The “Select a hash function” module has no inputs, but it prompts the user to select a hash algorithm to use for signing. It then passes the selected algorithm to the “Hash function” module for storage.

The “Hash function” module receives the selected hash function from the previous module and stores it. It then gets passed to the “Compute hash value” module.

The “Compute hash value” module takes the hash function, and a selected document as an input. It then processes the document with the hash function and generates a unique hash value based on the document.

The “Generate key” module prompts the user to enter values in order to generate an RSA key. It is then passed to the “RSA key” module.

The “RSA key” module stores the generated key from the previous step. It will then pass it to the “Encrypt hash value” module.

The “Encrypt hash value” module takes input from the RSA key, and the hash value. It then encrypts the hash value using the RSA key. It will then output the encrypted hash value.

The “Encrypted hash value” module takes input from the “Encrypt hash value” module and stores it, until it is needed. It will later send it to the “Generate signature” module.

The “Provide certificate” module prompts the user to enter personal information in order to sign the certificate. After the user has entered any required information, the module can generate a certificate, validating the document.

The “Certificate” module holds the certificate generated in the previous step, until it is needed.

The “Generate signature” module will take the certificate, alongside the encrypted hash as input. It will generate a signature based on the encrypted hash and the certificate from the user.

The “Signature” module holds the signature, based on the document hash and user details. It will then output it and apply that signature to the original document.