



## SICHERN MEHRERER DOMÄNEN MIT SSL

Subject Alternative Name (SAN)-Zertifikate  
und Unified Communications-Zertifikate (UCC)

## Sichern mehrerer Domänen mit SSL

Subject Alternative Name (SAN)-Zertifikate und Unified Communications-Zertifikate (UCC)

### Einleitung

Secure Sockets Layer (SSL) ist als Rückgrat der Sicherheit im Web ein Muss, um vertrauliche Daten zu sichern, die im Internet übertragen werden – unabhängig davon, ob E-Commerce-Datenverkehr, Fernzugriff auf interne Server oder andere sichere Kommunikationen.

Normalerweise wird mit einem SSL-Zertifikat nur ein Domänenname oder eine URL gesichert. Für bestimmte gängige Situationen sollte jedoch besser ein Zertifikatstyp verwendet werden, mit dem mehrere Domänen mit nur einem Zertifikat gesichert werden können. Sie haben vielleicht schon gehört, dass diese Multi-Domänen-Zertifikate als Subject Alternative Name (SAN)-Zertifikate oder Unified Communications-Zertifikate (UCC) bezeichnet werden. Mit diesen Zertifikatstypen können Sie in Abhängigkeit von den Bedürfnissen Ihrer Organisation im Vergleich zum Kauf und zur Verwaltung einzelner Zertifikate erheblich Zeit und Geld sparen.

In diesem Leitfaden erfahren Sie mehr über typische Situationen, in denen Multi-Domänen-Zertifikate die Ideallösung darstellen. Außerdem wird die Funktionsweise von Multi-Domänen-Zertifikaten und die Auswahl des für Ihre Bedürfnisse passenden Multi-Domänen-Zertifikats erläutert.

### Benötigen Sie ein Multi-Domänen-Zertifikat?

Unabhängig davon, wie einfach es ist, sich ein einzelnes SSL-Zertifikat zu besorgen, kann die Sicherung mehrerer Domänen mit mehreren Einzelzertifikaten schnell teuer und arbeitsintensiv werden. Beispielsweise erfordert es zusätzlichen Aufwand, jede Domäne an das eigene Zertifikat zu binden und Zertifikate gegebenenfalls an geänderte Domännennamen anzupassen. Am Ende wird der Aufwand zur Sicherung mehrerer Domänen komplexer, als er sein müsste.

Wann sollten Sie anfangen, nach einem Multi-Domänen-Zertifikat anstelle von individuellen SSL-Zertifikaten Ausschau zu halten? Im Folgenden werden einige gängige Situationen beschrieben, in denen Multi-Domänen-Zertifikate oft viel praktischer und preiswerter sind:

- **Microsoft Exchange Server (Unified Communications):** Als Microsoft 2007 begann, Microsoft Exchange Server neue Funktionen hinzuzufügen, wie AutoErmittlung, nahm die Anzahl der Dienste, die von jedem Server mit SSL-Verschlüsselung geschützt werden musste, stetig zu. Infolgedessen benötigte Exchange Server 2007 ein Zertifikat, das mehrere Namen unterstützte – also das Unified Communications-Zertifikat (UCC). Wenn Ihre Organisation mit Technologien von Microsoft arbeitet, wie Microsoft Exchange 2007, Microsoft IIS 6 und Microsoft Communications Server 2007, benötigen Sie ein Multi-Domänen- oder UC-Zertifikat (UCC), um Server und Clients vor dem Zugriff durch das Internet zu sichern.
- **Zusammenschließen von zwei oder mehreren Unified Communications-Plattformen:** Wenn eine Firma mehr als eine UC-Plattform nutzt – beispielsweise Google Apps und Microsoft Office Communications Server – müssen diese Systeme zusammengeführt werden, sodass Mitarbeiter plattformübergreifend mit ihren Kollegen zusammenarbeiten können. Dieses Szenario ist ziemlich gängig, und SSL-Zertifikate sind zur Validierung von Verbindungen zwischen Servern über UC-Plattformen hinaus erforderlich.
- **Mehrere Domännennamen:** Mitunter verfügen Sie über mehrere Domännennamen, die alle auf eine Site verweisen. Sie haben beispielsweise eine URL mit Ihrem vollständigen Firmennamen, und eine weitere mit dem Akronym für Ihre Firma. Unter Umständen verfügen Sie über unterschiedliche Top-Level-Domains für Ihre Firmen-Website, wie .com, .net oder .org, oder Ihre Firma könnte in unterschiedlichen Ländern vertreten sein, weshalb Sie länderspezifische URLs verwenden (.uk, .de, .au usw.), die alle auf Ihre Hauptsite verweisen. Mit einem Multi-Domänen-Zertifikat können Sie Ihre Hauptsite sowie alle anderen Domännennamen mit einem Zertifikat sichern.

