UTG®

Shift4 Certificate Generator

Copyright Notice

Shift4 Corporation
1491 Center Crossing Road
Las Vegas, NV 89144
702.597.2480

www.shift4.com | info@shift4.com

Document Title: Shift4 Certificate Generator

Publication Date: February 15, 2018

Shift4 Certificate Generator

The Shift4 Certificate Generator utility provides the ability to create digital certificates. Digital certificates are used to prove the ownership of a public key. The Shift4 Certificate Generator offers several options for generating certificates that can be used to configure an Oracle Payment Interface, TCP/IP SSL, HTTP/SSL, or UTG4CloudSSL interface between your point of sale or Property Management System (POS/PMS) and the Universal Transaction Gateway® (UTG®).

Generating a Self-Signed Certificate Authority

To generate a self-signed certificate authority (CA) that can be used to generate multiple certificates, complete the following steps:

1. Open the Shift4 Certificate Generator utility.
2. Enter the appropriate information in the desired fields. The minimum fields required include the following:

    - Common Name – Used to identify the certificate. For CA certificates this does not have to match the server name.
    - Organization – The Organization Name (corporation, limited partnership, university, or government agency) must be registered with some authority at the national, state, or city level. Use the legal name under which your organization is registered. Do not abbreviate or use any of these symbols:

!	@	#
$	%	^
*	(	)
~	?	>
<	/	\

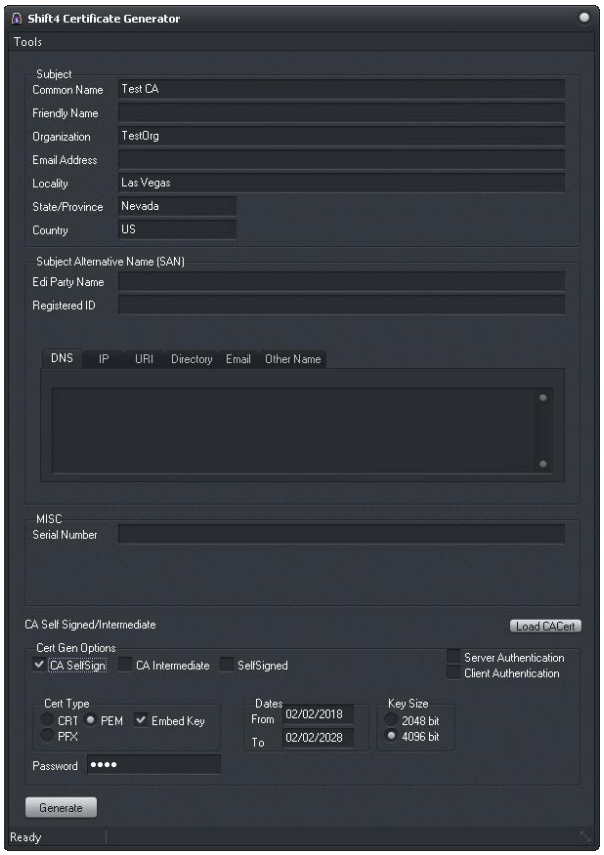
    - Locality – This usually denotes the city in which the organization is located.
    - State/Province – United States and Canadian customers must enter a State or Province name. Do not abbreviate. For example, if your organization is incorporated in the state of Delaware but is operating within the state of California, use California.
    - Country – This field contains the two-character ISO format country code. For example, GB is the valid country code for Great Britain, and US is the valid code for the United States.

3. Select **CA SelfSign**.
4. Select a Cert Type:

    - **CRT** – The CRT extension is used for certificates. The certificates will be encoded as ASCII PEM. The CRT and PEM extensions are nearly synonymous.
    - **PEM** – The PEM extension is used for certificates. The certificates will be encoded as ASCII PEM. The CRT and PEM extensions are nearly synonymous.
    - **PFX** – This is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encrypted file.

- *(If applicable)* **Embed Key** – The Embed Key in CRT/PEM option generates a single file containing both the certificate and key. When not selected, generated CRT files will have separate key files, and private/public PEM files will be created.

5. Set the valid cert dates in the Dates section. This is the amount of time the certificate can be used before having to be renewed.
   - From – The date the certificate will go into effect.
   - To – The date the certificate will no longer be accepted and must be renewed.
6. Select a Key Size:
   - **2048 bit**: In general, requests using this certificate will be faster.
   - **4096 bit**: In general, requests using this certificate will be more secure but slower.
7. Enter a Password. The password should be one that is difficult for someone to guess, but easy for you to remember.
8. Click **Generate** to create the self-signed CA. Depending on the Cert Type selected and whether or not the Embed Key option is selected, you will be prompted to save one or more files.



