

Version History

- 1.00 Original version.
- 1.01 Changed: **revocationReason** maximum length. Error message for errorCode -16.
Added: Error codes **-90, -91**.
- 1.02 Added: Error code **-43**.
- 1.03 Added: “codeReason” request parameter.
- 1.04 Changed: Allowed values of “codeReason” parameter.
- 1.05 Added: Description for the “revocationReason” parameter.

NOTES:

This API allows revocation of Code Signing Certificates.

When AutoRevokeCS is called for an order containing a certificate that has been “Issued”, the certificate will be “Revoked”.

When AutoRevokeCS is called for an order containing a certificate that has NOT been “Issued”, the certificate will be marked as “Rejected”.

After calling AutoRevokeCS with “includeInCRL=N” (to mark the certificate as “Replaced”), AutoRevokeCS may subsequently be called again with “includeInCRL=Y” (to change the certificate status from “Replaced” to “Revoked” and to include that certificate in the CRL).

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
loginName	string	64 chars		Account Username (case sensitive).
loginPassword	string	128 chars		Account Password (case sensitive).
<i>accountID</i>	integer			If specified, this is the Account ID of a Tier 2 Reseller account, and “loginName” and “loginPassword” must be the login credentials of the Tier 1 Reseller.
orderNumber	integer			This is the order number for the certificate you ask to revoke. This number could be previously returned. from the AutoApplySSL call.
revocationReason	string	497 chars ¹		Any comment you would like to provide about the reason why this certificate is being revoked. This information is used for your reference only. No action by Sectigo will be taken based on this information.
codeReason	integer		There should be ONE of the following integers specified: 0 = Unspecified 1 = keyCompromise 3 = affiliationChanged 4 = Superseded 5 = cessationOfOperation For explanation about when to choose each option, see the CPS.	Code of the reason for revocation. If omitted, its value defaults to 0 .

¹Actually **revocationReason**'s maximum length is 512 chars, but during *AutoRevoke* process in front of parameter's value will be added text 'AutoRevoke API'

Variable Name (case insensitive)	Type	Max. Length	Allowed Values	Description
<i>test</i>	char	1 char	'Y' or 'N'	If Y (or y), the certificate will not actually be revoked/rejected. If omitted, its value defaults to N.
<i>includeInCRL</i>	char	1 char	'Y' or 'N'	If Y (or y), the certificate's serial number will be included in CRLs. If omitted, its value defaults to Y.

2. Response

Line 1: StatusCode

Line 2 :Error Message (If StatusCode < 0)

Here are the 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.
-17	Request used GET rather than POST!
-20	The certificate request has already been Rejected!
-21	The certificate has already been Revoked!
-26	The certificate is currently being Issued!
-34	The certificate has already been Replaced!
-35	The Certificate does not allow revocation after expiry!
-43	Certificate is not in a revocable state
-90	Permission denied for using “voucher” with 'xxxx'
-91	Permission denied for 'xxxx'