GlobalSign APIs for MSSL Certificates

Implementation Guide and Definitions

Version 2.9 10/10/2019

Contents

1. Document History

Version	Release Date	Author	Description
1.3	06/02/2014	Doug Beattie	• Updated country codes to use CW or SX instead of AN • Fixed spelling error in RenewalTargetOrderID • Replaced list of ModificationEventName responses with new values
2.0	08/26/2016	Doug Beattie	• Added IntranetSSL product • Added support for ordering ExtendedSSL certificates • Reorganized and clarified many sections to improve technical accuracy and readability
2.1	8/26/2016	Doug Beattie	• Added a new command to change SANs in existing MSSL certificates: ChangeSubjectAltName • New API commands to add MSSL Domains to MSSL profiles via Email, HTTP or DNS verification methods • Identified new test system URLs • Removed SHA-1 references as SHA-1 has been deprecated • Updated list of error codes and descriptions • Clarified the definition of Custom Validity Period. • Added new API field to request specific values for KeyUsage and Extended Key Usage
2.2	11/30/2016	Doug Beattie	• Specified new location for performing HTTP Domain Verification • Added ContactInfo requirement to AddDomainToProfile
2.3	11/1/2017	Doug Beattie	• Added support for up to 500 SANs per certificate using the OrderOption ASYNC_ORDER, which makes the order request an asynchronous process. • Removed deprecated locations for HTTP validation, per CA/Browser Forum requirements
2.4	04/23/2018	Julie Olson	• Modified references to AutoCSR to specify IntranetSSL products only. • Changed validity period maximums to 825 days where appropriate.
2.5	08/16/2018	Julie Olson	• Added CloudSSL product information • Updated AddDomainToProfile Request code • Changed API query response from 1000 to 500 • Removed DecodeCSR command • Updated SubID description in Section 11 • Notated that AddMSSLDomain is being depreciated • Added new ModifyMSSLDomain API • Added new GetDomains API • Removed OCSP Must Staple reference

2.6	03/14/2019	Julie Olson	• Changed DomainID field from required to optional. • Added RenewalDomain API
2.7	04/23/2019	Julie Olson	• Updated IntranetSSL Order process
2.8	06/24/2019	Julie Olson	• Added missing FQDN field to GetDomainApproverList • Marked ProfileID in GetDomainApproverList as optional • Made assorted editorial updates
2.9	10/10/2019	Julie Olson	• Changed CloudSSL domain validity period • Removed EV self-service domain validation from AddDomaintoProfile API • Edited AddMSSLDomain API to include EV domain validation

2. Introduction

2.1 Overview

GlobalSign offers a Simple Object Access Protocol (SOAP) API for its partners and customers to order and manage certificates. Through this API, partners can perform functions such as ordering the different products, cancelling and fulfilling orders, and querying for order data. The API supports requests for SSL Certificates placed through the Managed SSL (MSSL) platform against previously validated organizational information and domains.

The API is organized as two Web Services – ORDER and QUERY. The operations in the ORDER Web Service are focused around initiating and cancelling orders, while the QUERY Web Service is focused on checking the status of orders and getting fulfilment information for orders (e.g. issued certificates, reports, and obtaining order details).

Typically, an API user will retrieve issued certificates using the QUERY function and then use its own methods to install or communicate the certificate to the end customer. However, the API also allows for certificates to be emailed directly to the order contacts.

If you have any questions about any of the information provided in this document, please contact your Account Manager.

2.2 Managed SSL Product Types

All Managed SSL Product Types require that the Organization information and at least one Domain be registered in the Managed SSL account prior to ordering. When ordering certificates, the Domain Names for the CommonName and all Subject Alternative Names (SANs) must be registered and approved for the account prior to placing the order. This information is generally referred to as PreVetted (PV), and is referenced in the list of supported Product Codes (refer to Section 8.9).

2.2.1 OrganizationSSL

When placing an OrganizationSSL order through an MSSL profile, the applicant has a number of options available to them:

- **Base Certificate Type**: OrganizationSSL supports Standard, Wildcard and GlobalIP (Publicly routable IP addresses) as values in the certificate CommonName.
- **SAN Options**: Depending on the options configured for your account, you can order certificates with a variety of SAN options including FQDN, SubDomain, GlobalIP, Unified Communications and Wildcard.
- **Unified Communications Support**: You may specify the entry of the following host names for no additional fee: www, owa, autodiscover and mail.
- Provide a CSR, or have GlobalSign generate the keys: The API allows you to enter a CSR or request that GlobalSign creates the keys and corresponding CSR for you (AutoCSR). This feature only applies to IntranetSSL (private hierarchy) products. Certificates requested using AutoCSR are returned in a packaged, encrypted PKCS#12 file containing both the certificate file and private key. Certificates requested by supplying a customer-generated CSR are returned as standard certificates.

2.2.2 ExtendedSSL

ExtendedSSL is the product name for GlobalSign's Extended Validation (EV) SSL offering. It is issued in strict adherence to the published CA/B Forum EV SSL guidelines covering certificate profile format, vetting method and workflow. This product is limited to a 2-year validity period (up to a maximum of 27 months with added renewal/bonus months). It does not support wildcard or IP address options. Refer to Section 2.2.5 for more information.

2.2.3 IntranetSSL

IntranetSSL certificates are issued under a set of Non-Public Roots, which are not distributed within major browser or operating system Root Key Stores. The use of Non-Public roots allows the issuance of certificates that do not need to comply with CA/B Forum guidelines or Root Key Store requirements, specifically to issue certificates with internal server names.

IntranetSSL supports many of the options in OrganizationSSL, plus the use of Internal Server names or reserved IP addresses in the CN or SAN, as well as a certificate validity period up to 5 years. Refer to Section 2.2.5 for more information.

2.2.4 CloudSSL

CloudSSL is an SSL distribution service designed specifically for providers of cloud-based services, such as CDNs, VDNs, eCommerce platforms, website builders, and other XaaS, that need to secure services or communications for many customers.

CloudSSL certificates are issued to the service provider at the Organization Validated (OV) level. Customer domains can then be added as Domain Validated (DV) SANs after domain control is verified. This set up means providers can secure multiple domains with one certificate, which may reduce the need for additional IP addresses.

2.2.5 Summary of MSSL Product Features

This table lists the key features for the suite of MSSL products:

Function	ExtendedSSL	OrganizationSSL	IntranetSSL	CloudSSL
Base Options • Wildcard • Global IP • Private	 N N N	 Y Y N	 Y Y Y	 N N N
Coupons or Promotional code	Y	Y	Y	N
Validity Period in request	825 days	825 days	Up to 5 years	825 days
Maximum cert validity period (months)	27	27	60	27
Order Options (OptionName) • SAN Option • Renewal Extension Option • Validity Period Customize Option (please refer to Section 8.2 for more information)	 Y Y Y	 Y Y Y	 Y N N	 Y N N
Order Kind • New • Renewal • Transfer	 Y Y Y	 Y Y Y	 Y Y N	 Y Y N
SAN Options: • Unified Communications • FQDN • SubDomain • GlobalIP Address • Wildcard • Internal SAN or Reserved IP address	 Y Y Y N N N	 Y Y Y Y Y N	 N Y Y Y Y Y	 Y Y Y N Y N
Extensions (custom values) • Extended Key Usage • Key Usage • TLS Feature Extension	 Y Y Future	 Y Y Future	 Y Y Future	 Y Y Future
AutoCSR with RSA 2048 bit keys (for IntranetSSL only)	N	N	Y	N
Domain Validity	13 months	825 days	825 days	366 days

CSR Key Types Supported • RSA 2048-4096 • ECC P-256 • ECC P-384	 Y Y Y	 Y Y Y	 Y Y Y	 Y Y Y
Signature Algorithms • sha1RSA • sha256RSA • sha256ECDSA • sha384ECDSA	 N Y N N	 N Y N N	 Y Y Y N	 N Y Y N
Post issuance actions • Reissue • Add/Delete SAN • Cancel • Revoke • Renewal	 Y Y Y Y Y	 Y Y Y Y Y	 Y Y Y Y Y	 Y Y Y Y Y

2.3 Web Service Functions – Order & Query Workflow Overview

Order processing for SSL Certificates and web identity products is asynchronous. For these types of orders, an API client places an order, and then checks the server for the completed order. The process is organized into two sections:

- **Managed SSL (MSSL) Functions**: Calls to place orders; modify or cancel orders; or modify or query MSSL specific account information.
- **Standard SSL Query Functions**: Calls needed to complete order calls (such as querying), and search for complete orders (such as "getting" issued certificates).