- **Interne IP-Adressen und Servernamen:** Sicherer Zugriff auf Intranets und andere interne Server muss von außerhalb der Firmen-Firewall möglich sein. Sie können ein Multi-Domänen-Zertifikat verwenden, um Aufwand und Kosten der Sicherung mehrerer IP-Adressen und interner Servernamen für den Fernzugriff zu reduzieren.

### Wie funktioniert ein Multi-Domänen-Zertifikat?

Das Multi-Domänen-Zertifikat funktioniert fast genauso wie ein reguläres SSL-Zertifikat. Es ermöglicht die Organisationsvalidierung oder Extended Validation, es bietet dieselbe Verschlüsselungsstufe usw., und die Verschlüsselungstechnologie funktioniert auch genauso.

Der Unterschied besteht in der Subject Alternative Name (SAN)-Erweiterung, die seit mehr als 10 Jahren Teil der X.509 Zertifikatsnorm ist. Sie können in der SAN-Felderweiterung in einem Multi-Domänen-Zertifikat eine Liste von Werten angeben, die durch ein einzelnes SSL-Zertifikat geschützt werden kann. Dies bedeutet, dass Sie das SAN-Feld zur Angabe unterschiedlicher Top-Level-Domains, IP-Adressen, interner Servernamen usw. verwenden können.

Da die SAN-Erweiterung zum X.509-Standard gehört, kann dieses Feld auch von fast allen Browsern und Mobilgeräten verwendet werden. So funktioniert es: Der Client-Browser sucht den Domännennamen im Zertifikat und gleicht ihn mit dem Wert in der Adressleiste ab. Im Feld für den Common Name und im SAN-Feld wird nach einer Übereinstimmung gesucht. Klicken Sie in Ihrem Browser auf einer HTTPS-Seite auf das Vorhängeschlosssymbol, um dies nachzuverfolgen und das SSL-Zertifikat zu überprüfen. Auf der Registerkarte "Details" sind im Feld "Subject Alternative Name" mehrere DNS-Namen für das Zertifikat aufgeführt (siehe Abbildung 1).

### Die X.509 Subject Alternative Name-Erweiterung

Ein X.509 v3-Zertifikat enthält ein Erweiterungsfeld, über das sich dem Zertifikat eine beliebige Zahl weiterer Felder hinzufügen lässt. Zertifikatserweiterungen sind eine Möglichkeit, Informationen hinzuzufügen, beispielsweise alternative Subjektnamen und Zugriffsbeschränkungen für Zertifikate.

Die Subject Alternative Name (SAN)-Erweiterung schließt einen oder mehrere alternative Namen für die Identität ein, die über die Zertifizierungsstelle (CA) an den zertifizierten öffentlichen Schlüssel gebunden wurde. Sie kann zusätzlich zum Subjektnamen des Zertifikats oder als Ersatz für diesen verwendet werden.



Abbildung 1. SAN-Feldwerte, dargestellt im Browser Firefox 3.x

### Ist ein Platzhalterzertifikat mit einer Multi-Domäne identisch?

Nein, Platzhalterzertifikate unterscheiden sich von Multi-Domänen-Zertifikaten. Platzhalterzertifikate sind sehr leistungsstark, da damit eine unbegrenzte Anzahl an Subdomänen geschützt werden kann. Mit einem Platzhalterzertifikat für \*.IhreDomäne.com werden beispielsweise Subdomänen wie info.IhreDomäne.com und shop.IhreDomäne.com gesichert. Platzhalter unterliegen jedoch einigen Einschränkungen, weil sie die gleiche Domäne und die gleiche Anzahl an Ebenen teilen müssen.

