GlobalSign API for CloudSSL

Implementation Guide and Definitions

Version 2.11
12/12/2016

Version Release Notes

Version 2.11 Changes

- Updated acceptable domain-validation locations (Section 5.1.1)

Version 2.10 Changes

- Reorganized the sections for improved readability and removed redundant descriptions of common API message

Version 2.9 Changes

- Reduced the number of valid ApproverURLs to better align with industry requirements
- Added CloudOVOrderByMultiVerification and CloudOVSANOrderByMultiVerification to allow validation by either Metatag or DNS

Version 2.8 Changes

- Updated country codes to use CW instead of SX
- Fixed spelling error in RenewalTargetOrderID
- Replaced list of ModificationEventName responses with new values

Version 2.7 Changes

- Updated “Reissue” Function for Hash Algorithm SHA-256, Section 5.5

Version 2.6 Changes

- Added missing CloudOrderByDNSVerification

Contents

1. Outline

This document outlines the web services of GlobalSign's CloudSSL SOAP/XML API. The CloudSSL API enables GlobalSign partners to purchase Organizationally Vetted (OV) Certificates with Domain Vetted SANS. This API also allows partners to add and remove SAN entries from existing CloudSSL Certificates. After ordering and modifying CloudSSL Certificates, partners may use the API to issue and retrieve the certificates. Throughout this document the CloudSSL Certificates will be referred to as CloudOV.

1.1 Quick Start - General Workflows

The following are the top level workflows we recommend to implement the CloudSSL process in your environment.

Ordering Initial CloudSSL Certificate

a. Place order with CloudOVOrder
b. GlobalSign vets order and approves
c. Check status with GetCloudOVOrderByOrderID
d. Request issuance with IssueRequestforCloudOV
e. Get certificate with GetCloudOVOrderByOrderID

Adding SANs to the order (URL method)

a. Add new SAN to an existing CloudOV Certificate with C*loudOVSANOrderByURLVerification*
b. Place the returned metatag on the applicable web page
c. Verify domain control for the added SANs with *URLVerificationRequest*
d. Check the status of the order with *GetCloudOVOrderByOrderID*
e. When the SAN has been approved, request the generation of the updated certificate with *IssueRequestForCloudOV*
f. Retrieve the updated certificate with *GetCloudOVOrderByOrderID*

1.2 Web Service Functions – Order & Query Workflow Overview

Order processing for CloudOV Certificates is asynchronous. For these types of orders an API client places an order and then later checks the server for the completed order to retrieve the status or the certificate.

1.2.1 Order Functions

Function	API Operation	Section in this document
Order CloudOV Certificate	`CloudOVOrder`	2.1
Order CloudOV Certificate (URL Verification)	`CloudOVOrderByURLVerification`	2.3
Order CloudOV Certificate (DNS Verification)	`CloudOVOrderByDNSVerification`	2.3
Order CloudOV Certificate (user can use DNS or URL verification)	`CloudOVOrderByMultiVerification`	2.3
Add or delete CloudOVSAN to CloudOV Certificate (Approver Email)	`CloudOVSANOrder`	3.2.1
Add or delete CloudOVSAN to CloudOV Certificate (Approver URL)	`CloudOVSANOrderByURLVerification`	3.2.1
Add or delete CloudOVSAN to CloudOV Certificate (DNS verification)	`CloudOVSANOrderByDNSVerification`	3.2.1
Add or delete CloudOVSAN to CloudOV Certificate (user can use DNS or URL verification)	`CloudOVSANOrderByMultiVerification`	3.2.1
Issue request for CloudOV Certificate	`IssueRequestForCloudOV`	3.3
Request URL Verification	`URLVerification`	3.2.2

Request DNS Verification	`DNSVerification`	3.2.3
Reissue CloudOV Certificate	`ReissueRequestForCloudOV`	4.1
Cancel or Revoke request	`ModifyCloudOVOrder`	4.2
Re-send Approver email	`ResendApproverEmail`	4.3

1.2.2 **Query Functions**

Function	API	Section in this document
Return a list of Approvers for a CloudOV order	`GetCloudOVApproverList`	4.4
Returns details for specified CloudOV order	`GetCloudOVOrderByOrderID`	4.5
Searching modified orders by modified date (from/to)	`GetModifiedCloudOVOrders`	4.6

1.2.3 **API and WSDL URLs**

WSDL URL's

	Feature	URL
PROD	Order WSDL	https://system.globalsign.com/bb/ws/GasOrder?wsdl
	Query WSDL	https://system.globalsign.com/bb/ws/GasQuery?wsdl
TEST	Order WSDL	https://test-gcc.globalsign.com/bb/ws/GasOrder?wsdl
	Query WSDL	https://test-gcc.globalsign.com/bb/ws/GasQuery?wsdl

API URL's:

	Feature	URL
PROD	Order Functions	https://system.globalsign.com/bb/ws/GasOrder
	Query	https://system.globalsign.com/bb/ws/GasQuery
TEST	Order Functions	https://test-gcc.globalsign.com/bb/ws/GasOrder
	Query	https://test-gcc.globalsign.com/bb/ws/GasQuery

**Test system accounts are available to API customers upon request*

2. Ordering new Cloud SSL Certificates

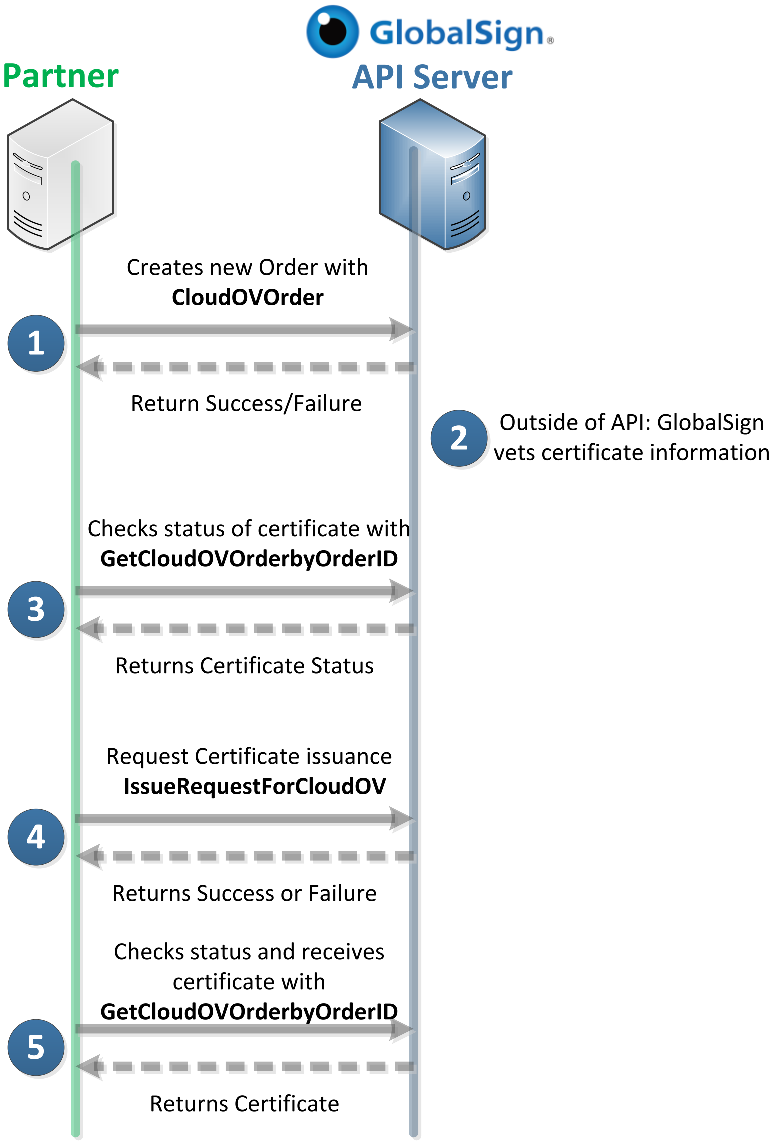
This section describes the process for obtaining your first CloudOV certificate. This section describes the 4 options for obtaining the CloudOV Certificate

- Via email verification
- Via URL (Meta-tag) validation
- Via DNS text record validation
- Via either URL or DNS validation

2.1 CloudOVOrder: Requesting a new CloudOV Certificate

At the top level the process for obtaining your initial CloudOV certificate is the same, the only difference is the process by which you validate control of the domain specified in the Common Name of the certificate (and optionally in additional SANs supplied with the initial order).

a. Place a CloudOVOrder request using the CloudOVOrderRequest
b. The GlobalSign vetting team will review and approve the order
c. Check the status with GetCloudOVOrderByOrderID until the status indicates approved
d. Once the certificate has been approved, you can use the IssueRequestForCloudOV request to request the issuance of the certificate
e. Use the GetCloudOVOrderByOrderID to obtain the updated status and to receive the certificate when it issued


GlobalSign
API Server
Partner
Creates new Order with
CloudOVOrder
1
Return Success/Failure
2
Outside of API: GlobalSign vets certificate information
Checks status of certificate with
GetCloudOVOrderbyOrderID
3
Returns Certificate Status
Request Certificate issuance
IssueRequestForCloudOV
4
Returns Success or Failure
Checks status and receives certificate with
GetCloudOVOrderbyOrderID
5
Returns Certificate

2.2 Common Data Structure

The same basic set of data is used regardless of the validation method (email, URL/Metatag or DNS). The message is defined in detail here and then referenced by the ordering methods below.

CloudOvOrderRequest

While the API does provide the option of adding SANs in the initial order, to simplify the workflows we recommend that the SANs are added after the initial order has been approved.

