WHITE PAPER

SECURING MULTIPLE DOMAINS WITH SSL

Subject Alternative Name (SAN) Certificates and
Unified Communications Certificates (UCC)

GeoTrust®

Securing Multiple Domains with SSL

Subject Alternative Name (SAN) Certificates and Unified Communications Certificates (UCC)

Introduction

As the backbone of web security, Secure Sockets Layer (SSL) is a must for securing sensitive data passing over the internet — whether that's e-commerce traffic, remote access to internal servers, or other secure communications.

Usually, one SSL certificate secures just one domain name or URL; however, some common situations are better handled with a type of certificate that allows multiple domains to be secured with just one certificate. You may have heard these multiple domain certificates referred to as subject alternative name (SAN) certificates or unified communications certificates (UCC). Depending upon your organization's needs, these types of certificates can save you considerable time and money compared with buying and managing many individual certificates.

In this guide, you'll learn more about typical situations where multiple domain certificates are the ideal solution. We'll also explain how multiple domain certificates work and how to select the right multi-domain certificate for your needs.

Do You Need a Multi-Domain Certificate?

Regardless of how easy it is to obtain a single SSL certificate, securing multiple domains with multiple, single certificates can quickly become expensive and cumbersome. For instance, there's the additional effort of binding each domain to its own certificate and adjusting certificates for domain name changes as they arise. In the end, it makes the job of securing multiple domains more complex than it needs to be.

So, when should you be looking for a multi-domain certificate instead of individual SSL certificates? Here are some common situations where multi-domain certificates are often much more practical and cost effective:

- **Microsoft Exchange Server (Unified Communications):** Starting in 2007, as Microsoft added new features to Microsoft Exchange Server such as auto-discovery, the number of services each server needed to protect with SSL encryption began to increase. As a result, Exchange Server 2007 needs a certificate that supports multiple names — hence the unified communications certificate (UCC). If your organization uses Microsoft technologies such as Microsoft Exchange 2007, Microsoft IIS 6, and Microsoft Communications Server 2007, you'll need a multi-domain or UC certificate (UCC) to secure client and server access from the internet.

- **Federating two or more Unified Communications platforms:** When a company uses more than one UC platform—for example, Google Apps and Microsoft Office Communications Server—those systems will need to be federated to allow employees to collaborate with their colleagues across platforms. This scenario is fairly common, and SSL certificates are necessary to validate cross UC platform server-to-server connections.

- **Multiple domain names:** Sometimes you may have multiple domain names that all point to one site, for instance you have one URL with your full company name and another with the acronym for your company. Perhaps you have different top-level domains for your company web site like .com, .net, or .org, or maybe your company is present in several different countries and you have country-specific URLs (.uk, .de, .au, etc.) all pointing to your main site. A multi-domain certificate lets you secure your main site as well as all the other domain names with one certificate.

- **Internal IP addresses and server names:** Intranets and other internal servers need to be accessed securely from outside the company firewall. You can use a multi-domain certificate to reduce the effort and cost of securing multiple IP addresses and internal server names for remote access.

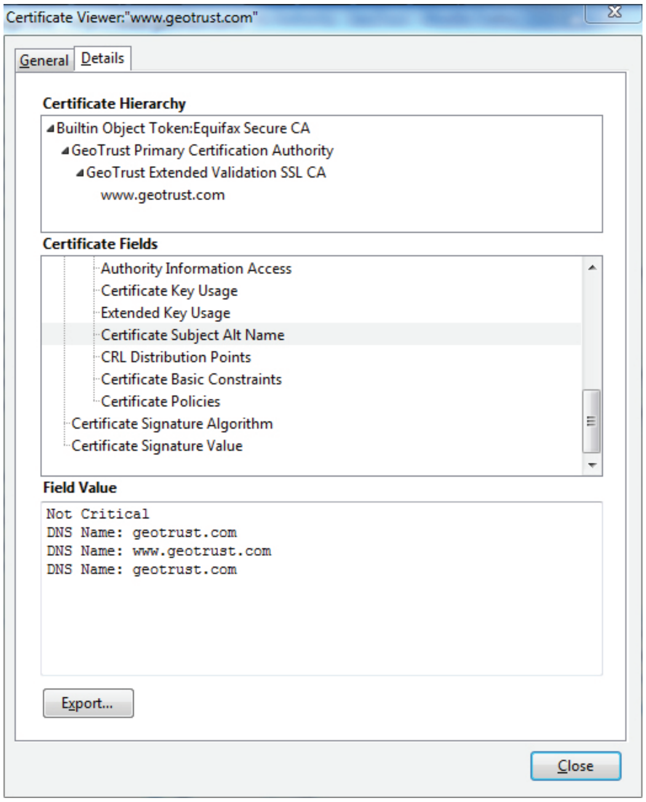
So How Does a Multi-Domain Certificate Work?