The general approach for ordering a certificate is to place orders using an **Order** function, and then use the **Query** function **GetModifiedOrders** to periodically request a list of orders that have changed status during a specified time interval (for example, the last four hours). This returns a list of all orders and detailed information for orders that have changed status in the specified time interval. The status of all returned orders can then be updated locally and used as necessary.

An alternative to querying for a set of modified orders is to request the status of a specific order. In this case, the user places an order using the **Order** function, and then uses the **Query** function **GetOrderByOrderID to** periodically check the status of a specific order. Once the order is complete, the fulfillment information is returned with the **GetOrderByOrderID** operation. This approach is less efficient, but might be more appropriate when there is a low volume of certificates being managed.

2.3.1 Managed SSL Functions

Function	API Request
Order Management	
Order an MSSL OV, MSSL EV or IntranetSSL certificate	PVOrder
Modify Existing MSSL Order	ModifyMSSLOrder
Change the SANs in an MSSL Order	ChangeSubjectAltName
Domain Management	
Get List of MSSL Domains	GetMSSLDomains (Deprecated)
Get List of MSSL Domains	GetDomains
Add domain to profile (Email, HTTP, DNS)	AddDomainToProfile (For OV/CloudSSL only)
Verify a domain (HTTP, DNS)	VerifyMsslDomain
Add domain to MSSL account (manually vetting)	AddMSSLDomain (For EV only)
Modify Existing MSSL Domain	ModifyMSSLDomain

Profile Management (Advanced)	
Get List of MSSL Profiles	GetMSSLProfiles
Add profile to MSSL account	AddMSSLProfile
Update existing MSSL Profile	UpdateMSSLProfile

2.3.2 Query Functions

The following functions are used to obtain information about existing orders or to perform utility functions.

Function	API Request
Searching order information by Order ID	GetOrderByOrderID
Searching orders by order date (from/to)	GetOrderByDateRange
Searching modified orders by modified date (from/to)	GetModifiedOrders
Get orders by expiration date	GetOrderByExpirationDate
Getting order list	GetCertificateOrders
Reissue a certificate	Reissue
Decode a CSR	DecodeCSR
Toggle Renewal Notices	ToggleRenewalNotice

2.4 Recommended Domain Validation and Ordering Scenarios

This section provides the recommended domain validation and ordering scenarios for using this API.

2.4.1 Domain Validation

Use **AddDomainsToProfile** to request and then validate domains. Using either the HTTP or DNS method permits fully automated domain validation for OV domains. Once you have placed the random value in the applicable location, use the **VerifyMSSLDomain** command to instruct GlobalSign to validate the domain. You will need to obtain the **ProfileID** prior to requesting a domain. See Section 9.3 for details.

2.4.2 Ordering

The process for placing orders through the API is as follows:

- Place an order using the **PVOrder** command.
- Receive the **OrderID**.
- Wait about a minute, and then use the **GetOrderByOrderID** command to get the order status. If the order is complete, this command will return the certificate.

When placing orders, use the **Async_order** command to improve performance and reduce the possibility of timeouts.

2.5 API and WSDL URLs

API URLs

	Feature	URL
PROD	MSSL Functions	https://system.globalsign.com/kb/ws/v1/ManagedSSLService
	Query	https://system.globalsign.com/kb/ws/v1/GASService
TEST	SSL Functions	https://test-gcc.globalsign.com/kb/ws/v1/ManagedSSLService
	Service / Query	https://test-gcc.globalsign.com/kb/ws/v1/GASService

WSDL URLs

	Feature	URL
PROD	MSSL Functions WSDL	https://system.globalsign.com/kb/ws/v1/ManagedSSLService?wsdl
	Query WSDL	https://system.globalsign.com/kb/ws/v1/GASService?wsdl
TEST	MSSL Functions WSDL	https://test-gcc.globalsign.com/kb/ws/v1/ManagedSSLService?wsdl
	Query WSDL	https://test-gcc.globalsign.com/kb/ws/v1/GASService?wsdl

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

3. Order Management

3.1 Ordering Certificates

This section defines the certificate order process.

3.1.1 PVOrder Request

This section lists the primary fields that are sent to the API server when a user places an order.The important fields in this message are:

- **Product Codes**: This field is used to order ExtendedSSL, OrganizationSSL, IntranetSSL and CloudSSL certificates.
  Note: IntranetSSL products that contain "SKIP" can be used in the next API message, **PVOrderWithoutCSR**. Refer to Section 3.2 for more information.
- **Base Option**: This field specifies Wildcard, GlobalIP or Private certificate types, if needed.
- **KindOrder**: This field specifies the type of order being made, New, Renewal or Transfer.
- **Options**: This field specifies order options for adding additional SANs, reciving 30 bonus days with renewal orders, setting custom certificate expiration dates, or setting the issuance process to be asynchronous. Refer to Section 8.7 for details.
- **Validity Period**: Validity period of certificate in months.

```
<PVOrder>
	<Request>
		<OrderRequestHeader>
		<OrderRequestParameter>
			<ProductCode>
			<BaseOption>
			<OrderKind>
			<Licenses>
			<Options>
			<ValidityPeriod>
			<CSR>
			<RenewalTargetOrderID>
			<TargetCERT>
			<SpecialInstructions>
			<Coupon>
			<Campaign>
		<MSSLProfileID>
		<MSSLDomainID>
		<SubID>
		<PVSealInfo>
		<ContactInfO>
		<SANEntries>
		<Extensions>
		<CertificateTemplate>
	</Request>
```

3.1.2 PVOrder Response

This section shows the API code that is sent back to the Client after the initial order is received.

```
<PVOrderResponse>
	<Response>
		<PVOrderResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<OrderID>
		<PVOrderDetail>
	</Response>
```

3.2 Ordering IntranetSSL Certificates

3.2.1 PVOrder Request

When ordering an IntranetSSL certificate through a private Dedicated Intermediate, it is similar to using the regular PVOrder API, except for the bolded fields below, which require specific inputs; `BaseOption` is set to "private" and `MSSLDomainID` is set to "INTRANETSSLDOMAIN."

```
<PVOrder>
	<Request>
		<OrderRequestHeader>
		<OrderRequestParameter>
			<ProductCode>
			<BaseOption>                    set to 'private'
			<OrderKind>                     set to 'new'
			<Licenses>
			<Options>
			<ValidityPeriod>
			<CSR>
			<RenewalTargetOrderID>
			<TargetCERT>
			<SpecialInstructions>
			<Coupon>
			<Campaign>
		<MSSLProfileID>
		<MSSLDomainID>                      set to 'INTRANETSSLDOMAIN'
		<SubID>
		<PVSealInfo>
		<ContactInfO>
		<SANEntries>
		<Extensions>
		<CertificateTemplate>
	</Request>
```

When ordering an IntranetSSL certificate through a public domain, `BaseOption` is set to its normal value and `MSSLDomainID` is set to the vetted domain ID.

3.2.2 PVOrder Response

This section shows the API code that is sent back to the Client after the initial order is received.

```
<PVOrderResponse>
	<Response>
		<PVOrderResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<OrderID>
		<PVOrderDetail>
	</Response>
```

3.2.3 Ordering IntranetSSL Certificate Using AutoCSR

IntranetSSL products that contain "SKIP" (refer to Section 8.9) can use this command to instruct GlobalSign to generate the certificate keys and return them via a PKCS#12 file in the API. This follows the same basic order processing as the PVOrder described above.

This section shows the API code that is sent to the API server when a user places an order. This order is essentially the same as PVOrder (refer to Section 3.1) except for the bolded fields listed below. This API is used only for ordering IntranetSSL certificates.

```
<PVOrderWithoutCSR>
	<Request>
		<OrderRequestHeader>
		<OrderRequestParameterWithoutCSR>
			<ProductCode>
			<BaseOption>
			<OrderKind>
```

```
                <Licenses>
                <Options>
                <ValidityPeriod>
                <CSR>
                <RenewalTargetOrderID>
                <TargetCert>
                <SpecialInstructions>
                <Coupon>
                <Pin>
                <KeyLength>                    See Section 8.4
        <SubID>
        <MSSLProfileID>
        <MSSLDomainID>                         The DomainID for the CommonName
        <PVSealInfo>
        <OVCSRInfo>
                <CommonName>
                <OrganizationUnit>
        <ContactInfo>
        <SANEntries>
        <Extensions>                           See Section 8.6
    </Request>
```

3.2.4 PVOrderWithoutCSR Response

This section shows the API code that is sent back to the Client after the initial order is received.

```
<PVOrderWithoutCSRResponse>
    <Response>
        <OrderResponseHeader>
            <SuccessCode>
            <Errors>
            <Timestamp>
        <OrderID>
        <PVOrderDetail>
    </Response>
```

3.3 Modifying Orders for MSSL Certificates

This section defines the process for modifying orders for MSSL certificates.