Field	Type	Size	Opt, Req, NA	Remarks
CloudOvOrderRequest			Y	
OrderRequestHeader			Y	
AuthToken			Y	
UserName	String	30	Y	
Password	String	30	Y	
OrderRequestParameter				
OrderID	string	50	NA	
ProductCode	String		Req	CLOUD_OV, CLOUD_OV_SHA2
BaseOption	String		NA?	NOTHING, WILDCARD, GIP
OrderKind	String		Req	NEW, TRANSFER, RENEWAL
License	int		NA	
Options			O	
Option+				
OptionName	string			See section 5.8
OptionValue	boolean			
ValidityPeriod			N	
Months	Int	4	Req	
NotBefore	String:date	25	NA	
NotAfter	String:date	25	NA	
CSR	string	4000	Req	
RenewalTargetOrderID	string	50	Opt	
TargetCERT	string	4000	Opt	
SpecialInstructions	string	4000	Opt	
Coupon	string	50	NA	
Campaign	string	50	NA	
SubID	String	50	Opt	
OrganizationInfo			Req	
OrganizationName	string	100	Req	
OrganizationUnitName	string	100	Opt	
CreditResearchKind	string	1	Opt	1:DUNS, 2:TDB
CreditResearchNumber	string	9	Opt	
OrganizationAddress			Req	
AddressLine1	string	100	Req	
AddressLine2	string	100	Opt	
AddressLine3	string	100	Opt	
Locality	string	200	Req	
StateOrProvince	string	255	Req	
PostalCode	string	20	Req	
Country	country	2	Req	
Phone	string	30	Req	
Fax	string	30	Opt	
ContactInfo			Req	
FirstName	string	100	Req	
LastName	string	100	Req	
Phone	string	30	Req	
Email	string	255	Req	
CloudSANEntries				
CloudSANEntry				Not recommended
CloudOVSAN	string	255		
ModifyOperation	string	10		See Section 5.7
ApproverEmail	string	255		Only applicable for Approver email option
AdditionalWildcardOption	boolean		Opt	

CloudOvOrderResponse

Field	**Type**	**Size**	**Remarks**
CloudOvOrderResponse			
OrderResponseHeader			
SuccessCode		2	
Errors			
Error+			
ErrorCode		5	
ErrorField	string	1000	
ErrorMessage	string	1000	
TimeStamp	string:date	24	
OrderID	string	50	Empty if error
CloudOVSANInfo			Not returned when doing Email Verification
CloudOVSANDetail+			
CloudOVSAN		255	
CloudOVSANStatus		5	
ApproverEmail		255	
OrderDate	string:date	24	
ApprovalDate	string:date	24	
IssueDate	string:date	24	
CancelDate	string:date	24	
OrderCompleteDate	string:date	24	
DeleteDate	string:date	24	
MetaTag	string	255	Returned when URL verification method is used
TxtRecord	string	255	Returned when DNS verification method is used

2.3 Advanced options

You may use one of these options to add SANs when ordering the initial CloudOV certificates; however we recommend using just CloudOVORderRequest with no additional SANs. Once approved you can add SANs using any available options as specified in section 3.

Command	Approval method	Description
CloudOVOrder	Email	Before submitting this command you will need to GetCloudOVApproverList so you have a valid approver email. You will receive a response status =0, then the approver email will be sent to the specified email address
CloudOVOrderByURLVerification	Metatag	The metatag is returned in the response
CloudOVOrderByDNSVerification	DNS	The DNS TXT record value is returned in the response
CloudOVOrderByMultiVerification	DNS or Metatag	Values for both DNS and Metatag are returned and either can be used to validate the SAN

Adding SANs (if using Email Verification)

a. GetCloudOVApproverList (must provide orderID that SANs will be added to)
b. Add SANs to order with CloudOVSANOrder
c. (out of API) GlobalSign sends approver email to domain owner, Domain owner approves
d. Check Status with GetCloudOVOrderByOrderID
e. Request issuance with IssueRequestforCloudOV when SANs show as approved
f. Get certificate with GetCloudOVOrderByOrderID

Adding SANs (if using MetaTag Verification)

a. Add SANs to order with CloudOVSANOrderByURLVerification, receive MetaTag string
b. (out of API) Customer adds MetaTag to valid MetaTag location
c. Verification request made with URLVerification at which point GlobalSign validates the specified ApproverURL and returns success/failure.
d. Check Status with GetCloudOVOrderByOrderID
e. Request issuance with IssueRequestforCloudOV when SANs show as approved
f. Get certificate with GetCloudOVOrderByOrderID

Adding SANs (if using DNS Verification)

a. Add SANs to order with CloudOVSANOrderByDNSVerification
b. (out of API) DNS verification code is added as a TXT record in DNS for domain being secured
c. Verification request made with DNSVerification at which point GlobalSign looks in DNS entry for ApproverFQDN for the text record and returns success/failure
d. Check Status with GetCloudOVOrderByOrderID
e. Request issuance with IssueRequestforCloudOV when SANs show as approved
f. Get certificate with GetCloudOVOrderByOrderID

Adding SANs (if using MultiVerificiation Verification)

a. Add SANs to order with CloudOVSANOrderByMultiVerification
g. (out of API) DNS verification code is added as a TXT record in DNS for domain being secured, and/or adds MetaTag to valid MetaTag location
b. Verification request made with DNSVerification or URLVerification at which point GlobalSign looks in DNS entry for ApproverFQDN for the text record, or checks for a valid metatag and returns success/failure
c. Check Status with GetCloudOVOrderByOrderID
d. Request issuance with IssueRequestforCloudOV when SANs show as approved
e. Get certificate with GetCloudOVOrderByOrderID

3. Requesting and Approving SANs for existing CloudOV Certificates

3.1 Overview

Once a CloudOV order has been approved you can add and delete SANs from the certificate to meet your business needs. Regardless of the SAN validation method (Email, DNS or Metatag), the process is the same and follows this basic flow:

1. If using email
    a. Use the Approver list for new SANs using the *GetCloudOVApproverList* to obtain the list of valid approver emails.
2. Use any one of the following operations to add new SANs to an existing CloudOV Certificate:
    a. *CloudOVSANOrder*: Email
    b. *CloudOVSANOrderByURLVerification*: Metatag
    c. *CloudOVSANOrderByDNSVerification*: DNS
    d. *CloudOVSANOrderByMultiVerification*: DNS and Metatag info both returned
3. Use the following to delete a SAN from an existing CloudOV Certificate:
    a. *CloudOVSANOrder*
4. Verify domain control for the added SANs using the applicable method
    a. For email approval methods: receive the email, click on the link and approve the SAN.
    b. For DNS: Update the applicable DNS record then ask to have it verified
        i. Call *DNSVerificationRequest*
    c. Metatag: Update web page at ApproverFQDN with metatag value then ask to have it verified.
        i. Call: *URLVerificationRequest*
    d. Repeat for all SANs which have been added to the CloudOV order
5. Check the status of the order (which contains the status for all SANs)
    a. Call: *GetCloudOVOrderByOrderID*
6. When all SANs have been approved, request the generation of the updated certificate.
    a. Call *IssueRequestForCloudOV*
    b. Note: If not all SANs are approved you cannot request the issuance of the updated certificate. You must cancel the unapproved SANs first then call *IssueRequestForCloudOV*
7. Retrieve the updated certificate
    a. Call: *GetCloudOVOrderByOrderID*

Changing SAN Approval method Example #1 (from Email Verification to Metatag Verification)

Sometimes you may find that the approver email you selected is not active or accessible and you need to change the verification method of the SAN from email to metatag.

a. Assuming SAN is in a pending status (0, 1, 2) – Cancel the SAN with ModifyCloudOVOrder
b. Then proceed to follow the steps for Adding SANs (using the metatag verification)

Changing SAN Approval method Example #2 (from Metatag Verification to Email Verification)

Sometimes you may find that you have difficulty updating the index of the domain you are securing or it is inaccessible, and you need to change the verification method of the SAN from metatag to email.

a. Assuming SAN is in a pending status (0, 1, 2) – Cancel the SAN with ModifyCloudOVOrder
b. Then proceed to follow the steps for Adding SANs (using email verification)

*For other SAN actions, please refer to the tables in 6.3 & 6.4 which outline the valid actions based on what the SAN's current status is in the certificate.

3.2 Common Data Structures

3.2.1 CloudOvSanOrder

CloudOvSanOrder Request

The following all use the same data structure:

- CloudOvSanOrder
- CloudOVSANOrderByURLVerificationRequest
- CloudOvSANOrderByDnsVerificationRequest
- CloudOvSANOrderByMultiVerificationRequest

Field	Type	Size	Req	Remarks
CloudOvSanOrderRequest				
OrderRequestHeader			Req	
AuthToken			Req	
UserName	String	30	Req	
Password	String	30	Req	
OrderRequestParameter				
OrderID	String	50	Req	The OrderID to have the SAN(s) added or removed from
CloudSANEntries			Req	
CloudSANEntry+			Req	Can request multiple SANs to be added in one operation
CloudOVSAN	string	255	Req	
ModifyOperation	String		Req	Supports Add and Delete, see Section 5.7
ApproverEmail	string	255	Opt	Required when email approval is used
AdditionalWildcardOption	boolean		Opt	See section 5.12

CloudOvSanOrder Response

Field	Type	Size	Req	Remarks
CloudOvSanOrderResponse				
OrderResponseHeader			Req	
OrderID	String	50	Req	
CloudOVSANInfo				Not returned when doing Email Verification
CloudOVSANDetail+				
CloudOVSAN	String	255	Req	
CloudOVSANStatus	String	2	Req	
ApproverEmail	String	255	Opt	
OrderDate	date	25	Opt	
ApprovalDate	date	25	Opt	
IssueDate	date	25	Opt	
CancelDate	date	25	Opt	
OrderCompleteDate	date	25	Opt	
DeleteDate	date	25	Opt	
MetaTag	String	255	N	Returned when URL verification method is used
TxtRecord	String	255	N	Returned when DNS verification method is used

3.2.2 URL Verification

URL Verification Request

Field	Type	Size	Req	Remarks
UrlVerificationRequest				
OrderRequestHeader			Req	
OrderID	Stting	50	Req	The OrderID to have the SAN(s) added to
ApproverURLEntries			Opt	
ApproverURLEntries+				
CloudOVSAN	string	255		
ApproverURL	string	255		See Section 5.1.1 for details

URL Verification Response

Field	Type	Size	Req	Remarks
UrlVerificationResponse				
OrderResponseHeader				
OrderID	String	50	Req	

3.2.3 DNS Verification

DNS Verification Request

This is used to validate the domain by checking that the value is located at the location specified in "ApproverURL".

Field	Type	Size	Req	Remarks
DnsVerificationRequest				
OrderRequestHeader				
OrderID	String	50	Req	
ApproverDNSEntries				
ApproverDNSEntry				
CloudOVSAN	String	64	Req	
ApproverFQDN	String	255	Req	See Section 5.1.2

DNS Verification Response

Field	Type	Size	Req	Remarks
DnsVerificationResponse				
OrderResponseHeader			Req	
OrderID	String	50	Req	

3.3 IssueRequestForCloudOV

Use this operation to request the generation of the certificate with the added or deleted SANs.
The following request is for issuing the CloudOV Certificate that includes (newly) approved SANs.
You have to set SANs that are to be included in an issued certificate and status of these SANs must be “approved”. Before submitting this request you should use the GetCloudOVOrderByOrderID request to check if the status of the SANs has been moved to “approved”.

