SECTIGO

A WHITEPAPER FROM SECTIGO

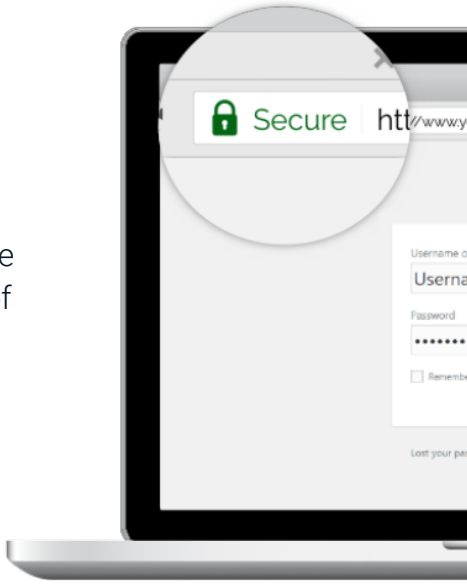
Extended Validation SSL: Your Key to Maximizing Online Trust

Introduction to SSL Certificates

Secure Sockets Layer (SSL) certificates exist primarily to authenticate the identity of a server on an open network like the internet. Each certificate contains a set of known information about the entity to which it has been issued. The exact information available in the certificate is a function of the certificate's authentication level, which by industry standard is set at one of three levels.

- **Domain Validation, or DV:** In a Domain Validation certificate, the only authenticated information is that the requestor has control over this domain. No other information about this organization's or individual's identity is available. DV certificates are frequently used in phishing and other online scams because they're easy to obtain and leave no paper trail back to the owner.
- **Organization Validation, or OV:** Organization Validation certificates include information about the organization or individual that requested the certificate. All trusted Certificate Authorities must follow certain standards in authenticating OV certificates. However, these authentication standards are relatively light, and there is a great deal of variability in how CAs choose to authenticate OV certificates. As a consequence OV certificates are considered more trustworthy than DV certificates but less so than Extended Validation certificates (see below).
- **Extended Validation, or EV:** Extended Validation certificates require a high level of authentication of the identity of the organization receiving the certificate. CAs must follow specific guidelines based on the best available information sources and known practices that have been proven successful over more than a decade of use in the real world. CAs must pass regular independent audits of their authentication practices. EV certificates are the most trustworthy SSL certificates.

Though the presence of a valid SSL certificate is required to enable encrypted data exchange between standards-based hardware and software, the certificates themselves do not actually perform any of the encryption or decryption involved. Rather, internet protocols are set up to require the presence of a valid certificate for encryption in order to prevent a series of potential threats, including man-in-the-middle and web site spoofing attacks, that can be used to steal sensitive data or otherwise damage online communication.



A small padlock icon is often used to indicate that the browser connection is secure.

EV certificates are the most trustworthy SSL certificates.

Encryption protects transmitted data from being spied upon by outsiders who are not involved in the communication. However, the strongest encryption in the world is irrelevant against a malicious party that is pretending to be the trusted recipient of your communication but actually is not. Therefore these two components—encryption and authenticated identity—work in conjunction. In the absence of a trusted certificate, connecting systems by design will not enable encryption since the presence of encrypted traffic may disguise the fact that this connection is not safe.

A good analogy is the physical security of a building. You can think of encryption as a locked door that prevents outsiders from entering the building. But the strongest door in the world is irrelevant if any individual can simply open it up and walk right through. Authentication is like a security badge reader on that door, only allowing access to known parties who are trusted with access.

In the 2000s a challenge emerged for this paradigm, which was the meteoric rise of phishing and other social engineering attacks involving counterfeit sites from known businesses. Though there are many variations on the theme, the basic attack involves tricking a visitor into navigating to a site controlled by the phisher, a site is designed to be indistinguishable from some real site that the visitor trusts. On these counterfeit sites even savvy and experienced users can accidentally give online thieves their logins, personally identifiable information (PII), credit card details, and other critical information.