Generating a Signed Certificate

To generate a signed certificate, complete the following steps:

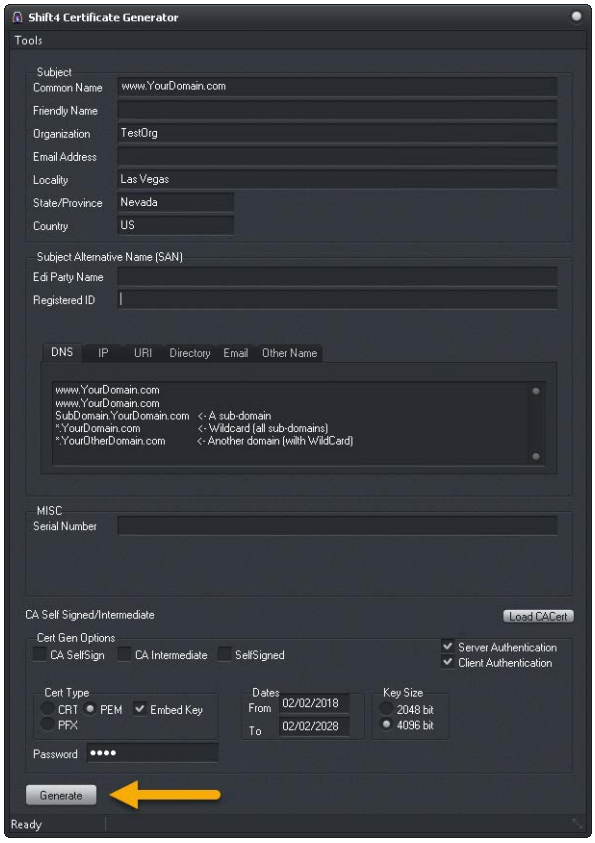
1. Open the Shift4 Certificate Generator utility.
2. Click **Load CACert** to load the CA or CA Intermediate certificate that will be used to sign the new certificate.
    - You may be prompted for a password.
    - If you created the CA certificate without selecting Embed Key, you may be prompted to select the key file.
    - Enter the appropriate information in the desired fields. The minimum fields required include the following:
        - Common Name – Also known as the URL, the common name is the fully qualified domain name (FQDN) used for DNS lookups of your host server (such as www.mydomain.com). Browsers use this information to identify your website. If you change your hostname, you must request another Digital ID. Client browsers connecting to your host check for a match between your Digital ID's common name and your URL. Most applications will verify the URL in the Subject Alternative Name rather than the Common Name if the Subject Alternative Name extension is set.
        - Organization – The Organization Name (corporation, limited partnership, university, or government agency) must be registered with some authority at the national, state, or city level. Use the legal name under which your organization is registered. Do not abbreviate or use any of these symbols:

!	@	#
$	%	^
*	(	)
~	?	>
<	/	\

        - Locality – This usually denotes the city in which the organization is located.
        - State/Province – United States and Canadian customers must enter a State or Province name. Do not abbreviate. For example, if your organization is incorporated in the state of Delaware but is operating within the state of California, use California.
        - Country – This field contains the two-character ISO format country code. For example, GB is the valid country code for Great Britain, and US is the valid code for the United States.
        - DNS – Enter domain and/or host names.
        - *(If applicable)* Click the **IP** tab and enter the IP address if you will be connecting by IP address. If your connection is not by IP address, you may leave this field blank.
3. Ensure CA SelfSign, CA Intermediate, and SelfSigned are not selected.
4. *(If applicable)* Select **Server Authentication** if the certificate's intended use is for server-side applications. This is the most common usage and is used to verify server authentication.
5. *(If applicable)* Select **Client Authentication** if the certificate's intended use is to identify clients/users.
6. Select a Cert Type:

- **CRT** – The CRT extension is used for certificates. The certificates will be encoded as ASCII PEM. The CRT and PEM extensions are nearly synonymous.
- **PEM** – The PEM extension is used for certificates. The certificates will be encoded as ASCII PEM. The CRT and PEM extensions are nearly synonymous.
- **PFX** – This is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encrypted file.
- *(If applicable)* **Embed Key** – The Embed Key in CRT/PEM option generates a single file containing both the certificate and key. When not selected, generated CRT files will have separate key files, and private/public PEM files will be created.

7. Set the valid cert dates in the Dates section. This is the amount of time the certificate can be used before having to be renewed.
   - From – The date the certificate will go into effect.
   - To – The date the certificate will no longer be accepted and must be renewed.
8. Select a Key Size:
   - **2048 bit**: In general, requests using this certificate will be faster.
   - **4096 bit**: In general, requests using this certificate will be more secure but slower.
9. Enter a Password.
10. Click **Generate** to create the signed certificate. Depending on the Cert Type selected and whether or not the Embed Key option is selected, you will be prompted to save one or more files.