IssueRequestForCloudOV Request

Field	Type	Size	Req	Remarks
IssueRequestForCloudOV				
OrderRequestHeader			Req	
OrderID	String	50	Req	

IssueRequestForCloudOV Response

Field	Type	Size	Req	Remarks
IssueRequestForCloudOV				
OrderResponseHeader			Req	
OrderID	String	50	Req	

4. Other Operations

This section describes how to:

a. Reissue a CloudOV certificate
b. Cancel or Revoke a CloudOV certificate
c. Resend approver email
d. Obtain email approver list
e. Get order details

4.1 ReissueRequestForCloudOV

If you want to change the keys (CSR) in the CloudOV certificate, or if you want to change the hashing algorithm used to sign the certificate, then you want to use the *ReissueRequestForCloudOV* operation. For improved security you should reissue the certificates on a regular basis to rotate the private keys.

- If HashAlgorithm is not specified, certificates will be issued based on the hash algorithm of the certificate being reissued.
- If "SHA1" is specified, SHA1 certificates will be issued, if supported by that product code.
- If "SHA256" is specified, SHA-256 certificates will be issued.

Note: When you reissue a certificate you will get a new OrderID as compared to IssueRequest it retains the same OrderID.

ReissueRequestForCloudOV Request

Field	Type	Size	Req	Remarks
ReissueRequestForCloudOV				
OrderRequestHeader				
OrderRequestParameter				
CSR	String	4000	Req	
TargetOrderID	String	50	Req	
HashAlgorithm	String	10	Opt	SHA1, SHA256

ReissueRequestForCloudOV Response

Field	Type	Size	Req	Remarks
ReissueRequestForCloudOV				
OrderResponseHeader			Req	
OrderID	String	50	Req	

4.2 ModifyCloudOVOrder – Cancel/Revoke CloudOV Certificates

ModifyCloudOVOrder Request

Using the ModifyCloudOVOrder API you can Cancel or Revoke a Certificate or Certificate Request by using the OrderID of the Order.

Note: When you revoke a specific OrderID, ALL certificates with that OrderID will be revoked. You receive a new certificate each time you add/delete SANs and call the IssueRequest operation.

Field	Type	Size	Req	Remarks
ModifyCloudOVOrder				
OrderResponseHeader			Req	
OrderID	String	50	Req	
ModifyOrderOperation	String	10	Req	CANCEL, REVOKE

ModifyCloudOVOrder Response

Field	Type	Size	Req	Remarks
ModifyCloudOVOrder				
OrderResponseHeader			Req	
OrderID	String	50	Req	

4.3 ResendApproverEmail

Use this operation to resent an approver email

ResendApproverEmail Request

If the user did not receive or lost their Approver Email message you can use the ResendApproverEmail API operation to re-send the email for a specific SAN(s).

Field	Type	Size	Req	Remarks
ResendApproverEmail				
OrderRequestHeader			Req	
OrderID	String	50	Req	
CloudOVSAN+	String	255	Req	

ResendApproverEmail Response

Field	Type	Size	Req	Remarks
ResendApproverEmail				
OrderResponseHeader			Req	
OrderID	String	50	Req	

4.4 GetCloudOVApproverList

GetCloudOVApproverList Request

This function is used to retrieve the approver email list from the WHOIS database for the SANs to be used in CloudOV Certificate. The approver list function must be requested before the CloudOVOrder and CloudOVSANOrder requests can be made. For adding SANs to an existing CloudOV Certificate, you must enter the OrderID and FQDN of the certificate to which you wish to add the SANs.

Field	Type	Size	Req	Remarks
GetCloudOVApproverList				
QueryRequestHeader			Req	
OrderID	String	50	Req	
FQDN	String	255	Req	
CloudOVSAN+	String	255	Req	

GetCloudOVApproverList Response

Field	Type	Size	Req	Remarks
ResendApproverEmail				
QueryResponseHeader			Req	
Approvers+				
CloudOVSAN	String	255	Req	
Approver+				
ApproverEmail	String	255	Req	
ApproverType	String	10	Req	Domain, Generic
OrderID	String	50		

This response will contain a success code, a list of approver contact details for the end user to choose from, and an OrderID for continuing with the order. If the success code is -1, the request procedure will stop and the error codes reference will have to be consulted.

4.5 GetCloudOVOrderByOrderID

GetCloudOVOrderByOrderID Request

This function is used to obtain certificate, order status, and SANs approval status from selected Order ID.

Field	Type	Size	Req	Remarks
GetCloudOVOrderByOrderID				
QueryRequestHeader			Req	
OrderID	String	50	Req	
OrderQueryOption	String	255		
OrderStatus	Boolean	5	Opt	
ReturnOrderOption	Boolean	5	Opt	
ReturnCertificateInfo	Boolean	5	Opt	
ReturnFulfillment	Boolean	5	Opt	
ReturnCACerts	Boolean	5	Opt	

GetCloudOVOrderByOrderID Response

Field	Type	Size	Req	Remarks
GetCloudOVOrderByOrderID				
QueryResponseHeader				
OrderID				
OrderDetail				
OrderInfo				
OrderSubInfo				
CloudOVSANInfo				
OrderOption				
CertificateInfo				
Fulfillment				
ModificationEvents				

4.6 GetModifiedCloudOVOrders

GetModifiedCloudOVOrders Request

Similar to the GetCloudOVOrderByOrderID request described previously, the GetModifiedCloudOVOrders API request will return a list of orders modified within a specified time frame.

Note: The response to this API command does not return “ContactInfo”. If you need that information then use the GetCloudOVOrderByOrderID API command

4.7 OrderDetail

The OrderDetail data structure is long and complex and used in a number of the query messages. It's detailed below for references purposes.

Field	Type	Size	Req	Remarks
OrderDetail				
OrderInfo	string			
OrderID	string			
ProductCode	string			
OrderKind	string			
BaseOption	string			
Licences	int			
ValidityPeriodCustomizeOption	boolean			
InsuranceOption	boolean			
GSSupportOption	boolean			
RenewalExtensionOption	boolean			
DomainName	string			
OrderDate	date			
OrderCompleteDate	date			
OrderDeactivatedDate	date			
OrderStatus	int			
Price	int			
Currency	string			
ValidityPeriod				
NotBefore	date			
NotAfter	date			
OrderSubInfo				
CSRSkipOrderFlag				
DNSOrderFlag				
TrustedOrderFlag				
P12DeleteStatus				
P12DeleteDate				
VerificationUrl				
SubID				
CloudOVSANInfo				
CloudOVSANDetail				This will repeat to list the SAN's in the CloudOVOrder
CloudOVSAN	string			
CloudOVSANStatus	int			
ApproverEmail	string			Only included if approved with approval email
OrderDate	date			
OrderCompleteDate	date			
MetaTag	string			
OrderOption				
ApproverNotifiedDate				
ApproverConfirmDate				
ApproverEmailAddress				
OrganizationInfo				
OrganizationName				
CreditResearchKind	string			
CreditResearchNumber				
OrganizationAddress				
AddressLine1	string			
AddressLine2				
AddressLine3				
Locality	string			
StateOrProvince	string			
Country	string			
Fax				
ContactInfo				No data is returned, please use GetCloudOVOrderByOrderID if ContactData is needed
FirstName	string			
LastName	string			
Phone	string			
Email	string			
CertificateInfo				
CertificateStatus	int			
StartDate	date			

EndDate	date			
SerialNumber	string			
Fulfillment				
CACertificates				
CACertificate				
CACertType	string			ROOT or INTER
CACert	string			
ServerCertificate				
X509Cert	Base64			
PKCS7Cert	Base64			
ModificationEvents				
ModificationEvent				
ModificationEventName	int			
ModificationEventTimestamp	date			

5. Certificate Order Entry Parameters

5.1 ApproverFQDN values for Metatag and DNS

5.1.1 HTTP Validation

The GlobalSign Validator identifies itself with the User-Agent string:

```
GlobalSign-Approver-URL-Domain-Control-Verification-Agent-www.globalsign.com
```

Based on the SAN being validated, the Validator will only accept certain locations as valid.

The following option **must** be used by February 27, 2017:

<CloudOVSAN> Parameter examples	Valid <ApproverURL> options
*.example.com or example.com	http(s)://example.com/.well-known/pki-validation/gsdv.txt
*.sub.example.com or sub.example.com	http(s)://example.com/.well-known/pki-validation/gsdv.txt http(s)://sub.example.com/.well-known/pki-validation/gsdv.txt
*.www.example.com or www.example.com	http(s)://example.com/.well-known/pki-validation/gsdv.txt http(s)://www.example.com/.well-known/pki-validation/gsdv.txt

The following options are valid only until February 27, 2017:

<CloudOVSAN> Parameter examples	Valid <ApproverURL> options
*.example.com or example.com	http(s)://example.com http(s)://example.com/.well-known/globalsign/domain-validation/gstext.html
*.sub.example.com or sub.example.com	http(s)://example.com http(s)://example.com/.well-known/globalsign/domain-validation/gstext.html http(s)://sub.example.com http(s)://sub.example.com/.well-known/globalsign/domain-validation/gstext.html
*.www.example.com or www.example.com	http(s)://www.example.com http(s)://www.example.com/.well-known/globalsign/domain-validation/gstext.html http(s)://example.com http(s)://example.com/.well-known/globalsign/domain-validation/gstext.html

This is an example metatag value:

```
<meta name="globalsign-domain-verification"
content="8Aetu7b1LEMGdrwZD069ghBGZ-Szq5Md93_DpS44Iq" />
```

5.1.2 DNS Validation

Example DNS Values

<CloudOVSAN> Parameter	Valid <ApproverFQDN>
example.com	example.com
a.sub.example.com	a.sub.example.com sub.example.com example.com
www.example.com	www.example.com example.com

This is an example DNS text record:

```
_globalsign-domain-verification=BK0LemDQJyYzJeHVO8B0oL4mhwmcss6iqIbkTi0_dL
```

5.2 Country

List of country two digit codes and currently supported status, Y = supported N = not supported.

Code	Name	Status
AD	ANDORRA	Y
AE	UNITED ARAB EMIRATES	Y
AF	AFGHANISTAN	N
AG	ANTIGUA AND BARBUDA	Y
AI	ANGUILLA	Y
AL	ALBANIA	Y
AM	ARMENIA	Y
AN	NL ANTILLES (USE CW or SX)	N
AO	ANGOLA	N
AQ	ANTARCTICA	Y
AR	ARGENTINA	Y
AS	AMERICAN SAMOA	Y
AT	AUSTRIA	Y
AU	AUSTRALIA	Y
AW	ARUBA	Y
AX	ALAND ISLANDS	Y
AZ	AZERBAIJAN	Y
BA	BOSNIA AND HERZEGOVINA	Y
BB	BARBADOS	Y
BD	BANGLADESH	Y
BE	BELGIUM	Y
BF	BURKINA FASO	Y
BG	BULGARIA	Y
BH	BAHRAIN	Y
BI	BURUNDI	Y
BJ	BENIN	Y
BM	BERMUDA	Y
BN	BRUNEI DARUSSALAM	Y
BO	BOLIVIA	Y
BR	BRAZIL	Y
GW	GUINEA-BISSAU	Y
GY	GUYANA	Y
HK	HONG KONG	Y
HM	HEARD ISLAND AND MCDONALD ISLANDS	Y
HN	HONDURAS	Y
HR	CROATIA	Y
HT	HAITI	Y
HU	HUNGARY	Y
ID	INDONESIA	Y
IE	IRELAND	Y
IL	ISRAEL	Y
IM	ISLE OF MAN	Y
IN	INDIA	Y
IO	BRITISH INDIAN OCEAN TERRITORY	Y

Code	Name	Status
IQ	IRAQ	N
IR	IRAN, ISLAMIC REPUBLIC OF	N
IS	ICELAND	Y
IT	ITALY	Y
JE	JERSEY	Y
JM	JAMAICA	Y
JO	JORDAN	Y
JP	JAPAN	Y
KE	KENYA	Y
KG	KYRGYZSTAN	Y
KH	CAMBODIA	Y
KI	KIRIBATI	Y
KM	COMOROS	Y
KN	SAINT KITTS AND NEVIS	Y
KP	NORTH KOREA (DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA)	N
BS	BAHAMAS	Y
BT	BHUTAN	Y
BV	BOUVET ISLAND	Y
BW	BOTSWANA	Y
BY	BELARUS	Y
BZ	BELIZE	Y
CA	CANADA	Y
CC	COCOS (KEELING) ISLANDS	Y
CD	CONGO, THE DEMOCRATIC REPUBLIC OF THE	Y
CF	CENTRAL AFRICAN REPUBLIC	Y
CG	CONGO	Y
CH	SWITZERLAND	Y
CI	COTE D'IVOIRE	Y
CK	COOK ISLANDS	Y
CL	CHILE	Y
CM	CAMEROON	Y
CN	CHINA	Y
CO	COLOMBIA	Y
CR	COSTA RICA	Y
CU	CUBA	N
CV	CAPE VERDE	Y
CW	CURACAO	Y
CX	CHRISTMAS ISLAND	Y
CY	CYPRUS	Y
CZ	CZECH REPUBLIC	Y
DE	GERMANY	Y

Code	Name	Status
DJ	DJIBOUTI	Y
DK	DENMARK	Y
DM	DOMINICA	Y
DO	DOMINICAN REPUBLIC	Y
DZ	ALGERIA	Y
KR	KOREA, REPUBLIC OF	Y
KW	KUWAIT	Y
KY	CAYMAN ISLANDS	Y
KZ	KAZAKSTAN	Y
LA	LAO PEOPLE'S DEMOCRATIC REPUBLIC	Y
LB	LEBANON	Y
LC	SAINT LUCIA	Y
LI	LIECHTENSTEIN	Y
LK	SRI LANKA	Y
LR	LIBERIA	N
LS	LESOTHO	Y
LT	LITHUANIA	Y
LU	LUXEMBOURG	Y
LV	LATVIA	Y
LY	LIBYAN ARAB JAMAHIRIYA	N
MA	MOROCCO	Y
MC	MONACO	Y
MD	MOLDOVA, REPUBLIC OF	Y
ME	MONTENEGRO	N
MG	MADAGASCAR	Y
MH	MARSHALL ISLANDS	Y
MK	MACEDONIA, THE FORMER YUGOSLAV REPUBLIC OF	Y
ML	MALI	Y
MM	MYANMAR	Y
MN	MONGOLIA	Y
MO	MACAU	Y
MP	NORTHERN MARIANA ISLANDS	Y
MQ	MARTINIQUE	Y
MR	MAURITANIA	Y
EC	ECUADOR	Y
EE	ESTONIA	Y
EG	EGYPT	Y
EH	WESTERN SAHARA	Y
ER	ERITREA	Y
ES	SPAIN	Y
ET	ETHIOPIA	Y
FI	FINLAND	Y
FJ	FIJI	Y

Code	Name	Status
FK	FALKLAND ISLANDS (MALVINAS)	Y
FM	MICRONESIA, FEDERATED STATES OF	Y
FO	FAROE ISLANDS	Y
FR	FRANCE	Y
GA	GABON	Y
GB	UNITED KINGDOM	Y
GD	GRENADA	Y
GE	GEORGIA	Y
GF	FRENCH GUIANA	Y
GG	GUERNSEY	Y
GH	GHANA	Y
GI	GIBRALTAR	Y
GL	GREENLAND	Y
GM	GAMBIA	Y
GN	GUINEA	Y
GP	GUADELOUPE	Y
GQ	EQUATORIAL GUINEA	Y
GR	GREECE	Y
GS	SOUTH GEORGIA AND THE SOUTH SANDWICH ISLANDS	Y
GT	GUATEMALA	Y
GU	GUAM	Y
MS	MONTSERRAT	Y
MT	MALTA	Y
MU	MAURITIUS	Y
MV	MALDIVES	Y
MW	MALAWI	Y
MX	MEXICO	Y
MY	MALAYSIA	Y
MZ	MOZAMBIQUE	Y
NA	NAMIBIA	Y
NC	NEW CALEDONIA	Y
NE	NIGER	Y
NF	NORFOLK ISLAND	Y
NG	NIGERIA	Y
NI	NICARAGUA	Y
NL	NETHERLANDS	Y
NO	NORWAY	Y
NP	NEPAL	Y
NR	NAURU	Y
NU	NIUE	Y
NZ	NEW ZEALAND	Y
OM	OMAN	Y
PA	PANAMA	Y

Code	Name	Status
PE	PERU	Y
PF	FRENCH POLYNESIA	Y
PG	PAPUA NEW GUINEA	Y
PH	PHILIPPINES	Y
PK	PAKISTAN	Y
PL	POLAND	Y
PM	SAINT PIERRE AND MIQUELON	Y
PN	PITCAIRN	Y
PR	PUERTO RICO	Y
PS	PALESTINIAN TERRITORY, OCCUPIED	Y
PT	PORTUGAL	Y
PW	PALAU	Y
PY	PARAGUAY	Y
QA	QATAR	Y
RE	REUNION	Y
RO	ROMANIA	Y
RS	SERBIA	N
RU	RUSSIAN FEDERATION	Y
RW	RWANDA	N
SA	SAUDI ARABIA	Y
SB	SOLOMON ISLANDS	Y
SC	SEYCHELLES	Y
SD	SUDAN	N
SE	SWEDEN	Y
SG	SINGAPORE	Y
SH	SAINT HELENA	Y
SI	SLOVENIA	Y
SJ	SVALBARD AND JAN MAYEN	Y
SK	SLOVAKIA	Y
SL	SIERRA LEONE	N
SM	SAN MARINO	Y
SN	SENEGAL	Y
SO	SOMALIA	N
SR	SURINAME	Y
ST	SAO TOME AND PRINCIPE	Y
SV	EL SALVADOR	Y
SX	SINT MAARTEN	Y
SY	SYRIAN ARAB REPUBLIC	N
SZ	SWAZILAND	Y

Code	Name	Status
TC	TURKS AND CAICOS ISLANDS	Y
TD	CHAD	Y
TF	FRENCH SOUTHERN TERRITORIES	Y
TG	TOGO	Y
TH	THAILAND	Y
TJ	TAJIKISTAN	Y
TK	TOKELAU	Y
TL	TIMOR-LESTE	Y
TM	TURKMENISTAN	Y
TN	TUNISIA	Y
TO	TONGA	Y
TR	TURKEY	Y
TT	TRINIDAD AND TOBAGO	Y
TV	TUVALU	Y
TW	TAIWAN, PROVINCE OF CHINA	Y
TZ	TANZANIA, UNITED REPUBLIC OF	Y
UA	UKRAINE	Y
UG	UGANDA	Y
UM	UNITED STATES MINOR OUTLYING ISLANDS	Y
US	UNITED STATES	Y
UY	URUGUAY	Y
UZ	UZBEKISTAN	Y
VA	HOLY SEE (VATICAN CITY STATE)	Y
VC	SAINT VINCENT AND THE GRENADINES	Y
VE	VENEZUELA	Y
VG	VIRGIN ISLANDS, BRITISH	Y
VI	VIRGIN ISLANDS, U.S.	Y
VN	VIET NAM	Y
VU	VANUATU	Y
WF	WALLIS AND FUTUNA	Y
WS	SAMOA	Y
YE	YEMEN	Y
YT	MAYOTTE	Y
ZA	SOUTH AFRICA	Y
ZM	ZAMBIA	Y
ZW	ZIMBABWE	Y

5.3 CreditAgency/OrganizationCode

CreditAgency/OrganizationCode is added to help GlobalSign validate the customer's organization. If the customer has one of these numbers it should just be flagged as available, the actual code is not to be entered.

Value	Credit Agency
1	Dunn and Bradstreet number
2	Teikoku Databank Code (TDC)

5.4 Date/Time Formatting

Date/Time is based on UTC and includes milliseconds. eg: 2006-12-07T18:16:33.594Z
This format is defined* as “xsd:dateTime XML Simple Type”.

* http://www.w3.org/TR/xmlschema-2/#dateTime

5.5 Hash Algorithm

When an order is being placed the Product Code is used to specify the hash algorithm, but when reissuing a certificate there is no Product Code, thus the need for Hash Algorithm.

- If this is not specified, certificates will be issued based on the hash algorithm of the certificate being reissued.
- If SHA1 is specified, the SHA1 product option will be issued.
- If SHA256 is specified, SHA-256 product option will be issued.

Note that when changing the hash algorithm the issuing CA will also change so a new Subordinate CA certificate will need to be configured on the server as part of the certificate installation process.

Since the validity period of SHA-1 certificates is shorter, per industry standards, if a certificate is reissued from SHA256 to SHA-1 it may result in a truncated validity period. This can be recovered in subsequent reissues using an algorithm other than SHA-1.

Not all products support all Hash Algorithms, see section 5.10.

5.6 KeyLength

This reflects the Key Length to be used if the keys are being created on GlobalSign servers. Only RSA key generation is supported and valid values 2048 or 4096.

5.7 ModifyOperation

This defines the operations you can do to SAN entries.

OptionName	Description
ADDITION	Add a SAN to an existing CloudSSL certificate
DELETE	Delete a SAN from an existing CloudSSL certificate
CANCEL	Cancel a pending request to add a SAN to a CloudSSL certificate. You need to do this if you want to issue the certificate but there are some pending SANs.

