Securing your brand and your reputation

A straightforward guide to understanding TLS/SSL certificates

ENTRUST

SECURING A WORLD IN MOTION

A foundation for protection, privacy, and brand integrity in the digital realm

Almost every organization, from global enterprises to local shops, is on the path to digital transformation. For most, websites serve as the epicenter of those emerging digital infrastructures – and they provide the most common points of interaction for organizations and the people they serve. Online interactions often include high-value financial transactions or involve the exchange of private information, while others are more basic exchanges of information. But no matter how simple they may seem, every online interaction needs to be protected against malicious attacks.

Website visitors need to know they are connecting to their intended sites and organizations. Increasingly, consumers are paying attention to cybersecurity events and making buying decisions and forming brand loyalties accordingly. A 2020 Frost & Sullivan Report, in fact, found that 48 percent of consumers terminated paid-for relationships with companies that reported a breach. Website owners need to ensure that communications, personal information, and financial data are protected from the beginning of a website visit to the end.

TLS/SSL certificates provide the foundation for this protection and privacy. They establish trust between parties and provide encryption-based protection for identity and transaction data. This guide provides you with a working understanding of TLS/SSL certificates and offers advice on how to select, buy, and deploy them.

What exactly is a digital certificate?

A TLS/SSL certificate uses asymmetric encryption and public/private key pairs to provide secure communication between entities such as websites, individuals, and organizations. Public keys encrypt data, while private keys decrypt data. Certificates provide identity assurance and encryption to prevent the risk of theft or interception of data in transit.

What are TLS/SSL certificates?

One point of clarity is important before we explain TLS/SSL certificates. The certificates we're discussing here are most often called "SSL certificates." SSL stands for secure socket layer, and it refers to an explicit cryptographic method of ensuring online identity and security that was developed in 1994. As with most technologies, the original SSL protocol became vulnerable over time to malicious attacks and was improved over the years to provide the necessary protection. After several iterations to provide more secure versions of the protocol it evolved to Transport Layer Security (TLS), which is based on implicit connections. The industry is currently on TLS 1.3, but the most common certificates are TLS 1.2.

Many users of certificates still use the "SSL certificate" vernacular out of habit or convenience. However, they are most likely referring to TLS certificates. TLS/SSL certificates serve two vital purposes. First, through the encryption of communications technology, they ensure the security and integrity of information that's transmitted over the internet. Without the shield of encryption, data is left in the clear and susceptible to attack. Secondly, digital certificates provide identity assurance, so website visitors know precisely who they are interacting with.

The digital landscape provides a lucrative opportunity for bad actors to pursue fraud and identity theft in an enterprise setting. Stealing data and money is incredibly easy for cyber criminals. This concept of identity is critical. TLS/SSL certificates are analogous to digital passports that provide site visitors with the ability to view a business's identity online along with encryption to protect the confidentiality and integrity of website communication with browsers. When a valid EV or OV TLS/SSL certificate is present on a website, visitors can be confident that they are dealing with a legitimate entity as they share personal information, credit card numbers, and other sensitive data. In today's environment, browsers issue negative security indicators to users where websites do not have a valid TLS/SSL certificate. So, the absence of a valid certificate is sure to turn valued visitors away.

Why are TLS/SSL certificates so important?

Deploying TLS/SSL certificates is key to protecting your organization, prospects, and customers from increasingly menacing and costly cyberattacks related to website transactions. Your reputation, your financial stability, and your visitors' privacy are all at stake. The total amount of money generated by hackers in 2020 was more than $6T, which would make cybercrime the third-largest global economy after the U.S. and China.[1] Search engines are cracking down on websites that pose security threats to visitors by implementing negative security indicators and removing sites from search engine listings. Here are other reasons why trusted TLS/SSL certificates from a reputable certification authority are necessary:

Data security
Your data and your visitor's data are always encrypted with a comprehensive certificate strategy. All transmitted data is secured and can be accessed only by intended recipients. This is critical for protecting passwords, credit card numbers, financial transactions, and other high-value data.

Trusted identity
The issuance of EV and OV TLS/SSL certificates is tightly controlled by certification authorities (CAs). Depending upon the type of certificate, the CA verifies the identity of requesting organizations, confirms the organization has control over the domains, and ensures the requestor of the certificate is employed by the organization.

Search engine ranking
Google and other search engines use algorithms that determine the existence and validity of TLS/SSL certificates on websites. If certificates are missing, not installed correctly, or expired, the site's search ranking suffers. This is true for all websites, even those that do not conduct financial transactions or collect highly sensitive personal data.

Escalating compliance requirements
There are a variety of global standards for websites that are largely focused on protecting the privacy and assets of consumers. A notable law is the General Data Protection Regulation (GDPR), which has been implemented in Europe, but is being widely emulated throughout the world. Organizations that violate GDPR standards are subject to a fine of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. Organizations that process online payments typically need to meet PCI DDS requirements. The latest PCI DSS regulation requires that organizations use TLS/SSL certificates that use the SHA-2 hashing algorithm.

[1] Cybersecurity Ventures, 2020 study

Secure handshake: step-by-step view

1 Browser/server connects to a website secured with TLS/SSL certificate

2 Browser requests certificate-based identity confirmation

3 Web server sends a copy of its TLS/SSL certificate

4 Browser verifies the certificate and sends a session request to the web server

5 Web server sends back a digitally signed acknowledgement to begin the session

6 Encrypted data is shared between the browser and the web server

How do TLS/SSL certificates work?