Ein Multi-Domänen-Zertifikat wird erstellt, wenn Sie einem SSL-Zertifikat SAN-Felder hinzufügen, um mehrere Domänen zu schützen. Diese Multi-Domänen-Zertifikate sind flexibler als Platzhalter. Multi-Domänen-Zertifikate sind nicht auf die gleiche Domäne oder die gleiche Anzahl an Ebenen begrenzt. Sie sind jedoch hinsichtlich der Gesamtzahl der Domänen, die geschützt werden können, eingeschränkt. Dies hängt davon ab, wie viele SANs Sie von Ihrem Zertifikatsaussteller erworben haben.

Obwohl mit einem Multi-Domänen-Zertifikat eine begrenzte Zahl an Platzhalter-Subdomänen geschützt werden kann, trifft das Gegenteil nicht zu. Mit einem Platzhalterzertifikat kann www.IhreDomäne.com, www.IhreAndereDomäne.com und www.IhreDomäne.net nicht geschützt werden. Hierfür benötigen Sie ein Multi-Domänen-Zertifikat.

	SAN Multi-Domänen- Zertifikat	Platzhalterzertifikat
*.IhreDomäne.com	Nein	Ja
www.IhreDomäne.*	Ja	Nein
www.*.com, www.*.*	Ja	Nein
Microsoft Exchange Server	Ja	Nein
Unified Communications-Server	Ja	Nein
SSL VPN	Ja	Nein

Als Faustregel gilt, ein Platzhalterzertifikat zu verwenden, wenn Sie eine unbegrenzte Anzahl an Subdomänen mit einem Zertifikat sichern müssen. Verwenden Sie ein Multi-Domänen-Zertifikat zur Sicherung von UC-Umgebungen, unterschiedlichen Domänen, internen IP-Adressen usw.

### Auswählen des richtigen Multi-Domänen-Zertifikats

Obwohl SSL genormt ist, gibt es Unterschiede zwischen SSL-Anbietern und den angebotenen Zertifikaten. Die folgenden wichtigen Kriterien sollten Sie beim Kauf eines Multi-Domänen-Zertifikats berücksichtigen:

- **Reputation:** Vergewissern Sie sich, dass Sie ein SSL-Zertifikat von einem angesehenen Sicherheitsunternehmen auswählen. Dies gilt insbesondere für E-Commerce- oder B2B-Sites, bei denen Kunden und Partner darauf achten, wer Ihre SSL bereitstellt, um zu beurteilen, wie sehr sie dem Schutz ihrer vertraulichen Informationen vertrauen können.
- **Komfort:** Finden Sie heraus, wie einfach Domännennamen hinzugefügt, geändert oder gelöscht werden können. Achten Sie auf Self-Service-Funktionen, mit denen Sie das Zertifikat selbst warten können, damit Sie sich nicht wegen jeder Änderung an den Anbieter wenden oder eine Dienst- oder Supportanforderung schicken müssen.

- **Preis:** Obwohl Sie zweifellos die Preise vergleichen werden, sollten Sie auf die Preisgestaltung für mehrere Domänen besonders achten. Bei einigen SSL-Anbietern sind nur wenige Domänen im Grundpreis enthalten, für zusätzliche Namen wird dann eine hohe Gebühr fällig.
- **Anzahl der Domännennamen:** Das von Ihnen gewählte Zertifikat muss zwar alle Domänen unterstützen, die Sie sichern müssen, aber Sie sollten sich nicht zum Kauf von unnötigen Domänen verführen lassen.

