

<https://secure.trust-provider.com/products/!AutoReplaceCS>

**Version History**

- 1.00 Original version.
- 1.01 Added: “csr” parameter.
- 1.02 Updated: Allowed values of “*contactEmailAddress*” request parameter.

**1. Request**

The request should be POSTed (rather than GETed) to the above URL.

Required variables are in **bold**.  
Optional variables are in *italics*.

Variable Name (case insensitive)	Type	Max. Length	Allowed Values	Description
<b>loginName</b>	string	64 chars		Account Username (case sensitive).
<b>loginPassword</b>	string	128 chars		Account Password (case sensitive).
<b>orderNumber</b>	string	128 chars	The Order Number of a certificate ordered previously	Order Number of certificate to replace
<i>contactEmailAddress</i>	string	255 chars	If specified with a value, the resulting certificate’s email address will be set to this value.  If specified with a blank value, no email address will be included in the resulting certificate.  If omitted, the resulting certificate’s email address defaults to the current certificate’s email address.	A contact email address to include in the certificate
<i>privateKeyFilename</i>	string	255 chars		The .PVK filename (this should always be provided when SPC/PVK files are being used instead of storing the certificate and private key in the CSP).
<b>pkcs10</b>	string	32767 chars		Certificate Signing Request (PKCS#10, Base-64 encoded, with or without the ----BEGIN xxxxx----- and ----END xxxxx----- header and footer) ( <b>required if spkac</b> variable is not present, but should not be used together)
<b>spkac</b>	string	32767 chars		A Netscape / Mozilla / Firefox “SPKAC” public key. ( <b>required if pkcs10</b> variable is not present, but should not be used together)
<b>csr</b>	string	32767 chars		Certificate Signing Request (PKCS#10, Base-64 encoded, with or without the ----BEGIN xxxxx----- and ----END xxxxx----- header and footer) ( <b>required if spkac/pkcs10</b> variable is not present, but should not be used together)
<i>signatureHash</i>	string	<b>64</b> chars	<b>NO_PREFERENCE</b> – Let Sectigo decide (the default, if this parameter is omitted).  <b>INFER_FROM_CSR</b> – If the CSR was signed using sha1WithRSAEncryption or md5WithRSAEncryption, then PREFER_SHA1; Else PREFER_SHA2.  <b>PREFER_SHA2</b> – If a suitable SHA-2 capable Sub-CA is available, Sectigo will use SHA-2; Else PREFER_SHA1.  <b>PREFER_SHA1</b> – If the current industry regulations and Sectigo policies permit, Sectigo will use SHA-1; Else REQUIRE_SHA2.  <b>REQUIRE_SHA2</b> – If a suitable SHA-2 capable Sub-CA is available, Sectigo will use SHA-2; Else, issuance	Preference for the signature hash algorithm to be used when issuing the certificate.

Variable Name (case insensitive)	Type	Max. Length	Allowed Values	Description
			of the certificate will be blocked until a suitable Sub-CA becomes available.	
<i>caCertificateID</i>	integer		If specified, this overrides Sectigo's default choice of CA certificate/key to be used to issue this certificate. This functionality is only available by special agreement with Sectigo.	Use a particular CA certificate/key
<i>organizationName</i>	string	64 chars		Organization Name (for a new certificate)
<i>organizationalUnitName</i>	string	64 chars		Organizational Unit Name (e.g. Company Department, for a new certificate)
<i>postOfficeBox</i>	string	40 chars		Post Office Box (for a new certificate)
<i>streetAddress1</i>	string	128 chars		Street Address 1 (for a new certificate)
<i>streetAddress2</i>	string	128 chars		Street Address 2 (for a new certificate)
<i>streetAddress3</i>	string	128 chars		Street Address 3 (for a new certificate)
<i>localityName</i>	string	128 chars		Locality Name (for a new certificate)
<i>stateOrProvinceName</i>	string	128 chars		State or Province Name (for a new certificate)
<i>postalCode</i>	string	40 chars		Postal Code (for a new certificate)
<i>countryName</i>	string	2 chars		Country Name (ISO3166 2-character country code, for a new certificate)

## 2. Response

Line 1: StatusCode

Line 2 :Error Message (If StatusCode < 0)

Possible values for "StatusCode" and "ErrorMessage":

StatusCode	ErrorMessage
0	Successful
-1	Request was not made over HTTPS!
-2	'xxxx' is an unrecognized argument!
-3	The 'xxxx' argument is missing!
-4	The value of the 'xxxx' argument is invalid!
-14	An unknown error occurred!
-16	Incorrect login details, account is locked, password has expired or your source IP is blocked. Permission denied!
-17	Request used GET rather than POST!
-20	The Certificate has already been Revoked!
-21	The Certificate has already been Replaced!
-22	The Certificate is currently being Issued!
-31	Either provide pkcs10 or spkac. Do not provide both.
-32	Unsupported key size!