When someone wants to engage with a website – for a wide range of reasons from online banking to distance learning to scheduling appointments – a browser or server attempts to connect to the intended website. If the site is not secured by a trusted TLS/SSL certificate, the visitor receives a security warning presented by the browser. If a visitor receives this warning, it is highly recommended that they abandon the session, because their data and their privacy are likely at risk.

If a trusted TLS/SSL certificate is present, the browser asks the web server to identify itself. In response, the web server transmits a copy of its own TLS/SSL certificate. The browser that initiates the session checks the validity of the certificate and determines if the site can be trusted. If the site's identity is validated, the browser sends a message to the web server, which, in turn, transmits a digitally signed acknowledgement to initiate an encrypted session. Once the session is initiated, all data is encrypted. This provides a strong line of defense against "man-in-the-middle" attacks that are intended to steal data or otherwise corrupt communications between visitors and websites.

Various types of certificates

Most certificate providers offer a range of certificate types depending upon a number of factors, including desired assurance levels, compliance requirements, and the number of domains being secured.

EV SSL Certificates
Extended Validation (EV) SSL certificates provide the highest assurance security, and the application process is the most rigorous. When deployed on a website, a padlock icon, the organization's name, and the HTTPS designation become visible to visitors. This type of certificate is generally used for web applications that require identity assurance for collecting data, processing logins, or conducting online payments.

OV SSL Certificates
Organization Validation (OV) SSL certificates provide identity assurance and encryption and are best suited for encrypting user information during transactions. Most consumer-facing websites are legally required to deploy OV SSL certificates to ensure information communicated during a session remains confidential.

DV SSL Certificates
Domain Validation (DV) SSL certificates offer low assurance and lesser identity validation than EV or OV certificates only proving domain control. They're often used for low-risk applications, such as blogs, user communities, or informational sites. This makes DV certificates less expensive and easier to obtain.

Wildcard SSL Certificates
Wildcard SSL certificates are verified to the Organization Validation level and a cost-effective solution for securing a base domain and any number of affiliated subdomains. In addition to lower costs (than buying multiple individual certificates), they offer greater simplicity because users don't have to submit multiple certificate signing requests (CSRs) or manage the expiration dates for multiple TLS/SSL certificates across multiple URLs.

UC SSL Certificates
Unified Communications (UC) SSL certificates are verified either to the extended validation or organization validation levels. An efficient way to consolidate multiple certificates is by leveraging Subject Alternative Names (SANs) for cost savings. UC SSL certificates establish trusted identities and eliminate browser notifications that warn visitors against entering your site.

WANT TO SIMPLIFY THE BUYING EXPERIENCE?

Not all TLS/SSL certificates are the same. Use our interactive certificate selector tool below to find the certificate that best suits your needs. You can view our certificate selector here.

Tips for choosing and acquiring certificates

Getting started with the right certificates

The EV and OV TLS/SSL certificate process begins when you generate a Certificate Signing Request (CSR) and submit it to Entrust. Please note, you must own your domain name: Entrust cannot process Server Certificates if a domain name is not registered to the requesting company, its parent organization, or one of its subsidiaries. You'll be required to provide a business telephone number that can be found using a third-party search directory, along with valid contact information. An authorization contact must be a senior member of your organization and have the authority to request certificates on behalf of the organization.

A technical contact will be notified regarding initial purchases, renewals, and updates. This technical contact is typically someone responsible for daily management of your website or the Web Server, where the certificates will be installed. If your server(s) are hosted by a third-party or hosting provider, someone within that organization should be listed as the technical contact.

When applying for a TLS/SSL certificate, you will need the following information:

- Valid payment information
- Authorizing contact
- Technical contact
- Billing contact
- CSR
- List of domains
- Organization name

When Entrust issues a TLS/SSL Certificate, that certificate leverages the trust of the Entrust® Root Certificate, which is embedded in the internet browsers that your customers or other visitors will use to access your websites. By issuing a certificate, Entrust is attesting that the certificate we issued to you confirms your organization's identity and ensures visitors can communicate and transact safely with your site.

Please note, it takes typically three to five business days to receive certificates within North America and five to 10 business days in other parts of the world.

Why the world trusts Entrust TLS/SSL certificates

Entrust is a founding member of the Certificate Authority (CA) Security Council and the CA/Browser Forum. Our digital security experts actively contribute to the development of industry standards for TLS/SSL, S/MIME, document signing, mobile device, code signing certificates, and certificate management. We also offer the most trusted portfolio of digital certificates, including Entrust SSL Certificates and Qualified Certificates to meet a full range of enterprise requirements. With unique features, including strong encryption and browser trust, our certificates provide best-in-class security and help ensure compliance with regulations, including PSD2 and eIDAS.

Advantages of Entrust digital certificates

- 24x5 support
- Unlimited reissues
- SHA-2/2048-bit keys
- SSL server test
- Website security
- Unlimited server licensing
- 128- to 256-bit encryption
- Compatible with 99.9% of browsers

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all of these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us. To learn more, visit entrust.com.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact