Quick Start API Guide

This document will help you get started with API integration

This is the general information needed to start understanding how to integrate with our SSL system via our Restful API. If you need help during integration at any time, please feel free to contact support@SSLhelpdesk.com and/or contact your dedicated account manager.

Introduction to SSL

Basic Introduction

SSL is a cryptographic protocol which is designed to provide communication security over the Internet. They use X.509 certificates and have asymmetric cryptography to assure the counterparty with whom they are communicating, and to exchange a symmetric key. This session key is then used to encrypt data flowing between the parties. This allows for data/message confidentiality and message authentication codes for message integrity and as a by-product, message authentication. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging, and voice-over-IP (VoIP). An important property in this context is forward secrecy, so the short term session key cannot be derived from the long term asymmetric secret key.

Sites without SSL basically expose all the information between the site and it's user in plain text. For example, if there's a login form without SSL, username and passwords are clearly visible to any router in the path to the server. It's very easy to run all kinds of phishing scams, identity thefts, etc. for non-secure sites.

When you say you are buying an SSL for the site, it essentially means that we are buying an X.509 certificate from a trusted vendor. Trusted vendors are the ones that the CA/B forum (Certificate Authority/Browser Organisation) trusts. You are able to have a self-signed certificate, however it only protects against transport layer theft. Self-signed certs are vulnerable to phishing scams.

At The SSL Store™, we sell SSL certificates from globally recognized & trusted vendors. We provide SSL certificates from Symantec, Comodo, RapidSSL, GeoTrust, Thawte, and Certum. Our list of trusted vendors is constantly growing, so a long-term relationship and commitment with us is likely to be tremendously beneficial. The more products we

introduce, the more you can provide to your clients with single ubiquitous API calls. You don't have to constantly go vendor hunting, sign contracts and you'll only have to change your code minimally to consume our API for newer products.

How to Get a Certificate for a Site

Typically, to get a certificate, you need to fill out a form to provide contact details about you and your company and also provide a CSR (Certificate Signing Request). A CSR can be generated via http://openssl.com or your hosting control panel, along with a private key that only you have access to. Once you submit a CSR, you need provide a way to authenticate your domain name. All this means is that you have to prove that the domain name for which you want a certificate issued is actually in your possession or control. This is typically done by using one of the two options:

1. **via Email Mode (Email Based Authentication or DCV Email)**
2. **via File Mode (File-Based Authentication)**

