(https://www.websecurity.digicert.com/en/in)

Products (https://www.websecurity.digicert.com/en/in/products?inid=prodmenu_nav_prodhome)
Buy/Renew (https://www.websecurity.digicert.com/en/in/buy-renew?inid=brmenu_nav_brhome)
Support (https://www.websecurity.digicert.com/en/in/support)
Security Topics (https://www.websecurity.digicert.com/en/in/security-topics)
Partners (https://www.websecurity.digicert.com/en/in/partners)

SIGN IN

Manage your certificates in DigiCert® CertCentral

All legacy Symantec account portals have moved to CertCentral. Log in below if you've already activated your CertCentral account. If not, contact our sales or support teams here (https://www.websecurity.digicert.com/en/in/support/contact). They will send you an email with a unique link to access your account. Login (https://www.digicert.com/account/login.php)

THE ULTIMATE GUIDE

What is SSL, TLS and HTTPS?

What is an SSL Certificate?

CONTACT US

SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details. The two systems can be a server and a client (for example, a shopping website and browser) or server to server (for example, an application with personal identifiable information or with payroll information).

It does this by making sure that any data transferred between users and sites, or between two systems remain impossible to read. It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection. This information could be anything sensitive or personal which can include credit card numbers and other financial information, names and addresses.

TLS (Transport Layer Security) is just an updated, more secure, version of SSL. We still refer to our security certificates as SSL because it is a more commonly used term, but when you are buying SSL (https://www.websecurity.digicert.com/ssl-certificate?inid=infoctr_buylink_sslhome) from DigiCert you are actually buying the most up to date TLS certificates with the option of ECC, RSA or DSA encryption (https://www.websecurity.digicert.com/security-topics/how-ssl-works).

HTTPS (Hyper Text Transfer Protocol Secure) appears in the URL when a website is secured by an SSL certificate. The details of the certificate, including the issuing authority and the corporate name of the website owner, can be viewed by clicking on the lock symbol on the browser bar.

COMPARE SSL PRICES (HTTPS://WWW.WEBSECURITY.DIGICERT.COM/SSL-CERTIFICATE?INID=HOWWORKS_COMP_SSLHOME#COMPARE)

Introduction to SSL

Learn how SSL works to protect online information and increase trust in websites.

1 SSL Topics for Small Businesses (https://www.symantec.com/content/en/us/enterprise/other_resources/b-ssl-topics-for-small-businesses-ebook-en-us.pdf)

2 How SSL Works (https://www.websecurity.digicert.com/security-topics/how-does-ssl-handshake-work)

3 Extended Validation (EV) (https://www.websecurity.digicert.com/security-topics/what-is-ev-ssl)

4 SSL Algorithms (https://www.websecurity.digicert.com/security-topics/ssl-algorithms)

5 How EV SSL Works (https://www.websecurity.digicert.com/security-topics/what-is-ev-ssl)

6 Check SSL Installation (https://ssltools.digicert.com/checker/)

CONTACT US

For online businesses or websites which accept credit or debit card payments, or involve the transfer of personal or sensitive information such as names and addresses, an SSL certificate is a necessity for website security. It's an essential way of making sure sites are secure and customers are protected, but crucially it also adds the appearance of security to online sites.

An SSL certificate is installed on the server side but there are visual cues on the browser which can tell users that they are protected by SSL. Firstly, if SSL is present on the site, users will see https:// at the start of the web address rather than the http:// (the extra "s" stand for "secure"). Depending on what level of validation a certificate is given to the business, a secure connection may be indicated by the presence of a padlock icon or a green address bar signal.

Google now advocates that HTTPS, or SSL, should be used everywhere on the web (https://www.websecurity.digicert.com/security-topics/https-everywhere) and, as of 2014, the search engine has been rewarding secured websites with improved web rankings (https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html), another great reason for any site to install SSL.

Transport Layer Security (TLS) is the successor protocol to SSL. TLS is an improved version of SSL. It works in much the same way as the SSL, using encryption to protect the transfer of data and information. The two terms are often used interchangeably in the industry although SSL is still widely used. When you buy an 'SSL' certificate from DigiCert, you can of course use it with both SSL and TLS protocols.