5.8 OptionName

The following option types must be added for ordering certificates with extended options. Set to TRUE to activate.

OptionName	Description
SAN	Activates the Subject Alternative Name (SANs) options – see section on Subject Alternative Names (SANs) Entry
REX	Optionally adds an additional 30 days to a Renewal order
VPC	Allows the start date and end date of the certificate to be customized – see section on Setting validity period of the certificate (by Not before/Not after date)

5.9 Order Type

The following OrderTypes can be ordered through the API.

Value	OrderKind	Notes
1	New	A new order
2	Renewal	A renewal order for replacing an expiring certificate with fewer than 90 days remaining
3	Transfer	A competitive switch – a certificate is being traded in from another SSL provider and the remaining validity will be added onto this order (up to specified validity period limits set by the industry requirements.

5.10 Product Codes

Currently for Cloud OV orders there are only two product types which can be used. SHA-1 will be depreciated on December 14, 2015.

Code	Certificate Type
CLOUD_OV	CloudOV certificate signed with SHA1
CLOUD_OV_SHA2	CloudOV certificate signed with SHA2

5.11 Validity Period

You can control the validity period of ordered certificates by setting the number of months.

Number Of Months
12
24
36

5.12 WildCard Subject Alternative Names (SANs) Entry

Given the CN value listed in the first column (<CloudOVSAN>) and the presence or not of the <AdditionalWildcardOption>, the SANs included in the certificate are listed below:

<CloudOVSAN> Parameter	SANS in Issued Certificate if <AdditionalWildcardOption> ==		<AdditionalWildcardOption> Not specified
	false	true	
example.com	example.com	example.com *.example.com	example.com
*.example.com	*.example.com	*.example.com example.com	*.example.com
www.example.com	www.example.com	www.example.com *.www.example.com	www.example.com
sub.example.com	sub.example.com	sub.example.com *.sub.example.com	sub.comain.com
*.sub.example.com	*.sub.example.com	*.sub.example.com sub.example.com	*.sub.example.com

6. Status Explanations

6.1 Order/Certificate Status

Order/Certificate status of any certificate request can be obtained at any time, via GetModifiedOrders API call.

Value	Order Status
1	INITIAL
2	Waiting for phishing check
3	Cancelled – Not Issued
4	Issue completed
5	Cancelled - Issued
6	Waiting for revocation
7	Revoked
8	SAN Canceled
9	SAN Deleted

6.2 ModificationEventName

ModificationEventName is returned from GetModifiedOrders. At any time all modified orders and their modification can be returned from the API.

Code	ModifictionEventName	Description
0	ORDER_REQUEST	Certificate application accepted
1	ORDER_CONSENT	Certificate application permitted
2	ORDER_NOT_CONSENT	Certificate application refused
3	ORDER_VALIDATE_REGISTER	Vetting requested to RA
6	ORDER_APPROVE_DENIAL	Order rejected by RA
7	CERT_ISSUE	Issue certficate
8	ORDER_ISSUE_BEFORE_CANCEL	Order cancelled before issue
9	ORDER_ISSUE_AFTER_CANCEL	Order cancelled after issue
10	ORDER_CANCEL_REQUEST	Request to cancel order
11	CERT_REVOKE_REQUEST	Request to revoke certificate
12	CERT_REVOKE	Certificate revoked
13	CERT_REVOKE_DENIAL	Certificate revocation refused
14	CERT_CA_REVOKE	Certificate revoked by CA
15	CERT_TRANSFER	Certificate transferred to other corporations
16	CERT_REISSUE	Certificate reissue
17	ORDER_ERROR_RECOVERY	Error recovered
23	CERT_REVOKE_CANCEL	Certificate revocation cancelled
24	ORDER_REISSUE_REQUEST	Application for certificate reissue
25	REORDER_CANCEL_REQUEST	Cancelled certificate reorder
27	CERT_RENEWAL_INFORMATION	Certificate renewal notice
28	CERT_REVOKE_REGISTER	Request vetting for revoke to RA
29	ORDER_RESEND_APPROVAL_MAIL	Resend approval e-mail
30	ORDER_CHANGE_APPROVAL_MAIL	Change approval e-mail address
31	ORDER_CHANGE_PAY_AFTER	Change the payment method to after payment
32	ORDER_CHANGE_CONTRACTOR	Change the contractor
33	ORDER_CHANGE_SALES	Change the sales group, sales staff
35	SEAL_REGISTER	Request for seal register
36	SEAL_REVOKE	Request to delete seal
37	SEAL_CHANGE	Request to change seal
38	DELETE_PKCS12	Delete PKCS12

39	DOWNLOAD_PKCS12	Download PKCS12
40	VALIDATE_PHISHING	Caught in Phishing, vetting
41	EDIT_CONTACT	Change the contact information
42	AGENCY_AUTHENTIC	Approve order application from agency
43	CHANGE_AUTH	Change authenticate information
44	ORDER_REISSUE_REGISTER	Request reissue to RA
45	ORDER_REISSUED_REQUEST	Reissue request from GAS
46	ORDER_CHANGE_SAN_REQUEST	Request to change the SAN
47	ORDER_CHANGED_SAN_REQUEST	Received request to change SAN
48	ORDER_CHANGE_SAN_REGISTER	Send request to change SAN to RA
49	EV_AUTHENTIC	Primary approval of EV
51	CERT_ISSUE_PAID	Card payment done when the certificate is issued
52	ORDER_CANCEL_REQUEST_4_RA_OPERATOR	Order cancel request by RA operator
53	ORDER_CANCEL_REQUEST_4_APPROVAL_EMAL	Request order cancel by approval e-mail
54	AUTHENTICATE_PHISING	Approve phishing
55	READY_VARIFICATION_URL	Ready for URL approval
56	VARIFICATION_URL	URL approval completed

6.3 CloudOVSAN Status

CloudOVSAN status of any certificate request can be obtained at any time, via GetModifiedCloudOVOrders API call.

Value	Order Status
0	INITIAL.(Waiting for approval)
1	INITIAL.(Waiting for approval)
2	SAN Approved (Not issued yet)
3	SAN Issued
7	Waiting for phishing check
8	SAN Canceled
9	SAN Deleted

6.4 Allowable SAN Actions & Status Combinations

Action	Allowable SAN statuses
Cancel	0,1,2,7
Delete	3
Addition	none, 8, 9
Resend Approver Email	0,1
Issue	2

6.5 Success / Error Codes

A SuccessCode is always returned from the API, if the SuccessCode is 0 or 1, the order will normally be able to continue. A SuccessCode of -1 will be a terminating point and will be combined in the reply with one or more ErrorCodes. ErrorCodes provide more information on the error created with the API call. In addition to the error message documentation below, the API returns more specific error details regarding the specific fields that may be causing problems in the XML response.

There are two types of errors: Client Error and Server Error.

Client error codes suggest that the error was caused by something on the client end. These issues are often due to malformed XML requests, incorrect or missing data, or other API implementation issues. A client error code indicates that the request has not been accepted and the user must make changes and resubmit.

Server error codes suggest a server-side issue caused the error and should be reported to api@globalsign.com. The request is received but it may not be processed immediately or the request cannot received by GCC system. A server error code is received, please view compare the error code and the table in the server error code section.

6.5.1 Success Codes

Code	Code Details	Notes
0	Success	
-1	Failure	The order/request has failed; please consult the Error Code list, as well as the error message in the XML response for remedial actions.
1	Warning	Indicates order has been flagged for Phishing. The order is valid, but will experience a delay in processing until the GlobalSign vetting team manually reviews and clears the order's phishing flag

6.5.2 Client Error Codes

Success Code	Error Code	Description	Notes
0	-	Success	-
-1	-101	Invalid Parameter	This error code can be caused by multiple types of errors. Please review the specific ErrorMessage returned in the XML response for parameter details and consult the XML Field definitions section of this document.
-1	-102	An essential parameter is missing	This error code can be caused by multiple types of errors/omissions. Please review the specific ErrorMessage returned in the XML response for parameter details and consult the XML Field definitions section of this document.
-1	-103	A parameter is too long	This one of the parameters in your request is too long. Please review the specific ErrorMessage returned in the XML response for parameter details and consult the XML Field definitions section of this document.
-1	-104	The format for a parameter is incorrect	This error code can be caused by multiple types of errors/omissions. Please review the specific ErrorMessage returned in the XML response for parameter details and consult the XML Field definitions section of this document.
-1	-105	Invalid Parameter	This error code can be caused by multiple types of errors. Please review the specific ErrorMessage returned in the XML response for parameter details and consult the XML Field definitions section of this document.
-1	-310	Transfer based certificate is invalid.	- Please ensure that the competitor's certificate is not expired. - The certificate must be publically accessible - If the above conditions are met, please contact your GlobalSign support representative and provide the transfer certificate for review.
-1	-3002	Domain not found in WHOIS database	Please review the submitted domain for accuracy; ensure it is in WhoIs and reachable online. If the problem persists, please report this error code to GlobalSign Support.
-1	-3007	DNS not found in WHOIS database	Please review the submitted domain for accuracy. If the problem persists, please report this error code to GlobalSign Support.