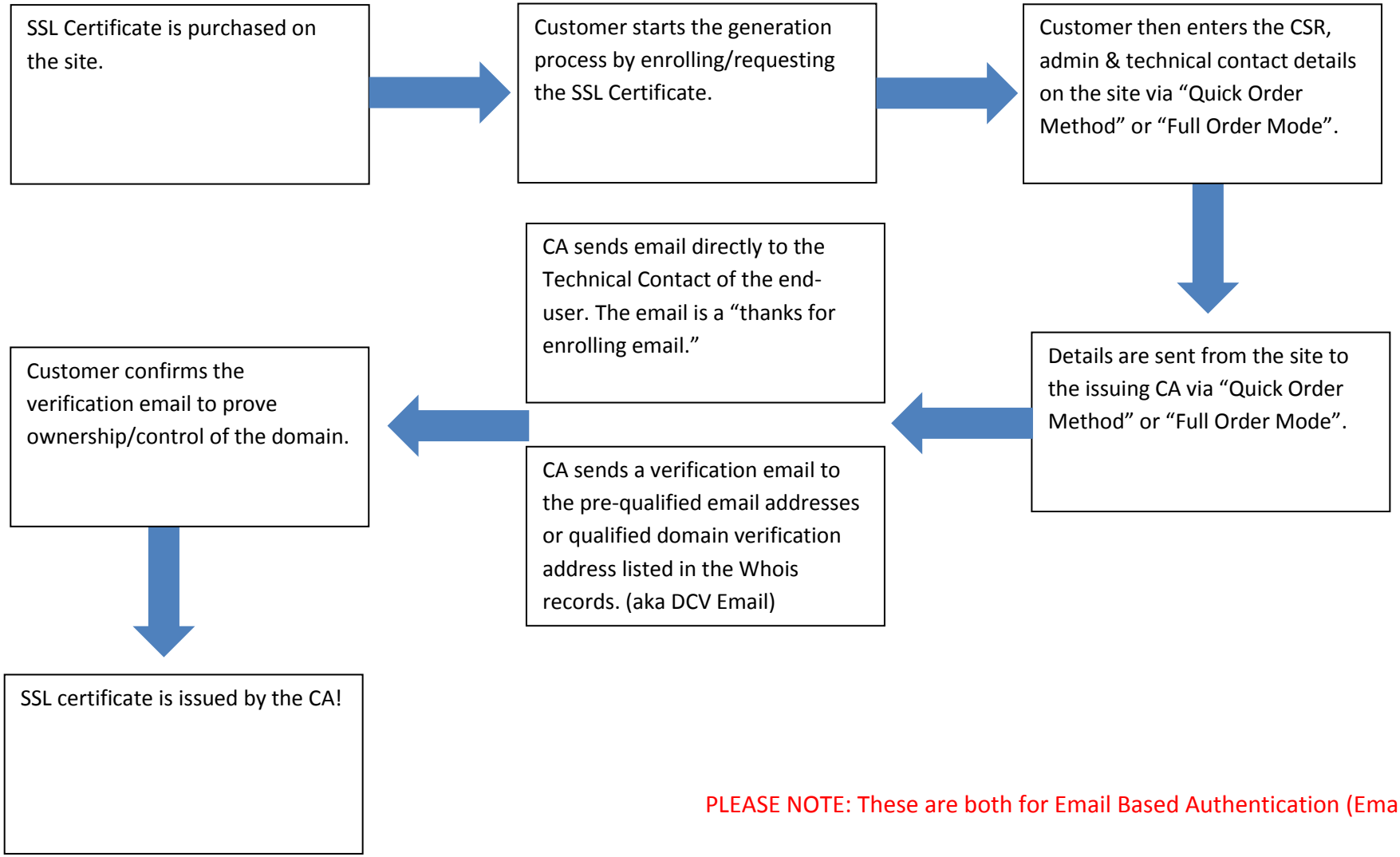
In Email mode, you need to pick from a pre-defined email address for the domain that you should be able to receive. This list is different from vendor to vendor and, as pointed out in our implementation below, it's better to call our API to get hold of this list. Once you select an email address, the CA (vendor, i.e.: Symantec) will send an email to that email address. You need to click a private link in that email to approve the request for your domain. For Domain Validated (DV) Certs (look at type of certificates below), you are mostly done, after confirming the link in Email Mode, you will be sent a certificate which you can now install on your server.

In File mode, the CA (vendor i.e.: Symantec) gives you a unique file to download which you then have to upload on to your site, typically the CA automatically detects this and for DV, they will send you the certificate.