CONTACT US

Levels of business authentication

As well as encryption, Certificate Authorities (CAs) can also authenticate the identity of the owner of a website, adding another layer of security. The SSL certificate is then used as proof of the company's identity. Certificates can be divided into three authentication groups, based on the level of authentication, which are:

1

DOMAIN VALIDATION CERTIFICATES (HTTPS://WWW.SYMANTEC.COM/CONNECT/BLOGS/DV-SSL-CERTIFICATES-AND-ECOMMERCE-DONT-MIX)

2

ORGANIZATION VALIDATION CERTIFICATES (HTTPS://WWW.SYMANTEC.COM/CONNECT/BLOGS/TYPES-SSL-CERTIFICATES-CHOOSE-RIGHT-ONE)

3

EXTENDED VALIDATION CERTIFICATES (HTTPS://WWW.WEBSECURITY.DIGICERT.COM/SECURITY-TOPICS/WHAT-IS-EV-SSL)

These vary slightly in purpose and function. It's worth knowing a little more how each of them works before deciding which is the most suitable.

(https://www.symantec.com/connect/blogs/dv-ssl-certificates-and-ecommerce-dont-mix)

CONTACT US

Domain Validation SSL Certificates

These require businesses to prove their control over just the domain name. The certificate contains the domain name that was supplied to the issuing authority as part of the request. Because the identity of the organization is not checked here, Domain Validated certificates are the most basic level of SSL certification, and are only appropriate for test servers and internal links.
(https://www.symantec.com/connect/blogs/dv-ssl-certificates-and-ecommerce-dont-mix)

(https://www.symantec.com/connect/blogs/types-ssl-certificates-choose-right-one)

Organization Validation SSL Certificates

This requires the applicant to not only prove they own the domain name they wish secure, but also prove that their company is registered and legally accountable as a business. The issued certificate is then proof of domain and company name. This level of authentication is suitable for public-facing websites that collect personal data from site users. Note that individuals cannot obtain such certificates, only organizations and businesses.
(https://www.symantec.com/connect/blogs/types-ssl-certificates-choose-right-one)

(https://www.websecurity.digicert.com/ssl-certificate/secure-site-ev?inid=infoctr_prod_ssev)

Extended Validation SSL Certificates

CONTACT US

Extended Validation SSL helps protect users from providing their details to fake website which can be used by criminals for

phishing. EV SSL requires both of the above validations for domain and company as well as several additional verification steps related to proving that the SSL certificate belongs to a registered company. This extra company information is then represented in the issued certificate on the address bar and can be accessed from many web browsers by clicking on the padlock icon. When visiting a site with EV SSL many browsers exhibit a green address bar as a highly visual sign of trust in the website and business to handle personal information. This type of certificate is also available to organizations and businesses only.
(https://www.websecurity.digicert.com/ssl-certificate/secure-site-ev?inid=infoctr_prod_ssev)

SSL Certificates

Optimize your website for security trust with SSL Certificates and the Norton Seal.

COMPARE SSL CERTIFICATES (HTTPS://WWW.WEBSECURITY.DIGICERT.COM/SSL-CERTIFICATE?INID=HOWWORKS_COMP_SSLHOME#COMPARE)

1 Secure Site Pro with EV (https://www.websecurity.digicert.com/ssl-certificate/secure-site-pro-ev?inid=infoctr_prod_sspev)

2 Secure Site with EV (https://www.websecurity.digicert.com/ssl-certificate/secure-site-ev?inid=infoctr_prod_ssev)

3 Secure Site Pro (https://www.websecurity.digicert.com/ssl-certificate/secure-site-pro?inid=infoctr_prod_ssp)

4 Secure Site Wildcard (https://www.websecurity.digicert.com/ssl-certificate/secure-site-wildcard?inid=infoctr_prod_sswc)

5 Secure Site (https://www.websecurity.digicert.com/ssl-certificate/secure-site?inid=infoctr_prod_sss)

How does an SSL certificate work?