They key for these sites to successfully steal information is to be as close to indistinguishable from the actual, trustworthy site as possible. One component of the real sites' experience is the presence of a security indicator in the browser to demonstrate that shared data is encrypted, and if that indicator is missing from the phishing sites, it will be a potential obstacle to the criminals' goals. Therefore, phishers quickly evolved their techniques to include DV SSL certificates on their fraudulent sites to help create the illusion of legitimacy.

In response to this problem, the CA and browser industries came together to create the standard for Extended Validation SSL. Because EV SSL is highly authenticated using techniques that are demonstrated to be successful in hundreds of thousands of instances over more than a decade, one of these certificates considered a strong proof point that a site is actually what it says it is. In fact, there has never been a known example of a phishing site using Extended Validation SSL.

EV SSL: Your Key to Offering the Highest Available Assurance of Identity

Extended Validation (EV) SSL is the highest-security form of SSL certificate available. EV SSL certificates take advantage of proven, highly trusted authentication methods to give the best possible assurance of a web site's legitimacy. The presence of an EV SSL certificate triggers visible trust indicators in all popular desktop browsers, which can increase transactions and other site usage, defend users from phishing attacks, improve your online brand experience, and help you meet compliance requirements.

EV SSL is the *de facto* standard for sites dealing in sensitive or confidential information including personally identifiable information (PII), personal health information (PHI), credit card information, or any kind of account login. It is used by leaders in the most prominent online industries, including:

EV SSL is the de facto standard for sites dealing in sensitive or confidential information.

- Banking
- Credit unions
- Online retail
- Social networks
- Securities trading
- Tax filing
- Credit and lending
- Insurance
- B2B provisioning and purchasing
- SaaS

These sites invest in assuring visitors of their identity to provide the safest possible online experience for customers, ecosystem partners, and their own employees. Web sites have long been ripe targets for phishing and other social engineering attacks that involve tricking users into inputting confidential information in sites that look like (but are not) these real online properties.

Businesses need to protect these three groups for these reasons:

- **Customers:** Protecting your customers from thieves is just plain good customer service. Furthermore, giving customers the tools to confirm they are on your real site and not a fraudulent counterfeit will improve their confidence doing business with you online, improving your overall brand impression and most likely resulting in increased online business. Some companies even seek to educate their regular online users to look for the green address bar to help them protect themselves from this kind of attack.

- **Partners:** Not only can partners fall for phishing schemes and lose their own data or money through sophisticated spear phishing schemes, but they also could be tricked into giving away confidential information or access that negatively affects your business as well. You can use EV SSL to create a clear indication of your legitimate site and then communicate to partners to train their employees to verify its presence before proceeding with sensitive transactions.
- **Employees:** Your employees are potential targets both for phishing schemes aimed at their own information or spear phishing attacks that attempt to gain secrets or access to systems and accounts. The authenticated identity of the green address bar helps fight these attacks. In this case the company should instruct employees to look for green address bars when accessing company systems or services.

EV SSL Trust Indicators in Browsers

Because EV SSL certificates provide a high level of confidence in the identity of the organization operating an online site or service, popular desktop and mobile browsers display "trust indicators" in their interfaces to identify sites that use these certificates.

All popular desktop browsers include some kind of "security indicator" in the web site address bar that displays when an SSL certificate (and therefore encryption) is in place. These indicators may include the word SECURE in addition to a padlock icon.

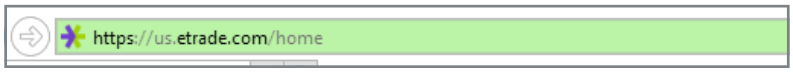
When an Extended Validation SSL certificate in particular is in place, the browser inserts the name and location of the company to which this certificate was issued, in green. Browsers use green because in the language of popular operating systems (Windows and Mac OS), green is the color most used to indicate safety. Prominently displaying the company name in the browser interface gives users a clear opportunity to distinguish true online businesses they trust from pretenders seeking to victimize them.

Since they can trust the real identity of an online business identified with EV SSL, consumers display greater confidence when using web sites and online services that display green address bars. This increased confidence can translate to improvement in key business goals such as online sales, new account signups, lead generation, and use of online services.