GENERAL SSL FLOW CHART ON NEXT PAGE

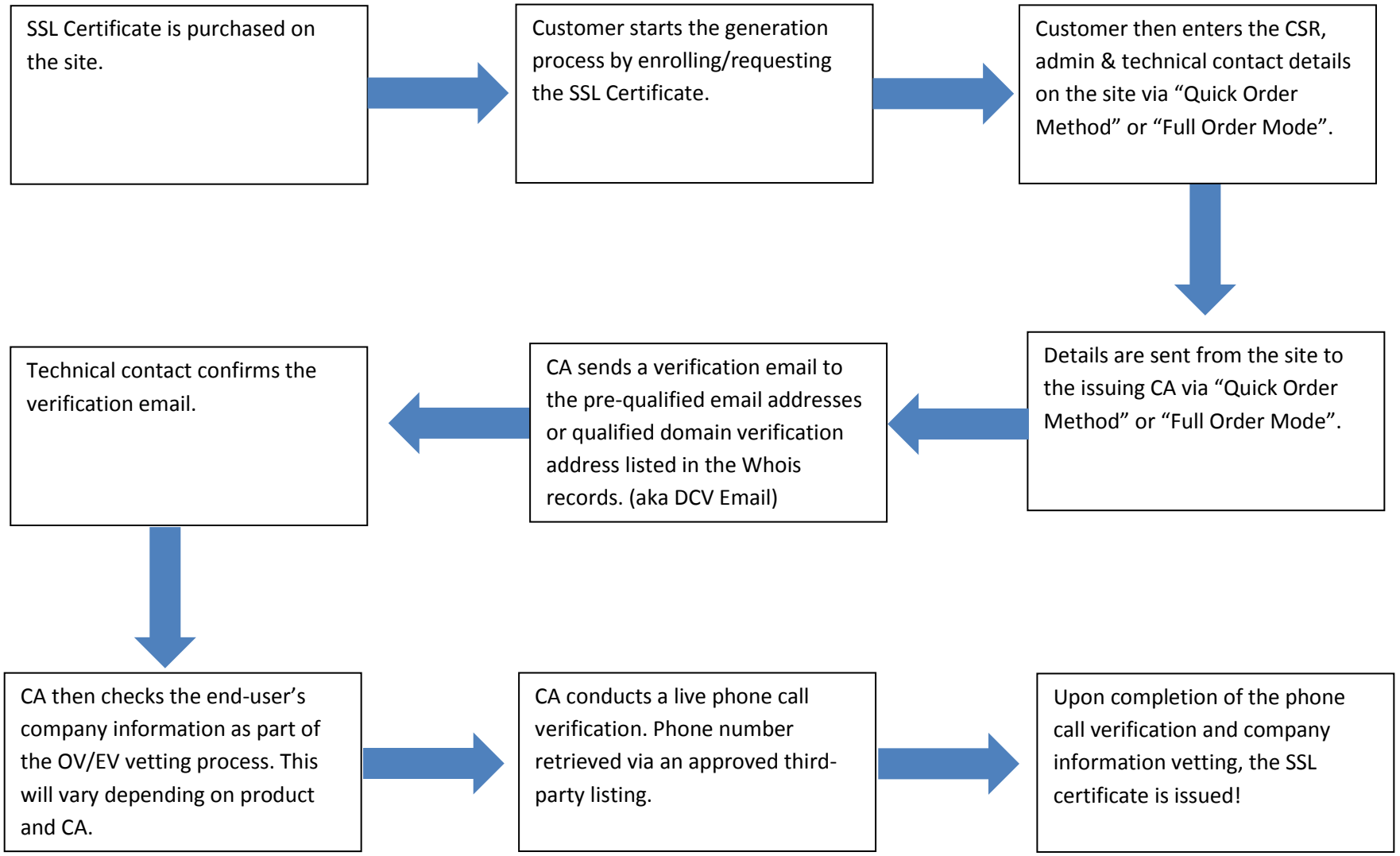
General SSL Process (DV & OV/EV)

Standard DV Certificates – Email Based Authentication Method



PLEASE NOTE: These are both for Email Based Authentication (Email Mode)

OV/EV Certificates –Email Base Authentication Method



Types of SSL Certificates

The example pointed out above is simplistic scenario for Domain Validated certificates, also known as DV certificates, Domain Vetted certificates, or Domain Validation certificates. There are different types of SSL certificates, such as:

- ✓ **Domain Validated Certificates**
  These are basic certificates that only proves you own the domain/site and the details between you and your user is encrypted. The CA (vendor i.e.: Symantec) just validates here that XYZ is your domain, but doesn't provide or display any details about you to the user. For this type of certificate, trust levels are low for the user.
- ✓ **Organization Validated Certificates**
  Typically known as OV certificates, the CA validates your domain as well as your organization details, to determine whether or not it's a legitimate organization doing business. Typically, CAs check details about your organization in various different ways (like your local business registry for example). The source of validation differs from product to product.
- ✓ **Extended Validation Certificates**
  Typically known as EV certificates, in addition to the steps in OV, the CA performs additional steps of validation before issuing an EV certificate. EV certs have highest level of encryption, security and trust. Some products have as many as 9 total variations of validation steps necessary. Once you go through the EV process directly with the CA, the certificate enables all of the browser trust indicators, such as the green bar in the browser's URL window, this is has highest trust-value with your users. When the whole address bar in the browser is green, it has been proven to result in higher conversion ratios.
- ✓ **Wildcard Certificates**
  Wildcard certificates are the ones that secure an umbrella of sub-domains. This can be a cost-effective way to secure many of your sub-domain sites with a single certificate. For example, a certificate issued to *.google.com , will secure abc.google.com as well as xyz.google.com or any other combinations, as long as there is .google.com in the end. Wildcard certificates typically come in DV and OV variants.
- ✓ **Multi-Domain Certificates**
  A multiple domain certificate allows you to secure multiple domains with a single certificate. The difference between Wildcard and Multi-Domain certs is that with multi-domains you can only secure a pre-defined list of domains, meaning you have to declare what domains you are going to secure upfront. To add or remove domains to that list during a validity period of an active/in-use certificate, you have to go through a process called "Re-issue of certificate".

