Boost Customer Trust with Validation

How to Select the Right SSL/TLS Certificate Validation for Your Business

Symantec Website Security
The last 5 years have shown a steady increase in attacks targeting businesses with <250 employees.

Over the past three years, more than 3/4 of websites scanned contained unpatched vulnerabilities, one in seven of which were deemed critical. And the last five years have shown a steady increase in attacks targeting businesses with less than 250 employees.¹

E-commerce businesses 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.

---

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Validation Process</th>
<th>Trust Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Validation (DV)</td>
<td>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) 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.</td>
<td>Low</td>
</tr>
<tr>
<td>Organization Validation (OV)</td>
<td>The CA will check up on the ownership of the domain name and carry out additional vetting of the organization and individual applying for the SSL/TLS certificate. This might include checking the address where the company is registered and the name of a specific contact. This takes a bit longer than DV, but not as long as EV.</td>
<td>Moderate</td>
</tr>
<tr>
<td>Extended Validation (EV)</td>
<td>The CA runs a rigorous identity check on the organization and individual applying for the certificate.</td>
<td>High</td>
</tr>
</tbody>
</table>

---

¹Source: [Symantec](https://www.symantec.com)
Almost every website involves some exchange of information. Whether it’s login details for an online application, or contact details on a landing page, site visitors want to know that their information is secure, and they won’t spend time on a site that they don’t trust. Many studies show that visitors are influenced by security indicators and trust marks displayed on websites and in browser address bars.

Unencrypted Sites to Be Marked “Non-Secure”
Google and other browsers are starting to flag non-secure sites that accept credit cards or use passwords. This is just the first step in a series of changes that will eventually include additional negative visual indicators many browsers will use to mark unencrypted websites. That’s why deploying the right SSL/TLS certificate from a trustworthy certificate authority (CA) is a must for any site owner.

Whether or not you accept credit cards or use passwords, now is the time to secure your site and start getting the advantages of increased visitor trust, a better search ranking and more control over what users see on your site.

Which Certificate Should You Choose?
From server administrators, to product managers, down to the one-person startup, at one stage or another, the same question pops up: “Which certificate do I need?”

Today there are three types of certificates that offer three levels of user trust for SSL/TLS negotiations: Domain Validation certificates (DV), Organization Validation certificates (OV) and Extended Validation certificates (EV).

All three levels of SSL/TLS certification check the legitimacy of the domain owner and enable the encryption of information exchanged on your website, such as credit card information or an email address. Where they differ is in the extent of vetting involved, how long the validation takes to complete and how much visitor trust they command.

EV is a must-have for websites that handle sensitive information.

Domain validation certificates 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 server.

However, the major concern with DV certificates is they are so easy to obtain that phishing sites increasingly use them to trick unsuspecting visitors into thinking they have a valid, safe website.

This certificate also does not contain any identifying information in the organization name field (the field may say “Persona Not Validated”). This leaves visitors unable to confirm the identify or safety of a DV website.

For these reasons, websites that require sensitive visitor information like passwords and credit card numbers cannot afford to take a risk with DV certificates and should go with a higher level of authentication.
Organization validation displays the final vetted company information for visitors, making the ownership of the site much more visible. Given the more thorough vetting process, OVs are a good option for public-facing websites that deal with less sensitive transactions since they allow visitors to view your company information on the certificate. If you're asking visitors to sign up for a white paper or e-book, for instance, you might deploy an OV SSL/TLS certificate.

Extended validation is the gold standard in SSL/TLS certificates, delivering the highest level of visitor trust through the strictest authentication standards. Extended validation certificates also offer added benefits like higher warranties, which lower your legal and financial risk in the event of a breach. As compared to OV, the CA runs an even more rigorous identity check on the organization and respective contact from the organization applying for the certificate. This can be a time-consuming process, but it's worth it to boost customer trust and eliminate risks.

EV is a must-have for websites that handle sensitive information, such as insurance records, credit card information or personally identifiable information (PII). PII is any data that could potentially identify a specific individual such as a full name, address, date of birth or telephone number. Also, if there's some ambiguity about whether or not 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. The assurances EV provides put customers at ease and give them the green light to purchase more and more often. Many e-commerce organizations quickly recoup the cost of an EV certificate through increased revenue from the increased conversion rates they see.

The visual cues offered by all validation certificates reassure visitors that they're on a legitimate site that they can trust. That's why choosing the right certificate is less about selecting the right level of security—and more about selecting the level of trust you need to gain to turn site visitors into repeat customers.

Reputable Certificates Can Turn Visitors Into Customers
Certificate Validation offers your visitors varying levels of confirmation that your site has been validated by a third party that confirms that your organization is real and authentic, and that any data transit is secure and encrypted. Just as your visitors would be influenced by seeing positive feedback and ratings about your business, having a certificate provides the same kind of clues to your visitors from a reputable source.

Because trust is so important, the certificate authority you choose to issue your SSL/TLS certificate is nearly as important as the kind of certificate you decide to deploy. You want to be backed by a name that not only you, but also your visitors, know and trust. No matter what kind of SSL/TLS certificate you choose, a highly reputable certificate authority like Symantec gives you the credibility that your customers look for when assessing your website.

Seeing a well-known name like Symantec inspires more confidence from visitors and can boost long-term revenue. To learn more about choosing the right certificate that will gain the most customer trust for your business, contact a sales representative today.

To learn more, contact our sales advisors:

- **Via phone**
  U.S. toll-free: 1-866-893-6565

- **Visit our website at**
  www.symantec.com/ssl
For global offices and contact numbers, please visit our website.

For product information in the U.S., call: 1-866-893-6565 or 1-520-477-3111

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/ssl

For product information in Asia Pacific, call:
Australia: +61 3 9674 5500
New Zealand: +64 9 9127 201
Singapore: +65 6622 1638
Hong Kong: +852 30 114 683

Symantec Website Security Solutions Pty Ltd:
3/437 St Kilda Road, Melbourne, 3004
ABN: 88 088 021 603
www.symantec.com/en/aa/ssl-certificates

For product information in the Americas (Non-U.S.), call:
Mexico: 554 738 0448
Brazil: 800 038 0598

For product information in the U.K., call:
0800 032 2101 or +44 (0) 208 6000 740

Symantec (UK) Limited.
350 Brook Drive
Green Park, Reading
Berkshire, RG2 6UH UK
www.symantec.co.uk/ssl

For product information in Europe, call:
+353 1 793 9053 or +41 (0) 26 429 7929
Germany: 0800 128 1000
France: 0800 90 43 51
Spain: 900 93 1298

Follow Us: