Comodo Certificate Issuance Push

Comodo has the ability to 'push' information about issued certificates to your system when the certificates are signed.
The signed certificate and certificate chain can optionally also be pushed to your system.

This 'push' mechanism allows us to notify you when your certificates change status or are signed and available. The signed certificate itself can also optionally be included along with the certificate chain, or you can choose not to have the certificate sent and use the status push to trigged a call to the CollectSSL API.

This system helps alleviate the requirement for frequent polling of order status.

Notes:
- Changes in state are communicated, when triggered by completion of various actions – e.g. DCV completed, OV or EV validation completed.

- We only push the details of signed **SSL (server) certificates**. Client/email and code signing certificates are not supported at this time.

- There is a 'failed' status that can be pushed. It should never occur. Please handle this error, but we would suggest notifying your Account Manager if this occurs.

- You should ensure that the endpoint URL to which we call is available as much as possible. Should there be a problem communicating the call to your system, we will log as a failure within our system. The call will be attempted **three (3)** times only. A 'failure' can be defined as: a network connectivity issue; verification failure of your SSL certificate; an authentication failure (if provided); a protocol error or server-issued error (HTTP error codes).

- While this system alleviates the need for frequent polling of CollectSSL for status, we understand it does not remove it altogether. We advise that if you do wish to continue with polling for status of your certificate orders you do so **no more frequently than once every 3 hours**.

- If you choose to have the signed certificate and chain pushed, our system will make a **POST** call instead of **GET** – including for status changes without certificates attached.

Setup:
To setup the certificate issuance push, you should setup a system to receive HTTP or HTTPS calls.
The system should accept all the parameters from the IP listed below. You do not need to utilise both orderNumber and certificateID unless you wish to.
The URL must be visible on the public internet, although you may wish to add IP-restrictions to only allow the call to be made from our system.
'Basic Authentication' is supported.

Call Information:
Comodo will make a call to a URL which you delegate.

WITHOUT certificate push:
These parameters will be passed as a HTTP(S) GET to your URL, as follows:

Parameter	Type	Description	Example
orderNumber	string	Comodo order number.	1234567repl#1
certificateID	integer	Comodo certificate ID.	1234567890
status	string	Certificate status.	issued
statusCode	integer	Certificate status as an integer value.	6
statusDesc	string	Brief description of the status.	Valid

WITH certificate push:
The above parameters are sent, with two additions. All parameters are POSTed to your URL.

Parameter	Type	Description	Example
certificate	string	PEM (Base64 with PEM headers) encoded certificate.	
caCertificate	string	PEM encoded certificate chain.	

A list of the 'status', 'statusCode' and 'statusDesc' parameters:

status	statusCode	statusDesc
6	issued	Valid
9	issued	Issued but not yet collected
8	revoked	Revoked
14	replaced	Replaced
12	awaitingbrandvalidation	Awaiting Validation (Brand)
5	failed	POST-SIGN FAILED

The call will be made from:

91.199.212.132 (secure.comodo.net)

Once you have your endpoint URL setup, please contact your Account Manager with both your account number or username and the URL (including basic authentication credentials if necessary).

Please also specify if you wish to have the signed certificate and chain pushed or not.