

# Installation und Nutzung von SSL-Zertifikaten Schritt für Schritt





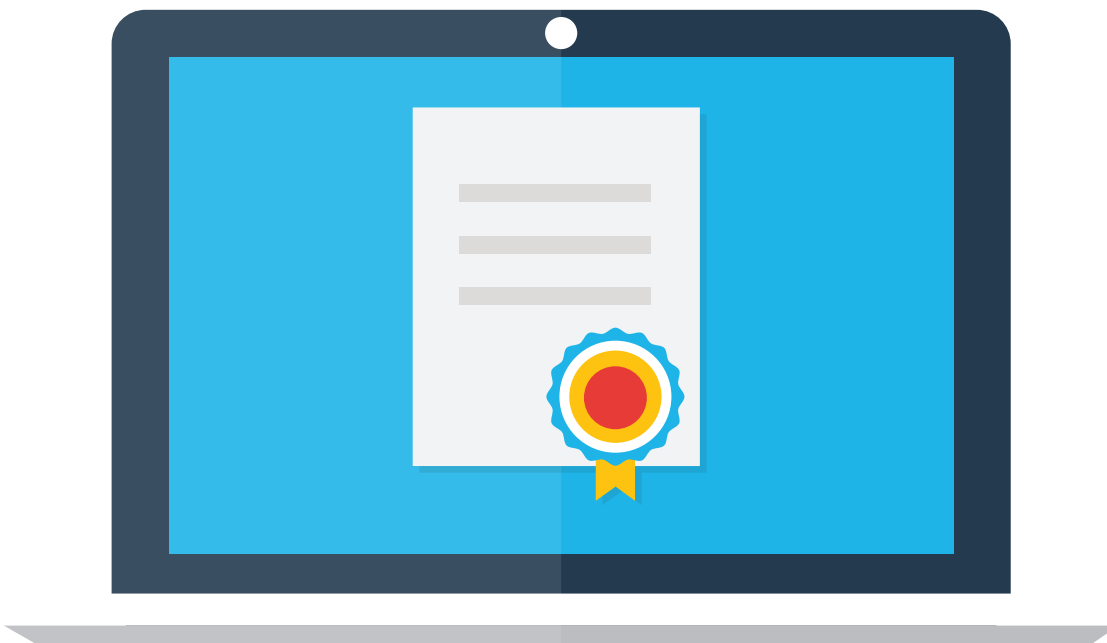
Sie haben Ihr(e) SSL-Zertifikat(e) gekauft.

Damit haben Sie den ersten Schritt zum Schutz Ihrer Website getan, doch Sie sind noch nicht am Ziel. Allzu oft werden Zertifikate nicht richtig installiert, sodass Seiten ungeschützt bleiben, Besucherdaten aus Online-Formularen unverschlüsselt übertragen werden und die Website weiterhin anfällig für Angriffe ist.

Die folgenden Tipps sollen Ihnen helfen, bei der Installation von Anfang an alles richtig zu machen. Richtig installierte SSL-Zertifikate sind der Schlüssel zu einer sichereren Website für Ihr Unternehmen, Ihre Mitarbeiter und Ihre Kunden. Doch bei der Installation gilt es, Fallstricke und riskante Praktiken zu vermeiden.

### **SSL hilft nur, wenn es richtig installiert ist**

Sie haben beschlossen, Ihre Website mit SSL zu schützen. Installieren Sie Ihr(e) Zertifikat(e) sorgfältig, um sie optimal zu nutzen und das Kundenvertrauen aufzubauen, das für Online-Geschäfte heute unverzichtbar ist.





## 1. Vorbereitung des privaten Schlüssels und der CSR



Bevor Sie ein digitales Zertifikat installieren, müssen Sie zuerst einen privaten Schlüssel und eine Signaturanforderung (Certificate Signing Request, CSR) für den Server generieren, auf dem das Zertifikat installiert werden soll. Danach schicken Sie die CSR an die Zertifizierungsstelle, um ein Zertifikat zu beantragen. So geht's:

Für die Installation auf einem Server mit Microsoft IIS 6.0 oder einer neueren Version bzw. Red Hat Linux können Sie den [Symantec SSL Assistant](#) herunterladen und sich von den benutzerfreundlichen Prompts durch den Prozess führen lassen. Im Artikel [Erzeugen eines Certificate Signing Request \(CSR\)](#) in der Symantec Knowledge Base finden Sie Anleitungen für andere Server. Um ein SSL-Zertifikat von Symantec zu beantragen, benötigen Sie die folgenden Angaben:

- die gewünschte Gültigkeitsdauer für das Zertifikat (1, 2 oder 3 Jahre),
- die Anzahl der Server, auf denen eine Domäne gehostet wird (bis zu 5),
- die Serverplattform,
- den Namen und die Adresse Ihres Unternehmens und ggf. der Abteilung, für die das Zertifikat bestimmt ist,
- Zahlungsdaten und eine Kontaktperson für die Rechnungslegung,
- den sogenannten Common Name, d. h. den Host- und Domänennamen, z. B. „www.meinefirma.de“ oder „webmail.meinefirma.de“,
- eine E-Mail-Adresse, unter der Symantec Sie kontaktieren kann, um diese Angaben zu überprüfen,
- die CSR für den zu sichernden Server.