The basic principle is that when you install an SSL certificate on your server and a browser connects to it, the presence of the SSL certificate triggers the SSL (or TLS) protocol, which will encrypt information sent between the server and the browser (or between servers); the details are obviously a little more complicated.

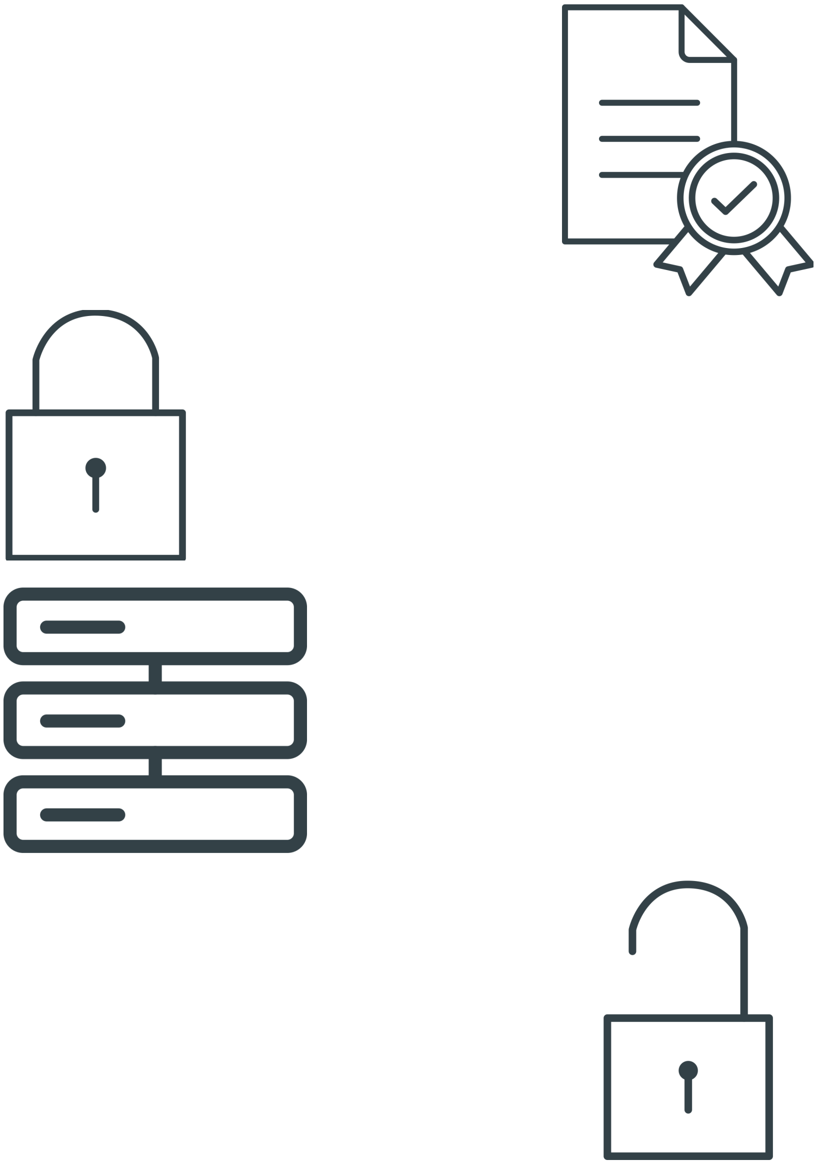
SSL operates directly on top of the transmission control protocol (TCP), effectively working as a safety blanket. It allows higher protocol layers to remain unchanged while still providing a secure connection. So underneath the SSL layer, the other protocol layers are able to function as normal.

^

CONTACT US

If an SSL certificate is being used correctly, all an attacker will be able to see is which IP and port is connected and roughly how much data is being sent. They may be able to terminate the connection but both the server and user will be able to tell this has been done by a third party. However, they will not be able to intercept any information, which makes it essentially an ineffective step.

The hacker may be able to figure out which host name the user is connected to but, crucially, not the rest of the URL. As the connection is encrypted, the important information remains secure.



