Erste Schritte mit TLS/SSL-Zertifikaten

Wie Sie aus der Vielfalt die beste Lösung für Ihre Online-Sicherheit wählen

digicert®

Inhaltsverzeichnis

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, über alle 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 …?“.

Was ist ein TLS/SSL-Zertifikat?

Transport Layer Security (TLS) und dessen Vorläufer Secure Sockets Layer (SSL) sind die heute am weitesten verbreiteten Sicherheitsprotokolle und dienen hauptsächlich zwei konkreten Zwecken:

1. **Authentifizierung und Überprüfung:** Das TLS/SSL-Zertifikat enthält Informationen über die Authentizität, also die Echtheit, bestimmter Angaben zur Identität einer Person, eines Unternehmens oder einer Website. Diese Angaben werden Besuchern der Website angezeigt, wenn sie auf das Vorhängeschloss-Symbol im Browser oder auf die Vertrauensmarke (z. B. das DigiCert® Secured-Siegel oder das Norton-Siegel „powered by DigiCert“) klicken. Überprüft wurden diese Angaben von der Zertifizierungsstelle (CA), die das TLS/SSL-Zertifikat ausgestellt hat. Es gibt verschiedene Validierungsstufen, auf die wir später näher eingehen werden.
2. **Datenverschlüsselung:** Das TLS/SSL-Zertifikat ermöglicht außerdem die Verschlüsselung von Daten. Durch diese wird es Außenstehenden unmöglich gemacht, vertrauliche Daten, die über die Website ausgetauscht werden, zu lesen oder zu nutzen.

Ähnlich wie Personalausweise und Pässe nur gültig sind, wenn sie von den zuständigen Behörden eines Landes ausgestellt werden, ist ein TLS/SSL-Zertifikat dann am aussagekräftigsten, wenn es von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgegeben wurde. Die CA muss dabei sehr strenge Regeln und Vorgaben einhalten, anhand derer entschieden wird, wer ein TLS/SSL-Zertifikat erhält und wer nicht. Ein gültiges TLS/SSL-Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle verschafft Ihnen mehr Vertrauen bei Ihren Kunden, Klienten oder Partnern.

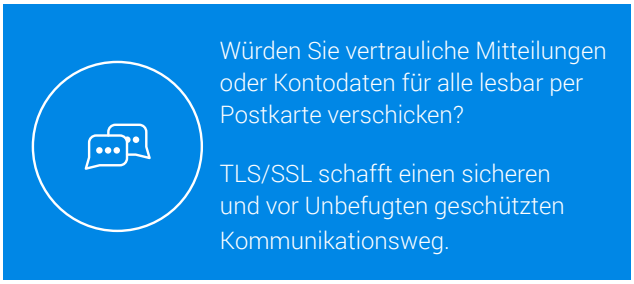
Wie funktioniert Verschlüsselung mit TLS/SSL?

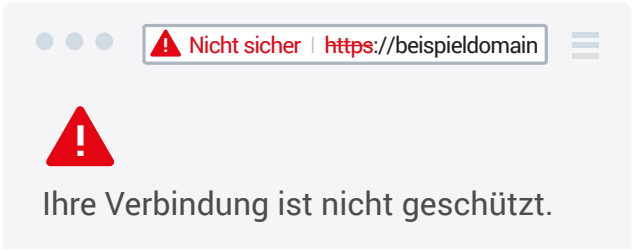
Genauso wie zum Auf- und Zuschließen einer Tür der passende Schlüssel nötig ist, werden zur Verschlüsselung Schlüssel eingesetzt, um die Daten lesbar bzw. unlesbar zu machen. Ohne den passenden Schlüssel kann auf die Daten nicht zugegriffen werden.

In jeder TLS/SSL-Sitzung werden zwei Schlüssel verwendet:

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

TLS/SSL steht für „Transport Layer Security/ Secure Sockets Layer“. Dahinter verbirgt sich ein Verfahren, das eine gesicherte Sitzungsverbindung zwischen dem Browser und der Website herstellt, sodass alle über diese Verbindung übertragenen Daten verschlüsselt werden und somit sicher sind.



