

# Understanding Validation

UNDERSTANDING THE ART AND SCIENCE OF SSL CERTIFICATE VALIDATION AND HOW TO  
PICK THE RIGHT APPROACH FOR YOUR BUSINESS

# Validation

SSL certificates don't range from 'insecure' to 'secure', but they do differ in the level of confidence they inspire in online visitors. This white paper 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.<sup>1</sup>

E-commerce businesses, dealing with customers sensitive data, in particular 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 certificate authority (CA) like Thawte is a must for any site owner.

But what sort of SSL certificate works best for you? How can you tell your common-or-garden domain validation 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, such as 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 quickly, 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 CAs.
- **Organization 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 organization and 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.
- **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 CA Browser Forum, require the CA to run a much more rigorous identity check on the organization 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 for.

<sup>1</sup> [http://www.symantec.com/content/en/us/enterprise/other\\_resources/b-istr\\_main\\_report\\_v19\\_21291018.en-us.pdf](http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf)

- 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 organization validation certificate, like [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 white paper or eBook, for instance, you might deploy an OV SSL certificate.
- EV is really a must-have for e-commerce and websites handling sensitive information, such as insurance records and credit card information. 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. For example, many organizations quickly recoup the cost of an EV certificate in the form of increased revenue due to the increase of conversion rates. 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 is nearly as important as the sort of certificate you deploy.

Seeing a well-known name on the certificate, in the browser address bar or on the trust mark, like the Thawte True Site Seal, makes a big difference in the level, makes a big difference 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.

### To learn more, contact our sales advisors:

- **Via phone**
  - US toll-free: +1 888 484 2983
  - UK: +44 203 450 5486
  - South Africa: +27 21 819 2800
  - Germany: +49 69 3807 89081
  - France: +33 1 57 32 42 68
- **Email [sales@thawte.com](mailto:sales@thawte.com)**
- **Visit our website at <https://www.thawte.com/log-in>**

*Protect your business and translate trust to your customers with high-assurance digital certificates from Thawte, the world's first international 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.*