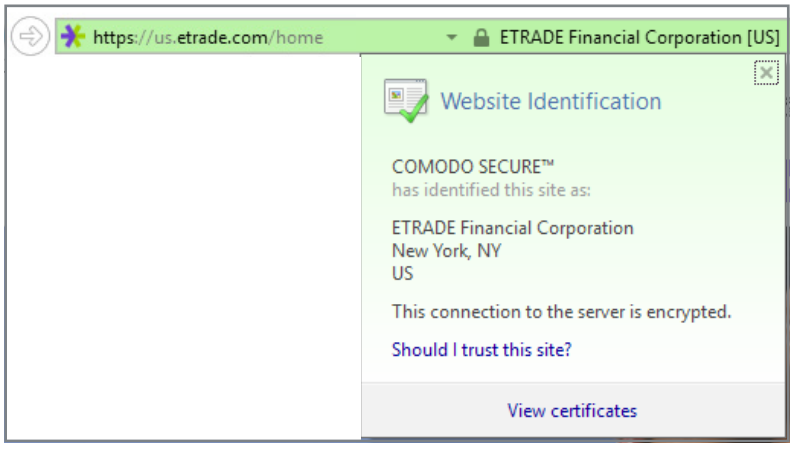
Consumers display greater confidence when using web sites and online services that display green address bars.

Internet Explorer

Internet Explorer was the first ever browser to give EV certificates a specific trust indicator, and today's implementation is still quite similar to its original interface. IE changes the color of the address bar background to green and includes the name and location of the company to the right of the address.

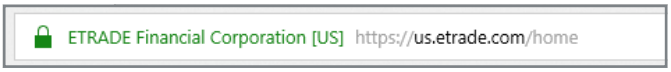


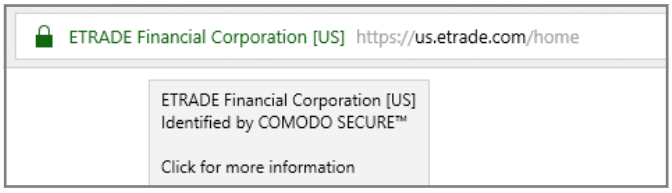
Hovering over or clicking on the address bar displays additional information about the entity that received this certificate.



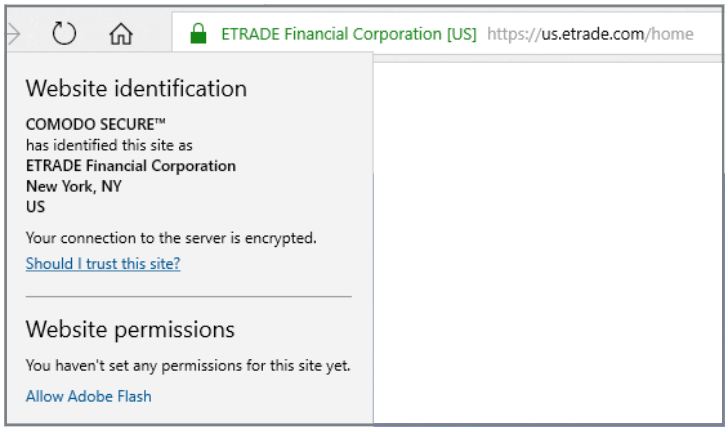
Edge

Microsoft Edge displays the company name to the left of the URL in the address bar and includes additional identity details upon mouse-over or click.





An EV SSL certificate triggers visible trust indicators in all popular desktop browsers.



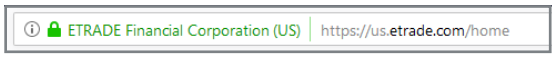
Testing has shown typical increases in completed transactions of about 10% when green address bars are present.

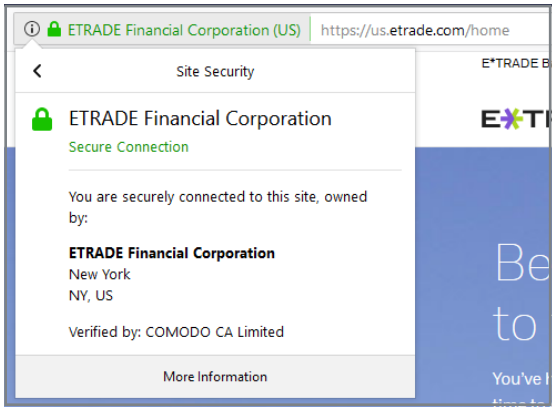
Chrome

Chrome displays the company name in green adjacent to the URL.

