What you pay for when you buy an SSL Certificate

The truth about SSL is that those certificates you pay for and those you get for free work identically, regardless of their validation method. In fact, the encryption levels are about the same for most certificates. However, certificate prices may vary steeply between vendors. How come? In this article, we will illuminate what it is that the price of an SSL Certificate really depends on.

What makes a secure SSL Certificate. Size of the key

The sole purpose of an SSL Certificate is to secure the website by protecting the data line between the server and the client. And the only factors directly responsible for SSL security are the encryption algorithm and length of the key.

An up-to-date SSL Certificate is supposed to use the encryption standard SHA 256 and the key length of 2048 bits. This is a must in order to fulfil the current browser requirements. A compliant certificate is deemed sufficiently secure.

But certificates can be issued with a key length of 3072 bits or longer. For example, GlobalSign certificates use the SHA 256 hashing algo and support RSA 2048+ and ECC 256 & 384-bit keys. Keys get as long as 4096 bits with some vendors. However, this encryption level is viewed as excessive at this point. The plan is to move to key lengths of RSA 3072 bits or longer sometime in the 2030s.

Now we know that a certificate's security level is all about its encryption algo. How does this affect the price of an SSL Certificate? It doesn't. You can get a 4096 bit SSL certificate for free from Let’s Encrypt, or you can buy a standard 2048 bit certificate.

The thing is, each certificate authority sets its own certificate prices. The price is typically in direct proportion to validation type, the presence of extra options, and confidence in the brand. Let's take a look at these pricing factors.

Certificate Validation type: DV, OV, EV

Validation type determines the information the certificate holds, or what browsers and site visitors will be able to learn about the domain owner.

A basic Domain Validated (DV) Certificate only carries the list of domains it will serve. This type of certificate is easy to obtain and easy to issue for the certificate authority as validation occurs automatically.

On top of the list of domains secured, Organization Validated (OV) and Extended Validated (EV) Certificates will identify the organization they are issued for, and specify its location. These types of certificates are only available to legal entities and sole proprietors. EV

Certificates contain a little more information than OV Certificates, indicating the entity's registration number and ownership format. Moreover, EV Certificates are vetted manually: the certificate authority will request the appropriate documents from the customer and vet them.

DV Certificates carry the least information and are the most affordable of all certificate types. DV SSL Certificates are even available for free: you can issue one yourself or order one from Let's Encrypt. The key size of a DV Certificate may actually exceed that of a much costlier EV Certificate. An EV or OV Certificate can be pricey.

Extra options: Wildcard and SAN

An SSL Certificate is typically issued for a single domain name: e.g., ispmanager.ru. Which means it will work for ispmanager.ru, but not for, say, my.ispmanager or ispmanager.com. But when you have procured a certificate with Wildcard or SAN attached, it's a different story!

The Subject Alternative Name (SAN) option lets you add another name to your certificate. An SSL Certificate with SAN support is able to serve multiple domains at the same time, e.g., ispmanager.ru and ispmanager.com.

The Wildcard option lets you secure both the master domain and its subdomains. For instance, a certificate with Wildcard support, issued for ispmanager.ru, will also protect my.ispmanager.ru, news.ispmanager.ru, and other subdomains.

Warranty

Every certificate authority offers a warranty against loss of money with its certificates. Warranty compensation can be claimed when the site owner or a visitor sustains a loss for which the certificate authority is responsible. For example, in the event that the certificate's cipher gets breached through some failure on the part of the certificate authority, or the certificate authority issues a certificate to some fraudsters posing as someone else. Each vendor has full discretion to set the amounts of their warranty compensation and define the events covered. The more complicated the vetting process and the associated validation type - DV, OV or EV, the more the certificate will cost and the larger the warranty that comes with it. The applicable warranty compensation amounts can be found on the websites of certificate authorities:
GlobalSign
Digicert
GeoTrust

Certificate authority's reputation

Commonplace as it may sound, the brand under which the certificate is issued is a factor in its price. The certificate of a widely recognized brand with a solid history will probably cost more. And the longer the company has been around, the more likely it is that its SSL is supported by a huge number of devices. In this case, the price can be even higher.

We have found out that the price of an SSL Certificate has nothing to do with its encryption level. On the other hand, the price hinges on the validation method, the availability of extra options, the warranty amount, and the certificate authority's reputation.

What to look for when shopping for an SSL Certificate

The encryption level of all SSL Certificates is basically the same, and pretty solid. But there are a few other points to keep in mind when shopping: we have already discussed them.

- Validation type: DV, OV or EV. DV Certificates are suitable for most websites. However, if you are a business that accepts payments on its website (not through an acquiring service, for instance) or you are a major brand, an OV or EV Certificate is more advisable for better protection against phishing.
- Extra options: SAN to secure multiple domains and Wildcard to secure the subdomains.
- Brands: When a certificate authority has been around a long time, there is a good chance that there will be no issues with their certificates and that browsers will trust them.