WHAT DO YOU MEAN I NEED AN SSL/TLS CERTIFICATE!
A Guide to SSL/Certificates and Their Use Cases
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is an SSL/TLS Digital Certificate?</td>
<td>3</td>
</tr>
<tr>
<td>EV or OV SSL/TLS Certificates</td>
<td>5</td>
</tr>
<tr>
<td>Domain Validated (DV) Certificates</td>
<td>7</td>
</tr>
<tr>
<td>Choosing the Right SSL/TLS Certificate</td>
<td>7</td>
</tr>
<tr>
<td>Use Cases for Common IT Environments</td>
<td>SSL/TLS Certificates</td>
</tr>
<tr>
<td>HTTPS Connection for a Single Domain</td>
<td>6</td>
</tr>
<tr>
<td>HTTPS Connection for Multiple Domains</td>
<td>6</td>
</tr>
<tr>
<td>Microsoft Exchange, Lync or Skype for Business Server</td>
<td>6</td>
</tr>
<tr>
<td>Server to Server</td>
<td>7</td>
</tr>
<tr>
<td>Front-end SSL/TLS Offloading</td>
<td>7</td>
</tr>
<tr>
<td>Enterprise Environment</td>
<td>8</td>
</tr>
<tr>
<td>Visual Indicators in the UI</td>
<td>9</td>
</tr>
<tr>
<td>Here’s Why SSL/TLS is Important to Organizations of All Sizes</td>
<td>10</td>
</tr>
<tr>
<td>Conclusion</td>
<td>11</td>
</tr>
<tr>
<td>Entrust Datacard - Recommended SSL/TLS Certificates</td>
<td>12</td>
</tr>
<tr>
<td>Two + domains</td>
<td>12</td>
</tr>
<tr>
<td>Microsoft Exchange, Lync or Skype for Business Server</td>
<td>12</td>
</tr>
</tbody>
</table>
WHAT IS AN SSL/TLS DIGITAL CERTIFICATE?
Organizations of all types and sizes employ SSL/TLS digital certificates to provide security in the form of encryption technology and in most cases identity assurance. Mostly the use of SSL/TLS certificates is voluntary; however, certain industry activity and local regulations can make it difficult for organizations to do business online without them.

SSL/TLS certificates can only be issued by a certification authority (CA) under the guidelines put forth by the CA Browser Forum. Used for website encryption and identity assurance SSL/TLS are arguably the most common type of digital certificate. The differences between the varieties of SSL/TLS certificates offered lie beyond the technology but instead are rooted in the level of trust you’re providing to the website visitor, as well as your relationship with the issuing CA and their reputation as a reliable and trustworthy vendor. If the issuing CA has a reputation for being “phishy”, chances are you’re not providing optimal security or much trust to your online customers.

Consumers expect the financial services institutions and ecommerce businesses that they transact with to secure their personal data. The SSL/TLS certificate prevents a third-party from hijacking personal information (e.g., user names, passwords and credit card information) while it is being transmitted from the customer’s device (client) to the organization (server).

Organizations want to protect private customer data and prevent browser error messages from thwarting website traffic. Browsers send up trust dialog boxes alerting website visitors when a website is not encrypted or if an SSL/TLS certificate has expired. Some major browsers require encryption on web pages where any customer data is requested regardless of whether or not it is a financial transaction (e.g., email address for newsletter registration).
SSL/TLS certificates serve two purposes – they encrypt information and provide identity assurance, which help online consumers to positively identify websites that are safe for transacting with. This is how an SSL/TLS certificate works:

The three SSL certificate types that provide public trust, in other words, over the Internet rather than internally, are: extended validation (EV), organization validated (OV) and domain validation (DV) certificates. Higher assurance SSL certificates like EV and OV strengthen security by including verified organization identity information in the certificate that was confirmed by an independent CA. This tells website visitors that the website is associated with a real organization, which is important information to prevent fraudulent activity like phishing. DV certificates provide the same level of encryption, but they are easy to attain anonymously and therefore are the highly preferred certificate of choice for fraudsters to use on their websites.

The regulating authority for online payments, PCI, makes this recommendation in their PCI Data Security Standard.

