Wildcard and SAN: Understanding Multi-Use SSL Certificates

LEVERAGING MULTI-USE DIGITAL CERTIFICATES TO SIMPLIFY CERTIFICATE MANAGEMENT AND REDUCE COSTS

Wildcard and SAN: Understanding Multi-Use SSL Certificates

When you employ web-based services on the Internet, SSL certificates are the industry standard for authentication and security. Depending on how you plan to use SSL certificates, multi-use certificates can provide greater flexibility than traditional certificates. Multi-use certificates protect multiple Fully Qualified Domain Names (FQDNs) and subdomains, lowering your administrative costs and simplifying certificate installation, management, and deployment.

About Digital Certificates

The best way to prove your identity on the Internet is to use a digital certificate. A digital certificate relies on a trusted third-party authority, or Certificate Authority, to verify your identity and then uses a chain of trust that begins with you and works up to the trusted authority to validate your identity. This chain of trust provides verifiable security on the internet. Digital certificates provide:

PROOF OF AUTHENTICITY

Digital certificates demonstrate and validate the authenticity of the source of the web content.

INTEGRITY

Digital certificates make it difficult to modify content in transit because the content is encrypted.

AVAILABILITY

Digital certificates enable the availability of secure information exchange online. By providing a constant verification service, Certificate Authorities identify bad risks for certificates and mitigate those risks through a series of lists and checks.

CONFIDENTIALITY

SSL encrypts data both in the content itself and in the transport mechanism that is used to send the data to a destination on the Internet, ensuring confidentiality.

Using SSL to Move HTTPS

Organizations that process transactions on the Internet, or offer Internet-based services, rely on digital certificates to validate that they are who they claim to be, ensuring trust in their services. Most organizations add certificates to their Internet-facing servers to ensure accurate proof of their identity.

When a customer accesses a web page that is hosted on a server with a digital certificate, their web browser automatically detects the certificate and modifies the session. The session moves from an “open” session that uses Hypertext Transfer Protocol (HTTP) to a secure HTTP (HTTPS). HTTPS allows for the encryption of all the data sent between the user’s computer and the server.

Secure Sockets Layer

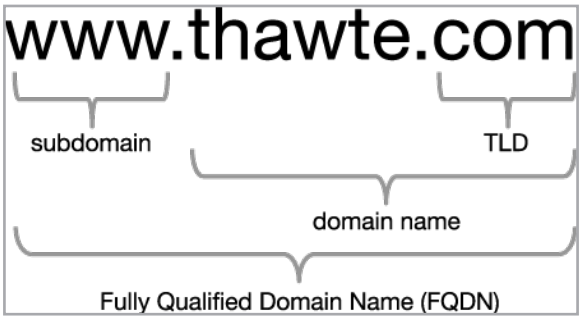
Secure Socket Layer (SSL) provides HTTPS data encryption. SSL creates an encryption tunnel between the client and the server that protects the transfer of data from one point to the other during the communication exchange. You know you are using SSL when the web address starts with https:, and your browser displays a closed padlock in its status bar, and/or you see a green background in the address bar. Note that the green background in the address bar and the padlock are hallmarks of an Extended Validation (EV) SSL certificate. Extended Validation certificates provides the highest level of authentication available for a SSL certificate. Because EV SSL authentication standards require strict issuance and management processes established by the CA/Browser Forum, EV SSL Certificates provide an extra layer of protection for online businesses and their customers.

A SSL trust mark or site seal lets your customers know that a Certificate Authority has authenticated and verified your organization.

Protecting Servers and Services with SSL Certificates

To enable SSL on an externally facing server, an organization must purchase a certificate from a trusted Certification Authority (CA). The organization purchases one certificate for each service that it plans to protect (e.g. email, instant messaging, mobile device management, and web-based interactions).

An SSL certificate contains the service's Fully Qualified Domain Name (FQDN) and ties a service's domain name to the server. This combination makes it possible for a browser (or another agent) to compare the domain name that the service accesses with the domain name of the certificate.



Maintaining SSL Certificates

Certificates last for a finite period of time: typically one, two, or three year periods. To avoid maintenance every year, it is recommended you purchase certificates that are valid for extended periods of time.

It's also convenient to select static service names because each time a service name changes, the certificate must change on each server that provides the service. These strategies reduce the workload associated with periodic renewal and installation of certificates on your servers.

