



EINSTIEGSLEITFADEN

DER EINSTIEG IN SSL- ZERTIFIKATE:

WIE SIE DIE BESTE LÖSUNG FÜR
IHRE ONLINE-SICHERHEIT WÄHLEN

DER EINSTIEG IN SSL-ZERTIFIKATE

EINLEITUNG

Für Einzelpersonen wie für Unternehmen gilt gleichermaßen, dass die Online-Sicherheit mit der gleichen Sorgfalt angegangen werden muss wie die Sicherheit der eigenen Wohnung oder der Geschäftsräume. Neben der angenehmen Tatsache, dass man sich natürlich selbst sicherer fühlt, dienen durchdachte Sicherheitsmaßnahmen auch dem Schutz der Besucher zu Hause, im Unternehmen oder auf der Website. Zunächst einmal muss man sich mit den möglichen Gefahren gründlich vertraut machen, und dann muss man für einen umfassenden Schutz sorgen. Angesichts des rasanten technischen Fortschritts ist es nicht immer einfach, bei allen Weiterentwicklungen auf dem Laufenden zu bleiben. Aus diesem Grund ist es klug, sich für einen renommierten Anbieter von Internet-Sicherheitslösungen zu entscheiden.

Dieser Leitfaden erläutert die technischen Hintergründe und liefert Ihnen die Informationen, die Sie benötigen, um aus allen Angeboten die richtige Lösung für Ihre Online-Sicherheit auszuwählen. Ein kleines Glossar finden Sie am Ende dieses Leitfadens im Abschnitt „Was genau ist eigentlich ...?“.

Unterstützung und weitere Informationen erhalten Sie von unserem Vertrieb unter 0800 128 1000 oder +41 26 429 7726 oder per E-Mail an sales@verisign.de.

WAS IST EIN SSL-ZERTIFIKAT?

Ein SSL-Zertifikat ist eine Computerdatei (bzw. ein kurzes Stück Code) mit zwei speziellen Funktionen:

- 1. Authentifizierung und Überprüfung:** Das SSL-Zertifikat enthält Informationen über die Authentizität, also die Echtheit, bestimmter Angaben zur Identität einer Person, eines Unternehmens oder einer Website. Wenn Besucher der Website auf das Vorhängeschloss-Symbol im Browser oder auf die Vertrauensmarke (z. B. das VeriSign-Siegel) klicken, werden ihnen diese Angaben angezeigt. Die strengsten Kriterien bei der Prüfung, ob ein SSL-Zertifikat ausgestellt werden darf, gelten für SSL-Zertifikate mit Extended Validation (EV), die daher die vertrauenswürdigsten SSL-Zertifikate auf dem Markt sind.
- 2. Datenverschlüsselung:** Das SSL-Zertifikat ermöglicht auch die Verschlüsselung von Daten. Diese sorgt dafür, dass es Außenstehenden nicht möglich ist, vertrauliche Daten, die über die Website ausgetauscht werden, abzufangen und zu lesen.

Ähnlich wie Personalausweise und Pässe nur von den entsprechenden Behörden eines Landes ausgestellt werden können, ist auch ein SSL-Zertifikat dann am aussagekräftigsten, wenn es von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt wurde. Die CA muss dabei sehr strenge Regeln und Vorgaben einhalten, anhand derer entschieden wird, wer ein SSL-Zertifikat erhält und wer nicht. Ein gültiges SSL-Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle verschafft Ihnen also mehr Vertrauen.

IDENTITÄT UND AUTHENTIFIZIERUNG ONLINE

Dienste zu Identität und Authentifizierung übernehmen im Internet die Aufgabe des Paketboten an Ihrer Tür, der sagt: „*Ich habe hier ein Paket für Sie. Würden Sie bitte unterschreiben?*“



WIE FUNKTIONIERT VERSCHLÜSSELUNG MIT SSL?