Firefox

Firefox displays the green company name to the left of the URL and additional details in a drop-down.

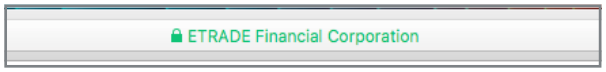




Giving site visitors the tools to confirm that your site is for real translates to increased confidence when doing business online.

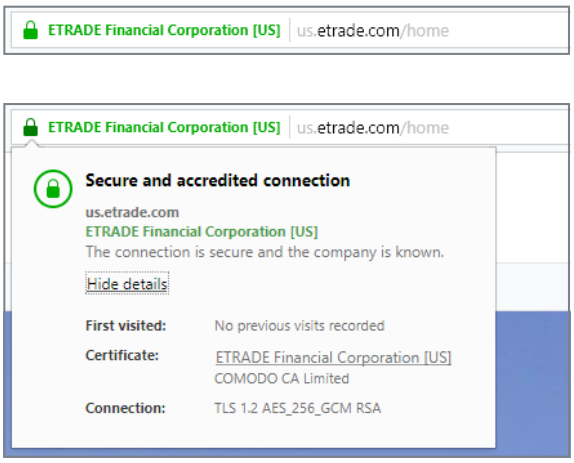
Safari

Safari displays the company name in green in the address bar.



Opera

Opera includes the company name and location in green to the left of the URL and displays additional certificate details in a drop-down.



Use EV SSL certificates to maximize transaction completion rates.

Business Benefits of EV SSL

By employing EV SSL certificates, your online business can realize a number of benefits.

- **Increase site transactions.** Show the green address bar and your company name in the browser interface to give visitors added confidence in safe transactions on your site. Use EV SSL certificates to maximize transaction completion rates, which can increase sales, form completions, new user signups, and engagement with online services.
- **Protect users against phishing sites.** Prominently display your company name in the browser interface to provide extra protection against phishing and other attacks involving a fake version of your site. That means greater security for your customers, partners, and employees.
- **Increase engagement with your business.** Users who are confident in a site will engage with it more thoroughly. That translates to increased time on site and pages visited and decreased bounce rates.
- **Show customers you care**. EV SSL shows online customers that you care enough to employ best-of-breed security for their protection.
- **Stay compliant**. Many standards and regulations such as PCI-DSS, HIPAA, HITECH, GDPR, and others require that online businesses take measures to protect consumers from theft of confidential information. Use Extended Validation for the strongest protection an SSL certificate can offer.

Improved Transaction Rates and Other Site Performance Metrics

Visible trust indicators such as green address bars and company names in the browser interface have been demonstrated in many tests to improve site visitors' likelihood to engage with sites, make purchases, use online services, and share sensitive or confidential information including credit card numbers and personally identifiable information (PII).

In a June 2018 study of more than 350 active internet users, research firm DevOps discovered that more than 90% of people worry about having their identities and credit card information stolen online*. The presence of an EV green address bar on a site is reassuring to consumers, and that translates to increases in use of web sites for a variety of transaction types.

Transaction type	% of users more likely to engage*
Engage in financial transactions	50.2%
Share personally identifiable information (PII)	57.0%
Make a purchase	36.5%
Use a credit card	28.4%
Sign up for a new account	42.5%
Fill out and submit an online form	37.5%
Use a payment service like PayPal	40.6%
Add recommended items to a shopping cart	32.3%

Over the years since EV SSL has been released dozens of businesses have measured the difference in completions between visitors who saw green trust indicators and those who did not. This testing has shown typical increases in completed transactions of about 10% when green address bars are present.

Protection Against Phishing and Social Engineering Attacks

By providing site visitors with a reliable way to confirm your web site's genuine identity, you reduce their vulnerability to phishing and other attacks that depend on counterfeit sites. The visible green trust indicators and the name of your company in the browser interface both serve as visible differentiators between genuine and spoof sites. Since the practice of phishing and site spoofing involves creating a perfect imitation of the trusted online property that is being mimicked, these indicators become important clues to differentiate real sites from criminal fakes.

