To download the Direct Link Library (DLL) of the FALCON Algorithm, click the download button for the Direct Link Library.