Um Türen und andere Schlösser auf- und zuzuschließen, verwenden wir Schlüssel, und ebenso werden zur Verschlüsselung Schlüssel benötigt, um die Daten zugänglich bzw. nicht zugänglich zu machen. Wer nicht den richtigen Schlüssel besitzt, kann die Daten nicht nutzen.

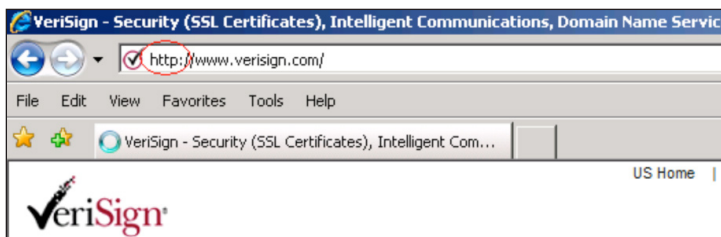
In jeder SSL-Sitzung werden zwei Schlüssel verwendet:

1. Mit dem öffentlichen Schlüssel werden die Daten verschlüsselt, d. h. unlesbar gemacht.
2. Mit dem privaten Schlüssel werden die Daten entschlüsselt, also wieder lesbar gemacht und in ihr ursprüngliches Format gebracht.

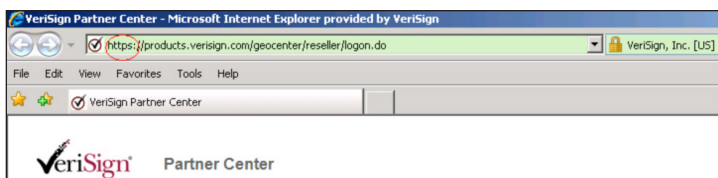
Der Ablauf: Jedes SSL-Zertifikat wird einer von der CA überprüften Organisation für einen bestimmten Server und für eine bestimmte Domain (also die Adresse einer Website) ausgestellt. Wenn vom Benutzer im Browser eine Website mit SSL-Zertifikat aufgerufen wird, tauschen Browser und Server einen sogenannten „SSL-Handshake“, eine Art Begrüßung, aus. Vom Server werden Daten angefordert, die dann im Browser für den Benutzer sichtbar dargestellt werden. Das Vorhandensein eines SSL-Zertifikats können Sie im Browser anhand bestimmter Merkmale feststellen (genauere Informationen dazu finden Sie weiter unten im Abschnitt „Woran erkennt man eine Website mit gültigem SSL-Zertifikat?“). Wenn Sie auf die Vertrauensmarke klicken, werden weitere Informationen angezeigt, etwa Gültigkeitsdauer und Art des SSL-Zertifikats, die Domain, für die es ausgestellt wurde, und die ausstellende CA. Für diese Sitzung wird nun eine sichere Verbindung mit einem eindeutigen Sitzungsschlüssel aufgebaut, und der sichere Datenaustausch kann beginnen.

WORAN ERKENNT MAN EINE WEBSITE MIT GÜLTIGEM SSL-ZERTIFIKAT?

1. Eine Website ohne SSL-Zertifikat zeigt in der Adressleiste des Browsers vor der Website-Adresse die Zeichenfolge „http://“ an. Dies ist die Abkürzung für das „Hypertext Transfer Protocol“, das gemeinhin zur Datenübertragung im Internet verwendet wird.



Bei einer Website mit SSL-Zertifikat wird dagegen vor der Adresse die Zeichenfolge „https://“ angezeigt. Dies bedeutet „sicheres HTTP“.



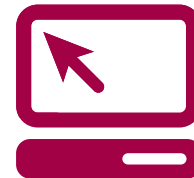
WAS IST SSL?

SSL steht für „Secure Sockets Layer“. Hinter diesen Buchstaben verbirgt sich ein Verfahren, das eine gesicherte Sitzungsverbindung zwischen dem Browser und der Website herstellt, so dass alle über diese Verbindung übertragenen Daten verschlüsselt werden und somit sicher sind. SSL wird auch zur sicheren Übertragung von E-Mails, Dateien und anderen Arten von Daten verwendet.