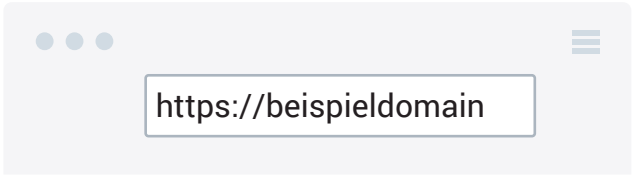


So funktioniert der Prozess: Jedes TLS/SSL-Zertifikat, das an eine von der CA überprüfte Organisation ausgegeben wird, wird für einen bestimmten Server und für eine bestimmte Domain (die Adresse einer Website) ausgestellt. Wenn vom Benutzer im Browser eine Website mit TLS/SSL-Zertifikat aufgerufen wird, tauschen Browser und Server einen sogenannten „TLS/SSL-Handshake“, eine Art Begrüßung, aus. Vom Server werden Daten angefordert, die dann im Browserfenster für den Benutzer sichtbar dargestellt werden. Anhand bestimmter Merkmale kann der Website-Besucher erkennen, dass eine sichere Verbindung aufgebaut wurde, z. B. durch die Anzeige einer Vertrauensmarke. Beim Anklicken der Vertrauensmarke werden weitere Informationen angezeigt, etwa die Gültigkeitsdauer und Art des TLS/SSL-Zertifikats, die Domain, für die es ausgestellt wurde, und die ausstellende CA. Damit besteht für diese Sitzung nun eine sichere Verbindung mit einem eindeutigen Sitzungsschlüssel und der sichere Datenaustausch kann beginnen.

Woran erkennt man eine Website mit gültigem TLS/SSL-Zertifikat?

1. Eine Website ohne TLS/SSL-Zertifikat zeigt in der Adressleiste des Browsers vor der Website-Adresse die Zeichenfolge „http://“ an, die Abkürzung für „Hypertext Transfer Protocol“. Mit diesem Protokoll sind die Daten bei der Übertragung im Internet ungeschützt. Die meisten modernen Browser zeigen beim Aufrufen einer Webseite ohne ordnungsgemäß installiertes TLS/SSL-Zertifikat eine Warnmeldung an. Dies kann dazu führen, dass Besucher die Website gleich wieder verlassen.

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



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

3. Oft findet sich auch auf der Website selbst eine Vertrauensmarke. Kunden von DigiCert™ verwenden als Vertrauenszeichen das DigiCert® Secured-Siegel oder das Norton-Siegel „powered by DigiCert“. Wenn Sie auf einer Website auf das DigiCert-Siegel, die Vertrauensmarke „powered by DigiCert“ oder das Vorhängeschloss klicken, werden Details zum verwendeten Zertifikat angezeigt, darunter alle von der CA überprüften und bestätigten Angaben zum Unternehmen.

4. Bei einem Klick auf das geschlossene Vorhängeschloss im Browser oder auf bestimmte TLS/SSL-Vertrauensmarken, wie etwa das DigiCert® Secured- oder das Norton Secured-Siegel wird der Name der überprüften Organisation angezeigt. In Browsern mit modernen Sicherheitsfunktionen wird dieser Name an gut sichtbarer Stelle angezeigt und die Adressleiste oder der Text darin wird grün eingefärbt, wenn ein TLS/SSL-Zertifikat mit Extended Validation (EV) festgestellt wird. Wenn die hinterlegten Angaben nicht übereinstimmen oder das Zertifikat abgelaufen ist, zeigt der Browser eine Fehlermeldung oder Warnung an.

Wann ist ein TLS/SSL-Zertifikat sinnvoll?

Kurz gesagt ist ein TLS/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 Datenaustausch zwischen Servern (*intern und extern*)
- Gesicherter Datenaustausch mit Mobilgeräten

Verschiedene Arten von TLS/SSL-Zertifikaten

Derzeit sind verschiedene Arten von TLS/SSL-Zertifikaten erhältlich.

- Zunächst einmal gibt es selbstsignierte TLS/SSL-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 TLS/SSL-Zertifikat von einer CA.
- Ein Zertifikat mit Domain-Validierung (DV) ist ein sehr einfaches TLS/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 Domaininhaber um ein tatsächlich existierendes Unternehmen handelt.
- Ein TLS/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 beantragende Unternehmen eine Reihe von Überprüfungen bestehen, bei denen die Existenz des Unternehmens, der Domaininhaber und die Befugnis des Antragstellers zur Beantragung eines Zertifikats festgestellt werden.

Alle TLS/SSL-Zertifikate von DigiCert werden erst nach umfassender Authentifizierung ausgestellt.

