White Paper

What do you mean I need a TLS/SSL certificate?

A guide to TLS/SSL certificates and their use cases

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

INTRODUCTION

What is a TLS/SSL digital certificate?

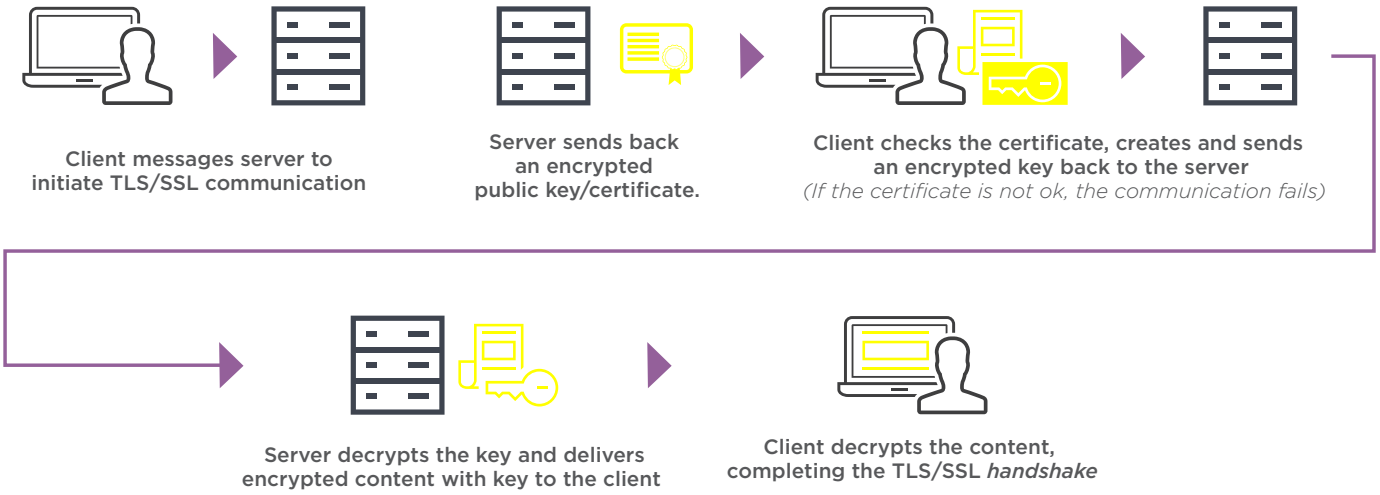
Organizations of all types and sizes employ TLS/SSL digital certificates to provide security in the form of encryption technology and in most cases identity assurance. Mostly the use of TLS/SSL certificates is voluntary; however, certain industry activity and local regulations can make it difficult for organizations to do business online without them.

TLS/SSL certificates can only be issued by a certification authority (CA) under the guidelines put forth by the CA Browser Forum. Used for website encryption and identity assurance, TLS/SSL are arguably the most common type of digital certificate. The differences between the varieties of TLS/SSL certificates offered lie beyond the technology and are instead rooted in the level of trust you're providing to the website visitor, as well as your relationship with the issuing CA and their reputation as a reliable and trustworthy vendor. If the issuing CA has a reputation for being "phishy," chances are you're not providing optimal security or much trust to your online customers.

Consumers expect the financial services institutions and ecommerce businesses that they transact with to secure their personal data. The TLS/SSL certificate prevents a third-party from hijacking personal information (e.g., user names, passwords, and credit card information) while it is being transmitted from the customer's device (client) to the organization (server).

Organizations want to protect private customer data and prevent browser error messages from thwarting website traffic. Browsers send up trust dialog boxes alerting website visitors when a website is not encrypted or if a TLS/SSL certificate has expired. Some major browsers require encryption on web pages where any customer data is requested regardless of whether or not it is a financial transaction (e.g., email address for newsletter registration).

