PRO TIPS:
PICKING THE RIGHT SSL CERTIFICATE

You know that many consumers are still wary about shopping online, and with good reason—faulty security has led to hundreds of thousands of credit card numbers being shared publicly. You also know that without the consumer confidence that comes from a secure site, a potential sale can be stopped dead in its tracks. This article teaches you how to be a savvy SSL Certificate shopper by explaining the technology and terminology behind SSL Certificates.

INTRODUCTION

You know that many consumers are still wary about shopping online, and with good reason—faulty security has led to hundreds of thousands of credit card numbers being shared publicly. You also know that without the consumer confidence that comes from a secure site, a potential sale can be stopped dead in its tracks.

Knowing this, you've decided that you need to purchase an SSL Certificate. But with so many different vendors, options, and so much complicated technology, you're not sure which certificate to choose.

You're not alone—many organizations know that online security is one of the most important parts of their business but don't have the background to be able to make the right decisions for their company. Because of this, purchasing an SSL Certificate usually leads to a lot of unnecessary headaches and additional costs.

This article teaches you how to be a savvy SSL Certificate shopper by explaining the technology and terminology behind SSL Certificates. With this information, you can break down the types of SSL Certificates that are available. This article also gives you a list of things to think about when deciding on an SSL Certificate vendor—like reputation, warranty, customer support, and free tools. And most importantly, this article will help you decide exactly which SSL Certificate(s) you need in your environment—so that you don't have to waste your money on certificates you don't need.

WHAT IS A CERTIFICATE AUTHORITY?

A Certificate Authority (CA) issues certificates to organizations and individuals. Publicly-trusted CAs each have different products, prices, features, and levels of customer satisfaction.

Browsers come with a pre-installed list of trusted CAs. These CAs have a root certificate in the browser's trusted root store. Publicly-trusted CAs are required to adhere to certain standards, meet audit requirements, and be approved by the browser operator, such as Microsoft, Mozilla, Opera, Oracle (Java), and other similar companies. SSL Certificates issued by trusted CAs establish an encrypted link between a website and a browser without displaying a warning message.

An SSL Certificate issued by a CA to an organization and its domain/website verifies that a trusted third party (the CA) has authenticated the certificate issued to that organization. Since the browser trusts the CA, the browser now trusts that organization's identity too. The browser lets users know that the website is secure, and the user feels safe browsing the site and even entering their confidential information.

Note that a private CA (one not inherently trusted by browsers) can issue certificates. However, only certificates from a publicly-trusted CA will prevent warning messages.

ABOUT VALIDATION

Validation refers to the process through which a CA verifies a certificate applicant's information before issuing them a certificate. There are currently three levels of validation: Extended Validation (EV), Organization or Business Validation (OV), and Domain Validation (DV).

Why Is the Level of Validation Important?
As discussed, CAs verify information about the organizations or individuals applying for a certificate. This is because SSL Certificates not only create secure, encrypted connections, but they also indicate the legitimacy of a website and the company behind it.

As ecommerce expands, customer trust is essential to financial success, customer conversion, and business growth. However, cybercriminals are becoming increasingly adept at fooling customers into thinking they are a legitimate website by purchasing low-validation certificates. A CA that does not conduct a thorough validation process is simply issuing an SSL Certificate to bypass a browser warning message. Though the certificate will be recognized by the browser because it is publicly trusted, the certificate does not prove that the company that owns the certificate is real.

With Organization Validation (OV), a CA representative contacts the requesting organization, checks the right of the applicant to use a specific domain name, and conducts some vetting of the organization.

Extended validation (EV) SSL Certificates were specifically created to repair and maintain customer confidence in ecommerce through specific, EV certificate-only browser cues like the green address bar. Extended validation raises the bar for the SSL validation processes, incorporating some of the highest standards for identity assurance to establish the legitimacy of online entities. Because of this rigorous verification process, customers can be assured that anyone with an EV certificate is who they say they are.

THE LEVELS OF VALIDATION

Extended Validation (EV)

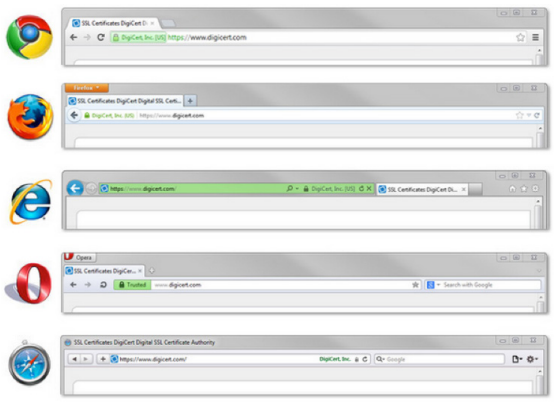
Extended Validation is the highest level of authentication. In 2007, some of the major CAs and web browsers came together to create a new type of SSL Certificate called the EV SSL Certificate. EV SSL Certificates are specifically targeted at repairing and maintaining customer confidence in ecommerce through a rigorous verification process and specific, EV certificate-only browser cues. EV certificates incorporate some of the highest standards for identity assurance to establish the legitimacy of online entities. CAs put applicant websites through rigorous evaluation procedures and meticulous documentation checks to confirm their authenticity and ownership. Any CA offering EV certificates has to comply with a strictly defined process created by the CAs and web browsers. This validation process includes:

- Verifying the legal, physical, and operational existence of the entity
- Verifying that the identity of the entity matches official records
- Verifying that the entity has exclusive right to use, or control over, the domain specified
- Verifying that the entity has properly authorized the issuance of the certificate

As part of this process, a CA representative contacts the requesting organization at a verified phone number to confirm that they requested the certificate and that the applicant is authorized to receive the certificate on behalf of the organization. By maintaining this human element in the validation process, it is very likely that fraudulent or phishing-related activity will be detected and prevented.

Because of the intensive work that is involved in the validation process, EV certificates can take longer to issue. However, some CAs have faster issuance times than others. For example, DigiCert® can usually issue EV SSL Certificates in a matter of hours rather than days. Browsers use visual cues to inform users about websites secured with an EV certificate. EV certificates include the following visual benefits:

- Green in the address bar
  (green bar or issuance name, see below)
- Website owner's company name in the address bar
- https:// at the beginning of the domain name
- Padlock in the address bar
- Organization information in the certificate details

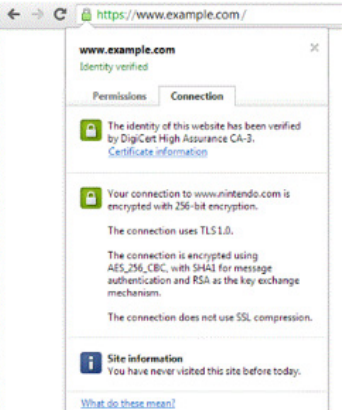


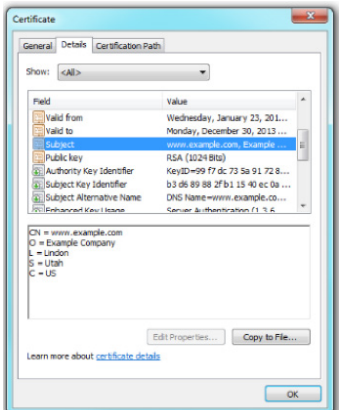
Organization Validation (OV) or Business Validation
OV certificates are also sometimes called high-assurance certificates and require that a CA representative contacts the requesting organization. The CA checks the right of the applicant to use a specific domain name and conducts vetting of the organization. Depending on the CA, a representative might complete this process—maintaining the human element.

The difference between OV and DV (low-validation certificates, see the next section) certificates is that your validated organization information will be in the certificate details (see the screenshots below).

OV certificates include the following visual benefits:

- https:// at the beginning of the domain name
- Padlock in the address bar
- Organization information in the certificate details (shown below)





Domain Validation (DV)
Domain Validation is the lowest level of validation. For Domain Validation, the CA checks that the applicant has either control over, or the right to use, the domain. The certificate only includes the domain in the certificate and does not include the business or organization name. With DV certificates, no company information is vetted.

To verify a company that has requested a DV certificate, the CA usually contacts the domain owner (in the WHOIS record) and makes sure that they requested the SSL Certificate. This is usually done through an automatic process, but may also be done by phone. The CA does not check who the domain owner really is or whether the business associated with the domain is real. This can be dangerous because an attacker could buy a domain specifically for a phishing or man-in-the-middle attack and still get a certificate.

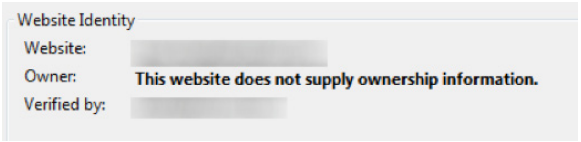
However, because human intervention is minimized and there are no validation checks, DV certificates are inexpensive and can be issued quickly. If you have budget constraints or can't wait for a more robust issuance process, a DV certificate may be a good option. However, DV certificates should not be used by ecommerce websites or websites handling sensitive customer information.

Because of the risk associated with DV certificates, not all CAs issue them.

DV certificates include the following visual benefits:

- Add the https:// at the beginning of the domain name
- Display the padlock in the address bar

Note: The certificate details will not contain any information other than the domain name and the certificate issuer name. See screenshot below for example.



TYPES OF CERTIFICATES

Every CA will have different names for their certificates—premium SSL Certificate, Wildcard Plus Certificate, Secure Site Pro Certificate, etc. But when it comes down to it, there are only a few types of SSL Certificates. Now that you understand the different levels of validation, all you need to be able to interpret certificate names is the underlying types.

Single-Name SSL Certificates

Single-name SSL Certificates are the most basic type of SSL Certificate. They provide encryption and validation for users and cover one domain/server. Most CAs have their own names for single-name certificates, like SSL Plus Certificate or Secure Site Certificate. Single-name SSL Certificates provide essentially the same encryption regardless of CA.

However, features and benefits of the certificate will vary largely between companies. For example, with some CAs a certificate for www.yoursite.com will not also work with yoursite.com. DigiCert is one of the few CAs that offers this benefit with all of their certificates.

Wildcard Certificates

Wildcard certificates secure a domain and all of its first-level subdomains. For example, a certificate for *.example.com secures www.example.com, mail.example.com, etc. A standard SSL Certificate would only secure www.example.com, requiring you to purchase an additional certificate for mail.example.com. Wildcard certificates cost more than single-name certificates, but if you have multiple subdomains it's usually worth the money you will save by not buying multiple single-name certificates.

However, wildcard certificates can pose potential problems. For example, if one of your servers is hacked and someone takes your private key, any systems secured by that key/certificate (potentially your entire network) could be compromised. To re-secure your environment you would have to reinstall the certificate on every server. If you have a wildcard certificate in your environment you simply need to have heightened security practices to keep problems like this

from happening. Mark all certificates as non-exportable and limit access to the servers that have your private key on them. You can also purchase a DigiCert wildcard certificate. With a DigiCert wildcard certificate you can issue and install unlimited duplicates rather than installing the same certificate on every server. Each duplicate has a different key pair, so if one duplicate was compromised, you would only have to replace that certificate.

Note that due to the EV process requirements EV wildcard certificates are not available.

SAN/Unified Communications (UC)/ Multi-Domain Certificates

SAN certificates (also called UC or multi-domain certificates) use Subject Alternative Names to secure a certain number of domains, sites, and subdomains with one certificate (number determined by CA). For example, with a SAN certificate you can secure www.example.com, www.example2.com, www.example3.net, mail.example.net, dev.example2.com, etc.

If you are hosting multiple domains on one IP address, the only way you can secure them is with a SAN certificate. SAN certificates are also perfect for Microsoft Exchange environments since you can use one certificate for your entire environment. (For more information on this, see the Choosing a Certificate for Your Environment section at the end of this article.)

As with wildcard certificates, SAN certificates can pose potential security risks. If you have a SAN certificate in your environment you need to increase security measures. Mark all certificates as non-exportable and limit the number of people who can edit the list of sites that are secured by your certificate. You can purchase a DigiCert UC/SAN certificate and issue duplicates to further secure your environment.

SGC (Server Gated Cryptography) Certificates

SGC certificates enable older browsers to create secure, 128-bit encrypted sessions even if the normal browser encryption rate is only 40 bit. They usually cost significantly more and are only available from certain vendors. And only browsers created before 2000 need them—making the percentage of people that benefit from them less than 1%. Most CAs do not recommend or sell SGC certificates for security reasons. For more information, read the following article:

http://www.sslshopper.com/article-say-no-to-sgc-ssl-certificates.html

OTHER THINGS TO THINK ABOUT

Now that you have the information you need to choose the type of SSL Certificate that you want, here are a few more things you can think about to narrow down your options.

Issuance Speed
If you need an SSL Certificate in the next couple of minutes or days, you have a few options: 1) you can get a low-level validation certificate, which are often issued in a matter of minutes; 2) you can find a CA that offers issuance for high-level validation certificates in a few hours or less (like DigiCert); or 3) you can install a temporary SSL Certificate (either a trial version or a low-level validation certificate) while you wait for your certificate to be issued.