Wenn Sie Ihr Zertifikat erhalten haben, folgen Sie den Anweisungen unter Punkt 3.

Falls Ihr Server nicht in der Liste aufgeführt ist oder Sie zusätzliche Informationen benötigen, konsultieren Sie bitte die Dokumentation oder den Anbieter des Servers. Wenn Sie nicht wissen, welche Software Ihr Server verwendet, wenden Sie sich an Ihren IT-Administrator.

Schicken Sie die CSR mit der folgenden Kopf- und Fußzeile ab, um ein Zertifikat zu beantragen:

-----BEGIN CERTIFICATE SIGNING REQUEST-----

XXXXXXXX

-----END CERTIFICATE SIGNING REQUEST-----



## 2. Richtige Installation des SSL-Zertifikats



Wenn Sie zum ersten Mal ein SSL-Zertifikat installieren, erscheint die Prozedur Ihnen vielleicht etwas komplex. Es sieht jedoch komplizierter aus, als es ist. So installieren Sie ein Zertifikat von Symantec auf Ihrem Server:

Die folgenden vier Schritte sind für alle Server gleich:

### 1. Zertifikat speichern

Folgen Sie den Anweisungen in der Bestätigungs-E-Mail, um Ihr SSL-Zertifikat von der angegebenen URL auf Ihren Desktop herunterzuladen. Auf diese Weise erhalten Sie Ihr Zertifikat und die erforderlichen Zwischenzertifikate.

### 2. Zertifikat installieren oder in einem Zertifikatordner ablegen

### 3. Zertifikat auf der Website konfigurieren

### 4. auf das Zertifikat verweisen

Weitere Informationen und schrittweise Installationsanleitungen für die verschiedenen Servertypen finden Sie [hier](#).

Zeigen Sie das Norton Secured-Siegel auf Ihrer Website an, um den vollen Nutzen aus Ihrem SSL-Zertifikat zu ziehen. Hierdurch fühlen sich Ihre Kunden sicherer, wenn sie Geschäfte mit Ihnen abwickeln.

Kopieren Sie dazu einfach den entsprechenden Code von der Symantec-Webseite für das Norton Secured-Siegel und fügen Sie ihn in den Code Ihrer Website ein. Am Ende dieses Abschnitts finden Sie einen Link zu einer ausführlichen Anleitung. Sie können Ihr Zertifikat testen, indem Sie den Domännennamen in den SSL Certificate Checker eingeben. Auch hierzu finden Sie im Anschluss einen Link.

Damit ist die Installation Ihres SSL-Zertifikats abgeschlossen.

### Probleme?

Symantec hat eine Reihe von Video-Anleitungen für verschiedene Server erstellt: [Video-Anleitungen ansehen](#)

### Überprüfen Ihrer Installation

Geben Sie einfach die URL des Servers ein, den Sie prüfen möchten: [Installation überprüfen](#)

### Siegel anzeigen

Binden Sie das Norton Secured-Siegel in Ihre Website ein: [Siegel anzeigen](#)

### Fehlerbehebung

Der Symantec Support steht zu Ihrer Verfügung: [Symantec Support](#)



### 3. Bestmöglicher Schutz der privaten Schlüssel



Öffentliche und private Schlüssel sind wichtig für die Funktionsweise von SSL. Ihr privater Schlüssel wird auf Ihrem Server gespeichert und genutzt, um Ihre Website zu verschlüsseln. Er muss unbedingt geheim bleiben. Ihr öffentlicher Schlüssel ist im Zertifikat selbst enthalten und dient damit der Identifizierung Ihrer Website, genauso wie der Domänenname und die Angaben zu Ihrem Unternehmen.

Betrachten Sie Ihre privaten Schlüssel als kostbare Ressourcen und gewähren Sie nur der kleinsten möglichen Anzahl Ihrer vertrauenswürdigsten Mitarbeiter und Partner Zugang zu ihnen. Stellen Sie sich vor, dass Sie ein Bankmanager und Ihre privaten Schlüssel die Schlüssel zum Tresorraum sind. Einige Best Practices für die Verwaltung privater Schlüssel:

- **Generieren Sie private Schlüssel nur auf einem sicheren Server.** Beauftragen Sie auf keinen Fall einen externen Anbieter mit dieser Aufgabe!
- **Schützen Sie die privaten Schlüssel mit Kennwörtern**, um den Diebstahl der Schlüssel aus Sicherungskopien zu verhindern.
- **Erneuern Sie Ihre Zertifikate jährlich** und generieren Sie dabei jedes Mal neue private Schlüssel.