1. SSL starts to work after the TCP connection is established, initiating what is called an SSL handshake.

2. The server sends its certificate to the user along with a number of specifications (including which version of SSL/TLS and which encryption methods to use, etc.).

3. The user then checks the validity of the certificate, and selects the highest level of encryption that can be supported by both parties and starts a secure session using these methods. There are a good number of sets of methods available with various strengths - they are called cipher suites.

CONTACT US

4 To guarantee the integrity and authenticity of all messages transferred, SSL and TLS protocols also include an authentication process using message authentication codes (MAC). All of this sounds lengthy and complicated but in reality it's achieved almost instantaneously.

Manage SSL Certificates

Optimize your website with the most robust TLS certificates in the industry and the most recognized trust mark, the Norton Seal.

1 DigiCert CertCentral (https://www.digicert.com/certificate-management/)

2 Enterprise SSL Solutions (https://www.digicert.com/enterprise-ssl-solutions/)

3 Better website security with Always On SSL (https://www.digicert.com/always-on-ssl.htm)

How to know if SSL is needed

The fact that Google is pushing for HTTPS across the web and prioritising sites that have an SSL certificate probably indicates just how much SSL is needed, but here are some other top reasons for getting an SSL certificate.

Secure purchases

According to Business Insider 74% of shopping carts are abandoned but up to 64% can be recovered with better checkout security and flow. Many of these 64% are more likely to complete a purchase if they know the checkout area is secure. That's not a number businesses can afford to ignore. Even if they're only using SSL for their checkout area, it's well worth it.

CONTACT US

Offering memberships

If sites offer membership or anything that involves collecting email addresses and other sensitive information, then SSL is a good idea. It's always sensible to keep customer information as safe as possible.

If forms are used

The same applies if they use any kind of form where users will be submitting information, documents, or images. It is surprising how much information is collected about a site's visitors, so it's worth keeping it safe.

If it's simply a blog or a standard 'info only' kind of site, HTTPS can help to protect the security of sites, reducing the risk or tampering and intruders injecting ads onto the page to break user experience. Plus, it really can't hurt in terms of search engine rankings.

CONTACT US

Does SSL work across all devices?

In short, the answer to this question is yes it does. Of course, there are some configurations that will not work 100% so it is can be valuable to talk with the Certificate Authority's sales team if unsure.

CONTACT US

^

CONTACT US

Devices and operating systems

Again all of the big operating systems for computers, tablets and mobile phones are supported. However, in the case of mobiles, it might be that some older devices won't support newer SSL or TLS protocols so it's worth doing the research to ensure maximum compatibility. The SSL certificate provider can help with this if there are any doubts.

Browser compatibility

People use a range of different browsers (Chrome, Firefox, Safari etc) to access web content. Just as sites are created to work on all browsing platforms, SSL/TLS from a reputable provider will also work in 99% of cases. Unless users are accessing the site from very niche browsers, all the big names will be covered.

CONTACT US

Servers

Thanks to the way SSL works, servers don't really need to have root certificates embedded but you will need to install the corresponding intermediate certificate(s). As long as the certificate is installed correctly, it can be supported by any server. It's up to the browser to determine if it's trusted or not during the handshake process.

CONTACT US

Key Services and Features

Learn more about how our services help extend security on your website beyond SSL.