TLS/SSL certificates serve two purposes: They encrypt information and provide identity assurance. Both help online consumers positively identify websites that are safe for transacting with. This is how a TLS/SSL certificate works:



The three TLS/SSL certificate types that provide public trust, in other words, over the internet rather than internally, are: extended-validation (EV), organization-validated (OV) and domain-validation (DV) certificates. Higher assurance SSL certificates like EV and OV strengthen security by including verified organization identity information in the certificate that was confirmed by an independent CA. This tells website visitors that the website is associated with a real organization, which is important information to prevent fraudulent activity like phishing. DV certificates provide the same level of encryption, but they are easy to attain anonymously and therefore are the highly preferred certificate of choice for fraudsters to use on their websites.

The regulating authority for online payments makes this recommendation in their PCI Data Security Standard:

Recommendations

For a relatively small additional cost (compared to a DV certificate), a legitimate business conducting e-commerce could purchase an OV or EV certificate. This would prove to the consumer the business has been validated by the CA and has provided address and other independently verified contact information in the certificate that the consumer could use in case of questions or problems.

Higher assurance certificates come with a higher price tag. The amount of verification checking behind the various certificate types attribute to the pricing variations. The cost of a higher assurance certificate is small, especially when considering the costs incurred when an organization suffers a data breach.

EV or OV TLS/SSL certificates

A mix of EV and OV certificates are widely used by organizations that want to provide their customers with strong encryption technology as well as deliver identity assurance. Identity assurance helps customers recognize whether or not a website is legitimate. It also prevents the brand from suffering damaging losses associated with phishing scams and other nefarious online activity.

EV and OV certificates are used primarily for client-to-server transactions where sensitive information (e.g., username, password, credit card information, etc.) is being transferred over the Internet. Encryption ensures the data cannot be stolen as it makes its way to the organization. The identity piece gives website visitors the ability to positively identify the website that they're on.

The amount of verification checking behind the various certificate types is reflected in the pricing variations. The increased vetting for EV and OV certificates is what makes high assurance certificates more expensive. EV certificates come with the most comprehensive verification checking, which includes domain verification, cross-checks among several governmental and internal checkpoints that tie the entity to a specific physical location. This type of verification leaves a detailed paper trail where customers have recourse should they be victimized by any nefarious activity that takes place while transacting on that website. EV certificates are represented differently in the various browsers, but can be distinguished by clicking on the locked padlock symbol in the URL. The Page Info shows the name of the domain owner, giving users a clear indication of whether or not they are on an authentic website.

Major browsers indicate that a website is secured with DV certificate by the padlock with HTTPS in the address bar, but do not show organization details because they do not exist. These certificates validate domain ownership only, and do not tie a domain to a person, place, or entity.

[1] *Best Practices for Securing E-commerce Special Interest Group by PCI Security Standards Council, January 2017.*

Domain-validated (DV) certificates

DV certificates are great at separating encryption from authentication. In the absence of identity checks, DV certificates lack the critical component of having digital forensics, and that's where they differ from EV or OV certificates. All three certificate types provide the same strong level of encryption technology.

DV certificates are best used for situations that do not necessitate the important aspect of identity assurance, making them a good choice when rapid acquisition of encryption-based technology for server-to-server communication is needed. DV certificates can be recommended for the following use cases:

- Basic websites that do not require personally identifiable information (e.g., email address, username, password, credit card information, etc.)
- Digitally transferred software updates

The purpose of a DV certificate is to provide IT professionals with a fast and affordable way to encrypt non-sensitive data that is passed over the Internet. Some CAs issue DV certificates via an automated process at no charge – the domain owner doesn't even supply a credit card – automated issuance of DV certificates has led to an increased number of certificates, allegedly used for phishing sites according to this phishing article by Vincent Lynch on hashedout (by The SSL Store). This protects the fraudster's identity, clearing the way for them to commit fraud.

Choosing the right TLS/SSL certificate

When you understand your customer's unique business needs, you will be able to recommend the right TLS/SSL certificate or certificate mix to encrypt their web application(s). Here are some good questions to help you drill down to the particular TLS/SSL certificate type(s) to recommend.

1. What will the TLS/SSL certificate be used for?

2. How much protection do you want to provide to your business and your customers?

- What level of identity assurance do you want to provide online shoppers?
- How important is it to protect your brand from phishing scams?

3. How many domain names need to be secured on this certificate or server?

- Are there multiple servers?