* DevOps. June 2018. https://library.devops.com/survey-learning-to-trust-your-browser

Many banks, online payment services, and other sites dealing in sensitive information choose not only to display their name in the green address bar but also to actively communicate with their customer bases to look for these indicators in their effort to protect consumers from being taken in by these scams.

Extended Validation can also protect your internal employees and processes from spear phishing and other sophisticated attacks by removing the ability for attackers to insert a perfectly executed imitation site in the middle of a sensitive business transaction.

Increasing Customer Engagement

Giving site visitors the tools to confirm that your site is for real translates to increased confidence when doing business online. Most security measures are invisible to site visitors, so they have to take it on faith that online businesses are protecting their very sensitive data. EV SSL is a clearly visible example of your business investing in best-of-breed security to protect your site visitors. Using EV SSL helps your site visitors be confident that you do everything you can to protect them.

This increased confidence with site security should be expected to translate to increased visitor engagement with your online information and services. Key metrics that are likely to improve this way include:

Increasing visitor engagement with your site makes your online effort more effective in building brand awareness and preference, influencing core constituencies, spreading your message, educating the public, sharing critical information with customers, and motivating action. Increasing

- Time on site
- Page views
- Bounce rates
- Collateral downloads
- Mailing list signups
- Form completions
- Logins
- Service usage
- Return visits

use of web site self-help and online services can translate to increased efficiency in serving customers. And by reducing overall anxiety, you give customers a more pleasant experience when dealing with your company, which translates to a more satisfactory online experience.

Visible green trust indicators and the name of your company in the browser interface are important clues to differentiate real sites from criminal fakes.

EV SSL is a clearly visible example of your business investing in best-of-breed security to protect your site visitors.

Communicating a Customer-centric, Caring Brand Message

Associating your web properties with visible trust indicators shows visitors that you take IT security seriously, reinforcing your overall positive brand impression. Furthermore, by displaying your company name in the browser interface, you increase exposure to your brand name. Putting EV SSL on all pages maximizes this positive branding affect.

Visitors to a site featuring the EV green address bar are more likely to perceive that online business as secure, reliable, and a source of good service.

Quality of online business	% with improved perception due to green address bar*
Safe site to do business with	52.8%
Trustworthy	51.2%
Secure	50.8%
Established and stable	22.1%
Meets its commitments	25.4%
Good customer service	22.4%
Cares about me	18.9%
Safe to make an expensive purchase on this site	32.5%
Uses the best available technology	45.0%

Note that the brand name used in the EV SSL certificate isn't limited to your company's name. EV SSL certificates can use trademark names or DBAs, so you can ensure the name that appears in the browser matches the name you use on your web site.

EV SSL certificates can use trademark names or DBAs.

Maintaining Compliance

A great many IT compliance standards require that businesses proactively protect confidential information such as PII, PHI (personal health information) and credit card numbers. Loss of this information can lead to fines, mandatory breach notifications, and damage to a company's reputation.

Since EV SSL undermines the success of social engineering attacks like phishing and site spoofing, it is widely considered a best practice in providing protection against loss of this information. In the event that such information is indeed stolen, a track record of providing EV SSL can be helpful for a company to demonstrate that it took available measures to protect against this kind of theft.

EV SSL is widely considered a best practice.

Furthermore, standards applicable to your business may specifically mandate EV SSL as a requirement. For example, the IRS requires that online providers of individual tax returns must use Extended Validation SSL. Since the details of industry and regulatory standards can be complex and nebulous, many online businesses choose to take a "better safe than sorry" approach by offering the highest level of SSL security available.

About

Sectigo provides web security products that help customers protect, monitor, recover, and manage their web presence and connected devices. As the largest commercial Certificate Authority trusted by enterprises globally for more than 20 years, with more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs for securing today's digital landscape. For more information, visit **www.sectigo.com.**

Contact a Sectigo website security specialist to find out how EV SSL can help your business.

SECTIGO

sales@sectigo.com