1 Vulnerability Assessment (https://www.websecurity.digicert.com/security-topics/vulnerability-assessment)

2 Malware Scanning (https://www.websecurity.digicert.com/security-topics/malware-scanning)

3 Strongest Encryption Algorithms (https://www.websecurity.digicert.com/security-topics/ssl-algorithms)

4 FATCA Compliance (https://www.websecurity.digicert.com/security-topics/fatca-ssl)

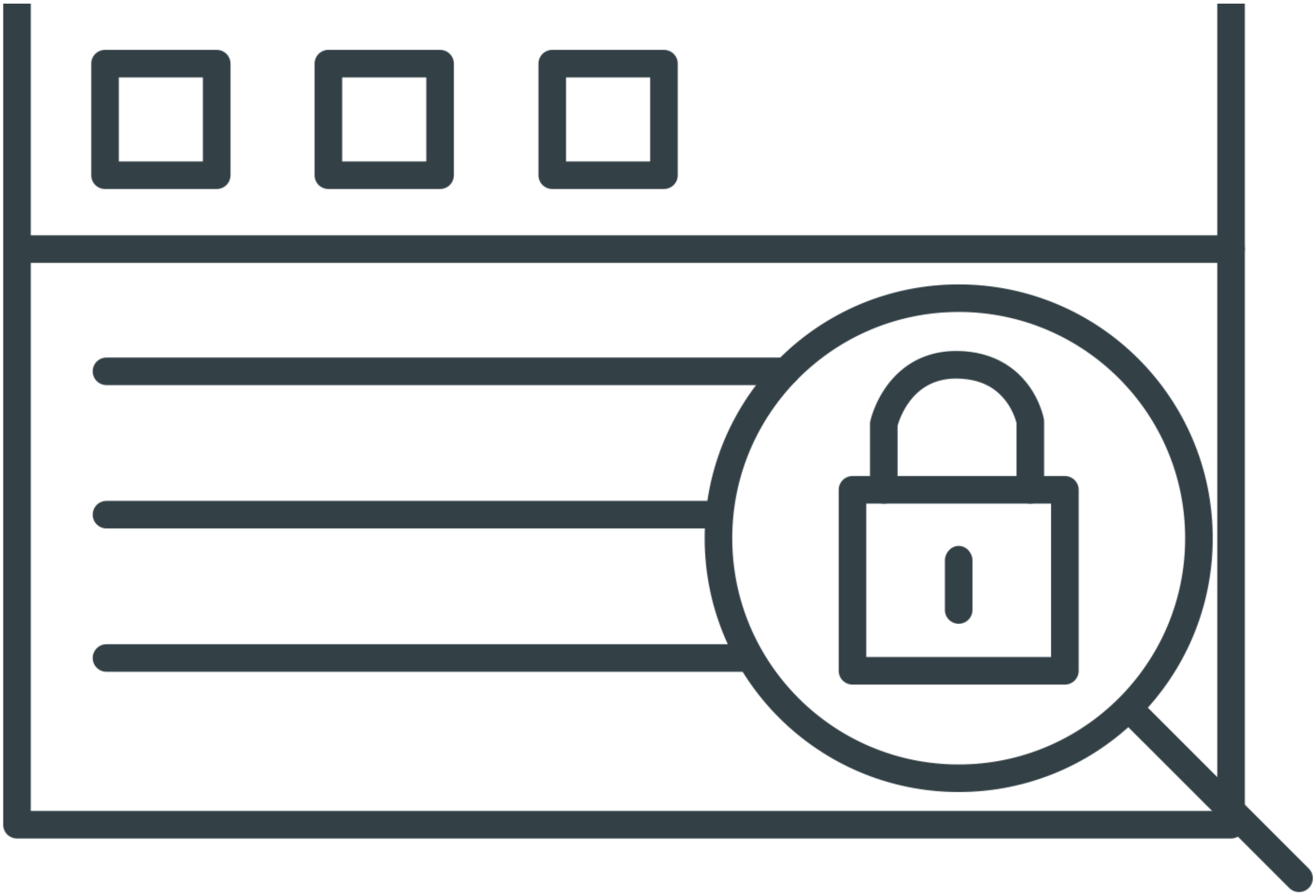
What are the visual implications of SSL?

As we've referred to a number of times throughout this guide, it is often the visual impact of an SSL certificate that has the biggest effect on users and potential customers. But how exactly does this work and what visual form will an SSL take on a site?

As with any purchase, online or not, most people will be more likely to buy from a reputable dealer. Certificates to prove authenticity or expertise in a certain field go a long way to making customers feel more secure.

That's exactly the visual impact an SSL certificate can have on potential clients. SSL and TLS are the industry's best and most accepted standards of security and certificates should be proudly displayed where everyone can see them.

CONTACT US



First of all, it will appear in the address bar. The site's pre-x will be https:// rather than the http:// and users are more frequently insisting on the difference.