Ein weiterer Faktor, den Sie vor der Auswahl eines Multi-Domänen-Zertifikats berücksichtigen sollten, ist die Frage, ob ein Extended Validation (EV)-Zertifikat gegenüber einem organisationsvalidierten Zertifikat die bessere Wahl wäre. Wenn Sie öffentliche Webseiten sichern, ist möglicherweise ein EV-Zertifikat die beste Wahl. Multi-Domänen-Zertifikate mit EV bieten den striktesten Businessverifizierungsprozess auf dem Markt und setzen für Besucher der Site ein eindeutiges Zeichen für Authentizität, nämlich in Form einer grüne Adressleiste in ihren Webbrowsern. Wenn Ihr Geschäft vom Web abhängt, ist ein EV-Zertifikat die bessere Wahl. Machen Sie es Kunden leichter, Vertrauen zu entwickeln, dass Ihre Site sicher ist.

### Sichern mehrerer Domänen mit GeoTrust

GeoTrust® bietet als führender SSL-Anbieter mit einer hohen glaubwürdigen Reputation für Sicherheit SSL-Zertifikate an, die ideal zum Sichern von UC-Umgebungen und für andere Situationen sind, die nach einer Multi-Domänen-SSL-Lösung verlangen. Mit GeoTrust True BusinessID-Zertifikaten können Sie bis zu 25 Domännennamen sichern, indem Sie Ihrem Zertifikat SAN-Felder hinzufügen. Dann installieren Sie einfach das Zertifikat ohne weitere Kosten auf einer unbegrenzten Anzahl an Servern.

GeoTrust bietet zudem ein Online-Management-Portal namens GeoCenter an, mit dem Sie SAN-Namen hinzufügen, bearbeiten oder löschen und Ihr Zertifikat neu ausstellen können, falls dies erforderlich sein sollte. Mit dieser Funktion wird die Verwaltung der UC-Sicherheit vereinfacht und der damit verbundene Arbeitsaufwand drastisch reduziert. GeoTrust Multi-Domänen-Zertifikate sind mit den neuesten UC-Plattformen vollständig kompatibel und sind somit eine anwenderfreundliche, kostengünstige Lösung für jede UC-Umgebung.

Mit GeoTrust können Sie Ihren Extended Validation-Zertifikaten auch SANs hinzufügen. Diese Zertifikate bieten alle Funktionen und Vorteile des True BusinessID-Zertifikats mit hinzugefügten SANs, jedoch mit dem zusätzlichen Vorteil der grünen Adressleiste. Die grüne EV-Leiste ist wie bereits erwähnt für Besucher eine klare Botschaft, dass eine Website sicher ist. Damit ist sie für öffentliche Websites eine entscheidende Sicherheitskomponente.

### Zusammenfassung

Mit der X.509 SAN-Erweiterung können mehrere Domännennamen, interne Server und IP-Adressen mit einem SSL-Zertifikat gesichert werden. Zertifikate, die die SAN-Erweiterung nutzen – so genannte Multi-Domänen- oder UC-Zertifikate – können eine kostengünstige und zeitsparende Alternative zu einzelnen SSL-Zertifikaten darstellen.

GeoTrust-Zertifikate mit zusätzlichen SAN-Feldern vereinen Bezahlbarkeit, Komfort und Zuverlässigkeit – alles, was Sie zur effektiven Sicherung mehrerer Domännennamen, Ihrer Exchange-Umgebung und anderer interner Server benötigen. Die als Organisationsvalidierung oder Extended Validation (EV) erhältlichen GeoTrust-Zertifikate bieten Ihnen die Funktionalität, die Sie für die kostengünstige Verwaltung aller Ihrer Domännennamen benötigen.

"Die EV SSL-Zertifikate sind fantastisch. Mit ihnen können wir unseren Kunden einen noch kostengünstigeren Schutz ihrer Sites bieten. Daher empfehlen wir sie immer öfter."

– Kurt Davey, Gründer und CEO,  
neoverve

"Bei GeoCenter kann ich mich anmelden und alle meine Zertifikate problemlos zentral einsehen. Ich kann bei Bedarf ein Zertifikat neu ausstellen oder verlängern und dann weiterarbeiten. In wenigen Minuten ist alles erledigt."