Würden Sie vertrauliche Mitteilungen oder Kontodaten für alle lesbar per Postkarte verschicken?



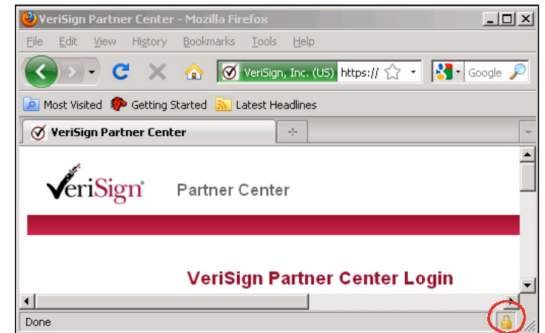
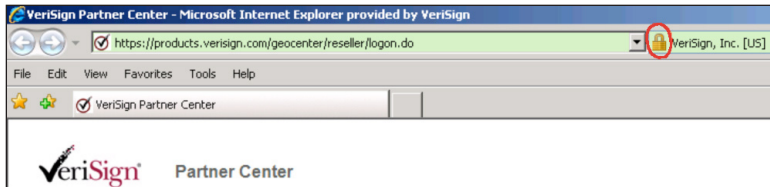
SSL schafft einen sicheren und vor Unbefugten geschützten Kommunikationsweg.



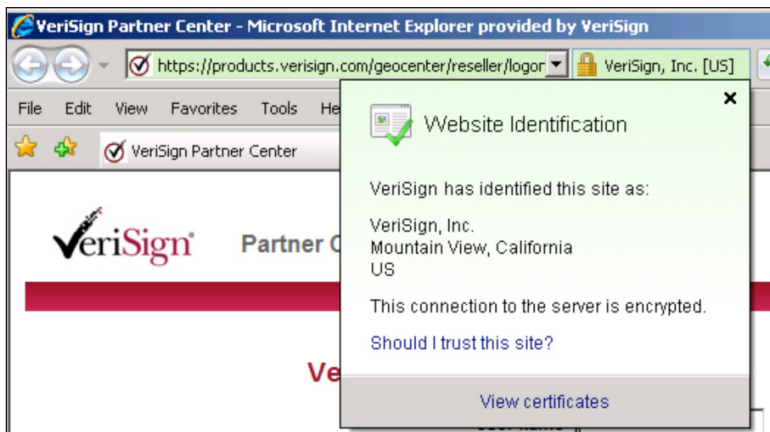


EINSTIEGSLEITFADEN

2. Außerdem zeigt der Browser ein Vorhängeschloss an (je nach dem verwendeten Browser oben oder unten im Bildschirm).



3. Oft findet sich auf der Website auch eine Vertrauensmarke. Kunden von VeriSign verwenden auf ihren Websites das VeriSign®-Siegel als Vertrauensmarke. Wenn Sie auf einer Website auf das VeriSign-Siegel oder das Vorhängeschloss klicken, werden Details zum verwendeten Zertifikat angezeigt, darunter alle von der CA überprüften und bestätigten Angaben zum Unternehmen.



4. Durch einen Klick auf das geschlossene Vorhängeschloss im Browser oder auf bestimmte SSL-Vertrauensmarken (z. B. das VeriSign-Siegel) wird der Name der überprüften Organisation angezeigt. In Browsern mit modernen Sicherheitsfunktionen wird dieser Name an gut sichtbarer Stelle angezeigt und die Adressleiste wird grün, wenn ein Extended Validation SSL-Zertifikat vorhanden ist. Wenn die hinterlegten Angaben nicht übereinstimmen oder das Zertifikat abgelaufen ist, zeigt der Browser eine Fehlermeldung oder Warnung an.





EINSTIEGSLEITFADEN

WANN IST EIN SSL-ZERTIFIKAT SINNVOLL?