The multi-domain certificate is just like a regular SSL certificate in nearly every way — you can get organization or extended validation, it offers the same level of encryption, and so on, and the encryption technology works in the same way, too.

The difference is the Subject Alternative Name (SAN) extension, which has been a part of the X.509 certificate standard for more than 10 years. With a multi-domain certificate, the SAN field extension lets you specify a list of values to be protected by a single SSL certificate. This means that you can use the SAN field to specify different top-level domains, IP addresses, internal server names, and more.

Because the SAN extension is part of the X.509 standard, nearly every browser and mobile device understands how to use this field as well. Here's how it works: the client browser looks to match the domain name in the certificate with the value in the address bar. It checks the common name field and the SAN field to find the match.

To see this process in action, click the padlock in your browser on an HTTPS page to examine the SSL certificate. In the details tab, the "Subject Alternative Names" field lists the multiple DNS names for that certificate (see Figure 1).



Certificate Hierarchy

- Builtin Object Token:Equifax Secure CA
  - GeoTrust Primary Certification Authority
    - GeoTrust Extended Validation SSL CA
      - www.geotrust.com

Certificate Fields

- Authority Information Access
- Certificate Key Usage
- Extended Key Usage
- Certificate Subject Alt Name
- CRL Distribution Points
- Certificate Basic Constraints
- Certificate Policies
- Certificate Signature Algorithm
- Certificate Signature Value

Field Value

```
Not Critical
DNS Name: geotrust.com
DNS Name: www.geotrust.com
DNS Name: geotrust.com
```

Figure 1. SAN field values shown in the FireFox v.3.x browser

The X.509 Subject Alternative Name Extension

An X.509 v3 certificate contains an extension field that permits any number of additional fields to be added to the certificate. Certificate extensions provide a way of adding information such as alternative subject names and usage restrictions to certificates.

The Subject Alternative Name extension includes one or more alternative names for the identity bound by the CA to the certified public key. It may be used in addition to the certificate's subject name or as a replacement for it.

Is a Wildcard Certificate the Same Thing as Multi-Domain?

No, wildcard certificates are different than multi-domain certificates. Wildcard certificates are very powerful because they can protect an unlimited number of subdomains. For instance, a wildcard certificate for *.yourdomain.com secures sub-domains such as info.yourdomain.com and shop.yourdomain.com. However, wildcards are also somewhat limited because they must share the same domain and the same number of levels.

A multi-domain certificate is created when you add SAN fields to an SSL certificate in order to protect multiple domains. These multi-domain certificates are more flexible than wildcards. Multi-domain certificates are not limited to the same domain or the same number of levels. However, they are limited in total number of domains that can be protected depending on how many SANs you have purchased from your certificate provider.

While a multi-domain certificate can protect a limited number of wildcard subdomains, the reverse is not true. A wildcard certificate cannot protect www.yourdomain.com, www.yourotherdomain.com, and www.yourdomain.net. For this you need a multi-domain certificate.

	SAN Multi-Domain Certificate	Wildcard Certificate
*.yourdomain.com	No	Yes
www.yourdomain.*	Yes	No
www.*.*com, www.*.*	Yes	No
Microsoft Exchange Server	Yes	No
Unified Communications Servers	Yes	No
SSL VPN	Yes	No

The general rule of thumb is to use a wildcard certificate when you need to secure an unlimited number of subdomains with one certificate. Use a multi-domain certificate for securing UC environments, different domains, internal IP addresses, etc.

Selecting the Right Multi-Domain Certificate

While SSL is standardized, there are differences between SSL providers and the certificates they offer. Here are some important criteria you should keep in mind when shopping for a multi-domain certificate:

- **Reputation:** Make sure you choose an SSL certificate from a reputable security company. This is especially important for e-commerce or B2B sites where customers and partners look at who supplies your SSL for a sense of confidence that you're protecting their sensitive information.
- **Convenience:** Find out how easy it is to add, change, or delete domain names. Look for self-service features that let you maintain the certificate yourself so that you don't have to call the vendor or submit a service or support request for each change.

- **Price:** While you'll undoubtedly compare price, pay special attention to pricing for multiple domains. Some SSL providers only give you a small number of domains included in the base price then charge a hefty fee for additional names.

- **Number of domain names:** While it's important that the certificate you choose can support all the domains you need to secure, don't be mislead into buying more than you need.

