Ref: <https://www.instantssl.com/ssl-certificate-support/guides/ssl-certificate-validation.html>

Since the SSL protocol was released by Netscape as a security technology in 1996 consumers have been educated to look for the SSL padlock before passing any critical details over the Internet. Technically, the SSL protocol provides an encrypted link between two parties, however in the eyes of the consumer, seeing the SSL padlock in their browser means much more:

* *That they have a secure (encrypted) link with the website*
* *That the website displaying the padlock is a valid and legitimate organization or an accountable legal entity*

**What is SSL?**

[Secure Sockets Layer](https://www.instantssl.com/ssl.html), SSL, is the standard security technology for creating an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browser remains private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. In order to be able to generate an SSL link, a web server requires an [SSL Certificate](https://www.instantssl.com/ssl-certificate.html).

SSL Certificate must be issued by a "trusted certifying authority" - trusted third party Certification Authorities that utilize their trusted position to make available "trusted" SSL Certificate.

**What is a Certification Authority?**

Browsers and Operating Systems come with a pre-installed list of trusted Certification Authorities, known as the Trusted Root CA store. As Microsoft and Netscape provide the major operating systems and browsers, they have elected whether to include the Certification Authority into the Trusted Root CA store, thereby giving trusted status.

Certification Authorities have a responsibility to ensure they only ever issue SSL Certificates to legitimate companies, by employing stringent validation processes to ensure issuance practices only allow the SSL Certificate to be issued to a legitimate company.

**All SSL Certificates are not equal!**

The value of SSL is protected by the strength of a standard two-point validation process:

Step 1: Verify that the applicant owns, or has legal right to use, the domain name featured in the application.   
Step 2: Verify that the applicant is a legitimate and legally accountable entity.

Companies such as GeoTrust, through its QuickSSL and FreeSSL products, and IPSCA, the Spanish SSL Provider, perform only the first stage of the two-step validation process (as employed by all other SSL Providers) by only verifying that the applicant owns the domain name provided during Certificate application.

**Trusted Certificates VS Browser Recognized Certificates**

If a website is only interested in providing encryption to its visitors it can do so by using a free self-signed Certificate - there is no need to pay a Certification Authority for a trusted SSL Certificate.

The "not trusted" warning message will even let the customer know that the website can provide encryption, it does not provide trust.

Without sufficient validation processes, SSL Certificates are simply encryption certificates in other words they are not trusted certificates, **they are simply browser recognized certificates**.

A Certification Authority that does conduct a sufficient two-step validation (as in above) is a **trusted certificate.**

**The commercial dangers of weak validation**

Companies using weakly validated Certificates risk losing the trust of customers who rely on such Certificates when they discover the Certificate stands for "encryption" only. Without the assurance that the company behind the site is legitimate, the customer will go elsewhere to conduct their business. Can a company really afford to lose customers simply because of their choice of SSL provider?

Only by choosing a strongly validated SSL Certificate from a provider who performs two-step validation processes can the user expectations of SSL be realised, and ultimately preserved. Consumers have long associated SSL with more than just encryption. Yet, by removing sufficient validation, the Certificate Authority is not fulfilling its responsibilities to deliver the trust in a "trusted certificate".

In an environment where trust goes hand in hand with commercial success, removing validation from the very products used to provide such trust is not only dangerous but also poses a long term threat to the Internet economy.

SSL Providers retailing non-validated Certificates will often attempt to sell a "Trust" only product. The downside to this exercise is that websites are forced to purchase both an SSL Certificate and a Trust product just to gain both encryption and trust functionality, whereas a fully validated SSL Certificate can already provide both.

Comodo, like Verisign, Thawte, Baltimore and Entrust, is serious about the validation employed in SSL Certificate applications. If you wish to maintain the trust of your customers, we strongly believe that you should be serious about validation too.

**Comodo Instant SSL - the only low cost fully validated SSL Certificate**

In May 2002 Comodo launched InstantSSL, the only low cost fully validated SSL Certificate. Prior to the launch of InstantSSL, GeoTrust offered the industry's cheapest SSL certificates through the QuickSSL brand (the low price being attributed to the due absence of strong validation processes). However, Instant SSL certificates are less than half the price of GeoTrust QuickSSL certificates, issued quickly, and unlike GeoTrust QuickSSL and IPSCA certificates, Instant SSL certificates are fully validated.

**What an SSL Certificate should tell the site's visitors**

Comodo is at the forefront of providing fully qualified SSL Certificate. Digital Signature legislation is catching up to how SSL certificate are used commercially and appreciates that applications such as SSL mean much more in commercial terms than just encryption. The EU Directive on Digital Signature is considered by many to be a milestone in how online identities and transactions are being aligned in legal terms with their physical world counterparts.

Part of the directive covers "Qualified Certificates" - Digital Certificate that have been issued to validated entities, and whose identities are contained within the certificate itself.

Comodo's Instant SSL Certificates contain the following critical identification information within the SSL Certificate:

Common Name - the fully qualified domain name for which the SSL Certificate is to be used  
Organization Name  
Organization Unit  
Street Address  
City / Town  
State / Province  
Zip / Postal Code  
Country

All the above information is validated quickly and efficiently by Comodo, ensuring customers receive their Certificate quickly but without the risks associated with weak validation. This places Comodo at the forefront in delivering SSL Certificate that comply with legislation even before it becomes law to do so!

**InstantSSL - combining strong validation with low costs**

Comodo is the only SSL Provider to offer responsible companies the option of low cost, fully validated and highly trusted SSL certificates. With the availability of InstantSSL, there is no longer any need to opt for more expensive non-validated, untrustworthy encryption-only SSL certificates.