The presence of the padlock icon in the address bar is also a big indication of safety. It reassures customers that their connection is secure and encrypted. And, as we've mentioned, it can make people more likely to complete a transaction.

By using the most secure form of certificate - the Extended Validation SSL certificate – the company name appears in green in the address bar. It's another sure-re way of letting customers know that it's 100% legitimate.

Lastly, many SSL certificates come with a seal image, which can be used on the site to display the brand of SSL which is being used. Let customers know that their security and information is protected and they'll be far more likely to trust the site with their cash. Research from 2013 shows that DigiCert SSL's SSL seal is the most recognized on the web (https://baymard.com/blog/site-seal-trust).

CONTACT US

What is an SSL Connection Error?

An SSL connection error occurs when the page being accessed has some security issues. They occur for users' protection, interrupting access to inform them that there may be some security concerns if they progress.

They can take a number of forms, often differing with the choice of browser. In some instances, the page may go red with the https:// prefix also highlighted in red. Using Google Chrome, there are a number of messages that users might see appear on their screen. These include 'your connection is not private' or simply that 'this webpage is not available'.

It might be as the result of outdated security code on the website and doesn't necessarily mean that the site being accessed is suspicious, but users should take connection errors seriously, especially if they are not 100% sure about the destination site.

Whilst there are ways to circumnavigate SSL connection errors, it is strongly recommended that users don't.

If in website development trials it is found that the site is suffering from SSL connection errors then it is imperative to do something about it quickly. This may involve updating the security settings or simply acquiring a more adapted SSL certificate. This will help browsers to establish that the site is secure and allow users to access it without safety warnings.

Does SSL Work on Email?

Most of the big email providers use SSL encryption to encrypt users' mail. In most cases, the SSL option will be automatically checked in email settings. To retrieve mail that has flagged up an error message the user may have to uncheck this option.

If the account where users retrieve mail supports SSL then they can select this option to have data sent through a secure connection.

If a company is setting up its own email service the IT team may need to check with their provider that they are also secured by SSL. This will eliminate security problems when sending out mail shots and individual mail.

How to implement an SSL certificate on a site

CONTACT US

Depending on how a site is hosted and where, there are various ways of adding an SSL certificate. In some cases, if there's an ecommerce element on the site, it will be a requirement to have a certificate. Major hosting providers often offer hosting packages including SSL certificates.

It may also be possible to transfer an existing SSL from other hosts (exporting it from the original server and importing it on the new server). It will be necessary to follow the special instructions on the webhoster's site. Note that some Certification Authorities require you to purchase a server license for each server that will host the certificate.

CLICK HERE FOR FULL INSTALLATION INSTRUCTIONS (HTTPS://KNOWLEDGE.DIGICERT.COM/GENERALINFORMATION/INFO212.HTML)

Trust and Your Business

Learn how DigiCert SSL helps boost your business by giving customers the confidence to click.

1 Hidden Dangers Lurking in E-Commerce - Reducing Fraud with the Right SSL Certificate (https://www.symantec.com/content/en/us/enterprise/images/mktg/Symantec/Email/12395/FY16_Q1_WP_Hidden_Dangers_Lurking_in_E-Commerce_0215.pdf)

2 The New Norton Seal (https://www.symantec.com/page.jsp?id=seal-transition)

3 The Psychology of Trust on Websites (https://www.symantec.com/ssl-certificates/psychology-of-trust/)

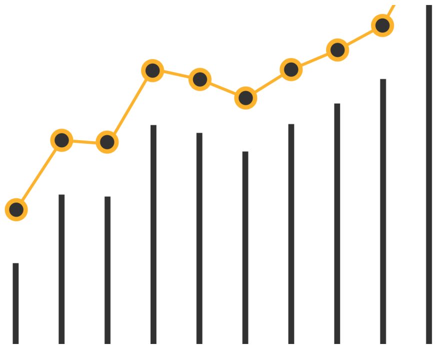
4 For Consumers - Stay Secure Online (https://www.staysecureonline.com/staying-safe-online/)

SSL Summary

SSL is an important security tool for business and one that is playing an increasing role in the success of online transactions. It's really not that complicated to buy and install, and help is available along the way with many SSL providers.

An https:// pre-x and padlock icon are just a few clicks away and can have a big impact on business; increasing sales, building consumer confidence and boosting web rankings all with one industry standard certificate.

CONTACT US



SSL Glossary

#

256-bit encryption (https://www.websecurity.digicert.com/security-topics/code-signing-sha-256-support)
Process of scrambling an electronic document using an algorithm whose key is 256 bits in length. The longer the key, the stronger it is.

A

Asymmetric cryptography
These are ciphers that imply a pair of 2 keys during the encryption and decryption processes. In the world of SSL and TLS, we call them public and private keys.

C

Certificate signing request (CSR) (https://knowledge.digicert.com/generalinformation/INFO235.html)
Machine-readable form of a DigiCert certificate application. A CSR usually contains the public key and distinguished name of the requester.

Certification authority (CA) (https://knowledge.digicert.com/generalinformation/INFO235.html)
Entity authorized to issue, suspend, renew, or revoke certificates under a CPS (Certification Practice Statement). CAs are identified by a distinguished name on all certificates and CRLs they issue. A Certification Authority must publicize its public key, or provide a certificate from a higher level CA attesting to the validity of its public key if it is subordinate to a Primary certification authority. DigiCert is a Primary certification authority (PCA).

Cipher suite
This is a set of key exchanges protocols which includes the authentication, encryption and message authentication algorithms used within SSL protocols.

Common name (CN)
Attribute value within the distinguished name of a certificate. For SSL certificates, the common name is the DNS host name of the site to be secured. For Software Publisher Certificates, the common name is the organization name.

CONTACT US

Connection error
When security issues preventing a secure session to start are flagged up while trying to access a site.

D

Domain Validation (DV) SSL Certificates (https://www.websecurity.digicert.com/security-topics/dangers-of-domain-validated-ssl)
The most basic level of SSL certificate, only domain name ownership is validated before the certificate is issued.

E

Elliptic Curve Cryptography (ECC) (https://www.websecurity.digicert.com/security-topics/ssl-algorithms)
Creates encryption keys based on the idea of using points on a curve to define the public/private key pair. It is extremely difficult to break using the brute force methods often employed by hackers and offers a faster solution with less computing power than pure RSA chain encryption.

Encryption (https://www.symantec.com/content/dam/symantec/docs/white-papers/how-endpoint-encryption-works-en.pdf)
Process of transforming readable (plaintext) data into an unintelligible form (ciphertext) so that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).

Extended Validation (EV) SSL Certificates (https://www.websecurity.digicert.com/ssl-certificate/secure-site-ev)
The most comprehensive form of secure certificate which validates domain, require very strict authentication of the company and highlights it in the address bar.

K

Key exchange (https://www.websecurity.digicert.com/security-topics/how-does-ssl-handshake-work)
This is the way users and server securely establish a pre-master secret for a session.

M

Master secret
The key material used for generation of encryption keys, MAC secrets and initialization vectors.

Message Authentication Code (MAC) (https://www.symantec.com/connect/articles/introduction-openssl-part-one?page=1)
A one way hash function arranged over a message and a secret.

O

Organization Validation (OV) SSL Certificates (https://www.symantec.com/connect/blogs/types-ssl-certificates-choose-right-one)
A type of SSL certificate that validates ownership of the domain and the existence of the organization behind it.

P

Pre-master secret (https://www.websecurity.digicert.com/security-topics/how-does-ssl-handshake-work)
The key material used for the master secret derivation.

Public key infrastructure (PKI) (https://www.symantec.com/ssl-certificates/managed-pki-ssl/)
Architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation (https://www.symantec.com/products/information-protection/pki/managed-pki-service) of a certificate-based public key cryptographic system. The PKI consists of systems that collaborate to provide and implement the public key cryptographic system, and possibly other related services.