Kurz gesagt ist ein SSL-Zertifikat immer dann sinnvoll, wenn Daten bei der Übertragung geschützt werden sollen.

Einige Beispiele:

- Gesicherter Datenaustausch zwischen Ihrer Website und den Browsern Ihrer Kunden
- Gesicherter interner Datenaustausch im Intranet Ihres Unternehmens
- Gesicherter E-Mail-Versand in das und aus dem Unternehmensnetzwerk (*oder von privaten E-Mail-Adressen*)
- Gesicherter Datenaustausch zwischen Servern, intern und extern
- Gesicherter Datenaustausch mit Mobilgeräten

VERSCHIEDENE ARTEN VON SSL-ZERTIFIKATEN

Derzeit sind verschiedene Arten von SSL-Zertifikaten erhältlich.

1. Zunächst einmal gibt es selbstsignierte Zertifikate.

Wie der Name schon sagt, wird ein solches Zertifikat für interne Zwecke selbst generiert und nicht von einer CA ausgestellt. Da sich hier der Betreiber einer Website selbst ein Zertifikat ausstellt, ist dieses bei Weitem nicht so aussagekräftig wie ein gründlich authentifiziertes und überprüftes SSL-Zertifikat von einer CA.

2. Ein Zertifikat mit Domainvalidierung ist ein sehr einfaches SSL-Zertifikat und kann schnell ausgestellt werden. Hierbei wird lediglich überprüft, ob der Antragsteller der Inhaber der Domain ist, auf der das Zertifikat eingesetzt werden soll. Es wird nicht weiter überprüft, ob es sich beim Domain-Inhaber um ein tatsächlich existierendes Unternehmen handelt.

3. Ein SSL-Zertifikat mit umfassender Authentifizierung stellt den ersten Schritt zu echter Online-Sicherheit und bestätigter Vertrauenswürdigkeit dar. Die Ausstellung dieser Zertifikate benötigt etwas mehr Zeit, denn zuvor muss das antragstellende Unternehmen eine Reihe von Überprüfungen bestehen, bei denen die Existenz des Unternehmens, der Domain-Inhaber und die Befugnis des Mitarbeiters zur Beantragung eines Zertifikats festgestellt werden.

4. Ein SSL-Zertifikat unterstützt zwar grundsätzlich die Verschlüsselung mit 128 oder sogar 256 Bit, allerdings können bestimmte ältere Browser und Betriebssysteme diese Verschlüsselung nicht leisten. SSL-Zertifikate, die ein Verfahren namens Server Gated Cryptography

(SGC) verwenden, ermöglichen über 99,9 Prozent aller Website-Besucher die Datenverschlüsselung mit 128 oder 256 Bit. Wenn auf dem Webserver kein SGC-Zertifikat installiert ist, ist mit den Browsern und Betriebssystemen, die keine 128-Bit-Verschlüsselung unterstützen, nur die Verschlüsselung mit 40 oder 56 Bit möglich. Beim Besuch einer Website mit SGC-fähigem SSL-Zertifikat können Benutzer mit bestimmten älteren Browser- und Betriebssystem-Versionen vorübergehend die 128-Bit-SSL-Verschlüsselung nutzen. Weitere Informationen zu SGC erhalten Sie hier: <http://www.verisign.de/sgc>.

5. Ein Domainname wird oft mit unterschiedlichen Erweiterungen (Suffixen) des Host-Namens verwendet. Aus diesem Grund gibt es sogenannte „Wildcard“-SSL-Zertifikate, mit denen Sie für jeden Host in Ihrer Domain die volle SSL-Sicherheit gewährleisten. Ein Beispiel: `host.ihre_domain.de` – „host“ ist hierbei variabel, aber der Domainname bleibt unverändert.

6. Im Ansatz ähnlich wie ein Wildcard-Zertifikat, aber etwas flexibler ist ein SSL-Zertifikat mit SAN (Subject Alternative Name): Ein solches SSL-Zertifikat kann für mehr als eine Domain verwendet werden.

