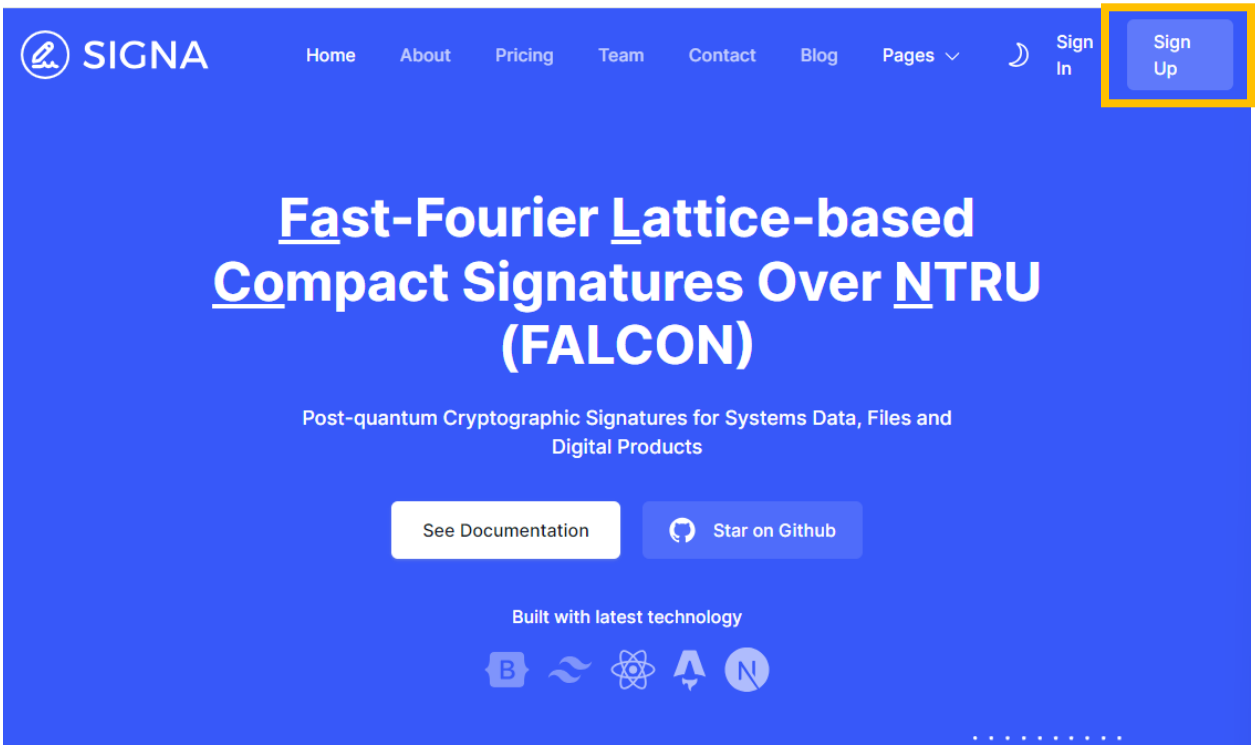
USER GUIDE

General Information

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

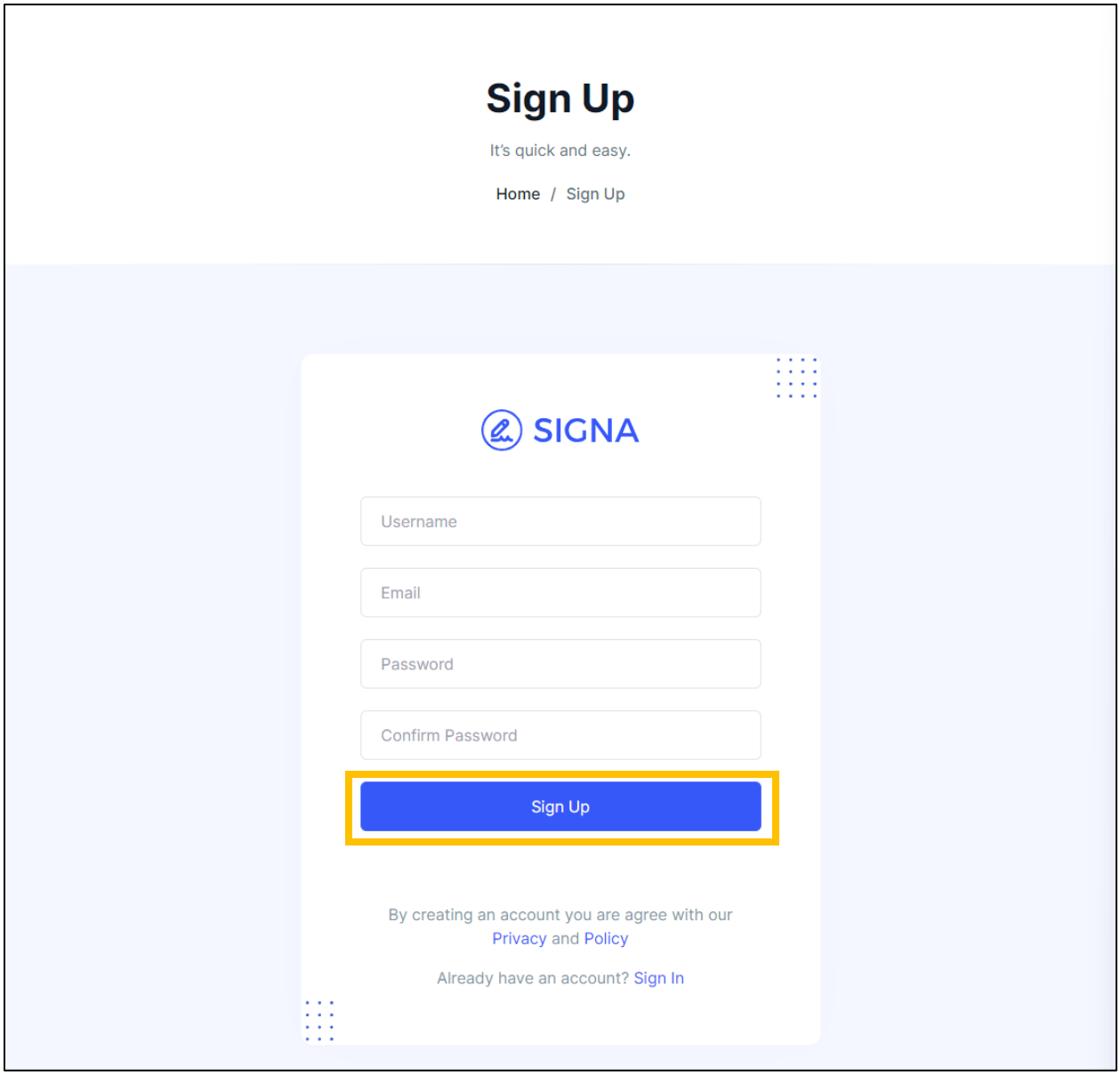
Welcome to the Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) user guide. Here, you'll find everything you need to know about leveraging our cutting-edge post-quantum cryptographic signatures to secure your system data, files, and digital products.