Success Code	Error Code	Description	Notes
-1	-3008	Could not connect to the target FQDN server.	Check if targeted FQDN server is reachable online.
-1	-3009	Specified FQDN does not match FQDN in specified VerificationURL.	Review the XML request to ensure there is a match between the FQDN and the Verification URL.
-1	-3010	CSR File Size Error	Review the CSR and confirm it is within the data size limits defined in the XML Field Definitions section of this document
-1	-3017	The CSR file cannot be acquired from specified VerificationURL.	Confirm the CSR is available at the Verification URL
-1	-3018	Domain not found in WHOIS database	Please review the submitted domain for accuracy; ensure it is in WhoIs and reachable online. If the problem persists, please report this error code to GlobalSign Support.
-1	-4001	Login failure - invalid user ID or password	Check your username and password and try again
-1	-4002	Specified ApproverEmail does not exist.	GetDVApproverList() needs to be carried out before you can proceed. Ensure you are using an email which is associated with the CN on the WhoIs database
-1	-4003	Specified OrderID/Voucher Number does not exist.	Confirm the OrderID/Voucher Number has been created/is valid and try again.
-1	-4004	OrderId has already been used	You must use a new OrderID, the OrderID provided is already in use.
-1	-4005	Your request has not been accepted due to a logical limitation. The notes describe the limitations that may be encountered for the request that was submitted.	ResendEmail - You cannot ResendEmail if The order status is complete, canceled, or revoked. - There is approval email for The product associated with The OrderID provided. ReOrder,ReOrderWithoutCSR - You cannot ReOrder when The order status is reissued. - The OrderID provided in The request has expired. You will not be able to ReOrder ModifyOrder - If you are trying to approve an order, the order status must be INITIAL or approval may not be required for the product associated with the OrderID provided - If you are trying to cancel an order, the order status must not be CANCELED. - If you are trying to revoke an order, the order status must be ISSUED DeletePkcs12 - The OrderID provided is not found, please confirm in the GCC GUI - The certificate may not have been issued yet
-1	-4006	Specified ProductCode is invalid.	Please review the ProductCode being used an ensure it is a valid code listed in the Certificate Order Entry Parameters section of this document
-1	-4007	Specified CSR is invalid.	- CN was not found in CSR. - FQDN in GetDVApproverList does not match to CN in CSR. - in ReOrder, FQDN does not match to CN in CSR.
-1	-4008	TargetCERT is expired or inaccessible	The Certificate in specified TargetCERT is expired and does not meet the requirements of transfer or is inaccessible on the CN by the GlobalSign system. Please ensure that the target certificate is active.
-1	-4009	Specified ApproverEmail is invalid.	You need to select an email address from GetDVApproverList response.
-1	-4011	The CSR did not match.	Specified CSR did not match CSR of VerificationURL.
-1	-4012	Specified FQDN is invalid.	Please review syntax of the FQDN and ensure it is accessible
-1	-4013	The PKCS#12 has been already deleted.	
-1	-4016	The certificate has been already reissued	Check the status of your certificate, the certificate has already been re-ordered
-1	-4024	Account Not Authorized for TrustedOrder	Your account has not yet been approved for TrustedOrders. Contact api@globalsign.com to review the activation status.

Success Code	Error Code	Description	Notes
-1	-4025	Default DvTemplateID Not Found	Your account has not yet been approved for TrustedOrders. Contact api@globalsign.com to review the activation status.
-1	-4026	EVOrderFlag and parameter combination error	There is an error with the combination of parameters the request contains. Please review the documentation for the EV order and resubmit the request.
-1	-4027	ProductCode and parameter combination error	There is an error with the combination of parameters the request contains. Please review the documentation for the type of order and resubmit the request.
-1	-4038	Host Name Does not Match in 'UC Cert Option'	There is not a match of the CN and the domains specified in the UC Sans. Please update the entries so that they are equal
-1	-4039	Host Name is not www	The host name for the request you are submitting must contain www as the subdomain.
-1	-4040	FQDN domain is not same as SubjectAltName domain	Review the SANS options of the certificate to ensure subdomains are the same domain as CommonName
-1	-4042	SANOptionType and ProductCode combination error	There is a conflict between the SANS options and the Product Code you are requesting. Please review the documentation for the order request you are using.
-1	-4043	Specified SubjectAltName is not a global IP address.	The following are unallowable SAN addresses: 10.0.0.0 - 10.255.255.255 172.16.0.0 - 172.31.255.255 192.168.0.0 - 192.168.255.255 127.0.0.0 - 127.255.255.255 224.0.0.0 - 255.255.255.255
-1	-4044	Specified SubjectAltName is not IP address format.	Review IP addresses used in the SAN Option to ensure they are accurate
-1	-4045	Specified SubjectAltName is not private IP address.	Review the private IP addresses provided in the request
-1	-4047	FQDN TLD is public domain in 'Internal SAN Option(InternalFQDN)'	The public domain cannot be specified with an InternalSAN address.
-1	-4048	SAN and FQDN are same	Update the SAN listing to eliminate the conflict
-1	-4049	FQDN must not be an IP address in the 'FQDN Option'	The specified FQDN SAN is an IP address. Change option or change FQDN to proper format
-1	-4050	FQDN must not be single word in 'FQDN Option'	Update the single word(s) to FQDNs
-1	-4052	Internal SAN Option' parameter is invalid	Review the address provided for the Internal SAN Option and ensure it is a valid format
-1	-4053	SAN Domain is not listed as an Account Domain in MSSL Account	Please register the domain in your MSSL account.
-1	-4054	Requested FQDN is not permitted by specified DomainID	Do not use the same SAN as CN in the request
-1	-4083	Specified domain is not available.	Please register the domain in your MSSL account
-1	-4101	Specified OrderID cannot be used in the "ModifyOrder" operation	Ensure you were using the appropriate OrderID.
-1	-4102	This UserID is not authorized for certificate approval.	Your user account needs additional privileges for certificate request approval. Contact api@globalsign.com.
-1	-4126	Error adding SAN	getCloudApproverList() needs to be carried out before you proceed adding the requested SAN
-1	-4127	Error Adding SAN	Requested SANs are already added to certificate
-1	-4201	This IP Address is not registered for API access	Please contact api@globalsign.com.
-1	-4202	The specified MSSL account is not approved yet.	Please retry request after registration of your MSSL account has completed. Contact api@globalsign.com.
-1	-4203	Specified domain is not approved yet.	Log into the GCC interface to review the status of your MSSL Domain registration. If no request was submitted, then follow the appropriate steps to submit a MSSL Domain registration
1	-5001 -5002	Phishing warning - CN matched in phishing database	The CN has expressions that match our Phishing warning list. This order will be delayed slightly until the vetting team can manually review the requested domain. This doesn't mean the order is invalid, only that it will be slightly delayed.
-1	-6001	Specified CSR is invalid.	Review the API response for further details and check your CSR submitted for correct format for the following errors:

Success Code	Error Code	Description	Notes
			- CN is not found. - Public key is invalid format or using unsupported algorithm - The length of Public key is short. - The Public key specified has already been used. - invalid country. specified TLD is Not supported. - It is not include wildcard in order with wildcard option. - It is not include public IP in order with GlobalIP option. - CSR invalid CN. CN ends with a dot. - CSR invalid C.
1	-6002	Specified certificate is invalid.	The CSR provided is invalid or corrupted. Please regenerate the CSR. The GlobalSign System cannot parse certificates generated with the IAIK library
-1	-6003	Specified PIN is invalid.	Please review the PIN generating process that was used and from section 16.17
-1	-6007 -6008	The public key is already used.	Please generate new private key and CSR.
-1	-6012	CN or O or L or ST or C Not Found in CSR	Please review CSR and ensure all required fields are included
-1	-6013	CN or C Not Found in CSR	Please review CSR and ensure all required fields are included
-1	-6014	CN or O or L or ST or C Not Found in CSR	Please review CSR and ensure all required fields are included
-1	-6017	Maximum number of SANs options have been exceeded	Please adjust an optional number to 40 entries or less.
-1	-6018	Specified SubjectAltName is invalid.	SubjectAltName is duplicated. Remove duplicates from request and resubmit
-1	-6019	The number of characters of CN exceeds the limitation.	Please adjust the number of characters to 1024 bytes or less.
-1	-6020	The size of CSR exceeds the limitation.	Please adjust the file size of CSR to 3000 bytes or less.
-1	-6021	CN in CSR and FQDN are not same	Review the request and ensure CN and FQDN match
-1	-6022	FQDN and SANEntries are not same	Review the request and ensure SANS options and FQDN match
-1	-6023	FQDN without [www. or *.] and SAN are same	CN beginning with "www" or "*" is automatically set to the specified SAN.
-1	-6101	Account Balance Error	Insufficient credit in your account to complete this order. Add deposit or increase credit levels.
-1	-6102	Specified order cannot be a renewal.	- The designated certificate is not renewable. Please confirm if it has not already been renewed. - CN in CSR do not match CN in renewal target order. - The renewal is allowed in the validity period only 90 days before expiration and after 14 days after expiration. - The status of renewal target order is invalid. Target order status must be "Issue completed"
-1	-9101	Illegal SAN Option	The SANS used in the ChangeSubjectAltName request are invalid. The SANS option type must be the same as the original order
-1	-9104	Process Sequence Error	You must run the GetCloudOVApprover list request before submitting a request for a new CloudOV order.
-1	-9105	Error Adding SAN	The SAN you've requested to add already exists on the order specified, so it cannot be added. If the approver email has been issued, but not approved, please try canceling the SAN if you need to remove it.
-1	-9106	Error Deleting SAN	The SAN you've requested to delete does not exist on the order specified, so it cannot be deleted. If the approver email has been issued, but not approved, please try canceling the SAN
-1	-9107	Error Canceling SAN	The SAN you've requested to cancel does not exist on the order specified, or has already been issued on the order so it cannot be canceled. If he SAN has been approved, please try deleting the SAN

Success Code	Error Code	Description	Notes
-1	-9108	Error Resending Approver Email	The SAN you've requested to send the approver email for has is not awaiting approval, so that you cannot resend an approval email.
-1	-9109	Error Issuing SAN	Certificate is in mid-process. Please wait a few minutes and retry the request again.

6.5.3 Server Error Codes

Success Code	Error Code	Description	Notes
-1	-1	Internal system error	The system has experienced an internal error. Please try to do what you were doing again, and if the problem persists, please report this error code to GlobalSign Support.
-1	-2	Network Connection Error	The GlobalSign system has experienced a network error. Cross-reference the appropriate API request action from Section .Please try to do what you were doing again, and if the problem persists, please report this error code to GlobalSign Support.
-1	-201 -204 -300 -301	Internal system error - Failed database operation	The system has experienced an internal error updating the database. Please try to do what you were doing again, and if the problem persists, please report the following error code to GlobalSign Support.
-1	-1001	Internal system error - CA connection error	The CA system has experienced a communication error. Your Order has been accepted and will be processed when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-1002	Internal system error - CA issuing error	The CA system has experienced an issuance process error. Your Order has been accepted and will be processed when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-1003	Internal system error - CA revoke error	The CA system has experienced a revocation process error. Your Order has been accepted and will be processed when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-1004	Internal system error - CA connection error	The CA system has experienced a communication error. Your Order has been accepted and will be processed when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-2001	Internal system error - Email sending warning	The CA system has experienced an email sending error. Your Order has been accepted and the email will be automatically sent when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-4010	Internal system error	The system has experienced an internal error. Your Order has been accepted and the email will be automatically sent when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-4059	Internal system error	The system has experienced an internal error. Your Order has been accepted and the email will be automatically sent when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-4064	Internal system error	The system has experienced an internal error. Your Order has been accepted and the email will be automatically sent when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-4065	Internal system error	The system has experienced an internal error. Your Order has been accepted and the email will be automatically sent when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-4066	Internal system error	The system has experienced an internal error. Your Order has been accepted and the email will be automatically sent when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-4071	Internal system error	The system has experienced an internal error. Your Order has been accepted and the email will be automatically sent when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-4072	Internal system error	The system has experienced an internal error. Your Order has been accepted and the email will be automatically sent when the system

Success Code	Error Code	Description	Notes
			recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-6004	Internal system error	The system has experienced an internal error. Your Order has been accepted and the email will be automatically sent when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-6005	Internal system error	The system has experienced an internal error. Your Order has been accepted and the email will be automatically sent when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.
-1	-6006	Internal system error	The system has experienced an internal error. Your Order has been accepted and the email will be automatically sent when the system recovers. This process may take some time. If the problem persists, please report the following error code to GlobalSign Support.

