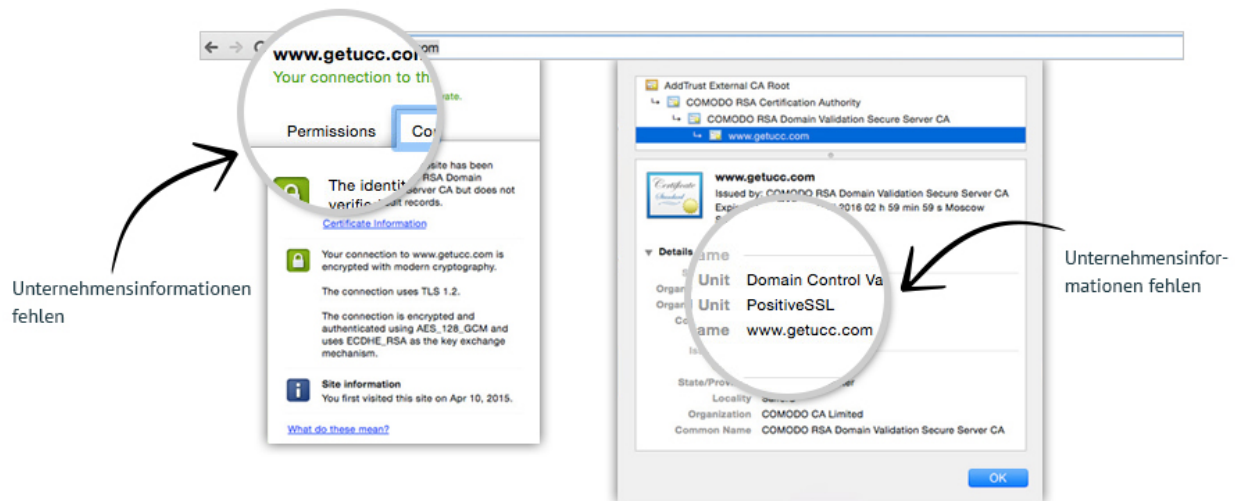


Unterschied zwischen DV- und OV-Zertifikaten

Wir wissen bereits, dass man SSL-Zertifikate in drei Typen unterteilt: DV, OV und EV. In diesem Artikel erklären wir die ersten beiden Zertifikate, DV und OV. Erfahren Sie im Folgenden mehr über ihre Unterschiede und Einsatzmöglichkeiten, und wann Sie welches Zertifikat benötigen.

Bei einem DV-Zertifikat steht die Abkürzung für Domain Validation, das bedeutet eine Validierung/Überprüfung der Domain. Dies ist das grundlegende Level für ein SSL-Zertifikat. Eine Zertifizierungsstelle (Certification Authority (CA)) bestätigt damit, dass Sie der Inhaber einer bestimmten Domain sind, und damit die Informationen des WHOIS-Eintrags. Dieses Zertifikat erlaubt selbstverständlich wie gewünscht eine sichere Datenverschlüsselung auf Ihrer Website, aber es verifiziert Sie nicht als Besitzer eines rechtmäßigen Unternehmens. Trotzdem ist dies ein absolut zulässiges Zertifikat und eine sehr schnelle Lösung für den effektiven Schutz einer Website per HTTPS. Dank des weit bekannten Schloss-Symbols neben der Adressleiste im Browser werden Kunden Ihrer Website im höheren Maße als vorher vertrauen.

Beispiel für ein DV-Zertifikat:



Ein DV-Zertifikat bietet sich überall da an, wo Sicherheit eine wichtige, aber keine übergeordnete Rolle spielt. Denn auch Internetbetrü gern und Hackern ist es leider möglich, DV-Zertifikate für Ihre gefälschten Phishing-Seiten zu verwenden. Hier werden arglose Nutzer mittels des vermeintlich sicheren Schloss-Symbols dazu verleitet, ihre persönlichen Daten anzugeben, welche dann in die Hände der Kriminellen fallen. Nur weil die Datenübertragung verschlüsselt wird heißt das nämlich nicht, dass die Daten auch beim richtigen Empfänger ankommen. Internetnutzer müssen deshalb auch sichergehen können, dass die aufgerufene Website auch zu einem rechtmäßigem Unternehmen gehört, bevor sie einen Kauf abschließen oder private Daten angeben.

Aus diesem Grund empfehlen wir für Websites mit höchsten Sicherheitsansprüchen ein OV-Zertifikat.

Ein OV-Zertifikat als Abkürzung für Organisation Validation, also mit einer Überprüfung des Unternehmens, benötigen vor allem Firmen und Organisationen, bei denen Kunden sensible Daten (Kreditkartennummern, Kontaktdaten, etc.) angeben müssen. Sie eignen sich damit insbesondere für eCommerce-Seiten und jede Art von Onlineverkauf. Ein OV-Zertifikat beglaubigt die Echtheit des Inhabers einer Website und benötigt dafür rechtmäßige Unternehmensinformationen von einer Firma. Der Validierungsprozess für solche Zertifikate dauert

deshalb etwas länger und ist umfangreicher. Die Zertifizierungsstelle bescheinigt nicht nur, dass Ihnen die entsprechende Domain gehört, sondern auch, dass Sie der rechtmäßige Besitzer des Unternehmens sind. Dafür muss die Firma in einem Unternehmensregister und einem Onlineverzeichnis gelistet sein, zum Beispiel dnd.com. Kriminelle können kein solches OV-Zertifikat bekommen, weil sie ihre „Firma“ nicht rechtmäßig überprüfen lassen können. Der Hauptvorteil eines OV-Zertifikats liegt darin, dass Ihr Unternehmen auf dem Zertifikat namentlich genannt wird.

Beispiel für ein OV-Zertifikat:



Erwägen Sie den Wechsel von einem DV-Zertifikat auf ein OV-Zertifikat, wenn:

- Sie sensible Nutzerdaten schützen müssen
- der Name Ihres Unternehmens auf dem Zertifikat stehen soll (für ein höheres Vertrauen der Nutzer)
- Sie Ihre Geschäftstätigkeiten ausweiten und auf ein neues Level heben möchten
- Nutzer Ihre Website als rechtmäßiges Unternehmen und keinesfalls als Phishing-Seite wahrnehmen sollen

Wenn Sie noch Fragen zu einem Zertifikatswechsel haben, oder überlegen von einem DV- auf ein OV-Zertifikat umzusteigen, fragen Sie unsere Experten von LeaderTelecom. Mit unserer jahrelangen Erfahrung und schlanken Prozessen bei der Kommunikation mit den Zertifizierungsstellen stellen wir Ihnen jede Art von Zertifikat komfortabel und schnell aus.