5. What is your budget?

Refer to the "Use Cases" section of this white paper for recommendations on matching the right certificate type(s) with specific business purposes.

Use cases for common IT environments – TLS/SSL certificates

HTTPS connection for a single domain

This represents someone with a basic website that has only one possible domain via HTTPS (e.g., https://www.example.com).,

Recommendation

a. If sensitive information is requested (e.g., login or credit card transactions) for client-to-server transmissions: EV certificate is recommended for highest identity assurance.

b. If sensitive information is not requested, but the customer wants the SEO benefits of HTTPS visual indicator or needs to transfer non-sensitive information from server-to-server (e.g., internal software updates): DV certificate

HTTPS connection for multiple domains

Useful for an organization with a basic website secured with TLS/SSL and the site allows multiple domains for HTTPs delivering the same web content (e.g., https://www.example.com and https://example.com).

Recommendation

a. If sensitive information is requested (e.g., login or credit card transactions) for client-to-server transmissions: EV certificate is recommended for highest identity assurance.

b. Sensitive information is not requested, but the customer wants the SEO benefits of HTTPS visual indicator or needs to transfer non-sensitive information from server-to-server (e.g., software updates): Two DV certificates (one for each URL)

Microsoft Exchange or Skype for business server

A unique domain for each service is usually required in desktop client-to-server environments using a Microsoft Exchange server: Webmail/IIS, SMTP, POP, IMAP and UM.

Recommendation

a. To secure multiple domains on one certificate: a UC Multi-domain/SANs certificate is recommended. UC Multi-domains are also useful whenever there's a need to secure multiple names across different domains.

Server-to-server

Situations when mutual authentication between two servers is needed and the certificate extension, EKU, requires client authentication (e.g., Exchange TLS between two organizations where one organization has a server with data that it needs to send it to a third party for processing. This is where mutual authorization is used, which does not require a browser).

Recommendation

a. OV certificate that supports Client and Server Authentication

Front-end TLS/SSL offloading

When a TLS/SSL connection needs to be offloaded from servers to a front-end device (e.g., F5 BIG IP), individual servers do not require a certificate, and EKU requires server authentication.

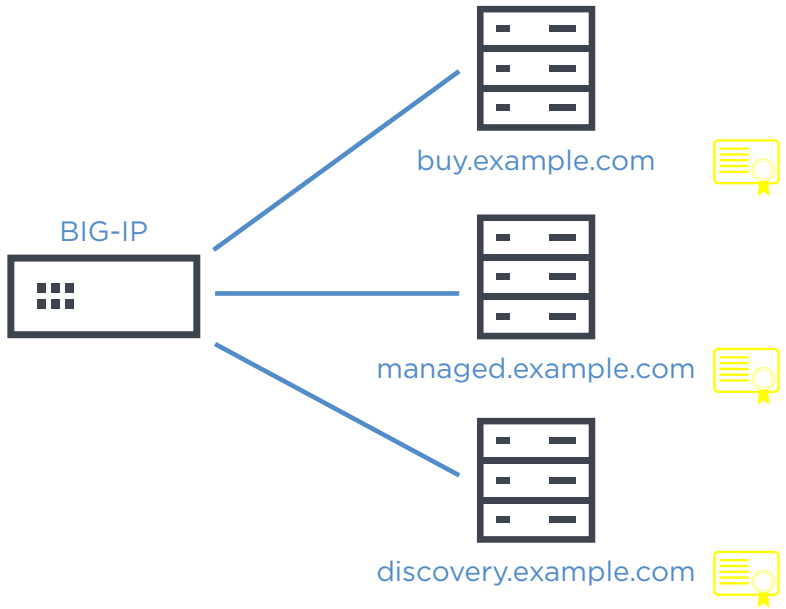
Recommendation (see image)

a. 1 OV certificate for each server

b. EV certificate(s) to secure each server
SAN = buy.example.com
SAN = managed.example.com
SAN = discovery.example.com