7. Field Definitions

This table lists all of the data types used in the API specification in alphabetical order.

DataType	Description
String	fixed-length character string
Boolean	logical Boolean (true/false)
Int	signed four-byte integer
DateTime	YYYY-MM-DDTHH:MM:SS.000Z

XML Structure	Description	DataType/ Max length
<AdditionalWildcardOption>	Option for the additional wildcard SAN. The SAN for Wildcard option must be prefixed with 'www.'	Boolean
<AddressLine1>	Part of the Address structure. Contains the first line of the address.	String/100
<AddressLine2>	Part of the Address structure. Contains the second line of the address.	String/100
<AddressLine3>	Part of the Address structure. Contains the third line of the address.	String/100
<Approver> <ApproverType> <ApproverEmail> </Approver>	This is the <Approver> information for each Approver in the <ApproverList>. Today only the e-mail address is returned, but there could be other fields returned in the future.	
<ApproverEmail>	This is the email of the Approver – For DomainSSL and DV_LOW and CloudOVSAN products the person responsible for approving the certificate order.	String/255
<ApproverEmailAddress>	This is the email of the Approver – For DomainSSL and DV_LOW products the person responsible for approving the certificate order.	String/255
<ApproverType>	The type of Approver email address. One of the following: Domain – From WHOIS data Generic – From the computed list	String/10
< Approvers> (<Approver>)+ </Approvers>		
<ApproverInfo> <Email> <FirstName> <Function>? <LastName> <OrganizationName> <OrganizationUnit>? <Phone> </ApproverInfo>	Approver Information for an EV certificate request	
<AuthorizedSignerInfo> <FirstName> <LastName> (<Function>)? <Phone> <Email> </AuthorizedSignerInfo>	Authorized Signer Details	
<AuthToken> <UserName> <Password> </AuthToken>	Used for partner authentication on each message posted to GlobalSign. This partner has to be set up by GlobalSign for API access.	
<BaseOption>	Options for the certificate. Currently allowed fields are: wildcard – certificate with * globalip – certificate with global ip address subaltname – certificate with alternative subject names	String /20
<BusinessAssumedName>		String/255
<BusinessCategoryCode>	Business Type	String /20
<CACert>	This is the content of a CA certificate in the certificate chain for the server certificate in Base64 encoded format.	String/4000

XML Structure	Description	DataType/ Max length

`<CACertificate>`
`<CACertType>`
`<CACert>`
`</CACertificate>`
	This identifies the type of certificate for each CA certificate in the chain, and also contains the actual certificate.	

`<CACertificates>`
`(<CACertificate>`
`<CACertType>`
`<CACert>`
`</CACertificate>)+`
`</CACertificates>`
	This is the list of CA certificates associated with the server certificate. If present, there must be one or more <CACertificate> fields in this structure. The Root certificate will always be present in this structure, and there may be one or more intermediate CA certificates.	

`<CACertType>`	The Type of CA certificate: ROOT or INTER	`String/15`
`<Campaign>`	Campaign can be used for payment。	`String/50`

`<CertificateInfo>`
`<DNSNames>?`
`<CertificateStatus>`
`<CommonName>`
`<EndDate>`
`<SerialNumber>`
`<StartDate>`
`<SubjectName>`
`</CertificateInfo>)?`
	This structure contains information stored related to the certificate in various Query operations.	

`<CertificateStatus>`	The current status of a certificate. 1 - Initial 2 - Waiting for phishing check 3 - Cancelled - Not Issued 4 - Issue completed 6 - Waiting for revocation 7 - Revoked	`Int`
`<CloudOVSAN>`	The CloudOVSAN FQDN	`String/255`

`<CloudSANEntries>`
`(<SANEntry>`
`<CloudOVSAN>`
`<ModifyOperation>`
`<ApproverEmail>?`
`</SANEntry>)+`
`</CloudSANEntries>`		

`<CloudOVSANInfo>`
`(<CloudOVSANDetail>`
`<CloudOVSAN>`
`<CloudOVSANStatus>`
`<ApprverEmail>`
`<OrderDate>`
`<OrderCompleteDate>?`
`<DeleteDate>?`
`<CloudOVSANDetail>)+`
`</CloudOVSANInfo>`		

`CloudOVSANStatus`	CloudOVSAN Status 1 – Initial.(Waiting for approval) 2 – Waiting for phishing check 3 – Approved 7 - Flagged for phishing 8 – Canceled 9 – Deleted	
`<CommonName>`	The common name in the certificate	`String/255`
`<CSRSkipOrderFlag>`		`Boolean`
`<City>`	Part of the Address structure.	`String/200`

`<ContactInfo>`
`<FirstName>`
`<LastName>`
`<Phone>`
`<Email>`
`</ContactInfo>`
	Contact Information of for a certificate request	

`<Country>`	Part of the Organization Address structure. The Country of the Organization. Must be a valid ISO country code.	`String/2`
`<Coupon>`	Coupons can be used for payment in some cases	`String/50`
`<CreditAgency>`	The Organizations name. 1 – DUNS No. 2 – TDB code	`String/50`
`<Currency>`	The Currency of the transaction	`String/10`

XML Structure	Description	DataType/ Max length
`<CSR>`	Certificate Signing Request. This is the Base64 encoded X.509 digital certificate signing request typically generated by the end user on their target web server. This is a critical element for all SSL orders.	String/4000
`<DNSOrderFlag>`		Boolean
`<DNSNames>`	Contains one or more DNSName values to be put into the certificate SubjectAltName extension. Each can be up to 64 characters. Values are comma delimited. Each DNSName may only contain alphanumeric values, plus dash and under bar – No periods.	String/300
`<DomainName>`	The domain name for an Order. For an SSL Order this can be a fully qualified Domain (e.g., www.globasign.com) or possibly a wildcard domain (e.g., *.globalsign.com.	String/255

`<DVCSRInfo>`
`<Country>`
`</DVCSRInfo>`
	CSR information for SKIP GSDVOrders.	

`<EndDate>`	Expired date of certificate.	DateTime
`<Email>`	From the ContactInfo structure. The Email Address of the contact.	String/255

`<Error>`
`<ErrorCode>`
`(<ErrorField>)?`
`<ErrorMessage>`
`</Error>`
	A structure that contains an ErrorCode and an ErrorMessage. Error is part of the Errors structure.	

`<ErrorCode>`	A unique code identifying the error.	Int
`<ErrorField>`	When there is a specific field that has caused the error, the XML tag for that field is placed in this structure. Where the tag is not unique in the entire message, one or more tags precede this so this field can be uniquely identified. For example, if the <Phone> field was invalid in the <AdminContact> structure, the return code would have <AdminContact><Phone>.	String/1000
`<ErrorMessage>`	A message describing an error in more detail. ErrorMessage is a part of the Error Structure	String/1000

`<Errors>`
`(<Error>`
`<ErrorCode>`
`(<ErrorField>)?`
`<ErrorMessage>`
`</Error>)+`
`</Errors>`
	A list of the errors returned from a request. An Errors structure can have multiple Error elements. Errors is a part of the OrderResponseHeader structure. If present, this structure contains one or more errors.	

`(<ExpressOption>)?`	To add Express Options set to true. If not false.	Boolean
`<Fax>`	From the OrganizationAddress structure. The Fax number for the organization.	String/30
`<FirstName>`	From one of the Contact structures. The First Name of the contact.	String/100
`<FQDN>`	Fully Qualified Domain Name	String/255
`<FromDate>`	The starting date used in various queries.	DateTime

`<Fulfillment>`
`<CACertificates>`
`(<CACertificate>`
`<CACertType>`
`<CACert>`
`</CACertificate>)+`
`</CACertificates>?`
`(<ServerCertificate>`
`<x509Cert>`
`<PKCS7Cert>`
`<ServerCertificate>)?`
`</Fulfillment>`
	Contains the CA certificate(s) and/or the ServerCertificate (in x509 and/or PKCS7 formats).	

`<Function>`	Requestor job function	String/255
`<GSSupportOption>`	To add GS Support set to true. If not false.	Boolean
`<IncorporatingAgencyRegistrationNumber>`		String/100
`<InsuranceOption>`	To add Insurance Options set to true.If not false.	Boolean
`<IsValidDomainName>`	Returns true if the domain name is valid for a certificate orders	Boolean

XML Structure	Description	DataType/ Max length

`<JurisdictionInfo>`
`<Country>`
`(<StateOrProvince>)?`
`(<Locality>)?`
`<IncorporatingAgencyRegistrationNumber>`
`</JurisdictionInfo>`
	Jurisdiction of Incorporation Details	

`<KeyLength>`		`String/4`
`<LastName>`	From one of the Contact structures. The Last Name of the contact.	`String/100`

`<Licenses>`	This is the Number of Licenses.	`Int`
		`1-99 Only`

`<Locality>`	The Locality field from the CSR or Certificate	`String/255`
`< MetaTag>`	The MetaTag that Globalsign will check for when the verification request is made. Follows the format: <meta name="globalsign-domain-verification" content="randomstring" />	`String/255`
`<ModificationEvent>`	One event in the set of ModificationEvents	
`<ModificationEventName>`	The name of the event.	`String/50`

`<ModificationEvents>`
`(<ModificationEvent>`
`<ModificationEventName>`
`<ModificationEventTimestamp>`
`</ModificationEvent>)+`
`</ModificationEvents>`
	The set of events for the order that caused the status to be changed within the specified time period. This is contained in OrderDetail. Used only in GetModifiedOrders.	

`<ModificationEventTimestamp>`	The time of the event	`DateTime`
`<ModifyCloudOVOrderOperation>`	Specifies the operation to be performed on the order or certificate. APPROVE CANCEL REVOKE	`String/20`
`<Months>`	The number of months that a certificate will be valid for.	`Int/4`
`<NotAfter>`		`DateTime`
`<NotBefore>`		`DateTime`
`<OrderDate>`	The date the order was created.	`DateTime`

`<OrderDetail>`
`<OrderInfo>`
`(<OrderOption>)?`
`(<CertificateInfo>)?`
`(Fulfillment>?`
`(<ModificationEvents>)?`
`</OrderDetail>`
	OrderDetail is returned in many Order Query operations. The specific content is dependent on the values in the request. ModificationEvents is only returned in GetModifiedOrders.	