Warranty
CA warranties are not for you (the purchaser) but rather for your users. If fraudulent activity occurs as a direct result of a customer's transaction with a website containing an improperly-issued SSL Certificate, most CAs will offer reimbursement for customers who meet the criteria found in the CA's relying party agreement. Though it's uncommon for this type of fraudulent activity to occur, your warranty amount shows your users how seriously you take website security.

Certificate Lifetime
A standard SSL Certificate lifespan is one year. However, many CAs offer a discounted rate if you purchase an SSL Certificate with a 2-3 year lifespan. Some CAs also allow you to change the domain name in your SSL Certificate at any time, so you don't have to worry about keeping the same domain for the lifetime of the certificate. If this is a feature you want, check with your CA to make sure they allow you to change the domain. Note that while some CAs will only allow you to change your domain name for the first 30 days.

Another benefit to buying a 2-3 year certificate is you don't have to worry about the validation, issuance, and installation process every year. Many people think this process is a hassle and would prefer to do it less often. You don't want to risk forgetting about your SSL Certificate renewal and have a period where your website is unsecured. Even if you remember to renew, the length of the validation, issuance, and installation process may cause you to have a period of time where you do not have an SSL Certificate installed. This can cause a loss in customer confidence since many browsers will show a warning message to users when they visit a website that has an expired certificate.

Choosing a Certificate Authority
There is a wide range of CAs that you can purchase an SSL Certificate from. Though the SSL technology used by CAs is similar, there are many important factors to consider when choosing a vendor.

Reputation
Since the CA that you choose conveys trust to your end users, it's a good idea to pick a vendor with a good reputation. SSL Shopper is a great website for checking CA reviews. Their reviews cover customer support, ease of managing certificates, issuance speed, and overall customer satisfaction.

http://www.sslshopper.com/certificate-authority-reviews.html

Customer Service
Being able to reach a real person can be a lifesaver when you're experiencing problems—especially if they are affecting your ability to accept payments or keeping your website from being live. Many organizations can only restart their servers or make changes after hours, and if your CA is only available from 9-5 you could encounter an emergency and not have anyone to help you. Check to make sure that your CA has customer

support representatives available by email, phone, online chat, or whatever method of communication works best for your business. You can also check SSL Shopper (link above) for customer satisfaction and customer support reviews of each CA.

Website Security Seals
A site seal is a small icon that you can display on your website. It broadcasts that you have an SSL Certificate and that you take website security seriously. This icon also gives your visitors another visual assurance of your site's security and credibility.

Concern about website security is one of the biggest motivators behind abandoned online shopping carts. Building trust with your visitors is a key component to converting them into loyal and profitable customers. Security seals can be especially useful for companies that want to build brand awareness and are seeking additional means to build online credibility.

Though all CAs offer security seals, it's a good idea to think about the name of your CA and how the security seal will look to visitors.

CHOOSING A CERTIFICATE FOR YOUR ENVIRONMENT

Now that you are a savvy certificate shopper, it's time to decide what certificate(s) are right for your environment. The below examples demonstrate a few common scenarios with certificate recommendations based on the environment.

Single-Domain Websites and Small Companies
For small, single-domain websites you should consider a single-domain SSL Certificate. EV or OV certificates are generally best, but EV certificates provide extra assurance and help establish credibility.

An SSL Certificate with OV is adequate for small to medium-sized companies or shopping sites. Note that if you are handling customer information (credit cards, etc.) PCI standards require you to have an SSL Certificate.

If you are a new company or if you want help establishing customer confidence, an EV certificate is your best option. EV certificates can help you build a credible brand by making your website look secure and legitimate. The visual benefits of EV certificates include the green address bar and your company name prominently displayed in the browser.

If you are a well-known brand that is likely to be a target of phishing attacks, an EV certificate is also your best option. Since EV certificates have different visual cues and can only be acquired by credible businesses, customers will instantly be able to tell the difference between your actual site and a scammer's copy.

School and Government Organizations
If you are a school or government organization, it is very likely that you will need certificates for multiple domains and subdomains. You should consider a SAN certificate if this is the case. Though wildcard certificates can secure multiple subdomains, SAN certificates may be a better option because of their increased flexibility. Either way, a SAN or a wildcard certificate is going to save you a considerable amount of money than if you tried to secure all of your sites with single-domain SSL Certificates.