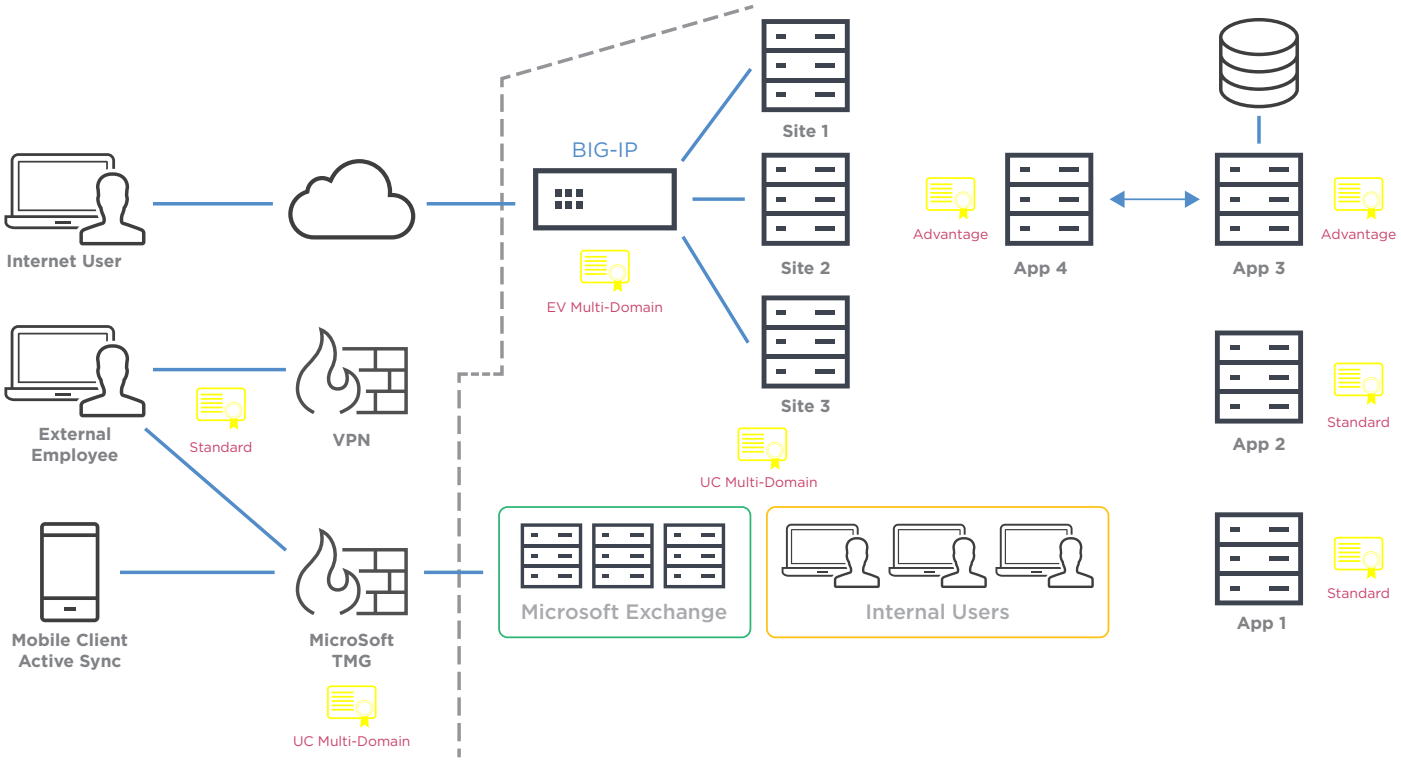
c. UC Multi-domain, secures multiple domains on one certificate
SAN = buy.example.com
SAN = managed.example.com
SAN = discovery.example.com

d. Wildcard, if they share a common root domain (e.g., *.example.com)