`<OrderKind>`	Type of order: new: a new request renewal: renewal of current certificate transfer: a commercial upgrade of a current valid certificate	`String/10`
`<OrderID>`	This is the OrderID assigned by GlobalSign to the order and provided to the person requesting the certificate.	`String/50`

XML Structure	Description	DataType/ Max length
<OrderInfo> <OrderID> <ProductCode> (<BaseOption>)? <OrderKind> <Licenses> (<ExpressOption>)? (<ValidityPeriodCustomizeOption>)? (<InsuranceOption>)? (<GSSupportOption>)? (<RenewalExtentionOption>)? <DomainName> <OrderDate> (<OrderCompleteDate>)? (<OrderCanceledDate>)? (<OrderDeactivatedDate>)? <OrderStatus> <Price> <Currency> <ValidityPeriod> <Months> (<NotBefore>)? (<NotAfter>)? </ValidityPeriod> (<SpecialInstructions>)? </OrderInfo>	This structure contains basic information that apply to most orders and is profiled within each order response structure.	
<OrderOption> <ApproverNotifiedDate>? <ApproverConfirmDate>? <ApproverEmailAddress>? <OrganizationInfo> <OrganizationName> (<CreditAgency>)? (<OrganizationCode>)? <OrganizationAddress> <AddressLine1> (<AddressLine2>)? (<AddressLine3>)? <City> <Region> <PostalCode> <Country> <Phone> (<Fax>)? </OrganizationAddress> </OrganizationInfo> (<ContactInfo> <FirstName> <LastName> <Phone> <Email> </ContactInfo>)? </OrderOption>	This structure is in many order request messages and contains basic order information common to all types of orders.	

XML Structure	Description	DataType/ Max length

<OrderParameter>
    <ProductCode>
    (<BaseOption>)?
    <OrderKind>
    <Licenses>
    (<ExpressOption>)?
    (<ValidityPeriodCustomizeOption>)?
    (<InsuranceOption>)?
    (<GSSupportOption>)?
    (<RenewalExtentionOption>)?
    <ValidityPeriod>
        <Months>
        (<NotBefore>)?
        (<NotAfter>)?
    </ValidityPeriod>
    <CSR>
    (<RenewalTargetOrderID)?
    (<TargetCERT>)?
    (<DNSNames>)?
    (<SpecialInstructions>)?
    (<Coupon>)?
    (<Campaign>)?
</OrderParameter>
	This structure is part of the order validation and order processes. It includes all details relating to the order and also the CSR for parsing.	

<OrderParameterWithoutCSR>
    <ProductCode>
    (<BaseOption>)?
    <OrderKind>
    <Licenses>
    (<ExpressOption>)?
    (<ValidityPeriodCustomizeOption>)?
    (<InsuranceOption>)?
    (<GSSupportOption>)?
    (<RenewalExtentionOption>)?
    <ValidityPeriod>
        <Months>
        (<NotBefore>)?
        (<NotAfter>)?
    </ValidityPeriod>
    <PIN>
    <KeyLength>
    (<RenewalTargetOrderID)?
    (<TargetCERT>)?
    (<DNSNames>)?
    (<SpecialInstructions>)?
    (<Coupon>)?
    (<Campaign>)?
</OrderParameterWithoutCSR>
	This structure is part of the order validation and order processes. It includes all details relating to the order without a CSR.	

<OrderQueryOption>
    (<OrderStatus>?)
    (<ReturnOrderOption>?)
    (<ReturnCertificateInfo>?)
    (<ReturnFulfillment>?)
    (<ReturnCACerts>?)
</OrderQueryOption>
	Specifies what is returned in the response message. All values default to false if not supplied so the corresponding data structure will not appear in the response.	

<OrderRequestHeader>
    <AuthToken>
        <UserName>
        <Password>
    </AuthToken>
</OrderRequestHeader>
	The OrderRequestHeader is used in all of the order operations.	

XML Structure	Description	DataType/ Max length
<OrderResponseHeader> <SuccessCode> (<Errors> (<Error> <ErrorCode> (<ErrorField>)? <ErrorMessage> </Error>)+ </Errors>)* <Timestamp> </OrderResponseHeader>	This is the header returned in all Order operations.	
<OrderStatus>	The current status of an Order. 1 - INITIAL 2 - Waiting for phishing check 3 - Cancelled - Not Issued 4 - Issue completed 5 - Cancelled - Issued 6 - Waiting for revocation 7 - Revoked	Int
<OrderSubInfo> <CSRSkipOrderFlag> <DNSOrderFlag> <TrustedOrderFlag> <P12DeleteStatus>? <P12DeleteDate>? <VerificationUrl>? <SubId> </OrderSubInfo>		
<Organization>	The Organization field from the certificate	String/255
<OrganizationCode>	Can be used to indicate company numbers lookup eg. For DUNS enter 1 in this field.	String/50
<OrganizationInfo> <OrganizationName> (<CreditAgency>)? (<OrganizationCode>)? <OrganizationAddress> <AddressLine1> (<AddressLine2>)? (<AddressLine3>)? <Locality> <StateOrProvince> <PostalCode> <Country> <Phone> <Fax>? </OrganizationAddress> </OrganizationInfo>	Organization Info sent with Certificate request.	
<OrganizationInfoEV> (<CreditAgency>)? (<OrganizationCode>)? (<BusinessAssumedName>)? <BusinessCategoryCode> <OrganizationAddress> (<AddressLine1>)? (<AddressLine2>)? (<AddressLine3>)? <City> <Region> <PostalCode> <Country> <Phone> (<Fax>)? </OrganizationAddress> </OrganizationInfoEV>	Organization Info sent with Certificate request.	
<OrganizationName>	The name of the Organization applying for a certificate.	String/255
<OrganizationUnit>	The OrganizationalUnit name from the CSR. .	String/255

XML Structure	Description	DataType/ Max length
<OVCSRInfo> <OrganizationName> (<OrganizationUnit>)? <Locality> <StateOrProvince> <Country> </OVCSRInfo>	Info to be used in the creation of the Certificate	
(<ParsedCSR> <DomainName> <Country> <Email> <Locality> <Organization> <OrganizationUnit> <State> <IsValidDomainName> </ParsedCSR>)?	Details from the CSR	
<Password>	Required for user authentication over the API	String/30
<Phone>	From one of the Contact or OrganizationAddress structures.	String/30
<P12DeleteDate>		DateTime
<P12DeleteStatus>		Int
<PKCS12File>	A bese64-encoded PKCS#12	String/4000
<PKCS7Cert>	A Base64-encoded PKCS#7	String/20000
<PostalCode>	From the Address structure. The Postal Code (e.g., Zip Code in the U.S.) for the Address	String/20
<ProductCode>	A code for the product that a particular request relates to. Note that a partner must have a valid contract for a product code for it to be valid in a request. Also, a product code must be valid for the context of the request.	String/20
<QueryRequestHeader> <AuthToken> <UserName> <Password> </AuthToken> </QueryRequestHeader>	The header on all Query Request operations.	
<QueryResponseHeader> <Errors>? <ReturnCount> <SuccessCode> <Timestamp> </OrderResponseHeader>		
<Region>	Region, state/prov From the Address structure. This is the region of the address such as state or province. If this is a U.S. state it must have a valid 2 character abbreviation	String/255
<RenewalExtentionOption>>	To add bonus to validity period set to true. If not false.	Boolean
<ReOrderParameter> <CSR> <DNSNames>? </ReOrderParameter>		
<ReOrderParameterWithoutCSR> <DNSNames>? <PIN> <KeyLength> </ReOrderParameterWithoutCSR>		
<RenewalTargetOrderID>	Original OrderID for renewal orders.	**String/50**
<RequestorInfo> <FirstName> <LastName> (<Function>)? <OrganizationName> (<OrganizationUnit>)? <Phone> <Email> </RequestorInfo>	Certificate Requestor Information	
<ResendEmailType>	Current values are: ApproverEmail – resend the approver email for any QuickSSL order.	String/20

XML Structure	Description	DataType/ Max length
<ReturnCACerts>	If set to true in the request message, the CACerts structure is populated in the Fulfillment structure of the response message.	Boolean
<ReturnCertificateInfo>	If set to true in the request message, the CertificateInfo structure appears in the response message.	Boolean
<ReturnCount>	The number of items returned in the message	Int
<ReturnFulfillment>	If set to true in the request message, the Fulfillment structure appears in the response message.	Boolean
<ReturnOrderOption>	In the response, product information will be in details if set to true.	Boolean
<SearchOrderDetail> <OrderID> <BaseOption>? <OrderKind> <RequestKind> <Licenses> <OrderRequestDate> <OrderIssueDate> <OrderCanceledDate>? <OrderStatus> <OrganizationName> <Months> <SubId> <FQDN> </SearchOrderDetail>		
<SerialNumber>	The serial number of a certificate specified as a hex string.	String/64
<ServerCertificate> <X509Cert> <PKCS7Cert> </ServerCertificate>		
<SpecialInstructions>	Special Instructions for the order	String/4000
<StartDate>	Start date of certificate.	DateTime
<State>	The value of the State in the ParseCSRResponse.	String/255
<StateOrProvince>		String/255
(<SubID>)?		String/50
<SubjectName>	The SubjectName in certificate.	String/255
<SuccessCode>	Code in the Order and Query Response Headers which indicates the success of failure of the request. A zero SuccessCode indicates a success with no warnings. A positive SuccessCode indicates a success with warnings. A negative SuccessCode indicates a failure. Note that if the Success in non-zero an accompanying Errors structure will be present.	Int
<TargetCERT>	The base64-encoded certificate you are transferring from	String/4000
<TargetOrderID>		String/50
<Timestamp>	A date timestamp used in a variety of contexts. Note that the XML format is: YYYY-MM-DDTHH:MM:SS.000Z (for example, 2001-01-01T24:00:00:000Z is for Jan 1, 2001 at midnight).	DateTime
<TrustedOrderFlag>		Boolean
<UserName>	Required for user authentication	String/30
<ValidityPeriod> <Months> (<NotBefore>)? (<NotAfter>)? </ValidityPeriod>	The number of months that a certificate or site seal will be valid for. Defaults to 12 if not present.	
<ValidityPeriodCustomizeOption>	To customize the validity period set to true. If not false.	Boolean
<VerificationUrl>	OneClickSSL - A mechanism whereby a web server publishes a CSR which is randomly named, allowing for an automated verification by an external RA system. The verification url includes the location of the randomly named CSR.	String/300
<X509Cert>	A bese64-encoded certificate.	String/4000