– Gene Thomas,  
Netzwerkadministrator,  
Washington State  
Department of Early Learning

## Nicht alle SSL sind gleich

Wählen Sie Ihr SSL von einer bekannten, zuverlässigen und sicheren unabhängigen Zertifizierungsstelle. Die 128-Bit-Verschlüsselung sollte mindestens unterstützt werden, optimal wäre eine 256-Bit-Verschlüsselung. Es sollte von einer global verfügbaren Root-Infrastruktur ausgestellt werden und mindestens 2048-Bit-RSA-Schlüssel verwenden. Die SSL-Genehmigungsinstanz sollte industriegerechte Rechenzentren und Notfallwiederherstellungs-Sites, die hinsichtlich Datenschutz und Verfügbarkeit optimiert sind, verwalten. Die Authentifizierungspraktiken Ihrer SSL-Zertifizierungsstelle müssen jährlich von einem vertrauenswürdigen Drittanbieter überprüft werden, wie KPMG, Deloitte & Touche oder Ernst & Young. GeoTrust erfüllt all diese Anforderungen.

## SSL-Produkte von GeoTrust

GeoTrust bietet eine Palette zuverlässiger, preiswerter SSL-Zertifikate für Ihre individuellen Anforderungen:

- **GeoTrust® True BusinessID with EV (GeoTrust® True BusinessID mit EV)** – Besorgen Sie sich die Glaubwürdigkeit eines etablierten SSL-Anbieters, die grüne Adressleiste und ein dynamisches, vertrauenswürdiges Seal von GeoTrust zu einem günstigen Preis
- **GeoTrust® True BusinessID** – Erwerben Sie ein Marken-SSL, mit dem Ihre Geschäftsidentität authentifiziert wird, zusammen mit einem dynamischen, vertrauenswürdigem Seal zu einem günstigen Preis
- **GeoTrust® True BusinessID Wildcard** – Schutz für eine unbegrenzte Anzahl von Subdomänen mit zuverlässiger SSL durch ein Zertifikat, das ein zuverlässiges Rechenzentrum mit militärischem Sicherheitsstandard unterhält
- **GeoTrust® QuickSSL® Premium** – Entscheiden Sie sich für die preiswerte SSL-Basisverschlüsselung mit dem schnellen und komfortablen Ausstellungssystem von GeoTrust
- **GeoTrust® Enterprise SSL** – Kaufen Sie SSL-Zertifikate in größeren Mengen, und stellen Sie sie nach Bedarf aus

## Kontakt

[www.GeoTrust.com/de](http://www.GeoTrust.com/de)

### UNTERNEHMENSSTZ

GeoTrust, Inc.  
350 Ellis Street, Bldg. J  
Mountain View, CA 94043-2202, USA  
Gebührenfrei in den USA +1-866-511-4141  
Tel +1-650-426-5010  
Fax +1-650-237-8871  
[enterprisesales@geotrust.com](mailto:enterprisesales@geotrust.com)

### EMEA VERKAUFSBÜRO

GeoTrust, Inc.  
8th Floor Aldwych House  
71-91 Aldwych  
London, WC2B 4HN, Großbritannien  
Tel +44.203.0240907  
Fax +44.203.0240958  
[sales@geotrust.co.uk](mailto:sales@geotrust.co.uk)

### APAC VERKAUFSBÜRO

GeoTrust, Inc.  
134 Moray Street  
South Melbourne VIC 3205  
Australien  
[sales@geotrustaustralia.com](mailto:sales@geotrustaustralia.com)

Die grüne Extended Validation-Leiste wird in Hochsicherheitsbrowsern angezeigt. © 2011 GeoTrust, Inc. Alle Rechte vorbehalten. GeoTrust, das GeoTrust-Logo, das GeoTrust-Design und andere Marken, Dienstleistungsmarken und Designs sind eingetragene oder nicht eingetragene Marken von GeoTrust, Inc. und deren Niederlassungen in den USA und anderen Ländern. Alle übrigen Marken sind Eigentum der jeweiligen Inhaber.