3.3.1 ModifyMSSLOrder Request

The **ModifyMSSLOrder** command is used to approve a pending order, cancel an order, or revoke a certificate. Refer to Section 8.5 for more information. This section lists the API code that is sent to the API server when a user executes the **ModifyMSSLOrder** command.

```
<ModifyMsslOrder>
    <Request>
        <OrderRequestHeader>
        <OrderID>
        <ModifyingOrderOperation>
    </Request>
```

3.3.2 ModifyMSSLOrder Response

This section lists the API code that is sent back to the Client after the **ModifyMSSLOrder** Request is sent.

```
<ModifyMSSLOrderResponse>
     <Response>
        <OrderResponseHeader>
            <SuccessCode>
            <Errors>
            <Timestamp>
     </Response>
```

3.4 Changing SANs

This section describes how to replace the current set of SANs in a certificate with a new set of SANs. To use this API, specify the **OrderID** you want to change and then specify a new set of SANs that will replace the current set of SANs. The Public Key and expiration date of the certificate remain the same, but the SANs are updated.

3.4.1 ChangeSubjectAltName Request

```
<ChangeSubjectAltName>
        <Request>
                <OrderRequestHeader>
                <OrderID>
                <TargetOrderID>             The OrderID which will have the SANs changed
                <ApproverEmail>             Not currently used
                <SANEntries>                If not supplied, then there will be no SANs other
                                            than the value from the CommonName
                <PIN>                       Not currently used
        </Request>
```

3.4.2 ChangeSubjectAltName Response

```
<ChangeSubjectAltNameResponse>
        <Response>
                <OrderResponseHeader>
                        <SuccessCode>
                        <Errors>
                        <Timestamp>
        </Response>
```

4. Domain Management

4.1 Get List of Approved Domains

4.1.1 GetDomainApproverList Request

This section lists the primary fields that are sent to the API server when a user executes the **GetDomainApproverList** query. Note: The **GetDomainApproverList** command must be used *before* the **AddDomainToProfile** command, when using email validation, and must supply the **DomainID** returned from **GetDomainApproverList**.

```
<GetDomainApproverList>
        <Request>
                <QueryRequestHeader>
                <FQDN>
                <ProfileID>                    Optional field
        </Request>
```

4.1.2 GetDomainApproverList Response

This section lists the primary fields that are sent back to the Client after the **GetDomainApproverList** Request is used.

```
<GetDomainApproverListResponse>
        <Response>
                <QueryResponseHeader>
                        <SuccessCode>
                        <Errors>
                        <Timestamp>
                <Approvers>
                <ApproverType>
                <ApproverEmail>
                <MSSLDOmainID>
        </Response>
```

4.2 Add Domains to Profiles

The **AddDomainToProfile** command allows customers to add domains to the specified profile within their GCC account, and then perform domain control to have it approved by GlobalSign. Each domain is reviewed by GlobalSign's Vetting Department prior to being activated. This command allows customers to fully automate domain validation.

Note: This API is only for OV and CloudSSL domains. To validate EV certificates, please use the **AddMSSLDomain** API described in section 4.5.

4.2.1 Vetting Level

When submitting domains to be added to an MSSL profile, the following vetting levels are supported:

Value	Description	Domain Validity Period
OV	Organizational Validation	825 days
CLOUDSSL	CloudSSL Validation	365 days

4.2.2 Vetting Type

The following values for **VettingType** are supported when used in the **AddDomainToProfile** and **VerifyMsslDomain** API messages.

Value	Description	AddDomainToProfile	VerifyMsslDomain
EMAIL	Email is used to approve the domain	X	NA
HTTP	The HTTP method is used to approve the domain. This is also known as URL or meta-tag.	X	X
DNS	The DNS method is used to approve the domain	X	X

4.2.3 AddDomainToProfile Request

This section lists the API code that is sent to the API server when a user executes the **AddDomainToProfile** request.

```
<AddDomainToProfile>
        <Request>
           <OrderRequestHeader>
           <MSSLProfileID>
           <DomainName>
           <VettingLevel>                    See Section 4.2.1
           <VettingType>                     See Section 4.2.2
           <DomainID>                        Only when VettingType=Email
           <ApproverEmail>                   Required when VettingType=Email
           <ContactInfo>
              <FirstName>
              <FirstNameNative>
              <LastName>
              <LastNameNative>
              <Phone>
              <Email>
        </Request>
```

4.2.4 AddDomainToProfile Response

This section displays the response sent to the Client after the **AddDomainToProfile** request is used.

```
<AddDomainToProfile>
       <Response>
              <OrderResponseHeader>
                     <SuccessCode>
                     <Errors>
                     <Timestamp>
              <MSSLDomainID>
              <MetaTag>
              <DnsTXT>
       </Response>
```

4.3 Cancel an MSSL Domain

4.3.1 ModifyMSSLDomain Request

The ModifyMSSLDomain Request is used to cancel an EV, OV or CloudSSL domain order.

```
<ModifyMsslDomain>
	<Request>
		<OrderRequestHeader>
		<MSSLDomainID>
		<ModifyDomainOperation>
	</Request>
```

4.3.2 ModifyMSSLDomain Response

```
<ModifyMsslDomainResponse>
	<Response>
		<OrderResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
	</Response>
```

4.4 Approve Domains to Demonstrate Domain Control

The **VerifyMsslDomain** command allows customers to approve domains that have been added to their profile using the DNS or HTTP validation methods, to demonstrate domain control. This function can approve MSSL OV and CloudSSL domain orders.

4.4.1 VerifyMsslDomain Request

```
<VerifyMsslDomain>
	<Request>
		<OrderRequestHeader>
		<DomainID>
		<TagLocation>                See Section 8.11
		<VettingType>                See Section 4.2.2
	</Request>
```

4.4.2 VerifyMsslDomain Response

```
<VerifyMsslDomainResponse>
	<Response>
		<OrderResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<DomainID>                   The DomainID for the added domain
	</Response>
```

4.5 AddMSSLDomain

The **AddMSSLDomain** command allows customers to add EV domains to the specified profile in their GCC account. Each domain is reviewed by GlobalSign's Vetting Department prior to being activated. In the case of EV profiles, additional industry-mandated vetting procedures must be followed (Email, HTTP, or DNS) which may add additional time prior to activation.

Note: Please use the **AddDomainToProfile** command described in Section 4.2 to validate OV domains.

4.5.1 AddMSSLDomain Request

```
<AddMSSLDomain>
        <Request>
                <OrderRequestHeader>
                        <AuthToken>
                                <UserName>
                                <Password>
                        </AuthToken>
                </OrderRequestHeader>
                <MSSLProfileID>
                <DomainName>
                <VettingLevel>                Enter "EV"
        </Request>
```

4.5.2 AddMSSLDomain Response

```
<AddMSSLDomainResponse>
        <Response>
                <OrderResponseHeader>
                        <SuccessCode>
                        <Errors>
                        <Timestamp>
                </OrderResponseHeader>
                <MSSLDomainID>
        </Response>
```

4.6 GetMSSLDomain - Deprecated

The **GetMSSLDomains** command has been deprecated. Please use is the **GetDomains** command described in Section 4.7.

4.7 Get List of Domains

The **GetDomains** command is used to obtain a list of domains based on customer-specified criteria, such as domain name, domain status, vetting type, and expiration date.

4.7.1 GetDomains Request

```
<GetDomains>
        <Request>
                <QueryRequestHeader>
                        <ProfileID>
                        <DomainName>          Returns only domains with the specified Domain
                                              Name
                        <DomainStatus>        Returns only domains with the specified domain
                                              status
                        <VettingLevel>        Returns only domains with the specified vetting
                                              level
                        <LastUpdateDateRange> Returns orders that have been updated within the
                                              specified date range.
                        <ExpirationDateRange> Date range for when the domains expire. This will
                                              not return domains that do not have an expiration
                                              date.
        </Request>
```

4.7.2 GetDomains Response

```
<GetDomainsResponse>
	<Response>
		<QueryResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<DomainDetails>
			<MSSLProfileID>
			<DomainID>
			<OrderDate>
			<DomainName>
			<DomainStatus>
			<VettingLevel>
			<VettingType>
			<DomainValidationCode>
			<ValidationDate>
			<ExpirationDate>
			<ContactInfo>
	</Response>
```

4.8 Renew Domains

The **RenewalDomain** command allows customers to renew domains before expiration. When a domain is submitted for renewal, certificates may still be issued from the domain, unless the domain has expired. Similar to the **AddDomainToProfile** API, the vetting level and type are selected during the renewal process.