- Ein Domainname wird oft mit unterschiedlichen Erweiterungen (Suffixen) des Host-Namens verwendet. Aus diesem Grund gibt es sogenannte Platzhalterzertifikate, mit denen Sie für jeden Host in Ihrer Domain die volle TLS/SSL-Sicherheit gewährleisten, zum Beispiel „host.ihre_domain.de“ (hierbei ist „host“ variabel, während der Domainnname unverändert bleibt).
- Im Ansatz ähnlich wie ein Platzhalterzertifikat, aber etwas flexibler, ist ein TLS/SSL-Zertifikat mit SAN (Subject Alternative Name): Ein solches TLS/SSL-Zertifikat kann für mehr als eine Domain verwendet werden.
- TLS/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 TLS/SSL-Zertifikat mit EV vorliegt, färbt sich die Adressleiste in manchen Browsern grün und in einem eigenen Feld werden der Name des Website-Eigentümers sowie der Name der Genehmigungsinstanz, die das EV TLS/SSL-Zertifikat ausgestellt hat, angezeigt. Außerdem werden die Namen des Zertifikatsinhabers und der ausstellenden Zertifizierungsstelle in der Adressleiste angezeigt. Diese optischen Sicherheitssignale haben bereits dazu beigetragen, das Kundenvertrauen in Online-Geschäfte zu stärken.

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 in ihr ursprüngliches Format umgewandelt.

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 anzuzeigen, zum Beispiel Microsoft Edge, Mozilla Firefox, Apple Safari und Google Chrome.

Fazit

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 Unternehmen, die Geschäfte online abwickeln oder eine E Commerce-Website betreiben. Die wirkungsvolle Implementierung von TLS/SSL-Zertifikaten und die sinnvolle Platzierung und Nutzung von Vertrauensmarken haben sich als Mittel zur Schaffung von Kundenvertrauen bewährt.

DigiCert ist der weltweit führende Anbieter von TLS/SSL-Zertifikaten und hilft Unternehmen, ihren Kunden zu signalisieren, dass ihre Website von der Suche über die Navigation und Anmeldung bis hin zur Bezahlung sicher ist.* DigiCert sichert über eine Million Webserver in aller Welt – mehr als jede andere Zertifizierungsstelle.* Außerdem schützt DigiCert mehr als zwei Drittel aller Websites mit einem TLS/SSL-Zertifikat mit Extended Validation, darunter die namhafter Online-Händler und Banken.* Wenn Sie sich für DigiCert entscheiden, können Sie sich darauf verlassen, dass Ihre Website und Ihr Ruf in den Händen einer Zertifizierungsstelle sicher sind, deren Zuverlässigkeit vielfach belegt ist und die das bekannteste Vertrauenssiegel im Internet ausstellt.

Weitere Informationen erhalten Sie unter https://resources.digicert.com/ssl-tls.

* einschließlich der Tochtergesellschaften, Partnerunternehmen und Vertriebspartner von DigiCert

Wenn Sie weitere Informationen wünschen, schreiben Sie unseren Sicherheitsexperten unter contactus@digicert.com

Nord- und Südamerika

Lehi, Utah, USA
2801 North Thanksgiving Way, Lehi, Utah 84043, USA

Mountain View, Kalifornien, USA
485 Clyde Ave., Mountain View, California 94043, USA

Asien-Pazifik und Japan

Bangalore, Indien
RMZ Eco World, 10th Floor, 8B Campus,
Marathalli Outer Ring Road, Bangalore - 560103, Indien

Melbourne, Australien
437 St Kilda Road, Melbourne, 3004, Australien

Tokio, Japan
Ginza Six 8F, 6-10-1 Ginza Chuo-Ku, Tokio,
104-0061, Japan

Europa, Naher Osten und Afrika (EMEA)

Nieuwegein, Niederlande
Nevelgaarde 56 Noord, 3436 ZZ Nieuwegein, Niederlande

Kapstadt, Südafrika
Gateway Building, Century Blvd & Century Way 1,
Century City, 7441, Cape Town, Südafrika

Dublin, Irland
Block 21 Beckett Way, Park West Business Park,
Dublin 12, D12 C9YE, Irland

St. Gallen, Schweiz
Poststrasse 17, St. Gallen, Schweiz, 9000

London, UK
7th Floor, Exchange Tower, 2 Harbour Exchange Square,
London, E14 9GE, Großbritannien

Mechelen, Belgien
Schaliënhoevedreef 20T, 2800 Mechelen, Belgien

München, Deutschland
Ismaninger Straße 52, 81675 München, Deutschland

digicert®