**Recommendations**

*For a relatively small additional cost (compared to a DV certificate), a legitimate business conducting e-commerce could purchase an OV or EV certificate. This would prove to the consumer the business has been validated by the CA and has provided address and other independently verified contact information in the certificate that the consumer could use in case of questions or problems. In addition, EV certificates provide another benefit: a visual cue (the green bar) in the browser tells the consumer the business has gone through the effort to obtain this enhanced certificate, the information has been verified by the CA, and there is a higher probability that online trust can be established.*

Higher assurance certificates come with a higher price tag. The amount of verification checking behind the various certificate types attribute to the pricing variations. The cost of a higher assurance certificate is small especially when considering the costs incurred when an organization suffers data breach.
**EV OR OV SSL/TLS CERTIFICATES**

A mix of EV and OV certificates are widely used by organizations that want to provide their customers with strong encryption technology as well as deliver identity assurance. Identity assurance helps customers recognize whether or not a website is legitimate. It also prevents the brand from suffering damaging losses associated with phishing scams and other nefarious online activity.

EV and OV certificates are used primarily for client-to-server transactions where sensitive information (e.g., user name, password, credit card information, etc.) is being transferred over the Internet. Encryption ensures the data cannot be stolen as it makes its way to the organization. The identity piece gives website visitors the ability to positively identify the website that they're on.

The amount of verification checking behind the various certificate types is reflected in the pricing variations. The increased vetting for EV particularly and OV certificates is what makes high assurance certificates more expensive. EV certificates come with the most comprehensive verification checking, which includes domain verification, cross-checks among several governmental and internal checkpoints that ties the entity to a specific physical location. This type of verification leaves a detailed paper trail where customers have recourse should they be victimized by any nefarious activity that takes place while transacting on that website. EV certificates are distinguished with a locked padlock, organization name and sometimes country ID in the web address bar in most major browsers. The organization's details can be found by clicking on the padlock and searching the certificate details, which is available on some major web browsers.

In addition to domain ownership, the organization is validated for OV certificates and the certificate details can be viewed on most major web browsers.

Major browsers indicate that a website is secured with DV certificate by the padlock with HTTPS in address bar, but do not show organization details because they do not exist. These certificates validate domain ownership only, and do not tie a domain to a person, place or entity.

---

DOMAIN VALIDATED (DV) CERTIFICATES

DV certificates are great at separating encryption from authentication. In the absence of identity checks, DV certificates lack the critical component of having an identifiable paper trail, and that’s where they differ from EV or OV certificates. All three certificate types provide the same strong level of encryption technology.

DV certificates are best used for situations that do not necessitate the important aspect of identity assurance making them a good choice when rapid acquisition of encryption based technology for server-to-server communication is needed. DV certificates can be recommended for the following use cases:

- Basic websites that do not require personally identifiable information (e.g., email address, usernames, passwords, credit card information, etc.)
- Digitally transfer software updates

The purpose of a DV certificate is to provide IT professionals with a fast and affordable way to encrypt non-sensitive data that is passed over the Internet. Some CAs issue DV certificates via an automated process at no charge, the domain owner doesn't even supply a credit card. The automated issuance of DV certificates has led to an increased number of certificates, allegedly used for phishing sites according to Vincent Lynch, hashedout, by the SSL Store. This protects the fraudster’s identity clearing the way for them to commit fraud.

Lately, there has been some discussion among industry leaders surrounding the context for using DV certificates and whether or not it is sufficient for ecommerce transactions.

Major browsers indicate that a website is secured with a DV certificate with only the padlock with HTTPS identifiers in address bar.

CHOOSING THE RIGHT SSL/TLS CERTIFICATE

When you understand your customer’s unique business needs, you will be able to recommend the right SSL/TLS certificate or certificate mix to encrypt their web application(s). Here are some good questions to help you drill down to the particular SSL/TLS certificate type(s) to recommend.

1. **What will the SSL/TLS certificate be used for?**
2. **How much protection do you want to provide to your business and your customers?**
   - What level of identity assurance do you want to provide online shoppers?
   - How important is it to protect your brand from phishing scams?
3. **How many domain names need to be secured on this certificate or server?**
   - Are there multiple servers?
4. **What is your budget?**

Refer to the “Use Cases” section of this white paper to match the certificate type(s) that is recommended to suit the business purpose.
USE CASES FOR COMMON IT ENVIRONMENTS | SSL/TLS CERTIFICATES

HTTPS Connection for a Single Domain
This represents someone with a basic website that has only one possible domain via HTTPS (e.g., https://www.example.com)

**Recommendation**
1. If sensitive information is requested (e.g., login or credit card transactions) for client-to-server transmissions, EV is recommended for highest identity assurance and the added visual cue or OV for identity assurance.
2. Sensitive information is not requested, but the customer wants the SEO benefits of HTTPS visual indicator or needs to transfer non-sensitive information from server-to-server (e.g., software updates), DV certificate.

HTTPS Connection for Multiple Domains
Useful for an organization with a basic Website secured with SSL/TLS and the site allows multiple domains for HTTPs delivering the same web content (e.g., https://www.example.com and https://example.com)

**Recommendation**
1. If sensitive information is requested (e.g., login or credit card transactions) for client-to-server transmissions, EV is recommended for highest identity assurance and the added visual cue or OV for identity assurance.
2. Sensitive information is not requested, but the customer wants the SEO benefits of HTTPS visual indicator or needs to transfer non-sensitive information from server-to-server (e.g., software updates), 2 DV certificates; one for each URL.

Microsoft Exchange, Lync or Skype for Business Server
A unique domain for each service is usually required in desktop client-to-server environments using a Microsoft Exchange server: Webmail/IIS, SMTP, POP, IMAP and UM

**Recommendation**
1. To secure multiple domains on one certificate, a UC Multi-domain/SANs certificate is recommended. UC Multi-domains are also useful whenever there’s a need to secure multiple names across different domains.

Server to Server
Situations when mutual authentication between two servers is needed and the certificate extension, EKU, requires client authentication (e.g., Exchange TLS between two organizations where one organization has a server with data that it needs to send it to a third party for processing. This is where mutual authorization is used, which does not require a browser)

**Recommendation**
1. OV that supports Client and Server Authentication.
Front-end SSL/TLS Offloading
When an SSL/TLS connection needs to be offloaded from servers to a front-end device (e.g., F5 BIG IP), individual servers do not require a certificate, and EKU requires server authentication.

Reccomendation (see image)

a. 1 OV certificate for each server

b. EV certificate(s) to secure each server
   SAN = buy.example.com
   SAN = managed.example.com
   SAN = discovery.example.com

c. UC Multi-domain, secures multiple domains on one certificate
   SAN = buy.example.com
   SAN = managed.example.com
   SAN = discovery.example.com

d. Wildcard, if they share a common root domain (e.g., *.example.com)
Enterprise Environment
A typical enterprise environment uses a variety of SSL/TLS certificates to encrypt communication throughout their diverse IT ecosystems.
VISUAL INDICATORS IN THE UI

Although all EV certificates are subject to the same rigorous vetting guidelines, each browser has autonomy when it comes to how they appear in the web address bar. Let’s take a look at how EV certs appear in the most popular browsers.

**Google Chrome**
Google Chrome is the most widely used browser worldwide. It’s interesting that when it comes to SSL/TLS certificates they use a binary systems that indicates whether a website is encrypted or not omitting the identifying information the further details that help users determine website authenticity.

![Google Chrome](image)

Check for locked padlock, company name and optional two character country ID

**Internet Explorer**
Internet Explorer is another popular website. Their browser provides a pathway for website visitors to view certificate details before deciding whether or not to interact with a website.

![Internet Explorer](image)

Click here to drill down to certificate details and view identity information

**Safari**
Safari is widely used by Mac users and provides an easy method for their users to determine website identity.

![Safari](image)

Click her to drill down to certificate details and view identity information

The visual indicators depicted here were current at the time of publishing and are subject to change.
HERE’S WHY SSL/TLS IS IMPORTANT TO ORGANIZATIONS OF ALL SIZES

Some major browsers require websites to have the security of an SSL/TLS certificate on web pages that request personal information (e.g., username, password, credit card information, etc.) to ensure that end-user transactions are encrypted. Some like Google Chrome reward encrypted websites with more favorable search rankings.

Web pages that are not protected with an SSL/TLS certificate may show a browser warning flagging your website as unsecure when a visitor approaches. Imagine a customer or prospect being greeted by this when they navigate to your website?

![SSL/TLS Warning Example](image_url)

Browsers also downgrade SSL/TLS certificates if certain conditions are not met – for example, an expired or revoked certificate (see image below) can also trigger a browser warning to website visitors.

![SSL/TLS Warning Example](image_url)

An expired SSL/TLS certificate might show this web browser warning

The visual indicators depicted here were current at the time of publishing and are subject to change.
CONCLUSION
Maintaining a trusted and valid SSL/TLS certificate is an important part of ecommerce. Encryption and identity assurance gives online customers confidence to transact on a website. And, it’s important for domain owners to comply with the practices established by the major web browsers to avoid browser warnings that could scare a customer away from the website. Having the right SSL/TLS certificate in place for your use case provides a trusted connection for customers to transact and a more secure Internet for organizations and the people who use it.