Generating a Self-Signed Certificate

To generate a self-signed certificate, complete the following steps:

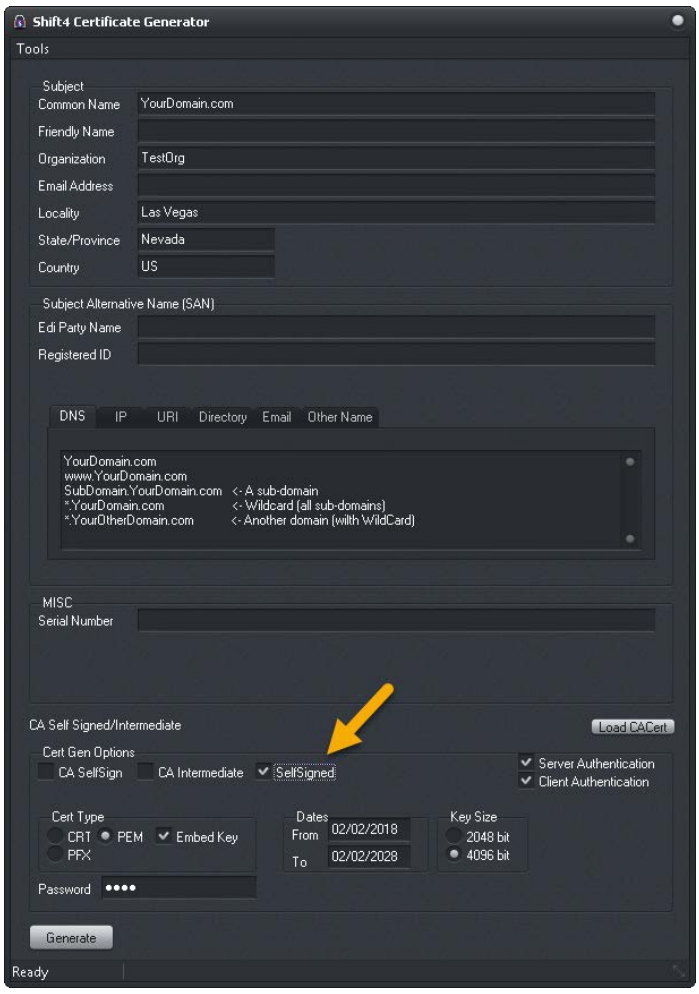
1. Open the Shift4 Certificate Generator utility.
2. Enter the appropriate information in the desired fields. The minimum fields include the following:

- Common Name – Used to identify the certificate. For CA certificates this does not have to match the server name.
- Organization – The Organization Name (corporation, limited partnership, university, or government agency) must be registered with some authority at the national, state, or city level. Use the legal name under which your organization is registered. Do not abbreviate or use any of these symbols:

!	@	#
$	%	^
*	(	)
~	?	>
<	/	\

- Locality – This usually denotes the city in which the organization is located.
- State/Province – United States and Canadian customers must enter a State or Province name. Do not abbreviate. For example, if your organization is incorporated in the state of Delaware but is operating within the state of California, use California.
- Country – This field contains the two-character ISO format country code. For example, GB is the valid country code for Great Britain, and US is the valid code for the United States.

3. Select **SelfSigned**.



4. *(If applicable)* Select **Server Authentication** if the certificate's intended use is for server-side applications. This is the most common usage and is used to verify server authentication
5. *(If applicable)* Select **Client Authentication** if the certificate's intended use is to identify clients/users.
6. Select a Cert Type:

   - **CRT** – The CRT extension is used for certificates. The certificates will be encoded as ASCII PEM. The CRT and PEM extensions are nearly synonymous.
   - **PEM** – The PEM extension is used for certificates. The certificates will be encoded as ASCII PEM. The CRT and PEM extensions are nearly synonymous.
   - **PFX** – This is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encrypted file.
   - *(If applicable)* **Embed Key** – The Embed Key In CRT/PEM option generates a single file containing both the certificate and key. When not selected, generated CRT files will have separate key files, and private/public PEM files will be created.

7. Set the valid cert dates in the Dates section. This is the amount of time the certificate can be used before having to be renewed.
    - From – The date the certificate will go into effect.
    - To – The date the certificate will no longer be accepted and must be renewed.
8. Select a Key Size:
    - **2048 bit**: In general, requests using this certificate will be faster.
    - **4096 bit**: In general, requests using this certificate will be more secure but slower.
9. Enter a Password.
10. Click **Generate** to create the self-signed certificate. Depending on the Cert Type selected and whether or not the Embed Key option is selected, you will be prompted to save one or more files.

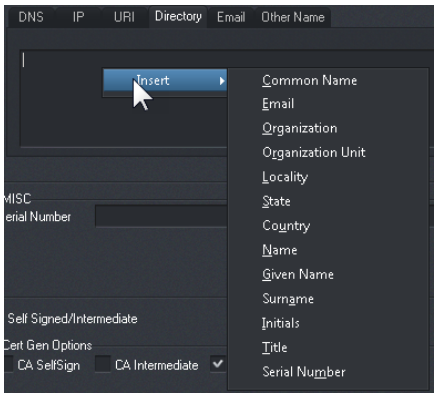
Subject Alternative Name (SAN)

Subject Alternative Name (SAN) is an extension to X.509, which is a standard that defines the format of public key certificates. The SAN extension allows various values to be associated with a security certificate.

Tabs

All entries are line delimited (one entry per line). Multiple SANs can be entered and all items are optional.

1. **DNS:** ex. node.TestOrg.com
2. **IP:** ex. 127.0.0.1
3. **URI:** ex. page.website.com
4. **Directory:** See the examples below:
    - 'C'= COUNTRY
    - 'ST'= STATE_OR_PROVINCE
    - 'L'= LOCALITY
    - 'O'= ORGANIZATION
    - 'OU'= ORGANIZATION_UNIT
    - 'CN'= COMMON_NAME
    - 'N'= NAME
    - 'G'= GIVEN_NAME
    - 'S'= SURNAME
    - 'I'= INITIALS
    - 'T'= TITLE
    - 'E'= EMAIL
    - 'SN'= SERIAL_NUMBER
5. To get started, directly enter the desired values to their corresponding options. Selecting the **Directory** tab, and then right-clicking on it will display the available options. Selecting any of the listed options will add a new key to the list (X=) where the value for X can be entered.



6. **Email:** ex user@TestOrg.com
7. **Edi Party Name:** Not used at this time.
8. **Registered ID:** Optional.
9. **Serial Number:** A serial number can be keyed or leave blank to have a random serial number generated.

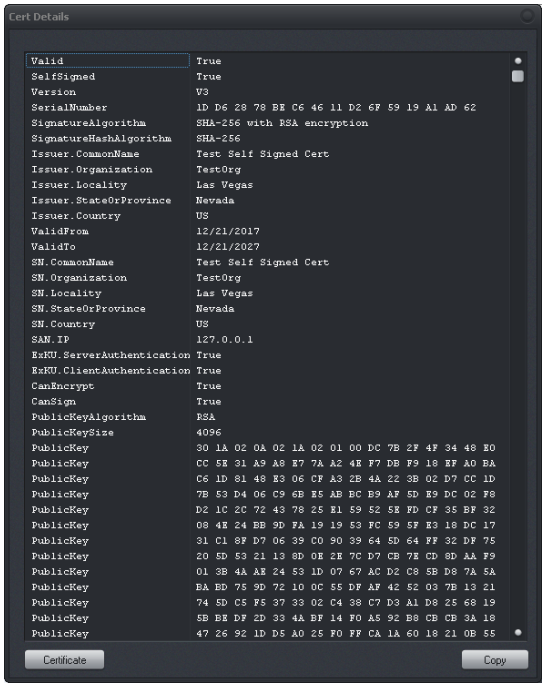
Tools

In the upper left corner of the Shift4 Certificate Generator screen, click **Tools** to display the two options below.

Inspect Cert

This is used to view public certificate details. To use this tool, complete the following steps:

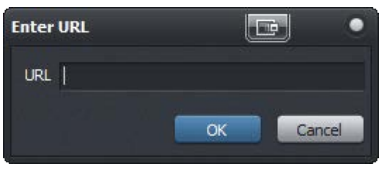
1. Click **Inspect Cert**.
2. Locate the desired certificate and click **Open**.
3. *(If applicable)* You may be prompted to enter a password.



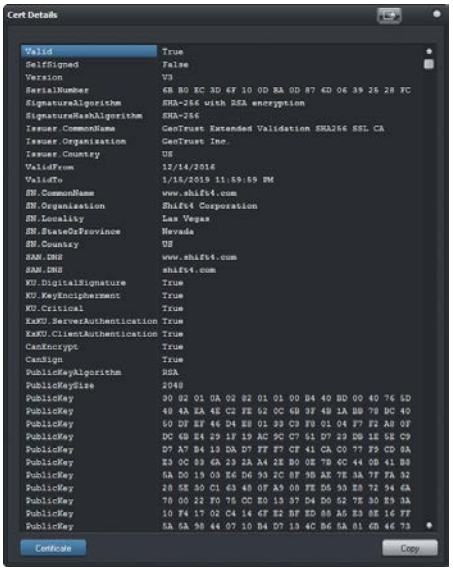
Inspect URL

This is used to view the public certificate details of a website. To use this tool, complete the following steps:

1. Click **Inspect URL**.
2. Enter the desired URL and click **OK**.



3. On the Cert Details screen, you can view all the certificate details. To see the Windows details, click **Certificate** at the bottom of the screen.



4. This will open the Certificate tab, where Windows provides several tabs for details.