4.8.1 RenewalDomain Request

```
<RenewalDomain>
	<Request>
		<OrderRequestHeader>
		<MSSLProfileID>                  If this is unknown, use the GetMSSLDomain
                                         command to retrieve the MSSLProfileID
		<VettingLevel>                   Options are EV or OV
		<VettingType>                    Options are EMAIL, HTTP or DNS.
		<ApproverEmail>                  If EMAIL is elected for VettingType, enter
                                         approval email into this field.
		<DomainID>                       The domain that needs to be renewed.
		<ContactInfo>
	</Request>
```

4.8.2 RenewalDomain Response

```
<RenewalDomainResponse>
	<Response>
		<OrderResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<MSSLDomainID>
		<MetaTag>
		<DnsTXT>
	</Response>
```

5. Profile Management

5.1 Retrieve List of MSSL Profiles

The **GetMSSLProfiles** command returns a list of MSSL profiles.

Note: A few bugs have been identified in this API:

- **CreditAgency** tag does not return a value in this API, or display in GCC
- **IncorporationAgencyRegistrationNumber** does not return a value in this API

5.1.1 GetMSSLProfiles Request

```
<GetMsslProfiles>
	<Request>
		<QueryRequestHeader>
		<MSSLProfileID>
		<VettingLevel>
		<MSSLProfileStatus>
	</Request>
```

5.1.2 GetMSSLProfiles Response

```
<GetMsslProfilesResponse>
	<Response>
		<QueryResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<SearchMSSLProfileDetails>
	</Response>
```

5.2 Add a New MSSL Profile

The **AddMSSLProfile** command is used to add a new MSSL profile. The profile is reviewed and activated by the GlobalSign Vetting Department once received.

5.2.1 AddMSSLProfile Request

```
<AddMSSLProfile>
	<Request>
		<OrderRequestHeader>
		<VettingLevel>
		<MSSLOVProfileInfo>          Either the OV or EV profile info must be present
	</Request>
```

5.2.2 AddMSSLProfile Response

```
<AddMSSLProfileResponse>
	<Response>
		<OrderResponseHeader>
			<SucessCode>
			<Errors>
			<Timestamp>
		<MsslProfileID>
	</Response>
```

5.3 Update MSSL EV Profiles

The **UpdateMSSLProfile** command is used to update MSSL EV profiles. Updating OV profiles is not currently supported via the API.

Note: Orders cannot be placed against the profile between the time that this request is made and the time when the profile has been approved. Please allow a few working days for the GlobalSign Vetting Department to review the updated information and to collect applicable approvals.

5.3.1 UpdateMSSLProfile Request

```
<UpdateMSSLProfile>
        <Request>
                <OrderRequestHeader>
                <MsslProfileID>
                <MSSLEVProfileInfo>
        </Request>
```

5.3.2 UpdateMSSLProfile Response

```
<UpdateMSSLProfileResponse>
        <Response>
                <OrderResponseHeader>
                        <SuccessCode>
                        <Errors>
                        <Timestamp>
                <MsslProfileID>
        </Response>
```

6. Query APIs

Note: All API query responses are currently limited to 500 items per response. We may further limit this in future updates to improve overall system performance.

6.1 Get Issued Certificate – Single Certificate

The **GetOrderByOrderID** command is used to obtain order information based on **OrderID**, and is the typical method to retrieve the order details for orders.

6.1.1 GetOrderByOrderID Request

```
<GetOrderByOrderID>
	<Request>
		<QueryRequestHeader>
		<OrderID>
		<OrderQueryOption>
	</Request>
```

6.1.2 GetOrderByOrderID Response

```
<GetOrderByOrderIDResponse>
	<Response>
		<OrderResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<OrderID>
		<OrderDetail>
	</Response>
```

6.2 Get Issued Certificate by Date Range

The **GetOrderByDateRange** command is used to obtain a list of orders issued during a specified date range.

6.2.1 GetOrderByDateRange Request

```
<GetOrderByDateRange>
	<Request>
		<QueryRequestHeader>
		<FromDate>
		<ToDate>
		<OrderQueryOption>
	</Request>
```

6.2.2 GetOrderByDateRange Response

```
<GetOrderByDateRangeResponse>
	<Response>
		<QueryResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<FromDate>
		<ToDate>
		<OrderDetails>
	</Response>
```

6.3 Get Recently Modified Orders

The **GetModifiedOrders** command is used to obtain order information based on changes made to an order during a specified time frame (e.g. four hours).

6.3.1 GetModifiedOrders Request

```
<GetModifiedOrders>
	<Request>
		<QueryRequestHeader>
		<FromDate>
		<ToDate>
		<OrderQueryOption>
	</Request>
```

6.3.2 GetModifiedOrders Response

```
<GetModifiedOrdersResponse>
	<Response>
		<QueryResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<FromDate>
		<ToDate>
		<OrderDetails>
	</Response>
```

6.4 Get Upcoming Renewals

The **GetOrderByExpirationDate** command is used to obtain a list of **OrderID**s with certificates expiring in a specified date range.

6.4.1 GetOrderByExpirationDate Request

```
<GetOrderByExpirationDate>
	<Request>
		<QueryRequestHeader>
		<ExpirationFromDate>
		<ExpirationToDate>
		<FQDN>
		<OrderKind>
		<OrderStatus>
		<SubID>
	</Request>
```

6.5 GetOrderByExpirationDate Response

```
<GetOrderByExpirationDateResponse>
	<Response>
		<QueryResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<SearchOrderDetails>
	</Response>
```

6.6 Get Certificate Orders

The **GetCertificateOrders** command is used to retrieve a list of orders based on your parameter selections (date, FQDN, OrderKind, OrderStatus). If no parameters are selected all orders in the profile will be returned.

6.6.1 GetCertificateOrders Request

```
<GetCertificateOrders>
	<Request>
		<QueryRequestHeader>
		<FromDate>
		<ToDate>
		<FQDN>
		<ProductCode>
		<OrderStatus>
		<SubID>
	</Request>
```

6.7 GetCertificateOrders Response

```
<GetCertificateOrdersResponse>
	<Response>
		<QueryResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<SearchOrderDetails>
	</Response>
```

6.8 ReIssue Certificates

The **ReIssue** command is used to reissue a certificate. A reissued certificate replaces the first certificate with an identical one, except for a new key pair. This action is useful for enterprises with multiple servers that all require the same type of certificate.

6.8.1 ReIssue Request

```
<ReIssue>
	<Request>
		<OrderRequestHeader>
		<OrderParameter>
		<TargetOrderID>
		<HashAlgorithm>
		<Extensions>
	</Request>
```

6.9 ReIssue Response

```
<ReIssueResponse>
	<Response>
		<OrderResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<OrderID>
		<TargetOrderID>
	</Response>
```

6.10 Turn Renewal Notice On/Off

The **ToggleRenewalNotice** command turns on/off renewal email notices.

6.10.1 Toggle Renewal Notice Request

```
<ToggleRenewalNotice>
	<Request>
		<OrderRequestHeader>
		<OrderID>
		<RenewalNotice>
	</Request>
```

6.11 Toggle RenewalNotice Response

```
<ToggleRenewalNoticeResponse>
	<Response>
		<OrderResponseHeader>
			<SuccessCode>
			<Errors>
			<Timestamp>
		<OrderID>
	</Response>
```

7. Account API Functions

7.1 QueryInvoices

The **QueryInvoices** command retrieves a list of invoices and calls out those that are outstanding.