7. Code-Signing-Zertifikate stellen einen Sonderfall dar und belegen, dass Software, die Sie aus dem Internet laden, unterwegs nicht manipuliert wurde. Es kommt häufig vor, dass Software, die im Internet zum Herunterladen bereitsteht, von Kriminellen manipuliert wird. So besteht die Gefahr, dass während der Übertragung ein Virus oder sonstiger Schadcode in eine an sich harmlose Software eingefügt wird. Code-Signing-Zertifikate sorgen dafür, dass dies nicht möglich ist.

8. SSL-Zertifikate mit Extended Validation (EV) erfordern die strengste Authentifizierung und bieten Kunden daher den besten auf dem Markt erhältlichen Schutz. Auf einer Website, für die ein SSL-Zertifikat mit EV vorliegt, färbt sich die Adressleiste in Browsern mit entsprechenden Sicherheitsmerkmalen grün und in einem eigenen Feld werden der Name des Website-Eigentümers sowie der Name der Genehmigungsinstanz, die das SSL-Zertifikat mit EV ausgestellt hat, angezeigt. Außerdem werden die Namen des Zertifikatsinhabers und der ausstellenden CA in der Adressleiste angezeigt. Diese optischen Sicherheitssignale haben bereits dazu beigetragen, das Kundenvertrauen in Online-Geschäfte zu stärken.

Alle SSL-Zertifikate von VeriSign® werden erst nach umfassender Authentifizierung ausgestellt.





WAS GENAU IST EIGENTLICH ...?

Verschlüsselung: Daten werden in unleserlichen „Zeichensalat“ umgewandelt, der nur vom vorgesehenen Empfänger wieder lesbar gemacht werden kann.

Entschlüsselung: Der „Zeichensalat“ wird wieder lesbar gemacht und die Daten werden wieder in ihr ursprüngliches Format überführt.

Schlüssel: Eine mathematische Formel (Algorithmus) zur Verschlüsselung oder Entschlüsselung von Daten. Je mehr Kombinationen für ein Zahlenschloss möglich sind, desto schwieriger ist es zu knacken – gleiches gilt für den bei der Verschlüsselung verwendeten Schlüssel: Je länger er ist, d. h. je mehr Bit er hat, desto stärker ist die Verschlüsselung.

Browser: Ein Computerprogramm, das verwendet wird, um Websites aus dem Internet anzuzeigen. Bekannte Browser sind Microsoft Internet Explorer (IE), Mozilla Firefox, Apple Safari, Flock und Google Chrome.

SCHLUSSFOLGERUNG

In der Geschäftswelt des Internets steht und fällt der Erfolg mit der Vertrauenswürdigkeit. Investitionen in Technologien, die Kunden schützen und ihr Vertrauen gewinnen, sind unverzichtbare Bausteine des Erfolgs für alle E-Commerce-Websites. Die wirkungsvolle Implementierung von SSL-Zertifikaten und die sinnvolle Platzierung und Nutzung von Vertrauensmarken haben sich als Mittel zur Schaffung von Vertrauen bei Kunden bewährt.

VeriSign ist der weltweit führende Anbieter von SSL-Zertifikaten, und das VeriSign-Siegel – die anerkannteste Vertrauensmarke des Internets – ist auf über 90.000 Domains in 160 Ländern zu sehen. Damit die Investitionen in die Sicherheit von bestehenden und zukünftigen Kunden auch angemessen wahrgenommen werden, sollten sich Unternehmen, die online erfolgreich sein möchten, für den Zertifikatsanbieter entscheiden, dessen Name am bekanntesten und am vertrauenswürdigsten ist. VeriSign hat sich seinen in der Branche führenden guten Namen und das damit einhergehende Kundenvertrauen durch zuverlässige und moderne Lösungen für Online-Sicherheit und -Vertrauen erarbeitet.

Weitere Informationen erhalten Sie unter www.verisign.de/ssl/index.html.