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



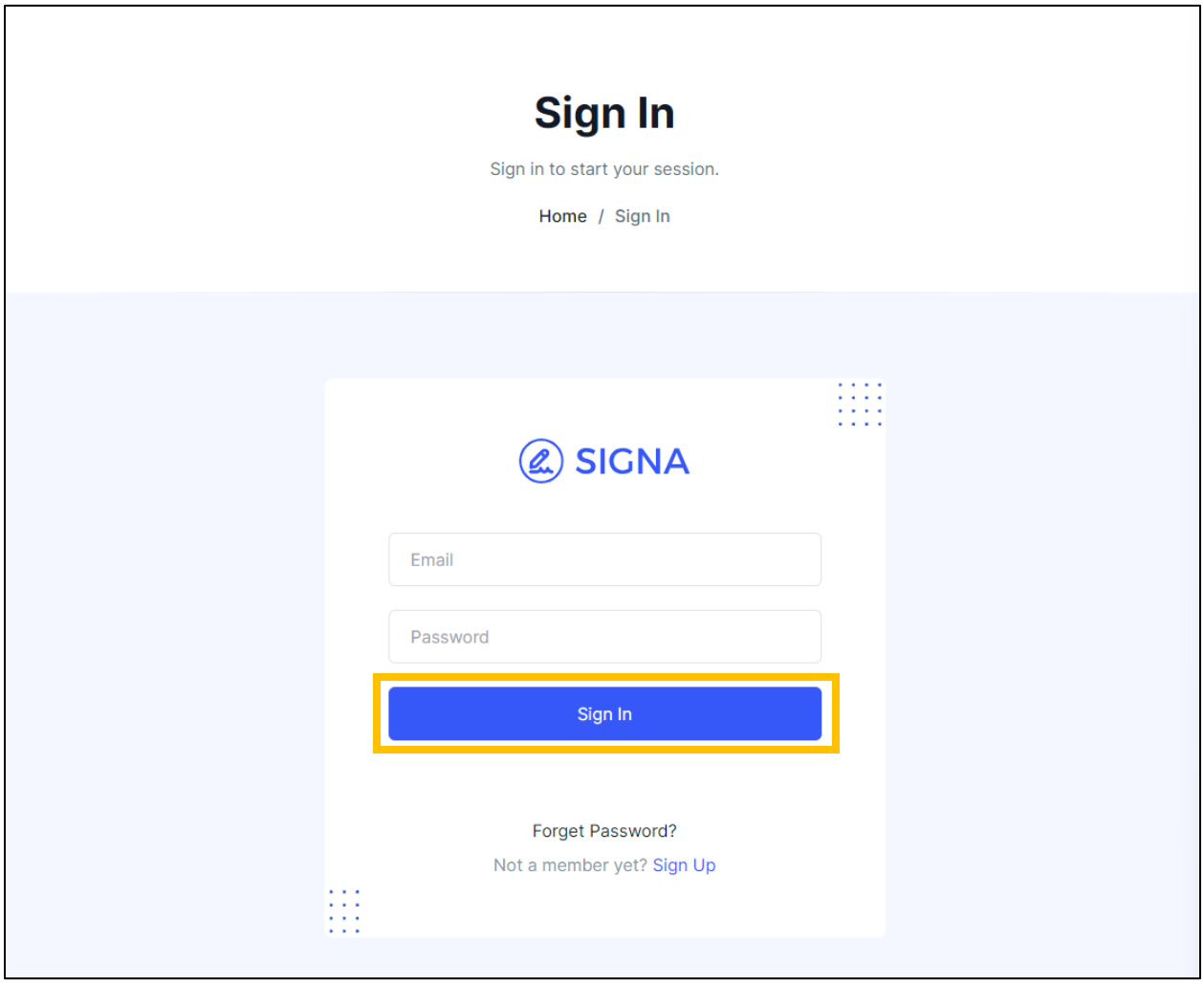
Signing Up

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.



