thawte®

SSL Validation Guide

Understanding the art and science of SSL certificate validation and how to pick the right approach for your business

An essential guide from Thawte

WHITE PAPER 2015

SSL certificates don't range from 'insecure to 'secure', but they do differ in the level of confidence they inspire in online visitors. This whitepaper helps you choose the level of validation that works for you.

With web-based attacks up by 23 percent in 2013 and phishing scams becoming ever more sophisticated, trust is in short supply online.[1]

E-commerce businesses, dealing with sensitive financial information, in particula , need to step up to the plate and provide the right assurances to customers if they want to see increased conversion rates and fewer abandoned carts.

But this isn't just a problem for e-commerce. Almost every website involves some exchange of information, whether it's login details for an online application or contact details on a landing page, and visitors want to know that their information is secure. So deploying an SSL certificate from a trustworthy Certificat Authority (CA) like Thawte is a must for any site owner.

But what sort of SSL certificate works for you? How can you tell your common-or-garden domain validatio from your extended validation?

All SSL certificates are equal, but some are more equal than others

The most crucial thing to note is that all three levels of SSL certification essentially do the same thing: they check the legitimacy of the domain owner and they enable the encryption of information exchanged on your website, be it credit card information or an email address. In essence, each level provides exactly the same standard of security.

Where they differ is in the extent of vetting involved and, therefore, how long the validation takes to complete – from minutes for domain validation to up to ten business days for extended validation – and how much confidence they command.

- **Domain Validation (DV).** This is the lowest level of authentication used to issue SSL certificates. The CA will issue a domain-validated certificate to anyone who is listed as the domain admin contact in the WHOIS record (the public record associated with each domain name) simply by sending an email to the contact email address. As a result, domain-validated certificates are issued very quickl , but no company information is checked or displayed on the certificate, making it easier for internet criminals to gain this type of certificate from irresponsible CA

- **Organisation Validation (OV).** OV is the more secure step up from DV. As well as checking up on the ownership of the domain name, the CA will also carry out additional vetting of the organisation or individual applying for the SSL certificate. This might include checking the address where the company is registered and the name of a specific contact. This vetted company information is displayed to visitors on the certificate, making the ownership of the site much more visible.

1 http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

- **Extended Validation (EV).** This is the gold standard in SSL certificates, delivering the highest level of consumer trust through the strictest authentication standards. EV verification guidelines, drawn up by the C Browser Forum, require the CA to run a much more rigorous identity check on the organisation or individual applying for the certificate. This can be a time consuming process, but it's worth it. Sites with an EV SSL certificate have a green browser address bar and a field appears with the name of the legitimate website owner and the name of the security provider that issued the certificate. These clear visual cues reassure the visitor that they're dealing with a legitimate site that cares about their security.

The right tools for the job

But it's not a simple case of DV bad, OV okay, EV good – they all have their uses. It all depends on what sort of business you're running and what you're using the SSL certificate fo .

- Domain-validated certificates, like **Thawte SSL 123**, work well for situations where trust and credibility are less important because the site is not customer facing, like an internal server, mail server or test and development servers. DV can also work in instances where there is no ambiguity about who owns the domain because your business is known by its domain name, like google.com.

- Given the more thorough vetting process, an organisation validation certificate, lik **Thawte SSL Web Server Certificate**, is a good option for public-facing websites that deal with less sensitive transactions, allowing visitors to view your company information on the certificate. If you're asking visitors to sign up for a whitepaper or eBook, for instance, you might deploy an OV SSL certificate

- **Thawte SSL Web Server Certificates** with EV are really a must-have for e-commerce and websites handling sensitive information, such as insurance records. The obvious visual assurances put the customer at ease and give them the green light to purchase more and more often, meaning you can quickly recoup the extra cost of an EV certificate in the form of increased revenue. Also, if there's some ambiguity that you own a particular domain name, because it differs from your company name, for example, you should consider an EV to reassure visitors that it's a legitimate site under your ownership

What you're choosing between, therefore, is not the level of security – they all offer the same encryption ability – but rather the level of trust you need.

Backing the right horse

For that reason, the Certificate Authority you choose to issue your SSL certificate from is nearly as important as the sort of certificate you deplo .

Seeing a well-known name on the certificate, in the browser address bar or on the trust marks provided by the C when you've been issued the SSL certificate, makes a big di ference in the level of confidence you inspire in visitors and can positively impact your bottom line by boosting long-term revenue.

And experimenting with the placement of these seals can make an even greater impact.

A highly reputable Certificate Authority like Thawte, the original international specialist in online security, gives you the credibility that your customers are looking for when assessing your website, no matter what sort of SSL certificate you choose.

Protect data in transit with an SSL certificate from Thawte today.

Not All SSL Is the Same

We make SSL our business in order to protect yours. Thawte online security is trusted by millions of people around the world. Here are just a few reasons to switch to Thawte:

- High- assurance digital certificates
- Global reputation for uncompromised reliability
- Up to 256-bit SSL encryption
- World-class, multilingual support
- New, lower prices that are within your security budget
- Thawte Trusted Site seal

Protect your data, safeguard your business, and translate trust to your customers with high-assurance, digital certificates from Thawte.

Visit www.cheapSSLsecurity.com or email support@cheapSSLsecurity.com

Protect your business and translate trust to your customers with high-assurance digital certificates from Thawte, the world's first internationa specialist in online security. Backed by a 17-year track record of stability and reliability, a proven infrastructure, and world-class customer support, Thawte is the international partner of choice for businesses worldwide.