S

Secure server (https://www.websecurity.digicert.com/security-topics/client-certificates-vs-server-certificates)
Server that protects host web pages using SSL or TLS. When a secure server is in use, the server is authenticated to the user. In addition, user information is encrypted by the user's web browser's SSL protocol before being sent across the Internet. Information can only be decrypted by the host site that requested it.

SAN (Subject Alternative Name) SSL certificates (https://www.websecurity.digicert.com/security-topics/san-ssl-certificates)
Type of certificate which allows multiple domains to be secured with one SSL certificate.

SSL
Stands for secure sockets layer. Protocol for web browsers and servers that allows for the authentication, encryption and decryption of data sent over the Internet.

SSL certificate (https://www.websecurity.digicert.com/ssl-certificate)
Server certificate that enables authentication of the server to the user, as well as enabling encryption of data transferred between the server and the user. SSL certificates are sold and issued directly by DigiCert, and through the DigiCert Managed PKI for SSL Center.

SSL Handshake (https://www.websecurity.digicert.com/security-topics/how-does-ssl-handshake-work)
A protocol used within SSL for the purpose of security negotiation.

Symmetric encryption
Encryption method that imply the same key is used both during the encryption and decryption processes.

T

TCP
Transmission control protocol, one of the main protocols in any network.

W

Wildcard SSL certificates (https://www.websecurity.digicert.com/ssl-certificate/secure-site-wildcard)
Type of certificate used to secure multiple subdomains.

(/content/websitesecurity/en/in.html) (https://www.websecurity.digicert.com/en/in) > Security Topics (https://www.websecurity.digicert.com/en/in/security-topics) > What is SSL, TLS and HTTPS?

Products (https://www.websecurity.digicert.com/en/in/products)

TLS/SSL Certificates (https://www.websecurity.digicert.com/en/in/ssl-certificate)

Code Signing Certificates (https://www.websecurity.digicert.com/en/in/code-signing)

Support (https://www.websecurity.digicert.com/en/in/support)

Support Information (https://www.websecurity.digicert.com/en/in/support)

Resources (https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https)

CONTACT US

Security Topics (https://www.websecurity.digicert.com/en/in/security-topics)

Security Fundamentals (https://www.websecurity.digicert.com/en/in/ssl-certificate#SSLTLSFundamentals)

What is SSL/TLS Validation (https://www.websecurity.digicert.com/security-

Partners (https://www.websecurity.d

Encryption Everywhere (https://www.websecurity.d everywhere/)

Become a Partner (https://www.digicert.com/p program/)

We have updated our Privacy Policy which can be found here (https://www.digicert.com/digicert-privacy-policy).

Help Me Choose (https://www.websecurity.digicert.com/en/in/help-me-choose)

Trust Center (https://www.websecurity.digicert.com/en/in/ssl-certificate/symantec-trust-center-enterprise)

Install the Seal (https://www.websecurity.digicert.com/en/in/install-norton-secured-seal)

SSL ement Tools (http w.digicert.com/certificate-mar ent/)

Contact Support (https://www.websecurity.digicert.com/en/in/support/contact)

Report Certificate Misuse (https://www.websecurity.digicert.com/en/in/support/contact)

Report Code Signing Abuse (https://www.websecurity.digicert.com/en/in/support/contact)

topics/what-is-ssl-tls-https)

Why DigiCert (https://www.digicert.com/)

Post Quantum Cryptography (https://docs.digicert.com/certificate-tools/post-quantum-cryptography/)

Enterprise PKI Solutions (https://www.digicert.com/

pki-platform/)

Legal Notices (https://www.websecurity.digicert.com/legal/repository) | Privacy Policy (https://www.digicert.com/digicert-privacy-policy) |
Terms Of Use (https://www.websecurity.digicert.com/en/in/legal/terms) | Site Map (https://www.websecurity.digicert.com/en/in/sitemap) | Cookie Settings

(https://twitter.com/digicert) (https://facebook.com/digicert) (https://www.linkedin.com/company/digicert-inc-)

(https://www.youtube.com/user/DigiCertSSL)

Certification Authorities WebTrust (https://www.digicert.com/webtrust-audits/)

CONTACT US