Since you will be managing many certificates and sites, you should also consider Managed PKI (MPKI)*.

Hosting Companies
If you are a hosting company, you may want to offer SSL Certificates to your customers. You can offer single-name SSL Certificates or EV SSL Certificates to dedicated hosting customers. If you want to secure multiple sites owned by the same company on one IP address, you can also consider getting a SAN certificate.

Note that most CAs offer reseller programs for hosting companies. Reseller programs allow you to sell a CA's certificates to your customers while making a profit. If you plan on selling a large number of certificates, becoming a reseller may be a good option for you. Check with your CA for details and programs.

Exchange Environments
Exchange 2003
If you have Exchange 2003 you do not need a SAN or wildcard certificate to cover your Exchange environment. A single-name SSL Certificate is sufficient.

Exchange 2007
If you have Exchange 2007, you should consider a SAN certificate. If you want EV, you can get an EV SAN certificate. SAN certificates let you use a single certificate to secure multiple names across multiple Exchange servers—saving you both time and money.

Exchange 2010 and newer
If you have a newer version of Exchange, you should consider either a wildcard or SAN certificate.

If you don't have multiple domains, a wildcard certificate is a good option. A wildcard certificate will allow you to secure as many subdomains as you want. And, with a DigiCert® wildcard certificate, you can secure multiple subdomains of a

**MPKI is a service that allows organizations with a large volume of SSL Certificates to take control of certificate management—including issuing new certificates and reissuing, replacing, and revoking existing certificates on demand. This service allows your account administrator to eliminate the waiting periods needed with requesting certificates through your CA. You can also usually get volume discounts with an MPKI account; however, check with your CA for prices and features.*

subdomain. For example, if you buy your wildcard certificate for *.domain.com, you can issue certificates for mail.dev.domain.com and 123.456.789.domain.com.

Note that you can use wildcard certificates with some older versions of Exchange; however, many versions don't work and the ones that do have been known to cause problems.

If you have multiple domains, or if you want EV, a SAN certificate is a good option. A SAN certificate lets you secure multiple domains and subdomains with a single certificate and should cover all of the names in your environment.

Environments with Multiple Subdomains
For environments with many subdomains (one for mail, forums, company applications, etc.) you should consider a wildcard certificate. Even though you can't get EV wildcard certificates, you can save a lot of money by being able to secure multiple subdomains with a single certificate.

Large/Enterprise Environments
It is difficult to recommend certificates for large/enterprise environments since their needs usually depend on what is in the environment (see previous sections). However, if you have a large environment you should consider getting a Managed PKI (MPKI) account*.

**With an MPKI account, you can take control of certificate management—including issuing new certificates and reissuing, replacing, and revoking existing certificates on demand.*

READY TO GET STARTED?

Now that you know the basics, it's time to dig into the details. Though the technology from each CA is generally comparable, the CA that you choose will impact ease-of-use, speed of issuance, uptime, OCSP/CRL latency, and a variety of features that make your network more secure and simple to manage. DigiCert® has been providing SSL Certificates and SSL management tools for over a decade. DigiCert assisted in developing the Extended Validation Certificate and worked in conjunction with Microsoft to develop and promote the use of Subject Alternate Names in SSL Certificates. Unlike other CAs who offer dozens or even hundreds of products unrelated to SSL encryption, creating and supporting top-shelf digital certificates is all DigiCert does. This focused energy results in better products and unmatched support.

DigiCert has an award-winning in-house technical support team and has some of the fastest certificate issuance times out of any CA—with EV certificates typically issued in a matter of hours! DigiCert doesn't outsource customer support or have phone queues. Experience the "DigiCert difference" for yourself by calling 1-855-800-3444 or visiting *www.digicert.com*.

About DigiCert, Inc.

DigiCert is a premier online trust provider of enterprise security solutions with an emphasis on authentication, PKI and high-assurance digital certificates. Headquartered in Lindon, Utah, DigiCert is trusted by a continually growing clientele of more than 60,000 of the world's leading government, finance, education and Fortune 500® organizations. DigiCert has been recognized for its excellence in customer support and the workplace, and was applauded for its value-added product features with the 2011 Frost & Sullivan Customer Value Enhancement Award for SSL Certificates.

DigiCert, Inc.
355 South 520 West
Canopy Building II, Suite 200
Lindon, UT 84045 USA
+1 (801) 701-9600
www.digicert.com