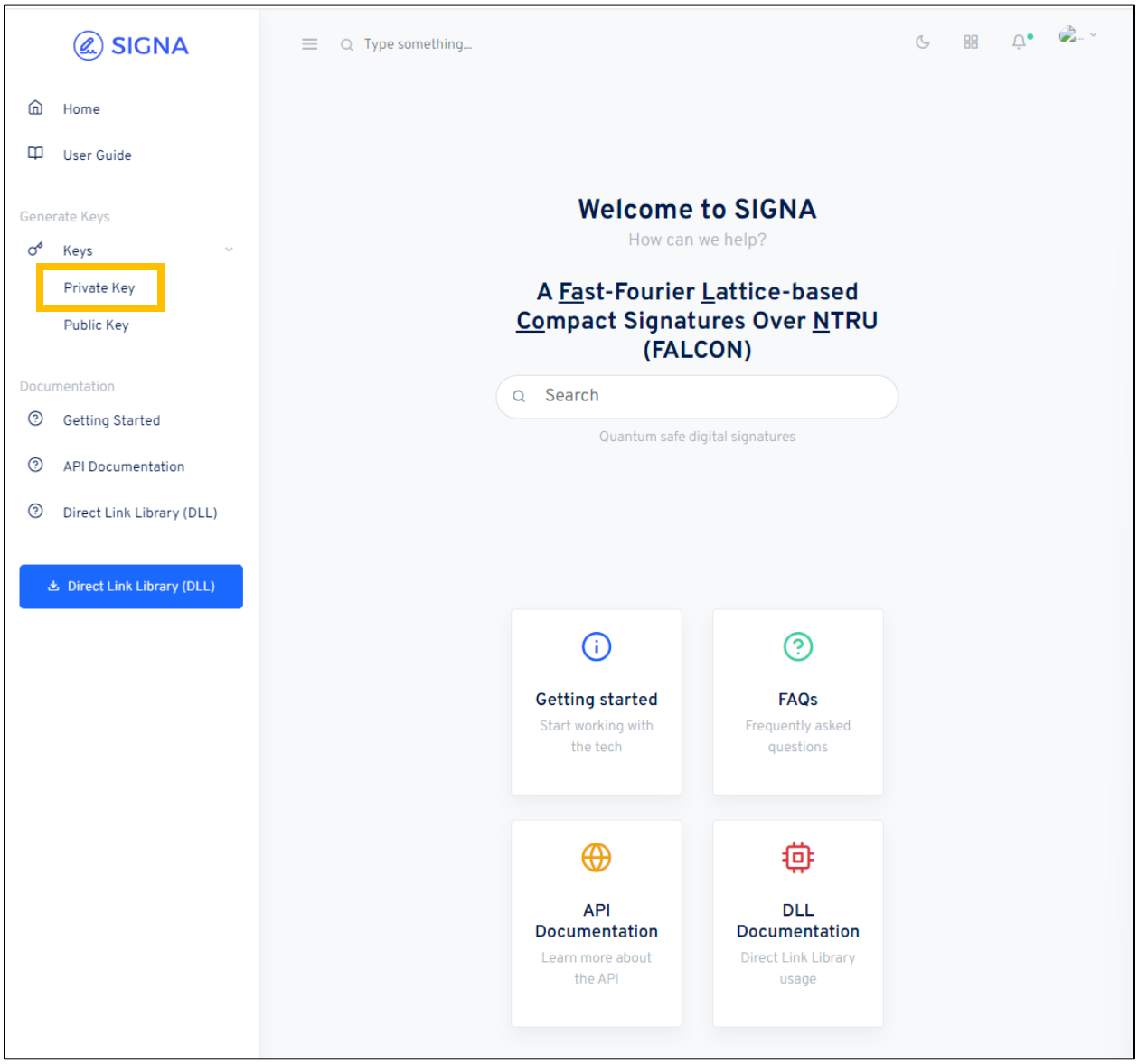
Signing In

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



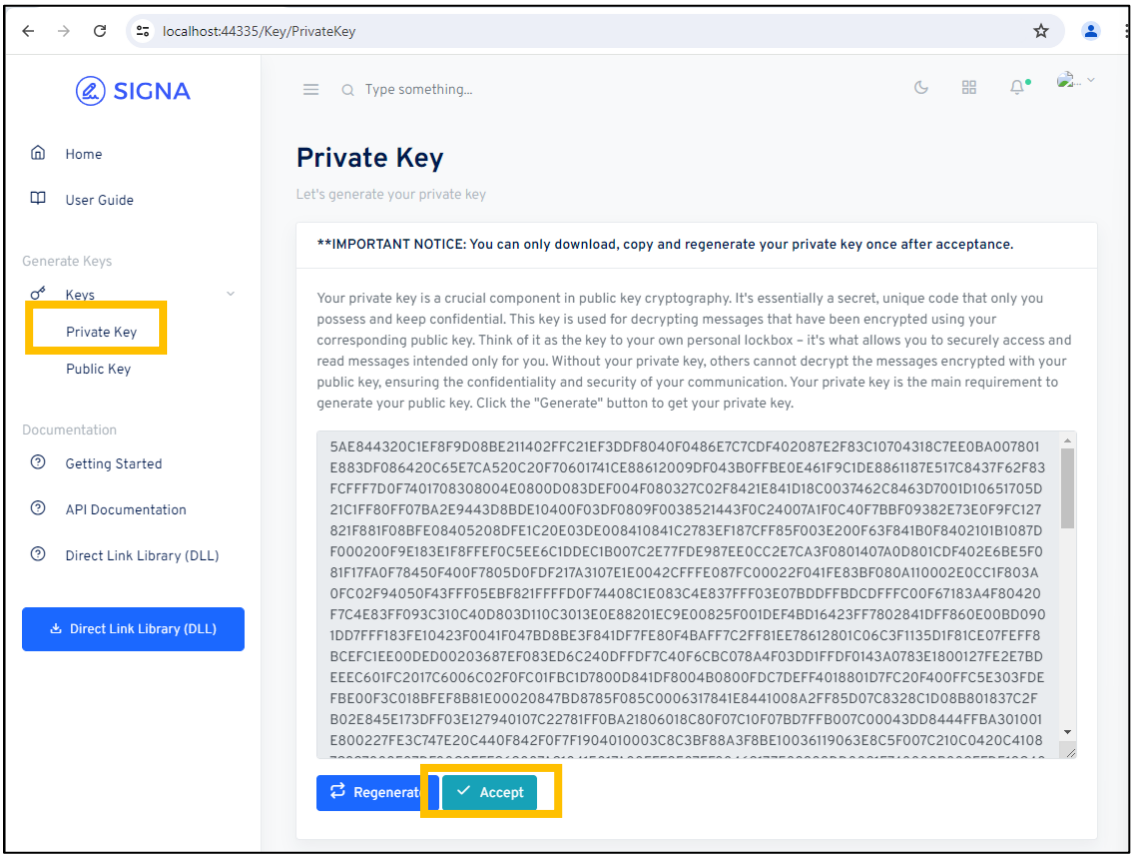
Homepage

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



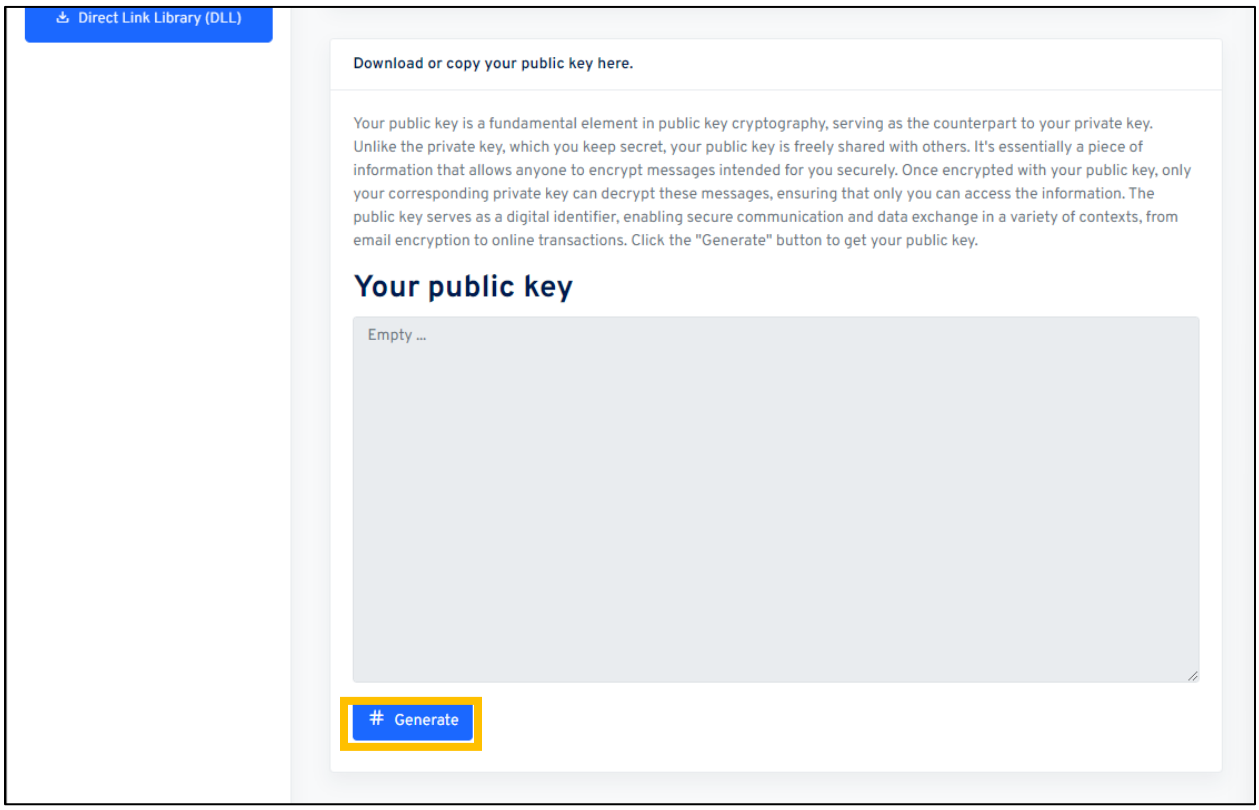
Private Key

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 re-generate 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.



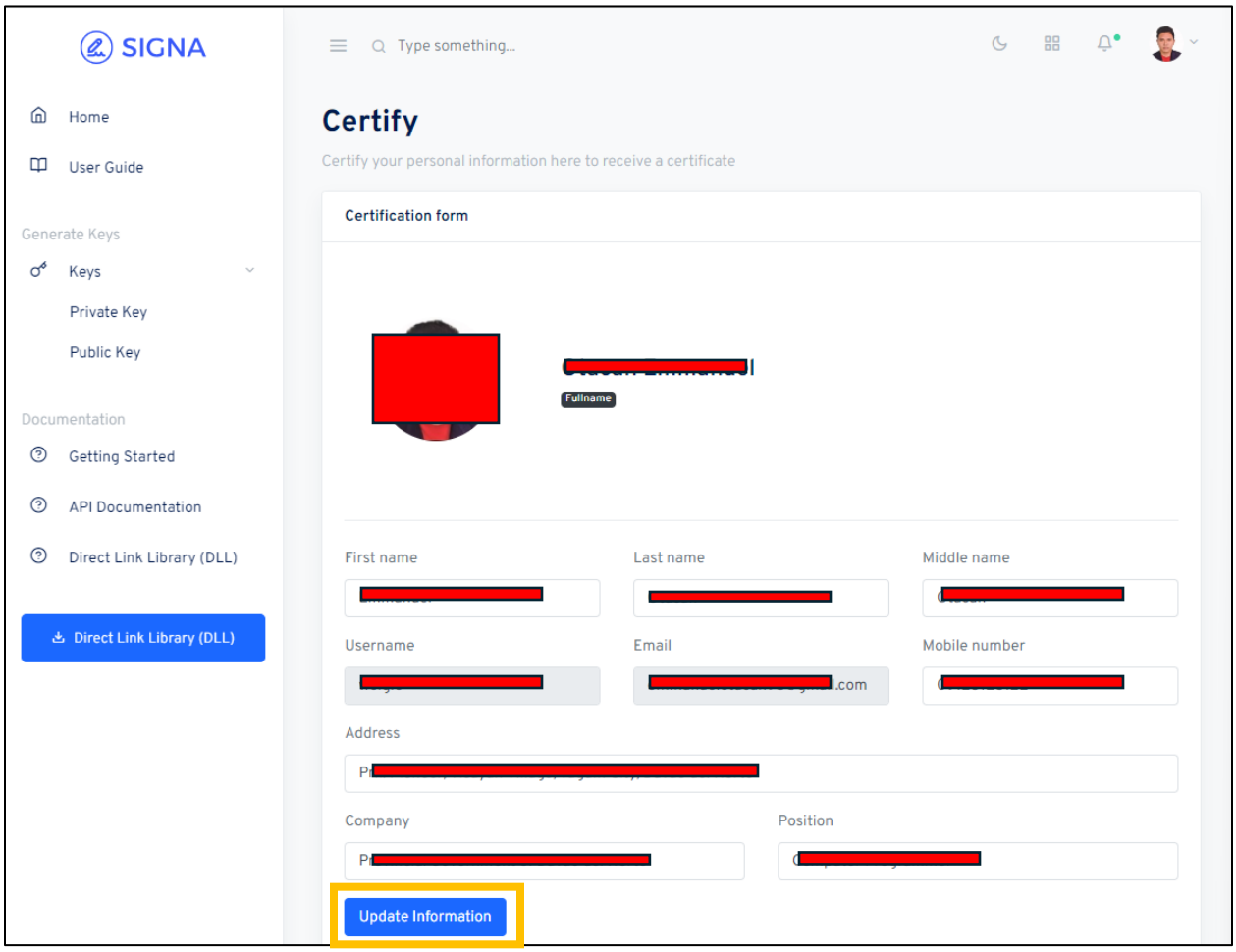
Public Key

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.



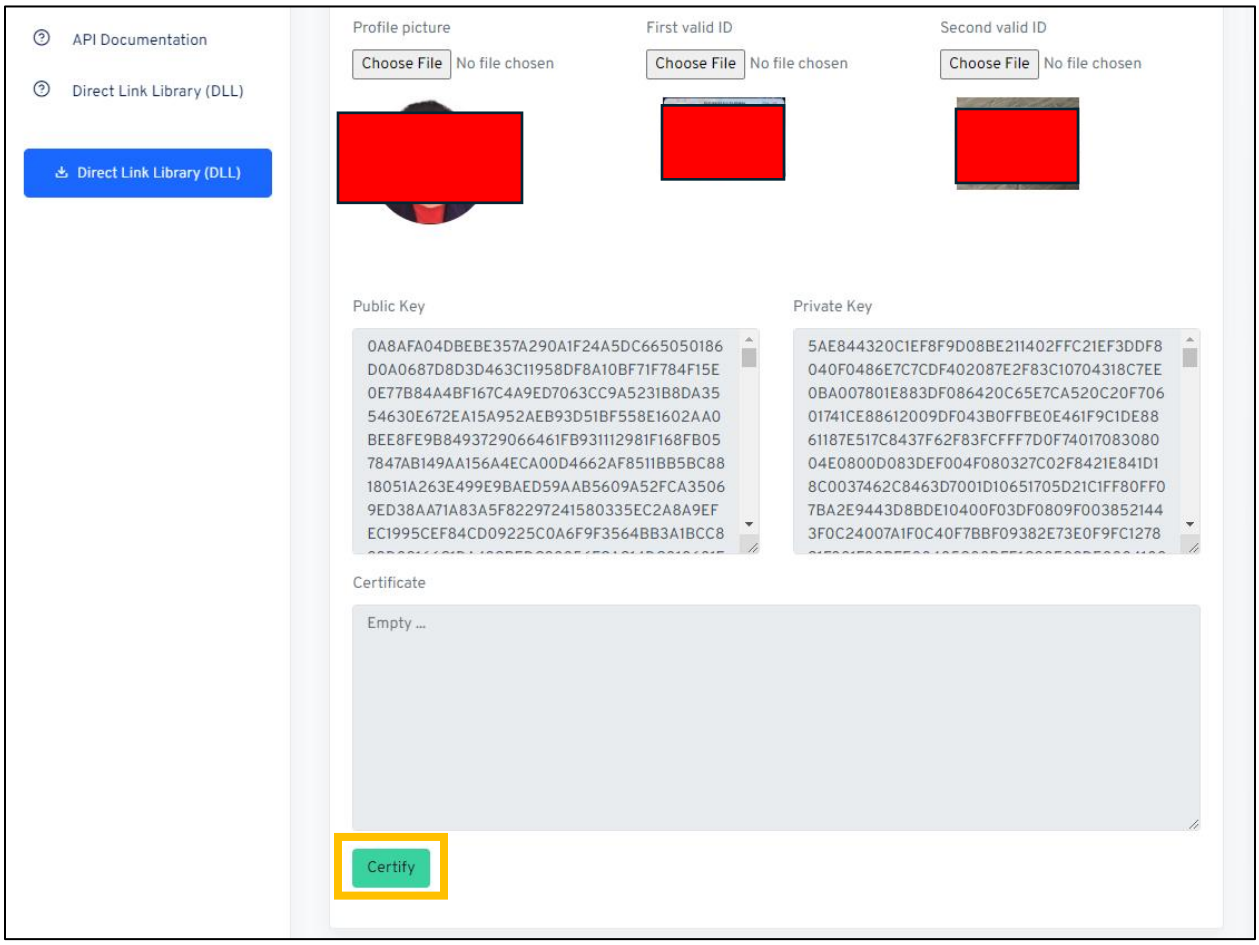
Certification

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.



Certification continued

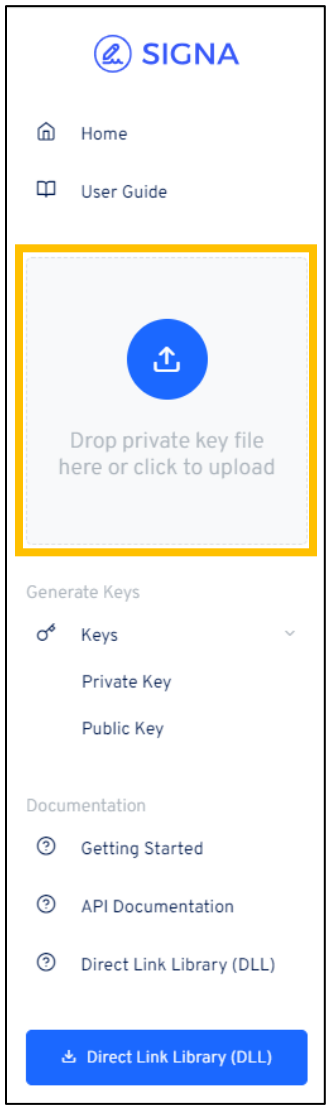
Upload your profile picture, first valid ID, and second valid ID using the "Choose File" button. Double-check your information for accuracy, as the administrator will use it to activate your account. Click the Certify button to generate your information signature. Wait for the administrator to activate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



