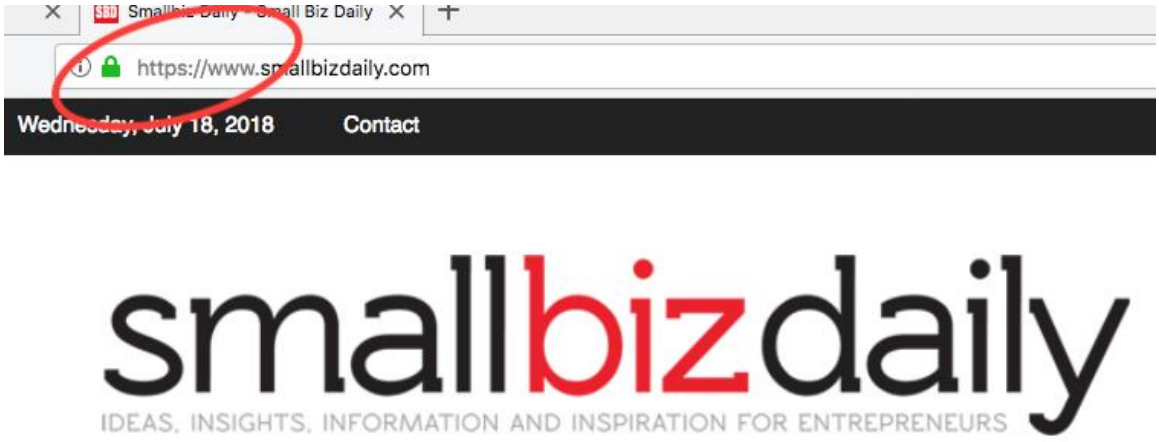
What Is The Best SSL Certificate To Buy?

Does your have an SSL certificate? SSL stands for "secure sockets layer," and its technology that protects the data customers share with you on your website. Google is making some changes to its Chrome browser this month that could seriously hurt your websites trustworthiness unless you have an SSL certificate.

Not sure if your site is secure? You don't need an SSL diagnostic tool to find out. Just type your domain name into any web browser, and see what comes up.

If your URL begins with HTTPS, your website is secure. (See the example below from my business's website.)



(Image Source)

If your URL begins with HTTP (no S), your website is **not** secure, and it's time to look for an SSL certificate provider.

In this post, we'll cover:

- Why not all SSLs are created equal
- What to look for when choosing a provider (a.k.a. certificate authority)
- The best SSL certificate to buy for your business

Where do you get an SSL certificate?

Organizations that issue SSL certificates are known as *certificate authorities* (CAs). If your small business is considering a choice of certificate authorities to issue your SSL

certificate, it's important to remember that not all certificate authorities are created equal.

You might be surprised, as I was, to learn that there is no minimum agreed-upon standard that SSL certificate authorities have to comply with. (There is, however, a voluntary organization of certification authorities and browser vendors called the CA/Browser Forum whose members agree to abide by certain standards.)

Certificate authorities are subject to the same risks as any website, including cyber attacks and data security breaches. However, to maintain their status as trusted organizations, they must have extremely strong security policies and standards, as well as pass an annual SSL audit by a licensed firm/practitioner. CAs that pass their audits in good standing are registered with WebTrust.

With all of your business and customer data at risk, selecting your SSL certificate authority is clearly a big decision. How can you be sure you're choosing the right certificate authority?

How to choose a certification authority

There are many resellers that offer Certificate Authority SSLs at a discount. However, for peace of mind, it's always safer and more secure to get the SSL directly from the company that issues it, even if it costs a little bit more.

By getting an SSL directly from the Certificate Authority, you'll get a higher level of customer support 24/7/365 and a faster response time than you'd get from a reseller. For something as important as your business website, being able to get help directly, when you need it, is crucial.

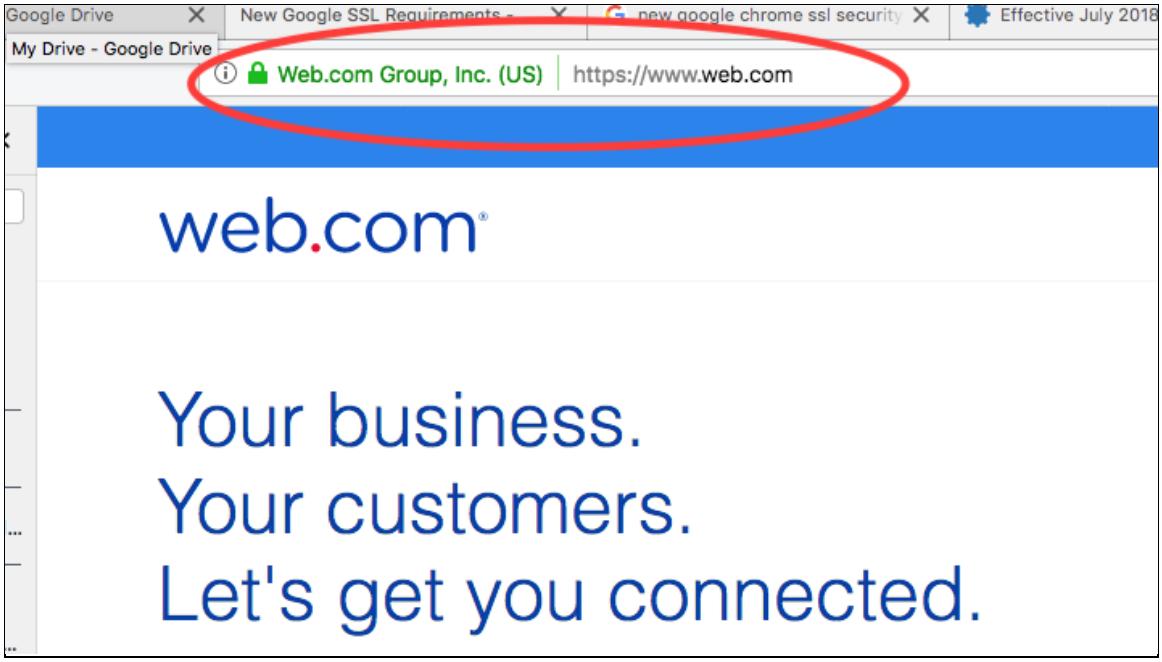
So how do you choose a CA? Start by looking for the same things that your customers are looking for when choosing a secure website to do business with. This includes:

- A padlock symbol that appears in your web browser when you open the CA's website
- A widely recognized trust mark from WebTrust
- The "https" instead of "http" prefix in the URL
- A green address bar indicating the site is secured by an Extended Validation certificate, the highest level of security

Source: WebTrust
http://www.webtrust.org/proper-use-of-seals/item64421.aspx

The image below shows an example of what to look for. As you can see, in the area circled in red, there are three indicators of site security:

1. The browser bar has a lock icon
2. There is an HTTPS in front of the URL, and
3. The address bar is green.



(Image Source: Web.com)

Doing a certificate authority comparison

The factors above are just the basics. Not all certificate authorities follow the same security practices or offer the same level of assurance. That's why you'll need to dig deeper into the security practices of the certificate authorities you're considering.

When you are doing a certificate authority comparison, here are some important questions to ask:

- **Does the certificate authority publish their security policies?** You should be able to see what the organization's policies are so you can assess their security. It is often referred to as a Certificate Practice Statement (CPS). A CA will have a main version for DV (Domain Validation) and OV (Organizational Validation) SSLs and then a different CPS if they offer EV (Extended Validation) SSLs. (For more on what these terms mean, see "What Type of SSL Certificate Do I Need?" below.)

- **Do they go through third-party audits on a regular basis?** Third-party audits are used to test and verify the security of a certificate authority's infrastructure.
- **Do they have appropriate network security in place?** This should include antivirus, anti-malware defenses, intrusion detection, and intrusion protection systems.
- **Does the company use best practices** regarding authentication and verification processes used to confirm ownership of a domain and/or business?
- **How long has the certificate authority been in business?** Companies with long experience in the world of SSL certificates know the ins and outs of the process and keep up with the latest standards regarding security.
- **What is the certificate authority's reputation?** Do an online search or talk to other business owners you know to turn up any problems.
- **Does the certificate authority conduct background checks on its employees?** Insider threats can be a risk if employees aren't properly vetted.
- **What are the physical security practices of the certificate authority?** Is physical access to server and storage equipment restricted only to those employees who need it?
- **How is the facility designed?** Look for what are called "hardened facilities" (kind of like a military bunker or bomb shelter). This can physically defend your data from disaster, intruders, or power loss.
- **Does the certificate authority offer 256-bit encryption?** This is the highest standard in the industry and offers the best protection for your data.
- **What type of warranty does the certificate authority offer?** SSL certificates come with warranties that can compensate your site visitors in case of a loss (up to a certain limit). The amount of the warranty varies depending on the type of SSL certificate you get. For example, the basic SSL certificate may come with a $10,000 warranty, while a higher-level SSL certificate will have a much higher warranty. In addition, different certificate authorities provide different warranty levels. The certificate authority should be able to help you determine what warranty offers the best protection for your business.

What type of SSL certificate do I need?

Of course, you must also look for an SSL certificate authority that provides the type of SSL certificate you want. There are several types of SSL certificate you can purchase, depending on your business needs. Different certificate authorities will have their own names for these certificates, but in general, most offer three levels:

1. Domain Validation (DV): This is the fastest and easiest type of SSL certificate to get. The certificate authority simply verifies that the owner has the right to use the domain name in question. Think of this as the "baseline" level SSL certificate. The padlock will show up in the browser, but if a user clicks on it to find out more about your certificate, they won't see your business name because it wasn't validated.

2. Organizational Validation (OV): This type of SSL certificate requires more thorough validation. The certificate authority validates the company name, domain name, and other information about the business based on what they find in publicly available databases. When a user clicks on the padlock icon next to your URL in their browser, information about your company name will show up. If you have an e-commerce website, you'll definitely want to obtain this type of SSL certificate, because it gives users more confidence in buying from you.

Does your website have different subdomains, such as e-commerce shopping carts, customer account pages, or shipping information? For example, *domain.com* might use the subdomain *checkout.domain.com* to handle customer checkouts, and *help.domain.com* for customer assistance. If this describes your business, you should get what's typically called a "**wildcard" SSL certificate**. A wildcard SSL certificate offers added protection for websites with multiple subdomains, while letting you secure all of the subdomains with one certificate.

3. Extended Validation (EV): The authentication process for issuing an EV SSL certificate is stricter than the other types of certificates. The certification authority will verify not only the domain and the owner, but also the business's legal structure (such as incorporation), physical location and address. This provides the highest level of security assurance for customers.

Deciding what is the best SSL certificate to buy

Thinking of the three types of SSL certificates above as silver, gold and platinum, you can see why the prices are typically a bit higher the further up you go on the scale. However, it's important not to make price the only factor (or even the primary consideration) when choosing a certificate authority.

Remember, you're placing your trust — and your business's good name — in the hands of your chosen certificate authority. Price is just one of many factors to weigh, and with so much at stake, it's important to remember the old saying, "You get what you pay for."

Are you looking for a trusted and experienced certificate authority? Web.com offers several SSL for small business options to help your business protect its own and your customers' data, establish trust, and grow your business.