How to Integrate with Our Restful API

Before you plan integration with The SSL Store™ API, you need to think about your requirements and work out what level of development it is that you want to do. We provide 2 methods of integration:

1. **Quick Invite Mode**
   You need to implement "invite order": https://www.thesslstore.com/api/invite-order. You can find details of the implementation in the URL. The basic idea is that you just send a minimum set of parameters in the API and you get returned a "TinyOrderLink" that you can save and present it to the user. This white-labeled URL has all the details a user will need for completing/submitting the certificate, i.e. accepting a CSR, inputting Admin & Technical contacts, etc. This is ideal if you don't want to spend too much development time for a full integration. The only real downside to this method is that your user goes to another website owned and hosted by us (which is white-labeled or white branded) which you may or may not like. Please note the URL is totally white-branded and it even allows you to customize the look by adding your company logo. You can even adjust the language for your customers. There is no link to TheSSLsstore.com with that URL (it uses the domain, CentralAPI.com) and your company is still the only company who can charge the user. Your customers are only given access to this link after they pay you.

2. **Full Order Mode**
   Full Order Mode gives you complete control over the entire API-integration. There is no third-party site (like in Quick Invite Mode) that comes into this picture. The steps to integrate with full order mode is as follows :
   a. Get approver email from the CSR : https://www.thesslstore.com/api/approves-list
   b. Call ValidateOrder to check if order details are fine https://www.thesslstore.com/api/validate-order-parameters
   c. Call neworder request. Details https://www.thesslstore.com/api/new-order

   Once done, you get a response back with the order number, depending on your inputs, you will either get an email to confirm the domain or the file that you need to upload to the server, etc. (Email Mode vs. File Mode) When viewing our API Wiki, it may sound a little complex, however we are providing you with pre-built SDKs in PHP and C#, that all you literally need to do is change the values to tie-up with our API.

How Renewal Orders Work

SSL certificates are not like domain names where you pay and it automatically renews. So you have to go through essentially the same steps as a new order. CAs enforce this because SSL is a security product and within any given time-span, lots of details may change about the site or organization. So the CA requires a user to go through the same steps as a new order to ensure its legitimacy. From the API's perspective too, it's the same thing, except you need to change few parameters in new-order code, because the CA will actually add-on the remaining time in the current certificate into the new certificate so that the user doesn't lose any time by simply renewing prior to the expiration. For a renewal, the CA will need to know what initial order the renewal is tied to. A Renewal Order is technically a New Order, the only difference is we need to know if it is a renewal so that we can tell the CA to add on the remaining time in their certificate. So, there are 2 things we need to know, one, we need to know that it is a renewal and two, we need to know what Order ID the original order is.

Here are the 2 calls pertaining to this:

- NewOrderRequest.isRenewalOrder
- NewOrderRequest.RelatedTheSSLStoreOrderID

Just to wrap up, to renew an order you just need to call https://www.thesslstore.com/api/new-order and for a renewal you need to set "True" value in field "isRenewalOrder" otherwise, if passed it's"False".

Please keep in mind, that for Symantec, Thawte, GeoTrust and RapidSSL products, you can do a renewal within 90 days of expiration. For Comodo products, it is only able to be renewed within 60 days of expiration.

How Certificate Re-Issue Works

The re-issue of a certificate is typically done if the server you had the certificate on has crashed or you want to change the details of some certificates. For example, in a multi-domain cert you have to re-issue the certificate if list of your domain names that you want to cover changes. From the API integration point of view, you need to call: https://www.thesslstore.com/api/re-issue. We have provided extensive details in the PHP and C# SDK, as well as in our detailed API specs document.

Don't forget, if you need any further clarification or guidance of any kind throughout the API integration process, please feel free to contact us via email at support@SSLhelpdesk.com.