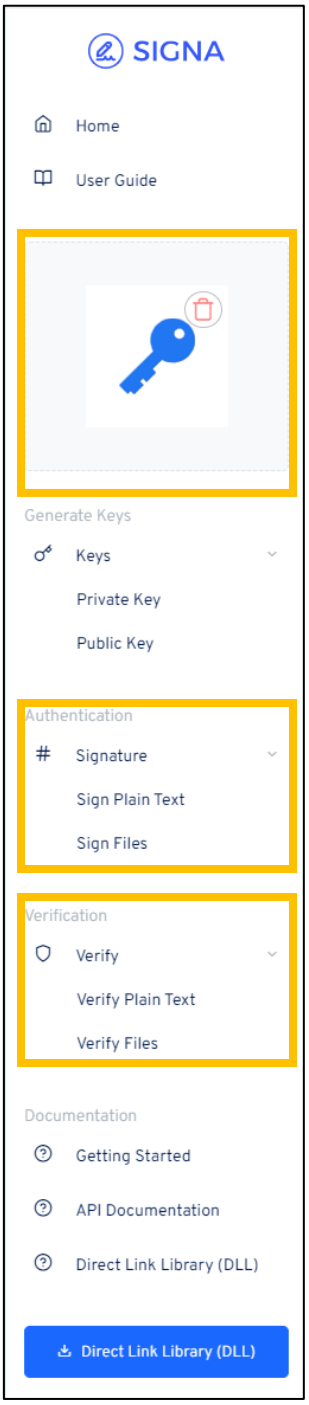
Private Key Slot

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

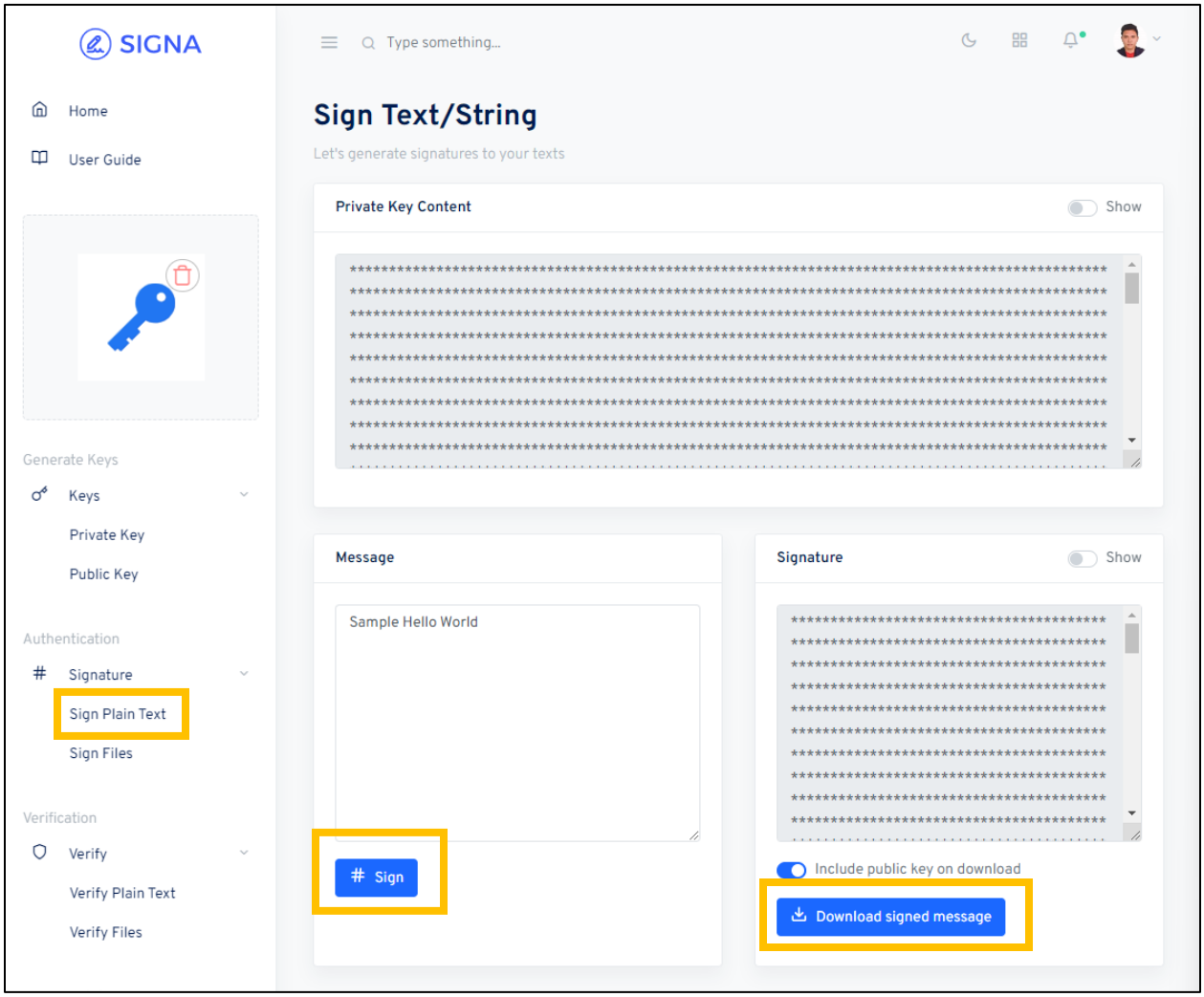


Private Key Slot with accepted private key



Signature – Sign Plain Text

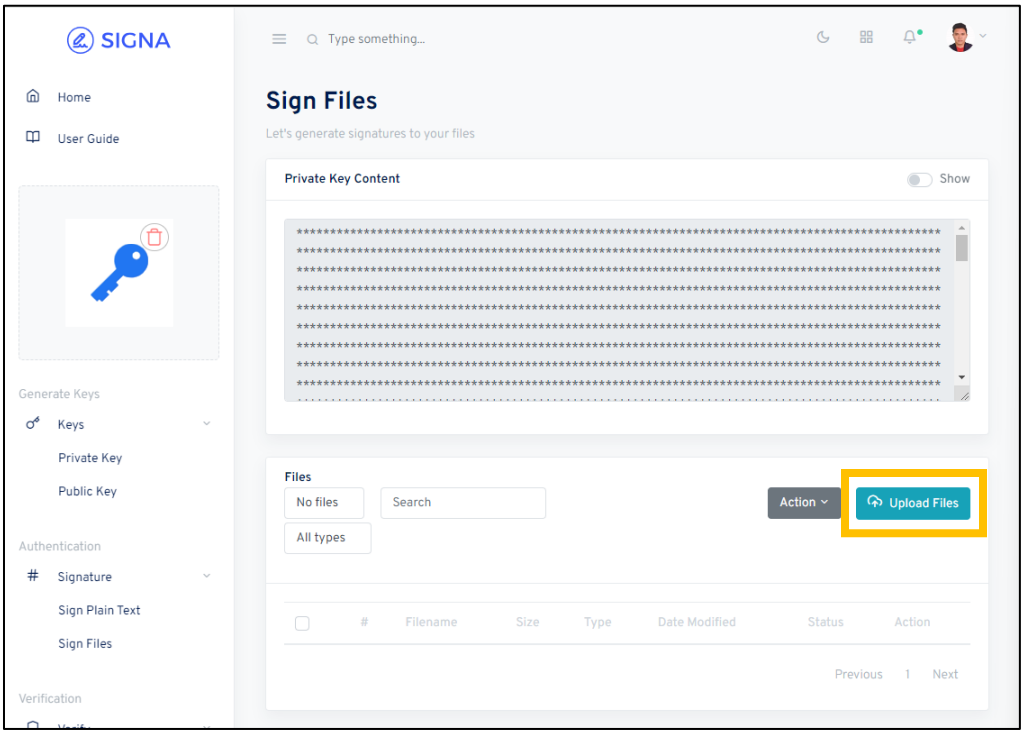
The "Sign a Plain Text" module allows you to sign any plain text. Enter your message in the Message section and click Sign. This generates a signature using your private key stored in the private key slot and the provided plain text message. You can download the zipped file of the signed message via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



Signature – Sign Files

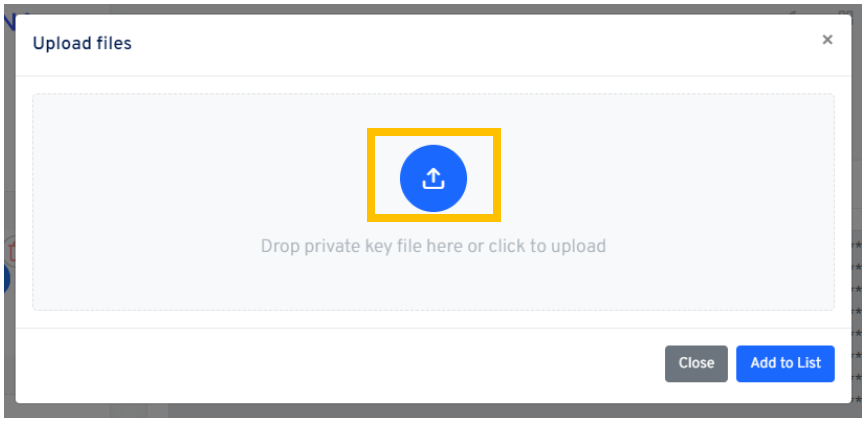
Sign files let you generate signatures of your files. First, you must click the Upload files button to show the file upload pop-up modal.

Upload Files Button



Empty Upload Files Pop-up modal

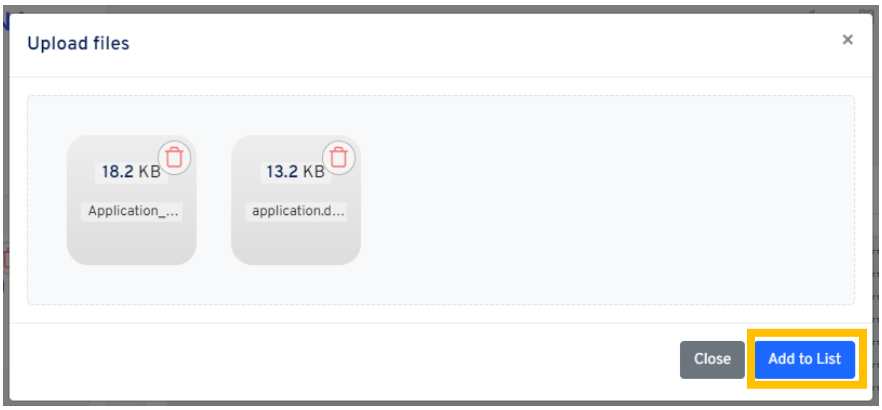
Click the circle upload button and choose your file to sign. The pop-up modal accepts any file type.



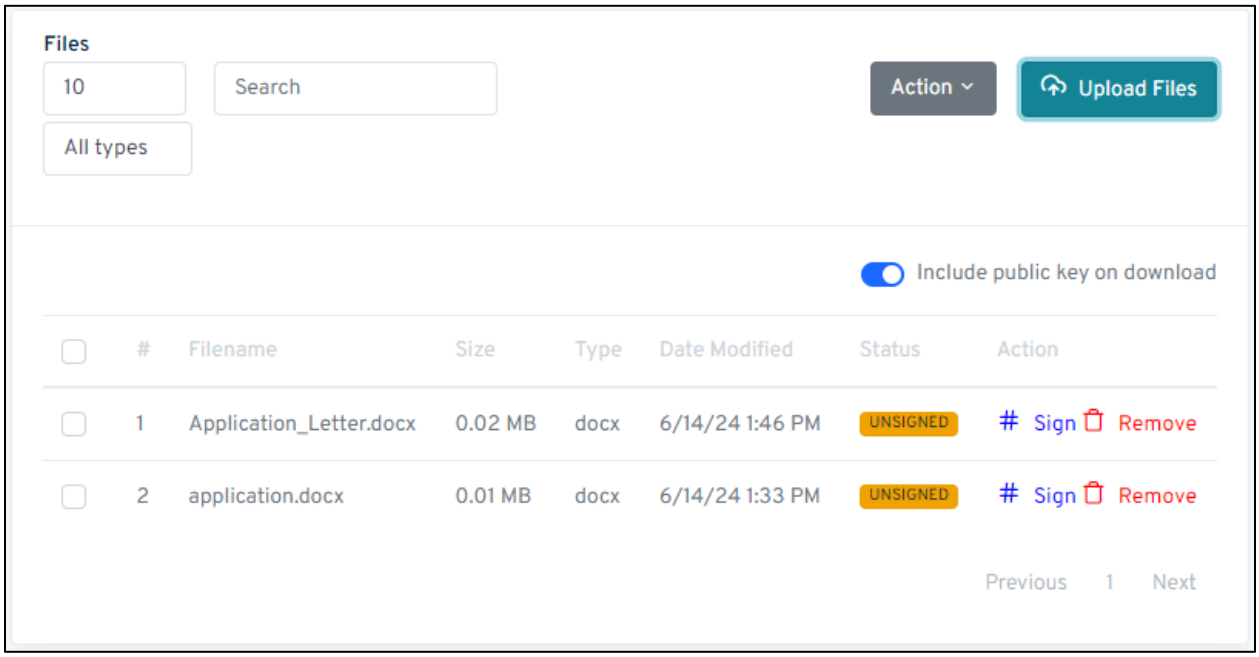
Signature – Sign Files continued

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.



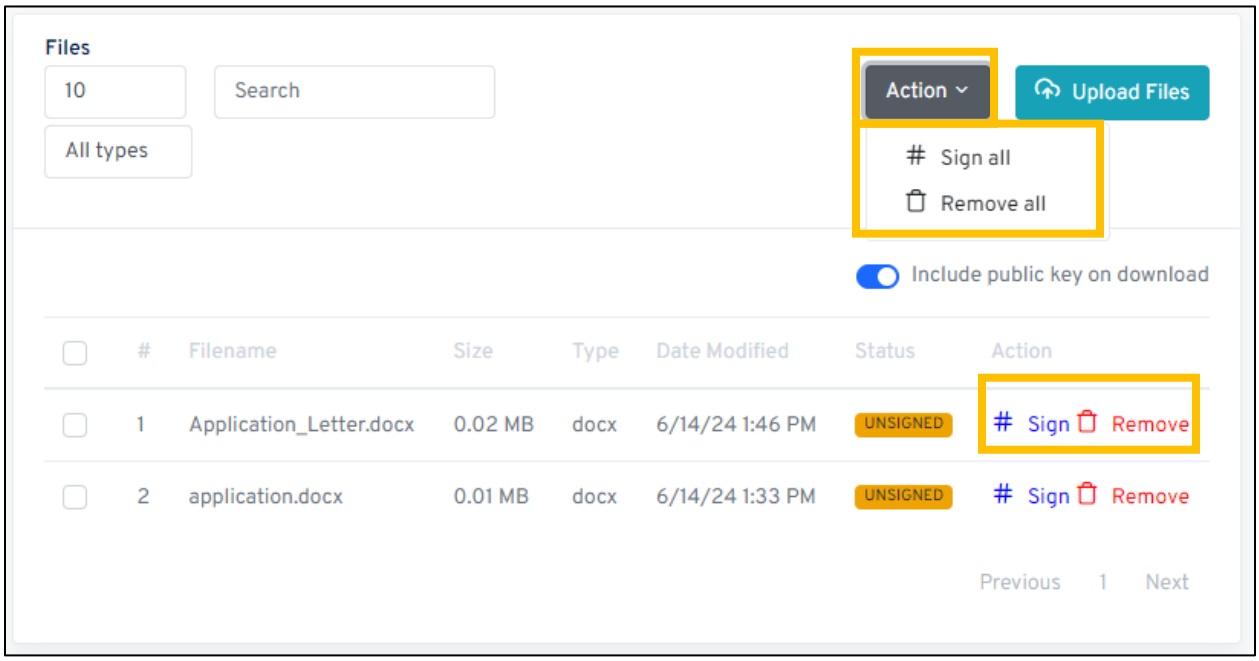
After clicking the Add to List button, all files in the pop-up modal will be transferred to the table below the private key section.