The other factor you'll want to consider before you select a multi-domain certificate is whether an extended validation (EV) certificate would be the best choice instead of an organization-validated certificate. If you will be securing publicly facing web pages, an EV certificate may be the way to go. Multi-domain certificates with EV offer the most rigorous business verification process available and give site visitors an unmistakable sign of authenticity—a green address bar in their web browsers. If your business depends on the web, an EV certificate is the better choice. Make it even easier for customers to feel confident that your site is secure.

"The EV SSL certificates are fantastic. They allow us to provide our clients with an even more cost-effective protection for their sites, so we're recommending them more and more."

—Kurt Davey, Founder and CEO, neoverve

Securing Multiple Domains with GeoTrust

As a leading SSL provider with a strong, credible reputation for security, GeoTrust® offers SSL certificates that are ideal for securing UC environments and other situations that call for a multi-domain SSL solution. With GeoTrust True BusinessID certificates, you can secure up to 25 domain names by adding SAN fields to your certificate. Then, you simply install the certificate on an unlimited number of servers all at no additional cost.

In addition, GeoTrust provides an online management portal called GeoCenter that you can use to add, edit, or delete SAN names and then re-issue your certificate whenever you need to, a feature that simplifies and significantly reduces the burden of managing your UC security. GeoTrust multi-domain certificates are fully compatible with the latest UC platforms, making them an easy-to-use, cost-effective solution for any UC environment.

"With GeoCenter, I can log in and easily see all my certificates in one place. I can reissue or renew a certificate if I need to, and then move on. I'm done in a matter of minutes."

—Gene Thomas, Network Administrator, Washington State Department of Early Learning

GeoTrust also allows you to add SANs to your extended validation certificates. These certificates offer all of the features and benefits of the True BusinessID certificate with added SANs , but with the added perk of the green address bar. As discussed earlier, the green EV bar sends a clear message to visitors that a web site is safe, making it a vital security component of public-facing web sites.

Conclusion

The X.509 SAN extension makes it possible to secure multiple domain names, internal servers, and IP addresses with one SSL certificate. Certificates that take advantage of the SAN extension — called multi-domain or UC certificates — can be a cost-effective and time-saving alternative to individual SSL certificates.

GeoTrust certificates with additional SAN fields combine affordability, convenience, and reliability — everything you need to effectively secure multiple domain names, your Exchange environment, and other internal servers. Available in organization or extended validation (EV), GeoTrust certificates give you the features and flexibility you need to manage all of your domain names at an affordable cost.

Not All SSL Is the Same

Choose your SSL from an established, reliable, and secure independent certificate authority. It should deliver at minimum 128-bit encryption and optimally 256-bit encryption. It should be issued from a globally available root infrastructure using 2048-bit RSA keys or better. The SSL issuing authority should maintain industrial-strength data centers and disaster recovery sites optimized for data protection and availability. Your SSL certificate authority must have its authentication practices audited annually by trusted third-party auditor such as KPMG, Deloitte & Touche, or Ernst & Young. GeoTrust meets all of these requirements.

SSL Products from GeoTrust

GeoTrust offers a range of reliable low-cost SSL certificates to meet your individual needs:

- **GeoTrust® True BusinessID with EV —** Get the credibility of a well-established SSL provider, the green address bar, and a dynamic trust seal from GeoTrust at an affordable price
- **GeoTrust® True BusinessID —** Get name brand SSL that authenticates your business identity along with a dynamic trust seal at an affordable price
- **GeoTrust® True BusinessID Wildcard —** Protect unlimited subdomains with reliable SSL from a certificate who maintains a reliable, military-grade data center
- **GeoTrust® QuickSSL® Premium —** Get inexpensive basic SSL encryption from GeoTrust's fast and convenient issuing system
- **GeoTrust® Enterprise SSL —** Purchase SSL certificates in bulk and issue them on-demand

Contact Us

www.GeoTrust.com

CORPORATE HEADQUARTERS
GeoTrust, Inc.
350 Ellis Street, Bldg. J
Mountain View, CA 94043-2202, USA
Toll Free +1-866-511-4141
Tel +1-650-426-5010
Fax +1-650-237-8871
enterprisesales@geotrust.com

EMEA SALES OFFICE
GeoTrust, Inc.
8th Floor Aldwych House
71-91 Aldwych
London, WC2B 4HN, United Kingdom
Tel +44.203.0240907
Fax +44.203.0240958
sales@geotrust.co.uk

APAC SALES OFFICE
GeoTrust, Inc.
134 Moray Street
South Melbourne VIC 3205
Australia
sales@geotrustaustralia.com