Services that use subdomain names (names that use the same root, or domain name, but have a different prefix, or subdomain name) have an additional maintenance overhead. Because subdomain names are embedded into SSL certificates, organizations usually buy one certificate per service. If the organization protects numerous services with unique certificates, this can become expensive and timeconsuming to manage.

Types of Multi-Use SSL Certificates

Two types of multi-use SSL certificates can greatly reduce the complexity of managing SSL for services and subdomains.

- A **Wildcard Certificate** allows you to secure multiple subdomains under a single unique FQDN. Using one wildcard certificate not only simplifies certificate management, but also lowers your administrative costs while providing immediate protection to current and future subdomains.

- A single **Subject Alternative Name (SAN) Certificate** can secure multiple FQDNs. SAN certificates provide flexibility when your websites do not share the same domain name. Unlike Wildcard Certificates, SAN certificates have the additional benefit of being able to support deployments that require Extended Validation (EV) certificates.

Wildcard Certificates

Wildcard certificates are regular SSL Certificates that support the wildcard character "*" as a prefix to the FQDN, allowing it to secure multiple services. Wildcard certificates do not include specific service names and always contain a wildcard character that prefixes the domain name.

A wildcard certificate can be more flexible than using multiple single purpose certificates because you can apply the wildcard certificate to a number of different services. You can also add, change, or replace services without needing to update the certificate or purchase new certificates.

A single wildcard certificate–like *.thawte.com–can secure the following domains:

www.thawte.com
finance.thawte.com
mail.thawte.com
sip.thawte.com
register.thawte.com

However, it cannot secure:

www.thawte.ca
mail.test.thawte.com

For example, suppose you want to protect servers that run an instant communication protocol like Session Initiation Protocol (SIP) and an email service. With single-use certificates, you need two certificates because you have to embed the name of each service into each certificate. As long as the domain is the same, however, you can secure both domains with one wildcard certificate. So the wildcard *.thawte.com can secure both sip.thawte.com and mail.thawte. com with just one certificate.

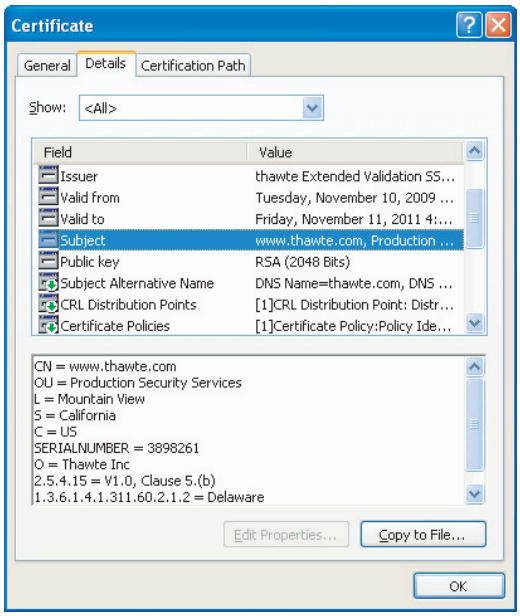
Using a wildcard character as a placeholder in the domain name embedded into the certificate makes the certificate more flexible. You can also apply it to any number of services since the wildcard character can represent any subdomain name, simplifying the certificate management process.

Because wildcard certificates manage multiple subdomains and the services names they support, they can be less secure than SAN certificates. We do not recommend their use as the primary certificate solution for enterprises. When you deploy a wildcard certificate, always make sure that you implement strong logical and physical policies to protect your assets.

Subject Alternative Name (SAN) Certificates

Subject Alternative Name (SAN) certificates enable you to include multiple FQDNs in one certificate. Unlike wildcard certificates that can support an unlimited number of prefix or subdomain names as long as the domain name remains the same, SAN certificates only support the FQDNs entered into the certificate. Depending on the issuing Certificate Authority, SAN certificates can support 100 or more different FQDNs in one certificate.

A SAN certificate includes the standard Subject Name field, which supports a single primary web-based service name. The subject name is what the certificate secures, as listed in the example below in the component fields. It consists of a Common Name, Organization, Organizational Unit, Locality, State, and Country. It has an additional field–the Subject Alternative Name (SAN) field–for additional service names. You can install a SAN certificate on several servers, where it supports internal and external service delivery.