7.1.1 QueryInvoices Request

```
<QueryInvoices>
       <Request>
              <OrderRequestHeader>
                     <AuthToken>
                            <UserName>                    30     String
                            <Password>                    30     String
                     </AuthToken>
              </OrderRequestHeader>                       30     String
              (<InvoiceNumber>)?                          30     String
              (<OrderID>)?                                30     String
              <PaymentDueDateFrom>                        YYYY-MM-DDTHH:MM:SS.000Z
              <PaymentDueDateTo>                          YYYY-MM-DDTHH:MM:SS.000Z
       </Request>
</QueryInvoices>
```

7.1.2 QueryInvoices Response

```
<QueryInvoices>
       <Response>
              <OrderResponseHeader>
                     <SuccessCode>                        2
                     (<Errors>
                            (<Error>
                                   <ErrorCode>           5
                                   (<ErrorField>)?       1000   String
                                   <ErrorMessage>        1000   String
                            </Error>)+
                     </Errors>)?
                     <Timestamp>                          YYYY-MM-DDTHH:MM:SS.000Z
              </OrderResponseHeader>
              <OrganizationAddress>
                     <AddressLine1>                       100    String
                     (<AddressLine2>)?                    100    String
                     (<AddressLine3>)?                    100    String
                     <City>                               200    String
                     <Region>                             255    String
                     <PostalCode>                         20     String
                     <Country>                            30     String
                     <Phone>                              30     String
                     (<Fax>)?                             30     String
              </OrganizationAddress>
              <Invoices>
                     <InvoiceInformation>
                            <InvoiceNumber>                      30     String
                            (<PurchaseOrderNumber>)?             30     String
                            <CustomerAccountNo>                  30     String
                            <SupplyDate>                         YYYY-MM-DDTHH:MM:SS.000Z
                            <InvoiceDate>                        YYYY-MM-DDTHH:MM:SS.000Z
                            <PaymentDueDate>                     YYYY-MM-DDTHH:MM:SS.000Z
                            (<InvoiceLineItem>
                                   <ProductName>                 255    String
                                   <CommonName>                  255    String
                                   <OrderID>                     30     String
                                   <Qty>                         10     String
                                   <UnitPrice>                   30     String
                                   <TaxAmt>                      30     String
                                   <TotalLineAmt>                30     String
                            </InvoiceLineItem>)+
```

```
                        <Net>                                   30      String
                        <Tax>                                   30      String
                        <InvoiceTotal>                          30      String
                    </InvoiceInformation>+
            <Invoices>
    </Response>
```

7.2 GetAccountSnapshot

The **GetAccountSnapshot** command allows customers to retrieve the balance and usage from their GCC account.

7.2.1 GetAccountSnapshot Request

```
<GetAccountSnapshot>
    <Request>
        <OrderRequestHeader>
            <AuthToken>
                <UserName>                  30      String
                <Password>                  30      String
            </AuthToken>
        </OrderRequestHeader>
    </Request>
```

7.2.2 GetAccountShapshot Response

```
<GetAccountSnapshot>
    <Response>
        <OrderResponseHeader>
            <SuccessCode>                   2
            (<Errors>
                (<Error>
                    <ErrorCode>             5
                    (<ErrorField>)?         1000    String
                    <ErrorMessage>          1000    String
                </Error>)+
            </Errors>)?
            <Timestamp>                     YYYY-MM-DDTHH:MM:SS.000Z
        </OrderResponseHeader>
        <AccountSnapShot>
            (<BulkDepositBalance>)?         255     String
            (<LastMonthUsage>)?             255     String
            (<BulkDepositValidity>)?        255     String
            (<AgreementValidityPeriod>)?    YYYY-MM-DDTHH:MM:SS.000Z
            (<DiscountRank>)?               255     String
            (<DiscountRankValidityPeriod>)? YYYY-MM-DDTHH:MM:SS.000Z
        </AccountSnapShot>
    </Response>
```

8. Certificate Order Entry Parameters

8.1 BaseOptions

The **BaseOptions** command is used to add a certain attribute to certificate orders. Specific types of certificates accept certain **BaseOptions**. Use the below table for the list of **BaseOptions** available by certificate type.

BaseOption	Supported Products	Notes
wildcard	OrganizationSSL IntranetSSL	Common Name must contain the * character in place of the subdomain
globalip	OrganizationSSL IntranetSSL	Common Name must contain a publicly accessible IP address
private	IntranetSSL	Common name must be an internal server name or a Reserved IP address

8.2 Custom Expiration Date

Users can control when a certificate expires by setting the Not After (N/A) date. The N/A date cannot be any further in the future than the current date plus the requested validity period, plus any added validity because of renewal, trade-in, etc. If the N/A date is set incorrectly the order will be rejected.

In order to set the certificate's expiration date, you must set the Order Option **VPC** (**ValidityPeriodCustomizeOption**) to "True," and then supply the N/A date in the **ValidityPeriod** field.

Not all validity periods are configured for every account due to MSSL agreements and pricing options. The actual validity period of a certificate depends on the selection of various options in the API, in addition to this **ValidityPeriod** field.

Number Of Months	Supported Products	Certificate Validity Period (days)
3	CloudSSL	90
6	ExtendedSSL OrganizationSSL IntranetSSL CloudSSL	184
12 (default)	ExtendedSSL OrganizationSSL IntranetSSL CloudSSL	366
24	ExtendedSSL OrganizationSSL IntranetSSL CloudSSL	731
36	IntranetSSL	1096
48	IntranetSSL	1461
60	IntranetSSL	1826

8.3 Hash Algorithm

When an order is placed, the Product Code is used to specify the hash algorithm. When reissuing a certificate, there is no Product Code, so users must instead use a Hash Algorithm. There are some important notes to keep in mind when using a Hash Algorithm:

- If a Hash Algorithm is not specified, certificates will be issued based on the hash algorithm of the certificate being reissued.
- If SHA1 is selected as the Hash Algorithm, the SHA1 product option will be issued (if supported for the specified product).
- If SHA256 is selected as the Hash Algorithm, the SHA256 product option will be issued.
- If SHA256ECDSA is selected as the Hash Algorithm, CSRs with either ECC P-256 or P-384 can be used (if supported for the specified product).

Not all products support all Hash Algorithms; refer to Section 8.9 for a list of products and supported hashing algorithms.

When changing the Hash Algorithm, the issuing CA will also change to a new Subordinate CA certificate, which will need to be configured on the server as part of the certificate installation process.

8.4 KeyLength

The **KeyLength** reflects the Key Length to be used if the keys for the certificate are being created on GlobalSign servers for an AutoCSR product (IntranetSSL only). Valid values for RSA keys are 2048 or 4096. ECC AutoCSR is not supported.

8.5 ModifyOrder

The **ModifyOrder** command has different options available for modifying an order through the API. The below table describes the list of **ModifyOrder** options available. These options are available for all product types.

ModifyOrder	Description
APPROVE	Approve a pending order. If a user placed an order and did not have sufficient permissions, it will be queued for review. The API can identify and then approve these pending orders.
CANCEL	An order can be cancelled within the first 7 days only.
REVOKE	Revokes all certificates in the order (all reissued and renewed certificates with the specified **OrderID**).

8.6 Extensions

The Extensions function allows users to change the default values included in the following extensions:

- ExtendedKeyUsage
- KeyUsage
- TLSFeature (future)

These options use name-value pairs, where the “Name” is the name of the extension (ExtendedKeyUsage, KeyUsage or TLSFeature) and the value is the value to be placed in the extension. Multiple name value pairs will be used to specify multiple values for an extension (e.g., to request Server Auth and Client Auth in the EKU extension, you would need to supply two name value pairs in the API).

8.6.1 Extension to Product Mapping

The values permitted for your account will depend on how each of the products are configured within your account (Default, Basic or Advanced). If you need to specify certain values in any of the supported extensions listed in the below table, please contact your account manager or GlobalSign Support and ask that the configuration be updated for the product(s) needing this flexibility.

- The Default behavior for all SSL products is listed in the **Default** column
- MSSL EV, MSSL OV, CloudSSL and IntranetSSL have Basic and Advanced options
- PV_ARG (Private hierarchies) has a Basic setting as shown in the last column

Name	Value	Name of OID/Bit Position of EKU	Default	Basic	Advanced	PV_AEG Basic
Extended KeyUsage	1.3.6.1.5.5.7.3.1	Server Authentication	X	X	X	X
	1.3.6.1.5.5.7.3.2	Client Authentication	X	X	X	X
	1.3.6.1.5.5.7.3.4	Email Protection (S/MIME)	-	X	X	X
	1.3.6.1.5.5.7.3.5	IPSec End System	-	-	X	X
	1.3.6.1.5.5.7.3.6	IPSec Tunnel	-	-	X	X
	1.3.6.1.5.5.7.3.7	IPSec User	-	-	X	X
	1.3.6.1.5.5.7.3.17	id-kp-ipsecIKE	-	-	X	X
	1.3.6.1.4.1.311.20.2.2	Smart Card Logon	-	-	X	X
	1.3.6.1.4.1.311.21.5	Key Archival	-	-		X
	1.3.6.1.5.2.3.5	KDC Authentication	-	-	X	X
	1.3.6.1.5.5.8.2.2	IKE Intermediate	-	-	X	X
	2.5.29.37.0	Any Extended Key Usage	-	-		X
KeyUsage (RSA keys)	digitalSignature	0	X	X	NA	X
	keyEncipherment	2	X	X	NA	X
	dataEncipherment	3	-	X	NA	X
	keyAgreement	4	-	-	NA	X
	encipherOnly	7	-	-	NA	X
	decipherOnly	8	-	-	NA	X

					NA	
KeyUsage (ECC keys)	digitalSignature	0	X	X	NA	X
	keyEncipherment	2	-	-	NA	X
	dataEncipherment	3	-	X	NA	X
	keyAgreement	4	X	X	NA	X
	encipherOnly	7	-	X	NA	X
	decipherOnly	8	-	X	NA	X

8.7 OptionName

If a certificate has extended options, the certificate should specify an **OptionName**. The below table lists available **OptionName** values; set the value to "True" to activate.