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.

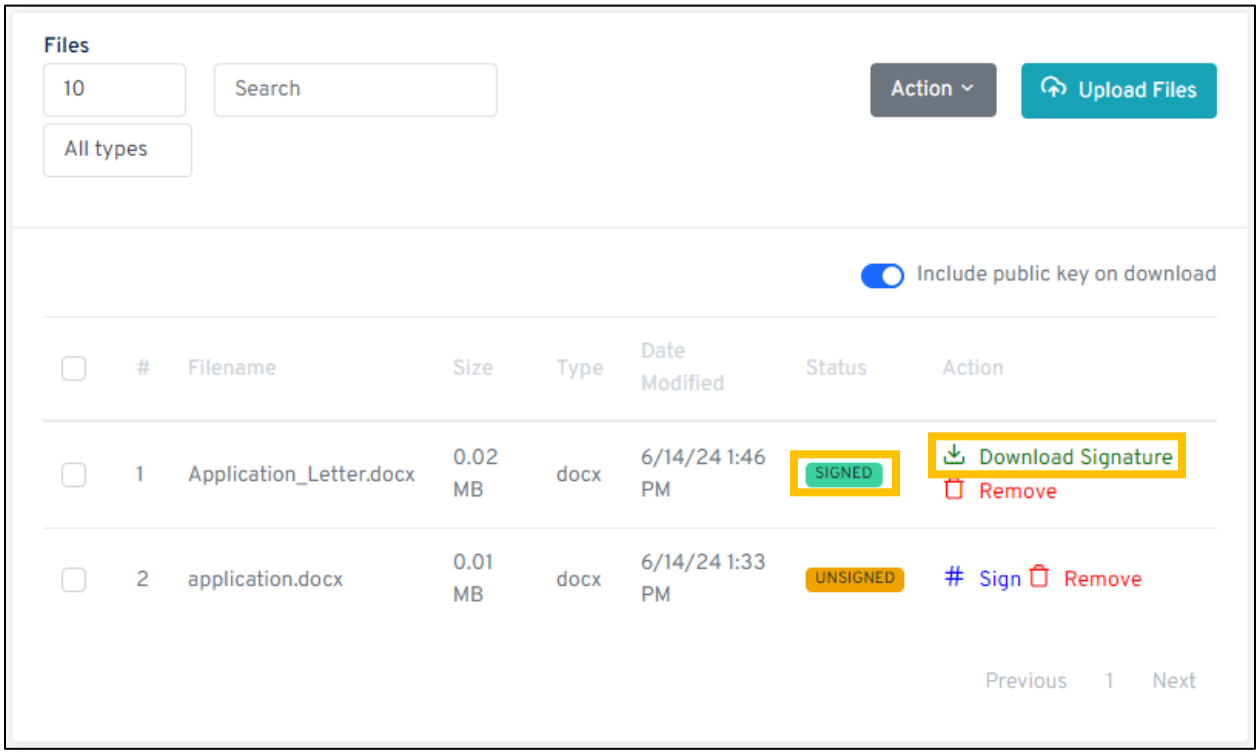
Action Dropdown Button and individual Sign and Remove button



Signature – Sign Files continued

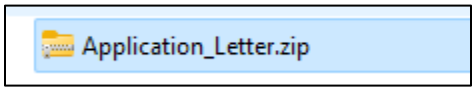
After clicking the sign buttons, the status will be changed to signed and the Download Signature will replace the Sign button. If you wish to download the signature of the signed file click the Download Signature button to download the zipped file of your original file and its corresponding signature.

Status and Download Signature button

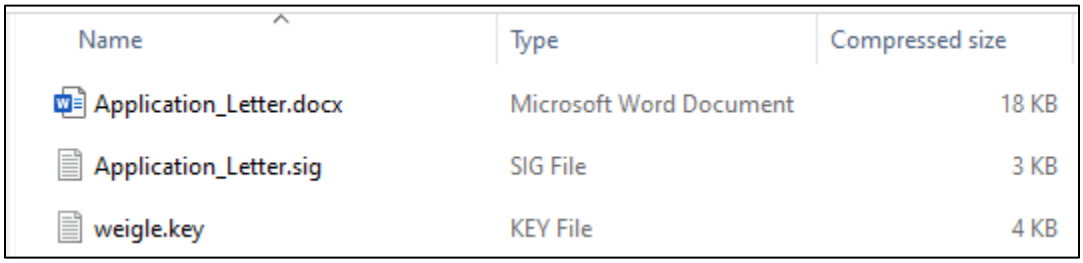


Sample Contents of the downloaded zipped signature for files

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



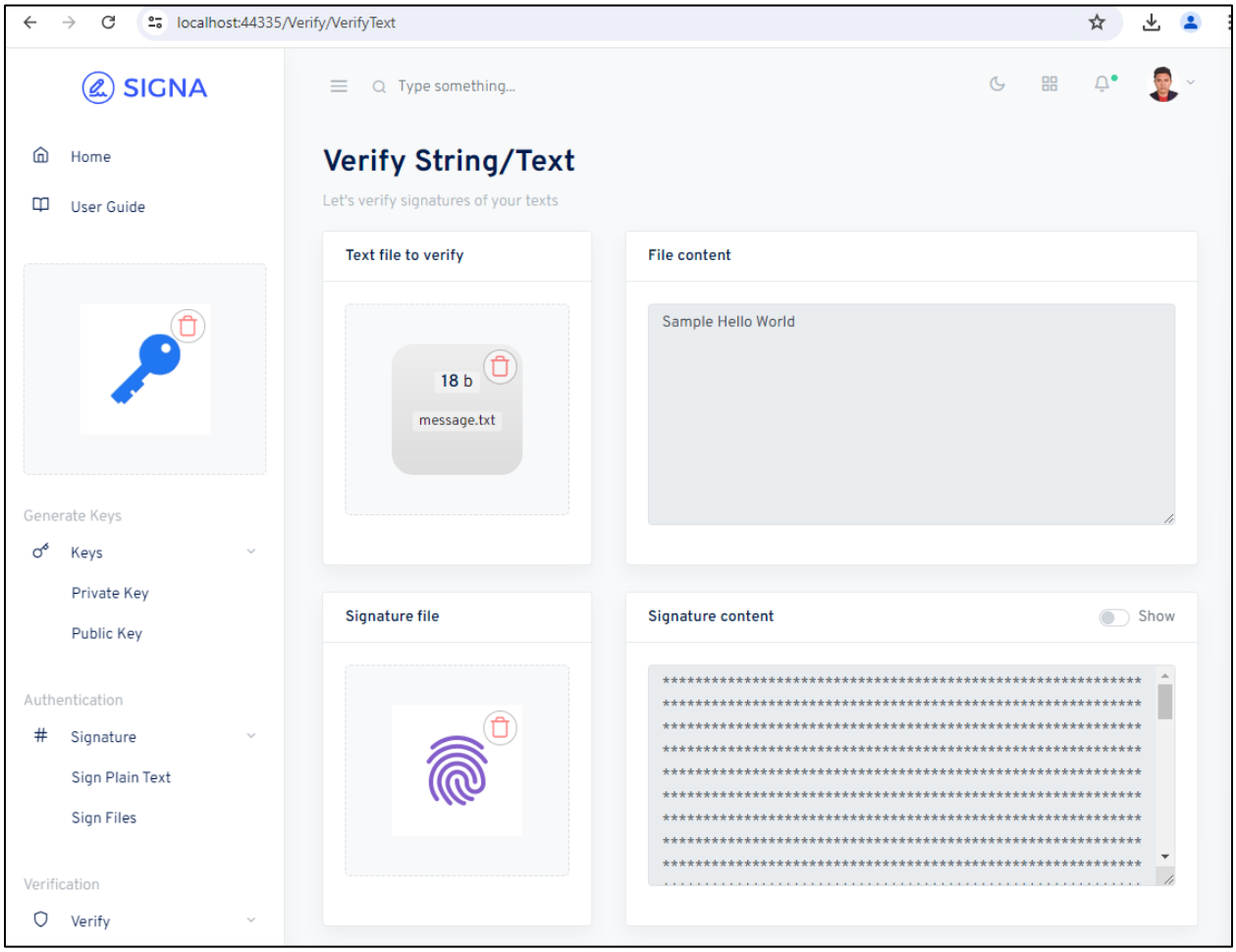
The contents of the zipped file will be the original file that is signed, the signature file (.sig), and the public key (.key) of the user with the username as the filename.