SAN EXAMPLE

One SAN certificate can protect:

- yourbusiness.co.uk
- mybusiness.com
- yourbusiness.net
- products.yourbusiness.com
- support.products
- yourbusiness.com

Subject Alternative Name (SAN) certificates are also called Unified Communications Certificates (UCC) because they were primarily designed to support real-time communications infrastructures.

SAN certificates, or UCCs, are useful when organizations want to use different root or domain names to run Internet-facing services. For example, an organization that provides internal (sip.thawte.net) and external domain (sip.thawte.com) unified communications services can use a single SAN certificate to secure both FQDNs. The organization would need two wildcard certificates because thawte.net and thawte.com are different domains.

Another way to use a SAN certificate is when you validate secure internal and external services.

You might have both an internal and external SIP service for instant messaging: internal sip.thawte.com and external sip.thawte.net. In this situation, you must have a certificate on each server in the internal and external service to allow your users to work whether they are in the office or on the road. The same scenario applies for instant messaging infrastructures where you want to encrypt both internal and external messages. Note that servers cannot include two certificates for the same purpose.

SAN certificates are also useful for Application Service Providers (ASP) who host applications for multiple clients with each client using their own domain name. By using a SAN certificate, ASPs can use a single certificate to support multiple clients. Note that the site seal and certificate are only for the primary domain name entered in the certificate and do not include any of the other domain names. The certificate includes all of the domain names verified at the time of purchase.

SAN certificates have the same issues as single-purpose certificates. When the actual service names are embedded into the certificate, your services must always use the same name otherwise you have to change the certificate. Because the certificate is a multi-use certificate, you change it on each of the servers that host the certificate-supported service. When you want to add services to provide further functionality to your users, you must update the SAN certificate with the new service names.

While SAN certificates are useful for supporting unified communications deployments, keep these caveats in mind:

- SAN certificates do not support wildcard characters. For this reason, you need to add subdomain names as unique domain name entries in the certificate at the point of purchase. Each time you want to add a new domain name or you remove an old one, you need to update and re-deploy the certificate to each host server.
- When hosting web sites for multiple clients, ASPs should be aware that all domain names are visible in a SAN certificate. If the ASP does not want one site to appear connected to another, use a different kind of certificate.

Making the Selection

Multi-use certificates can secure multiple web services using a single certificate. To accomplish this, these certificates either add a subject alternate name field to the common single-use certificate or use a wildcard to replace the subdomain or prefix name in the certificate.

Multi-use certificates save money and simplify management by including multiple names within the same certificate or replacing service names with a wildcard. Use SAN certificates when you need multiple domain names for each service.

WILDCARD CERTIFICATES

Use a wildcard certificate when you want:

- a single domain name for all services
- a single domain and multiple subdomains that cover all services

SAN CERTIFICATES

Use a SAN certificate when you want:

- unique domain names for each service
- the option of providing Extended Validation protection

In Summary

Most organizations use a least one public domain name and one private domain name to segregate their internal and external name spaces. In this case, only SAN certificates work.

For organizations that only use one single public domain name the wildcard certificate may be a good option.

Multi-use certificates make it much easier to deploy multiple secure services both internally and externally and have distinct advantages in lowering costs and reducing resources. This ease of deployment is particularly useful in environments that include several services such as mail, instant messaging, web, mobile device management, and File Transfer Protocol. If this is the situation that applies for your organization, then your best choice is a multi-use certificate designed to fit your needs.

Wildcard vs. SAN Certificates

The following table provides you with an overview of the differences between the SAN and wildcard certificates.