OptionName	Supported Products	Description
SAN	ExtendedSSL OrganizationSSL IntranetSSL CloudSSL	Activates the Subject Alternative Name (SANs) option – see Section 8.10
REX	ExtendedSSL OrganizationSSL	Adds an additional 30 days to a Renewal order
VPC	ExtendedSSL OrganizationSSL	Enables setting a custom certificate expiration date. See Section 8.2
ASYNC_ORDER	ExtendedSSL OrganizationSSL IntranetSSL CloudSSL	We highly recommend using the Async_Order function to improve API performance and reduce API timeouts. This will return the OrderID, which you can use to query the Order Status and download the certificate. If Async_Order is not used, there is a possibility of timeouts due to external communications for CAA checks and logging the certificate to CT, especially when there are multiple SANs. This is mandatory for certificates with more than 100 SANs.

8.8 OrderType

Customers can place different types of orders through the API. The below table defines the different **OrderTypes** available by product type.

No.	OrderKind	Supported Products	Notes
1	New	ExtendedSSL OrganizationSSL IntranetSSL CloudSSL	A new order
2	Renewal	ExtendedSSL OrganizationSSL IntranetSSL CloudSSL	A renewal order for replacing an expiring certificate with less than 90 days remaining
3	Transfer	ExtendedSSL OrganizationSSL	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 industry requirements). The **CommonName** on the requested certificate and the one issued by a competitor must be the same.

			Note: You can transfer the remaining validity period from a GlobalSign certificate to a new certificate using this option.

8.9 ProductCodes

The product code specifies the type of product the customer is placing. The below table defines the different **ProductCodes** available by product type.

ProductCode	Certificate Type
ExtendedSSL	
PEV	ExtendedSSL signed with SHA1 - DEPRECATED
PEV_SHA2	ExtendedSSL signed with SHA256
OrganizationSSL	
PV	OrganizationSSL signed with SHA1 - DEPRECATED
PV_SHA2	OrganizationSSL signed with SHA256
IntranetSSL	
PV_INTRA	IntranetSSL signed with SHA1
PV_INTRA_SHA2	IntranetSSL signed with SHA256
PV_INTRA_SKIP	IntranetSSL using AutoCSR signed with SHA1
PV_INTRA_SKIP_SHA2	IntranetSSL using AutoCSR signed with SHA-256
PV_INTRA_ECCP256	IntranetSSL signed with SHA256ECDSA
CloudSSL	
PV_CLOUD	CloudSSL signed with SHA256
PV_CLOUD_ECC2	CloudSSL signed with SHA256ECDSA under the CloudSSL ECC CA

Note: If any of the Depreciated SHA1 options are selected, the SHA-256 equivalent will be automatically used.

8.10 Subject Alternative Names (SANs)

SANs allow various values to be associated with a certificate (e.g. email addresses, IP addresses, URIs, DNS names etc.). When SANs are added to a certificate, set **OptionName** to “SAN” and **SANOptionType** to one of the following, along with the full SAN in **SubjectAltName**. In the future, we expect **SANOptionType** to be optional and the system will compute the SAN type.

Value	SANOptionType	Products	Explanation
1	UC cert option	ExtendedSSL OrganizationSSL CloudSSL	Unified Communication Cert - Allows only owa, mail or autodiscover subdomains to be added for no additional cost
2	Subdomain SAN option	ExtendedSSL OrganizationSSL IntranetSSL CloudSSL	Additional Subdomain
3	GIP SAN option	OrganizationSSL IntranetSSL	Public IP address (IPv4 only)
4	Internal SAN option	IntranetSSL	Internal Hostname or Reserved IP address
7	FQDN SAN option	ExtendedSSL OrganizationSSL IntranetSSL CloudSSL	Additional Fully Qualified Domain

13	Wildcard SAN	OrganizationSSL IntranetSSL CloudSSL	Allows the entry of a SAN value starting with :*."

8.11 TagLocation

The **TagLocation** tells GlobalSign where the domain validation control number has been placed, when verifying domain control using DNS or HTTP methods.

8.11.1 DNS TXT Record Validation

The random number can be posted in a DNS TXT record for a domain or any higher level in the domain hierarchy. Since there are multiple levels where the value can be posted, the exact location must be supplied as part of the Validation step. The CA/B Forum defines the acceptable locations as Authorization Domain Names. The following table provides some examples:

FQDN	TagLocation values
a.b.c.example.com	a.b.c.example.com b.c.example.com c.example.com example.com
store.example.com	store.example.com example.com
example.com	example.com

8.11.2 HTTP Validation

The GlobalSign Vetting Department identifies itself with this User-Agent string:

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

Based on the SAN being validated, the Vetting Agent will only accept certain locations as valid. The following table provides some examples:

Requested Domain	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

This is an example metatag value:

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

GlobalSign regularly updates validation requirements on its Support webpage. You can review the latest HTTP-based validation requirements at this link:
https://support.globalsign.com/customer/en/portal/topics/1015848

9. Profile Parameters

9.1 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	ALANDS 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

Code	Name	Status
IE	IRELAND	Y
IL	ISRAEL	Y
IM	ISLE OF MAN	Y
IN	INDIA	Y
IO	BRITISH INDIAN OCEAN TERRITORY	Y
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

Code	Name	Status
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
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

Code	Name	Status
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
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

Code	Name	Status
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
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

Code	Name	Status
SV	EL SALVADOR	Y
SX	SINT MAARTEN	Y
SY	SYRIAN ARAB REPUBLIC	N
SZ	SWAZILAND	Y
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

9.2 CreditAgency/OrganizationCode

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

Value	Credit Agency
1	Dunn and Bradstreet number
2	Teikoku Databank code

9.3 MSSL Profile and Domain IDs

To order MSSL Certificates, an **MSSLProfileID** and **MSSLDomainID** (for the Common Name) must be provided. These can be obtained from either GCC or the API by following the below instructions.

9.3.1 Retrieving the MSSLProfileID

GCC Method: To obtain the **MSSLProfileID** from GCC

1. Login to your account.
2. Click the **MSSL** tab.
3. Navigate to the **Manage Domains & Profiles** section.
4. The **ProfileID** is displayed in the upper left of each of the Profile Tiles. It will have a format similar to: 45678_SMS2_1234.

API Method: To obtain the **MSSLProfileID** from the API

If the **ProfileID**s are not known, use the **GetMSSLDomain** command to retrieve the **MSSLProfileID**; in addition to returning the **MSSLDomainID**s, this command will also return the **MSSLProfileID** for each of the domains. Assuming there is at least one domain in each profile, this will be a complete list of **MSSLProfileID**s. Using the **MSSLProfileID**, detailed information about the Profile can be obtained via the **GetMSSLProfiles** API message.

9.3.2 Retrieving the MSSLDomainID

GCC Method 1: To obtain the **MSSLDomainID** from GCC

1. Login to your account.
2. Click the **MSSL** tab.
3. Navigate to the **Manage Domains & Profiles** section.
4. Click **Manage Domains**.
5. The **MSSLDomainID** is displayed in the **Domain** column, and will be in a format similar to: DSMS23100002136.

GCC Method 2: To obtain the **MSSLDomainID** for domains that were ordered or renewed via the Multi-step Add Domain process

1. Login to your account.
2. Click the **MSSL** tab.
3. In the left navigation panel, click **Domain Order History**.
4. This lists all **MSSLDomainID**s for all Profiles. Click **Export to CSV** to save the list as an Excel file.
5. The **MSSLDomainID** is displayed in the **Domain** column, and will be in a format similar to: DSMS23100002136.

API Method: If you know the **ProfileID** then you can retrieve the **MSSLDomainID** by using the **GetMSSLDomain** command.

10. Order Status Fields and Codes

10.1 Order/Certificate Status

Use the **GetModifiedOrders** command to retrieve the Order/Certificate status of a certificate request. The order status will be indicated by a specific value, as described in the below table.

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

10.2 ModificationEventName

To understand what type of modification was made to an order, use the **GetModifiedOrders** command to retrieve the **ModificationEventName**. The type of modification will be indicated by a specific code, as described in the below table.

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 certificate
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_EMAIL	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

10.3 MSSL Domain Status

The **GetMSSLDomains** command returns the current Domain Vetting status of a domain in an account. The vetting status will be indicated by a specific value, as described in the below table.

Value	Description	Can Issue Certificate?
0	Vetting in process	No
1	Vetting in process	No
2	Vetting in process	No
3	Approved	Yes
5	Domain has been Canceled, Removed, or Revoked	No
6	Domain has been Canceled, Removed, or Revoked	No
7	Domain Renewal is in process	Yes (until expiration date)
8	Domain flagged for manual review	No
9	Domain Renewal is in process	Yes (until expiration date)
10	Domain Renewal is in process	Yes (until expiration date)
11	Domain Renewal is in process: Queued for manual review	No

10.4 MSSL Profile Status

The **GetMSSLProfiles** command returns the current Profile Vetting status of a domain in an account. The vetting status will be indicated by a specific value, as described in the below table.

Value	Order Status
1	INITIAL / Vetting in Progress
2	Vetting in Progress
3	Vetting Completed / Available
5	Cancelled / Suspended
6	Profile Rejected

10.5 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 indicates the order failed, and the API will provide one or more **ErrorCodes**. **ErrorCodes** provide more information on the Error created with the order, including 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. This type of error could indicate the order request was received but not processed immediately, or the request cannot be received by GCC. If a server error code is received, compare the error code with the table in Section 10.5.3. Report any server error codes to api@globalsign.com

10.5.1 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 Department manually reviews and clears the order's phishing flag

10.5.2 Client Error Codes

Success Code	Error Code	Description	Notes
-1	-101	Invalid parameter entered.	Invalid parameter entered. Please check that the parameters match the API specification. Please review the specific ErrorMessage returned in the XML response for parameter details and consult the XML Field definitions section of the applicable API document.
-1	-102	Mandatory parameter missing	Mandatory parameter missing. Please check that the parameters match the API specification. Please review the specific ErrorMessage returned in the XML response for parameter details and consult the XML

Success Code	Error Code	Description	Notes
			Field definitions section of the applicable API document.
-1	-103	Parameter length check error	Parameter length check error. Please check that the parameters match the API specification. Please review the specific ErrorMessage returned in the XML response for parameter details and consult the XML Field definitions section of the applicable API document.
-1	-104	Parameter format check error	Parameter format check error. Please check that the parameters match the API specification. Please review the specific ErrorMessage returned in the XML response for parameter details and consult the XML Field definitions section of the applicable API document.
-1	-105	Invalid parameter combination	Invalid parameter combination. Please that check the parameters match the API specification.
-1	-300	Database Error. Please retry and if the issue persists contact support with detailed information concerning the issue.	Database Error. Please retry and if the issue persists contact support with detailed information concerning the issue.
-1	-4001	Login failure invalid user ID	Login failure. UserName or Password is incorrect. Please make sure that you have specified the correct UserName and Password.
-1	-4008	The certificate is either expired, does not meet the requirements of transfer, or is inaccessible on the CN by the GlobalSign system. Please ensure that the certificate is correct and try again	Unable to process this request. It could be that the Common Name in the TargetCERT specified does not match the Common Name specified for this request or the TargetCERT is inaccessible on the Common Name by the GlobalSign system. Please review the contents and accessibility of the Common Name in the TargetCERT before proceeding with this request.
-1	-6101	The account used does not have enough balance to order a certificate	Your account does not have enough remaining balance to process this request. Please make sure you have enough remaining balance in your account before proceeding with this request.
-1	-6102	The renewal of the certificate failed. There may be lacking or incorrect information that is required for the renewal of the certificate	The renewal of the certificate failed. Please note that when renewing a certificate, the Common Name of the original certificate and this request must be the same. Please also check that the status of the original order is ISSUED and that the order has not been previously renewed.
-1	-9401	No profile was found using the supplied MSSLProfileID. Please make sure that the supplied MSSLProfileID is correct.	Unable to process this request because you do not have permission to access the MSSLProfileID or we were unable to find the MSSLProfileID specified. Please make sure that the supplied MSSLProfileID is correct.
-1	-9403	The account used does not have MSSL rights. Please make sure you are using. Please make sure you are	MSSL is not activated for this user. Please make sure that your UserName is correctly entered.

Success Code	Error Code	Description	Notes
		using an account with MSSL rights.	
-1	-9440	No domain was found using the supplied MSSLDomainID. Please make sure that the supplied MSSLDomainID is correct.	We were unable to find the MSSLDomainID specified. Please make sure that the supplied MSSLDomainID is correct.
-1	-9443	The account used does not have access to the domain associated with the supplied MSSLDomainID	You do not have permission to use the specified MSSLDomainID. Please make sure that the MSSLDomainID is correctly specified.
-1	-9450	Cannot request a certificate order. Please try again.	Unable to process this request. Please note that when requesting for EV orders, an MSSLProfileID with an EV Vetting level must be used. Also make sure that the ProductCode of your request is supported in MSSL.
-1	-9913	No valid coupons were found. Please recheck the supplied coupon.	We were unable to find the Coupon specified. Please make sure that it is correctly entered.
-1	-9914	No valid campaigns were found, Please recheck the supplied campaign.	We were unable to find the Campaign specified. Please make sure that it is correctly entered.
-1	-9915	Certificate was already cancelled	The OrderID you are trying to modify has been cancelled previously. Please make sure that the OrderID is correctly entered.
-1	-9916	Cannot find the certificate that is associated with the order id you have supplied	We were not able to find the OrderID specified. Please make sure that the OrderID is correctly entered.
-1	-9918	The coupon or campaign you supplied is invalid	The coupon or campaign you specified is already expired. Please make sure that the coupon or campaign is correctly entered.
-1	-9919	The coupon or campaign you supplied is already used	The coupon you specified has been used previously. Please make sure that the coupon is correctly entered.
-1	-9920	The coupon or campaign you supplied is not allowed to be used	The coupon or campaign you specified is not yet activated. Please make sure that the coupon or campaign is correctly entered.
-1	-9922	The coupon or campaign's currency is not the same with the currency of your user	The currency of the specified Coupon or Campaign is not the same with the currency of your user. Please make sure that the coupon or campaign is correctly entered.
-1	-9933	The expiration date you have entered is not compatible with the product you have selected	The calculated months of the NotBefore and NotAfter specified is beyond the specified Months. Please make sure that the NotBefore and NotAfter has been entered correctly.
-1	-9936	GlobalSign operates a security and vulnerability scan of the public key component of the CSR you have just submitted.	The key you used in your CSR is either too short (RSA minimum 2048, ECC minimum 256), or the key failed the Debian weak key check as well as key length. Please generate a new keypair and try again
-1	-9938	The status of the certificate has already been changed	The certificate you are trying to modify has already been modified. Please make sure that the OrderID is correctly entered.
-1	-9942	A problem was encountered when trying to request the certificate in the RA System	An internal server problem has been encountered. Please try again and if the issue persists contact GlobalSign support

Success Code	Error Code	Description	Notes
			with detailed information concerning the issue.
-1	-9943	A problem was encountered when trying to issue the certificate in the RA System	We were unable to issue this certificate request. It could be that your certificate has been modified previously. Please make sure that Data is correctly entered.
-1	-4201		Your IP Address {0} is not within the range of IP addresses that is allowed for API use. Please contact GlobalSign support to have this address added for API access
-1	-6002		There was an error when trying to parse the TargetCERT specified. Please make sure that the TargetCERT specified is correct.
-1	-6007		The Public Key of the CSR has been used previously. For security reasons we allow the keys to be used if they have the same CN. Please recheck the CSR specified and try again.
-1	-6017		The number of SANEntry has exceeded the maximum allowed number of SANEntry. Please do not exceed the maximum allowed number of SANEntry.
-1	-6021		Common Name in CSR and FQDN for check do not match. Please make sure that the CSR has been entered correctly.
-1	-9200		The type of your user is not allowed to use this API. Please check your permission and retry.
-1	-9404		You do not have permission to add a domain to this MSSLProfileID. Please make sure that the MSSLProfileID is correctly entered.
-1	-9405		Unable to process this request. You need to upgrade your account to MSSL Pro before you can add another profile. Please contact Globalsign Support to request for an upgrade to MSSL Pro.
-1	-9406		The DomainName already exists for the MSSLProfileID. Please make sure that the DomainName you are adding is unique or make sure that the MSSLProfileID specified is correctly entered.
-1	-9407		A Profile with that OrganizationName, StateOrProvince, Locality and Country already exists. Please make sure that the details mentioned above are correctly entered.
-1	-9430		You do not have permission to edit the specified MSSLProfileID. Please make sure the MSSLProfileID is correctly entered.
-1	-9442		You do not have permission to delete the specified MSSLDomainID. Please make sure that the MSSLDomainID is correctly entered.
-1	-9444		The specified DomainName or SubjectAltName is not supported. Note that wildcard gTLDs are not supported. Please make sure that the DomainName or

Success Code	Error Code	Description	Notes
			SubjecctAltName specified is correctly entered.
-1	-9445		Unable to process this request because the vetting level of the MSSLProfileID and the specified VettingLevel does not match. Note that when adding an EV Domain, the vetting level of the specified MSSLProfile should also be EV. Please make sure that the MSSLProfileID or the VettingLevel is correctly entered.
-1	-4083		The CommonName specified is not the same or is not a subdomain of the specified MSSLDomainID. Please make sure that the CommonName or the MSSLDomainID is correctly entered.
-1	-9901		The Product Group of this user does not allow ordering of the specified ProductCode. Please contact Globalsign Support if you wish to order using this ProductCode.
-1	-9902		Unable to process this request. You do not have permission to access the OrderID. Please make sure that the OrderID is correctly entered.
-1	-9934		The Top Level Domain used belongs to Globalsign's Banned List. Therefore, a certificate cannot be issued. Please make sure that Common Name is correctly entered.
-1	-9939		The state of this account is either invalid, stopped or locked. Please make sure that the account is correctly configured. Contact customer support for assistance.
-1	-9940		The specified NotBefore or NotAfter should not be before the current date. Please recheck these parameters before continuing with this request.
-1	-9940		The public key used in the CSR specified has been previously revoked. Please confirm you CSR and try again.
-1	-9949		The NotAfter specified is after the calculated BaseLine Validity Limit. Please take note that validity should not exceed 27 months.
-1	-9952		The Top Level Domain you specified belongs to the list of TLDs that is not allowed for ordering. Please make sure that Common Name is correctly entered.
-1	-9953		Cannot complete this request because the region or country of your Domain is not allowed for this partner. Please make sure that Common Name is correctly entered.
-1	-9961		The ECC CSR you specified is not allowed. Please enter an ECC CSR using either P-256 or P-384 curves.
-1	-9962		Key Compression is not allowed. Please make sure that CSR is correctly entered.
-1	-9964		Unable to process this request. It could be that the HashAlgorithm of this order is ECC but the key Algorithm of the CSR is RSA.

Success Code	Error Code	Description	Notes
			Please make sure that the CSR or the ProductCode are correctly entered.
-1	-9971		Due to industry requirements, you can no longer issue certificates with internal server names in Common Name. Please specify a non-internal Common Name.
-1	-9987		The certificate you are applying for exceeds GlobalSign's maximum certificate validity of 825 days.
-1	-9988		The certificate you are applying for exceeds GlobalSign's maximum certificate validity of 27 months for EV, or 60 months for IntranetSSL.

10.5.3 Server Error Codes

Success Code	Error Code	Description	Notes
-1	-201	Internal system error - Failed database operation	System Error. (Database error - database operation). Please retry and if the issue persists contact support with detailed information concerning the issue.
-1	-300	Internal system error - Failed database operation	System Error. (Database error - database operation). Please retry and if the issue persists contact support with detailed information concerning the issue.
-1	-301	Internal system error - Failed database operation	System Error. (Database error - inconsistent data). Please retry and if the issue persists contact support with detailed information concerning the issue.
-1	-2001	Internal system error - Email sending warning	Internal system error - Email sending warning. Unable to send email with the details of your order to your email address. Please contact support with detailed information concerning this issue.

11. Data Field Definitions

11.1 Data Types

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

11.2 Data Definitions

Data Structure	Description	Type/Length
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
Approvers Approver		
ApproverInfo Email FirstName Function LastName OrganizationName OrganizationUnit Phone	Approver Information for an EV certificate request	
AuthorizedSignerInfo FirstName LastName Function Phone Email	Authorized Signer Details	
AuthToken UserName Password	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
CACertificate CACertType CACert	This identifies the type of certificate for each CA certificate in the chain, and also contains the actual certificate.	

Data Structure	Description	Type/Length
CACertificates CACertificate CACertType CACert	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	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
CommonName	The common name in certificate.	String/255
CSRSkipOrderFlag		Boolean
City		String/200
ContactInfo FirstName LastName Phone Email	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。	String/50
CreditAgency	The Organizations name. 1. DUNS No. 2. TDB code	String/50
Currency	The Currency of the transaction	String/10
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

Data Structure	Description	Type/Length
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
EndDate	The Certificate NotAfter date.	DateTime
Email	From the ContactInfo structure. The Email Address of the contact.	String/255
Error ErrorCode ErrorField ErrorMessage	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 AdminContactPhone.	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.	
ErrorCode		Int
ErrorField		String/1000
ErrorMessage		String/1000
ExpressOption	To add Express Options set to true. If not false.	Boolean
Extension		
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

Data Structure	Description	Type/Length
IncorporatingAgencyRegistration Number		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
JurisdictionInfo Country StateOrProvince Locality IncorporatingAgencyRegistration Number 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 no longer used and should be set to 1. It used to be the number of server licenses, but all GlobalSign certificates are licensed for an unlimited number of servers.	Int 1-99 Only
Locality	The Locality field from the CSR or Certificate	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
ModifyOrderOperation	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
MSSLProfileID	ID associated with the Profile you are using	String/50
MSSLDomaindID	ID associated with the Domain being used	String/50
MSSLDomainName	fqdn being queried	String/64
MSSLProfileStatus	Status of profile	String/5
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.	

Data Structure	Description	Type/Length
OrderKind	Type of order: • new: a new certificate request • renewal: renewal of an existing certificate • transfer: a transfer of a certificate from another CA which extended the validity period of this certificate	String/10
OrderID	This is the OrderID assigned by GlobalSign to the order and provided to the person requesting the certificate.	String/50
OrderInfo OrderID ProductCode BaseOption OrderKind Licenses ExpressOption ValidityPeriodCustomizeOption InsuranceOption GSSupportOption RenewalExtentionOption DomainName OrderDate OrderCompleteDate OrderCanceledDate OrderDeactivatedDate OrderStatus Price Currency ValidityPeriod SpecialInstructions	This structure contains basic information that apply to most orders and is profiled within each order response structure.	
OrderOption ApproverNotifiedDate ApproverConfirmDate ApproverEmailAddress OrganizationInfo ContactInfo OrderOption	This structure is in many order request messages and contains basic order information common to all types of orders.	
OrderParameter ProductCode BaseOption OrderKind Licenses ExpressOption ValidityPeriodCustomizeOption InsuranceOption GSSupportOption RenewalExtentionOption 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.	

Data Structure	Description	Type/Length
OrderParameterWithoutCSR ProductCode BaseOption OrderKind Licenses ExpressOption ValidityPeriodCustomizeOption InsuranceOption GSSupportOption RenewalExtentionOption ValidityPeriod PIN KeyLength RenewalTargetOrderID)? TargetCERT DNSNames SpecialInstructions Coupon Campaign	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	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.	
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		

Data Structure	Description	Type/Length
Organization	The Organization field from the certificate	String/255
OrganizationAddress AddressLine1 AddressLine2 AddressLine3 City Region PostalCode Country Phone Fax OrganizationAddress		
OrganizationCode	Can be used to indicate company numbers lookup, i.e. For DUNS enter 1 in this field.	String/50
OrganizationInfo OrganizationName CreditAgency OrganizationCode OrganizationAddress	Organization Info sent with Certificate request.	
OrganizationInfoEV CreditAgency OrganizationCode BusinessAssumedName BusinessCategoryCode OrganizationAddress	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
OVCSRInfo CommonName OrganizationName OrganizationUnit Locality StateOrProvince Country	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

Data Structure	Description	Type/Length
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		
ReOrderParameterWithoutCSR DNSNames PIN KeyLength ReOrderParameterWithoutCSR		
RenewalTargetOrderID	Original OrderID for renewal orders.	String/50
RequestorInfo FirstName LastName Function OrganizationName OrganizationUnit Phone Email	Certificate Requestor Information	
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

Data Structure	Description	Type/Length
SANEntries SANEntry SANOptionType SubjectAltName SANEntry SANEntries	One or more SANs, each of a specified type	
SANOptionType	See Section 8.10 for the list of supported SANOptionTypes	
SubjectAltName	The SAN value must match the format of the specified SANOptionType. See Section 8.10 for the list of supported SANOptionTypes	String/64
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	This field is not used in any API. Please ignore.	String/50
SubjectName	The SubjectName in certificate.	String/255
SuccessCode	Code in the Order and Query Response Headers which indicates the success or failure of the request. • 0 - Success with no warnings. • 1 - Success with warnings. • -1 - Failure. Note that if the Success is non-zero an accompanying Error structure will be present.	Int
TargetCERT		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

Data Structure	Description	Type/Length
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
VettingLevel	The vetting level for an MSSL Profile	String
VettingType	The type of vetting to be applied when requesting a domain to be added to a profile	String
X509Cert	A base64-encoded certificate.	String/4000