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

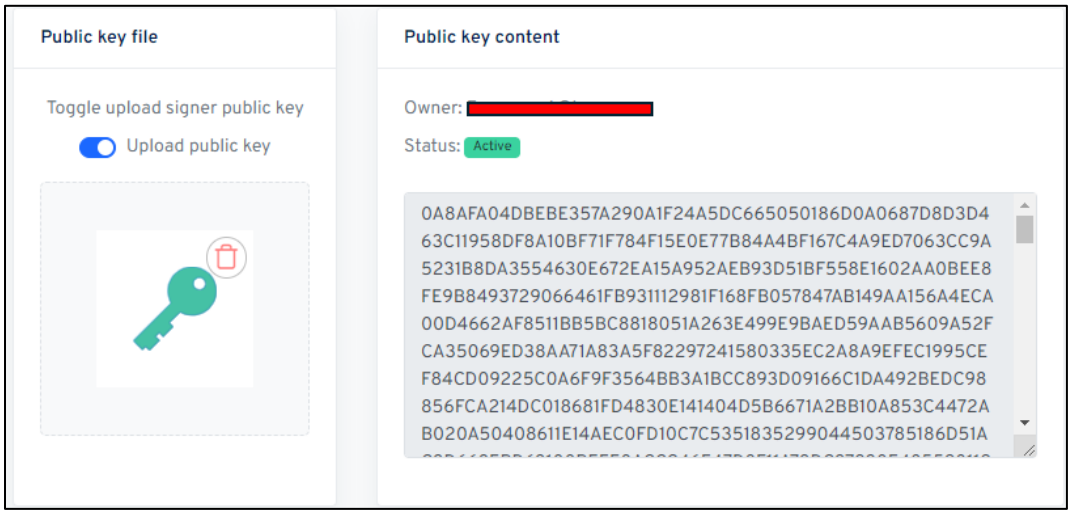
In the "Verify Plain Text" module, you can upload a .txt file in the "Text file to verify" section to open its contents. Additionally, upload a .sig file in the "Signature file" section to read the signature's contents.



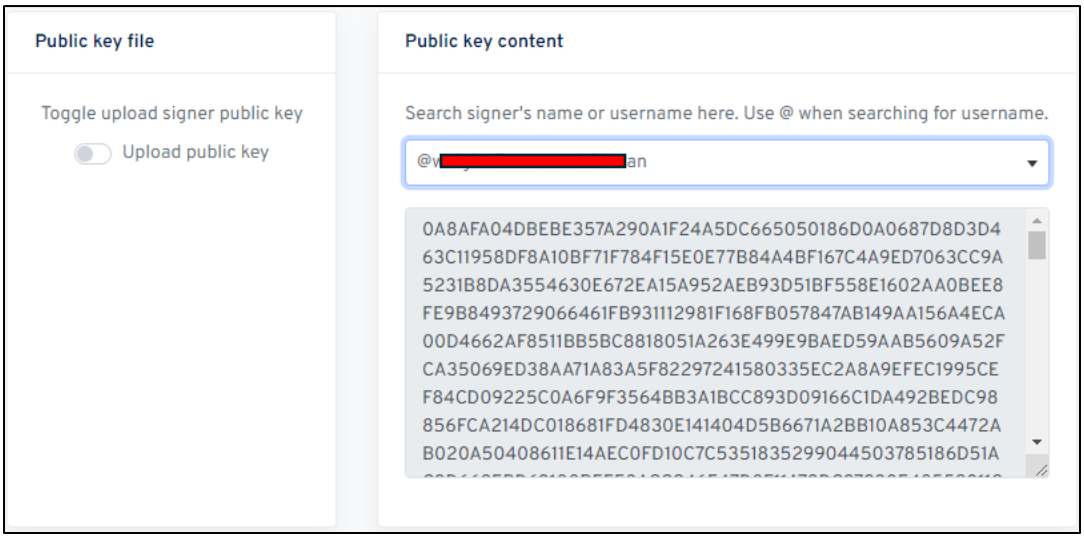
Verify – Verify Plain Text continued

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

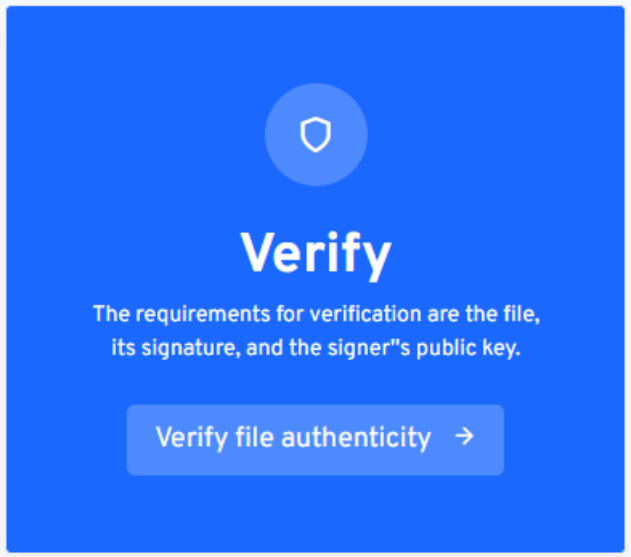


The Public Key file section using the select box

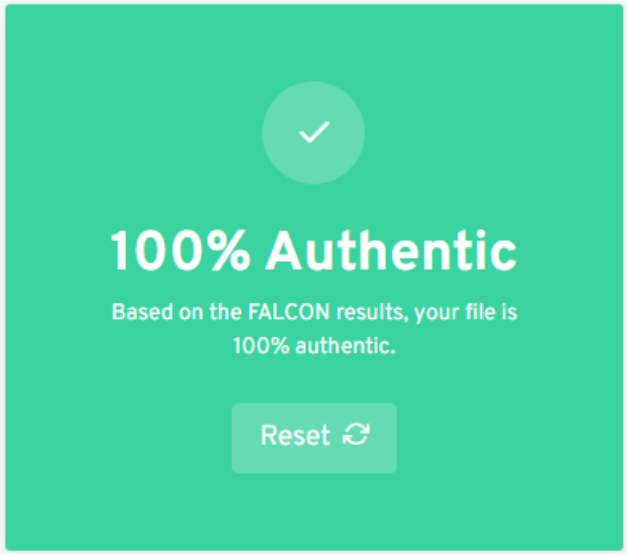


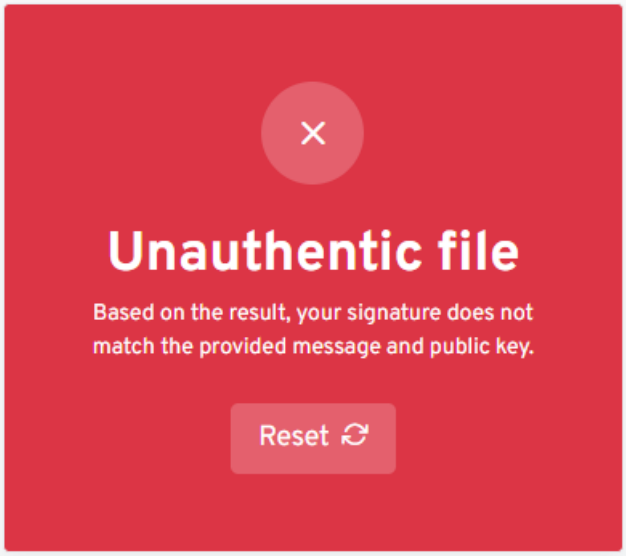
Verify – Verify Plain Text continued

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



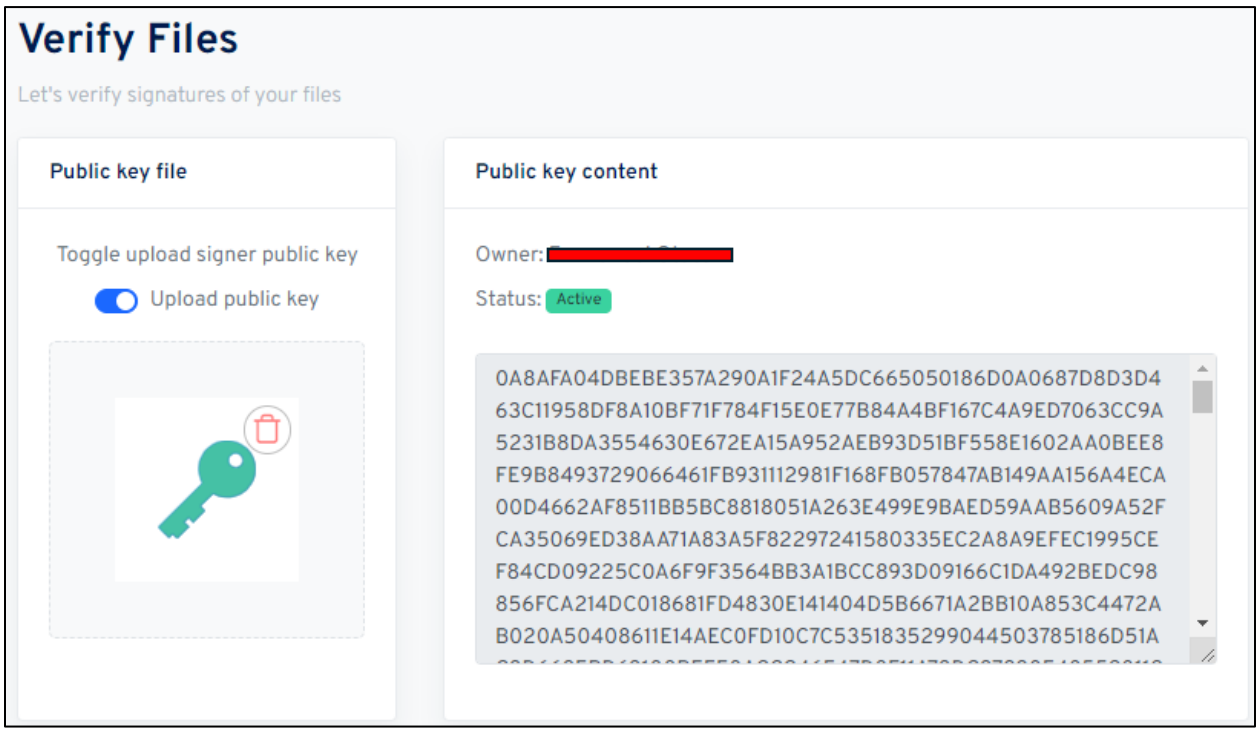
The system shows a green result section if the file and signature is authentic otherwise a red result section if it is unauthentic.



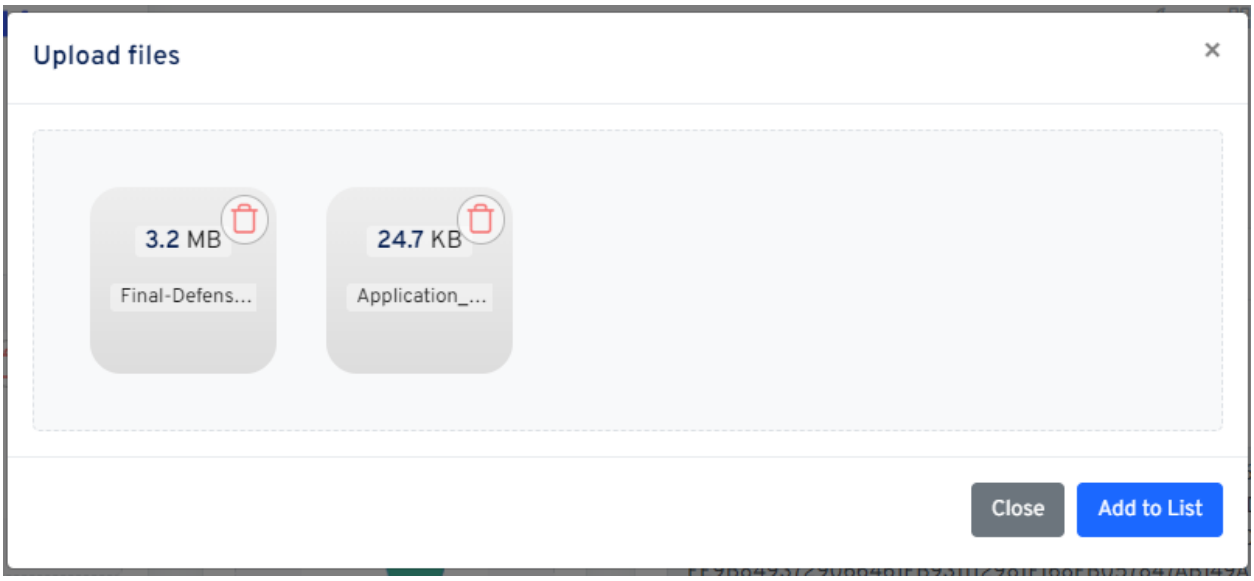


Verify – Verify Files

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.

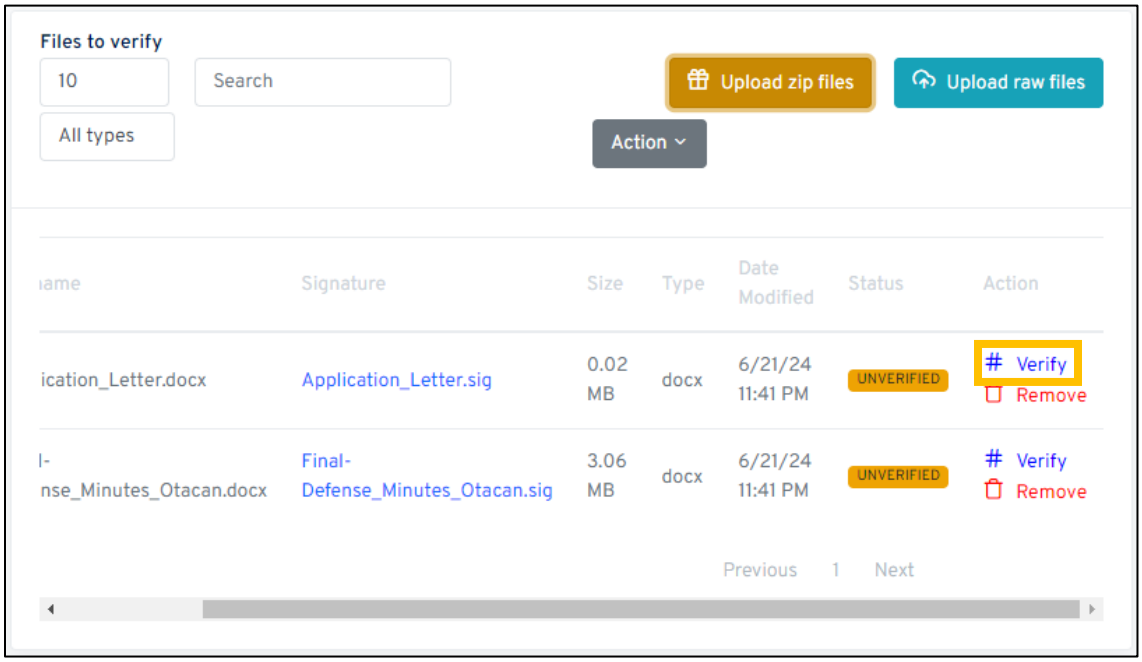


The same process of file uploading process of files is shown in the verification module.

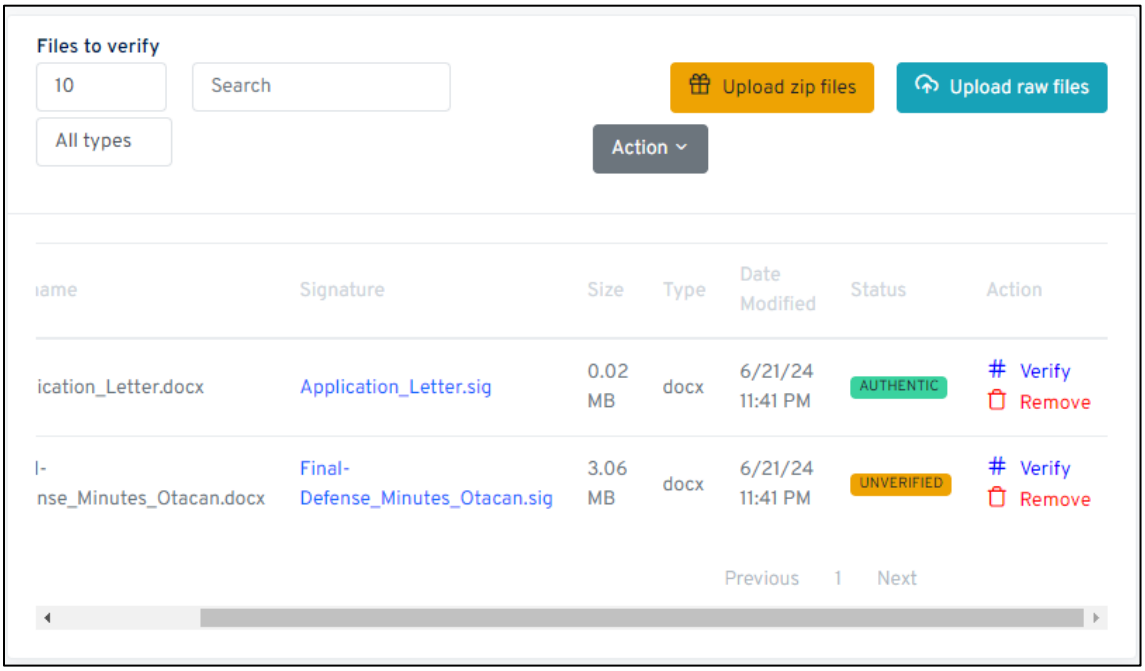


Verify – Verify Files continued

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

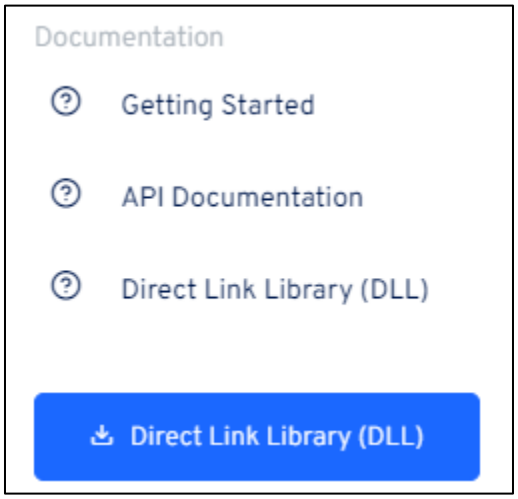


Authentic status shows on files that are verified authentic using the signature and the public key files.



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.