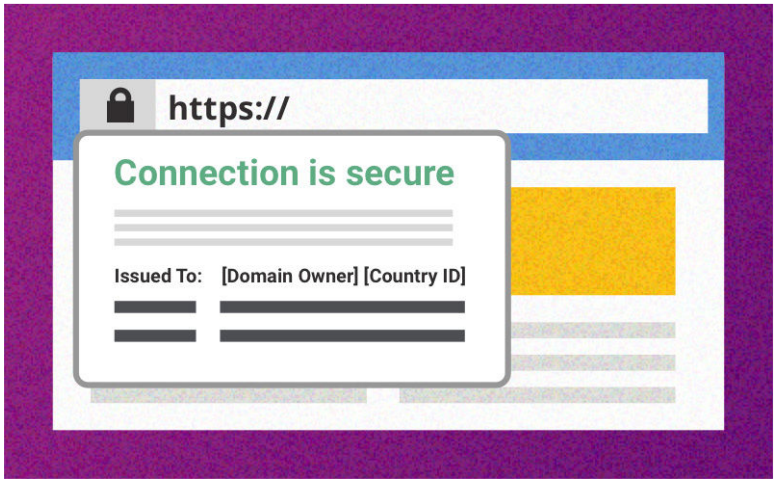
Enterprise Environment

A typical enterprise environment uses a variety of TLS/SSL certificates to encrypt communication throughout their diverse IT ecosystems.



Visual indicators in the UI

Visual indicators vary by browser and are subject to change. Users can find website identity information by clicking on the padlock and reviewing the Page Info for Google and Mozilla.

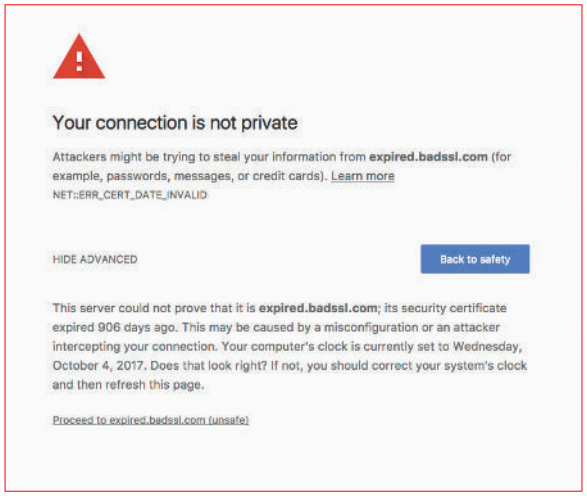


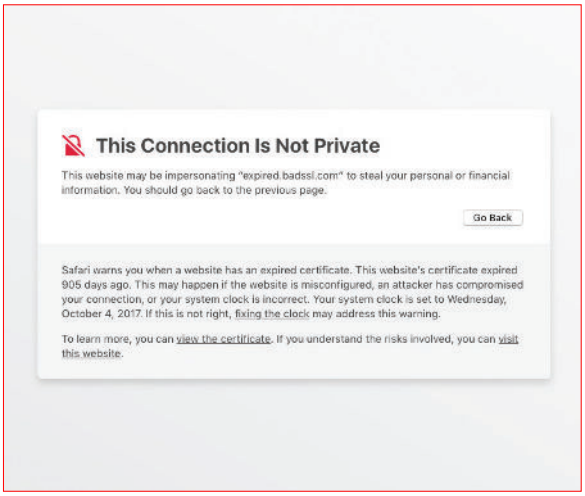
Here's why TLS/SSL is important to organizations of all sizes

Some major browsers require websites to have the security of a TLS/SSL certificate on web pages that request personal information (e.g., username, password, credit card information, etc.) to ensure that end-user transactions are encrypted. Some, like Google Chrome, reward encrypted websites with more favorable search rankings.

Web pages that are not protected with a TLS/SSL certificate may show a browser warning, flagging your website as unsecure when a visitor approaches. Imagine a customer or prospect being greeted by this when they navigate to your website?

Browsers also downgrade TLS/SSL certificates if certain conditions are not met. For example, an expired or revoked certificate (see image below) can also trigger a browser warning to website visitors.





An expired TLS/SSL certificate might show this web browser warning.

The visual indicators depicted here were current at the time of publishing and are subject to change.

CONCLUSION

Maintaining a trusted and valid TLS/SSL certificate is an important part of e-commerce. Encryption and identity assurance gives online customers confidence to transact on a website. And, it's important for domain owners to comply with the practices established by the major web browsers to avoid browser warnings that could scare customers away from the website. Having the right TLS/SSL certificate in place for your use case provides a trusted connection for customers to transact and a more secure Internet for organizations and the people who use it.

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

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 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.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com