

The Electronic Signature Act – ESA, was passed by the Florida Legislature in 1996. The Florida Statute states that electronic signatures have the same legal force as written signatures unless otherwise provided by law.

In Adobe Acrobat Reader if you double-click on a signature field the application should allow you to select a existing digital certificate or create a new certificate.

Find a Digital ID file ×

Digital ID files generally have a PFX or P12 extension and contain the public key file (Certificate) and the associated private key file.

To sign with a digital ID available as a file, follow the prompts to browse and select the file and type the password protecting the private key.

Browse for a Digital ID file. Digital ID files are password protected. You cannot access the Digital ID if you don't know its password.

Enter the Digital ID password

Select "Create a new Digital ID" and press **CONTINUE**

I would suggest that you save your certificate to a file. You can save your certificate store if you prefer, but if you save it to a file you can later export it to other computers.

Select the destination of the new Digital ID ×

Digital IDs are typically issued by trusted providers that assure the validity of the identity. Self-signed Digital ID may not provide the same level of assurance and may not be accepted in some use cases.

Consult with your recipients if this is an acceptable form of authentication.

- Save to File**
Save the Digital ID to a file in your computer
- Save to Windows Certificate Store**
Save the Digital ID to Windows Certificate Store to be shared with other applications

? Back Continue

Once you have made your selection, and press **CONTINUE**

Enter your name as you would if you were legally signing a document.

Create a self-signed Digital ID ×

Enter the identity information to be used for creating the self-signed Digital ID.

Digital IDs that are self-signed by individuals do not provide the assurance that the identity information is valid. For this reason they may not be accepted in some use cases.

Name	<input type="text" value="Enter Name..."/>
Organizational Unit	<input type="text" value="Enter Organizational Unit..."/>
Organization Name	<input type="text" value="Enter Organization Name..."/>
Email Address	<input type="text" value="Enter Email..."/>
Country/Region	<input type="text" value="US - UNITED STATES"/> ▼
Key Algorithm	<input type="text" value="2048-bit RSA"/> ▼
Use Digital ID for	<input type="text" value="Digital Signatures"/> ▼

? Back Continue

Enter your name and Email address, and press **CONTINUE**

I would STRONGLY suggest that you password protect you certificate. This will somewhat ensure that only you can use this certificate. I would suggest that you write down and save the address of your password file in case you might need it in the future.

Save the self-signed Digital ID to a file ×

Add a password to protect the private key of the Digital ID. You will need this password again to use the Digital ID for signing.

Save the Digital ID file in a known location so that you can copy it or back it up.

Your Digital ID will be saved at the following location :

Apply a password to protect the Digital ID:

Confirm the password:

Add a STRONG Password and press **Save**

Password security starts with creating a strong password. A strong password is: At least 12 characters long but 14 or more is better. A combination of uppercase letters, lowercase letters, numbers, and symbols. Not a word that can be found in a dictionary or the name of a person, character, product, or organization.