Certificate Feature	Wildcard	SAN	Comment
Multiple secure domain support	Yes	Yes	Both certificate types support multiple secure domain names. Wildcard supports multiple sub domains to one domain, per certificate. SAN-enabled certificates can support multiple domain names; the limitation is the number of SANs per certificate established by the CA.
UCC or SAN support		Yes	Both certificate types support multiple uses. Microsoft Exchange Server, Microsoft Office Communications Server and Microsoft System Center Mobile Device Manager use SAN.
Number of Fully Qualified Domain Names (FQDNs)	1	Multiple	Wildcard certificates only support one single domain name, but a nearly unlimited number of subdomains. SAN-enabled Certificates can support multiple domains, multiple host names, etc. The limitation is the amount of SAN's per certificate. This limitation is established by the Certification Authority.
Domain name ownership	1	Multiple	An organization must own, or be authorized to use, any and all domains in the certificate's subject. The Wildcard product and SAN functionality are subject to these basic requirements.
Domain name format	*.name.com	Multiple	Wildcard certificates use a single name format (*.name.com). SAN certificates can use any FQDN.
Name flexibility		Yes	In a Wildcard certificate, only the subdomain can change. Additionally, a subdomain must exist in place of the wildcard character; for example, https://*.thawte.com cannot secure https://thawte.com. By contrast, a certificate for https://www.thawte.com can support a SAN of https://thawte.com or https://www.thawte.org.
Cost control	Yes		Wildcards allow for future-proofing. You don't need to buy additional certificates later as long as you are securing subdomains under one domain.
Secure private key	Yes	Yes	Both certificate types include a secure private and public key pair. However, if you use a single wildcard certificate on multiple servers and one server is compromised, all servers become compromised. For this reason, each server hosting a wildcard certificate should have its own version of the certificate with its own private key. The same issue is possible with SAN certificates. Make sure you keep the private key secure at all times. Best PKI practice: Multiple servers sharing one key pair are prone to a single point of failure. We recommend unique key pairs in multi-server scenarios, where possible.

Certificate Feature	Wildcard	SAN	Comment
Simplicity of management	Yes	Yes	Wildcard certificates are easier to manage than SAN certificates because they support any subdomain. SAN certificates must be updated each time a new domain is added or an old domain is dropped. Note that due to the convenient nature of wildcard certificates, you have to keep careful track of the subdomains that the certificate secures. Keeping a close record of supported subdomains helps eliminate the chance that a "rogue" subdomain exists. Strong physical policy or access control measures to limit who can add/change/remove host headers are also recommended to eliminate the possibility of rogue subdomains.
Domain-only authentication			Because the wildcard certificate supports unlimited subdomains, it is not available in domain-only format. SAN certificates are also not available in domain-only format because they include multiple domains.
SHA-1	Yes	Yes	SHA-1 (a secure hash algorithm) is supported on both types of certificate.
Organizational validated authentication	Yes	Yes	Both types of certificate are only available in organizational validated format, which is more trustworthy than domain-only certificates. Organizational validated authentication certificates require both domain validation and organization validation.
SSL encryption	Yes	Yes	Both certificate types support 128-bit and better encryption.
Number of domains secured	Unlimited subdomains	Specified FQDNs	Wildcard certificates validate virtually an unlimited number of subdomains that are based on the same domain name (though for example, *.thawte.com does not secure group.test.thawte.com). SAN certificates support only the domain names entered in the certificate. The number of domains supported in a SAN certificate depends on the certificate authority.
Extended validation		Yes	Extended Validation SSL Certificates (EV SSL) instill customer confidence by enabling web browsers to display the green address bar, one of the most trusted and recognized security indicators available.
Site seal	Yes	Yes	Wildcard site seals are assigned to the domain name. SAN site seals are assigned to the primary domain name in the certificate.
Mobile device support	Yes	Yes	Note that some older devices, for example, Windows Mobile version 5, do not support the wildcard character. Check with your vendors to see if updates are available to support wildcard certificates. All devices support the SAN certificate.

Certificate Feature	Wildcard	SAN	Comment
Browser compatibility	99+%	99+%	All modern browsers support both types of certificates.
Validity duration	Multi-Year	Multi-Year	Both certificate types are available for multi-year spans.
Warranty	Yes	Yes	Certificate providers can provide warranties for both types of certificates.
Shared hosting usage		Yes	You can only use SAN certificates for shared hosting because they support multiple domain names.
Quality assurance testing usage	Yes	Yes	Wildcard certificates can only be used in QA testing environments that use the same domain name. SAN certificates can be used in environments that use either the same domain name or multiple domain names.

To learn more, contact our sales advisors:

- **Via phone**
  - **US toll-free: +1 888 484 2983**
  - **UK: +44 203 450 5486**
  - **South Africa: +27 21 819 2800**
  - **Germany: +49 69 3807 89081**
  - **France: +33 1 57 32 42 68**
- **Email sales@thawte.com**
- **Visit our website at https://www.thawte.com/log-in**

Protect your business and translate trust to your customers with high-assurance digital certificates from Thawte, the world's first international specialist in online security. Backed by a 17-year track record of stability and reliability, a proven infrastructure, and world-class customer support, Thawte is the international partner of choice for businesses worldwide.