Die Länge des privaten Schlüssels hat einen großen Einfluss auf den „SSL-Handshake“ beim Aufbau einer sicheren Verbindung. Ein zu kurzer Schlüssel bietet nicht genug Sicherheit, doch ein zu langer Schlüssel kann den Verbindungsaufbau deutlich verlangsamen.

In diesem Zusammenhang ist die Elliptische-Kurven-Kryptografie (ECC) interessant, da sie trotz kürzerer Schlüssellänge ein ebenso hohes Maß an Sicherheit bietet wie herkömmliche Verschlüsselungsverfahren. Bei gleicher Schlüssellänge ist das Knacken der ECC-Verschlüsselung von Symantec 10 000-mal so aufwendig wie das Knacken der RSA-Verschlüsselung. Ein ECC-Schlüssel mit 256 Bit ist daher beispielsweise ebenso sicher wie ein RSA-Schlüssel mit 3072 Bit. Deshalb bietet ECC bei geringerer Serverbelastung ein höheres Maß an Sicherheit und eine bessere Leistung.

Weitere Informationen über ECC finden Sie auf Seite 7.



## 4. Keine schwachen Glieder in der Kette



In den meisten SSL-Installationen reicht ein Serverzertifikat allein nicht aus: Drei oder mehr Zertifikate werden benötigt, um eine vollständige Vertrauenskette aufzubauen. Eine Vertrauenskette besteht aus sämtlichen Zertifikaten, die erforderlich sind, um die Identität des Servers zu bestätigen, für den das Endzertifikat ausgestellt wurde.

Eine solche Kette besteht in der Regel aus dem Endzertifikat, einem oder mehreren Zwischenzertifikaten und dem Root-Zertifikat.

Um die Echtheit und Gültigkeit Ihres neuen Zertifikats zu testen, müssen Sie alle Glieder in dieser Kette überprüfen, von der universell vertrauenswürdigen Root-Zertifizierungsstelle über die verschiedenen Zwischenzertifizierungsstellen bis hin zu der Zertifizierungsstelle, die Ihr Zertifikat – das sogenannte Endzertifikat – ausgestellt hat. Ein Zertifikat ist nur vertrauenswürdig, wenn jedes Zertifikat in seiner Zertifikatskette ordnungsgemäß ausgestellt und verifiziert wurde.

Ein häufig beobachtetes Problem ist, dass das Endzertifikat richtig installiert, aber die Zwischenzertifikate vergessen wurden. Nutzen Sie den [SSL Certificate Checker](#), um zu überprüfen, ob Ihre Zwischenzertifikate korrekt installiert sind.



## 5. RSA, ECC und die Bedeutung der Schlüssellänge



Elliptische-Kurven-Kryptografie (ECC) bietet Ihrem Unternehmen stärkere Sicherheit und bessere Leistung als herkömmliche Verschlüsselungsverfahren.

ECC ist ein von der US-Regierung anerkannter und von der NSA empfohlener Verschlüsselungsalgorithmus, der anhand von Punkten auf einer Kurve öffentliche und private Schlüssel erstellt. Er ist kaum mit den oft von Hackern eingesetzten Brute-Force-Angriffen zu knacken und trotz geringerem Ressourcenbedarf schneller als RSA-Verschlüsselung.

Der Verschlüsselungs- und Signaturalgorithmus RSA ist seit fast zwanzig Jahren die Grundlage der Internet-sicherheit und noch immer ein nützlicher Algorithmus. Im Laufe der Zeit wurden jedoch immer längere Schlüssel erforderlich, um Schutz vor immer raffinierteren kryptografischen Angriffen zu bieten. ECC bietet ein höheres Maß an Sicherheit mit kürzeren Schlüsseln und daher eine bessere Leistung. Ein ECC-Schlüssel mit 256 Bit bietet beispielsweise dasselbe Maß an Sicherheit wie ein RSA-Schlüssel mit 3072 Bit. Mit ECC können Sie Ihre Website also adäquat sichern, ohne Abstriche bei der Leistung zu machen.

Zudem lassen die kürzeren ECC-Schlüssel sich in kleineren Zertifikaten unterbringen, deren Übertragung eine geringere Bandbreite erfordert. Da immer mehr Kunden Mobilgeräte zum Abwickeln von Transaktionen nutzen, ist ECC auch in puncto Benutzerfreundlichkeit die bessere Lösung.

ECC-Rootzertifikate von Symantec sind seit 2007 in den drei meistgenutzten Browsern enthalten. ECC-Zwischen- und -Endzertifikate von Symantec sind ohne zusätzliche Kosten erhältlich. Wenn Sie und die Besucher Ihrer Website moderne Browser nutzen, fügen diese Zertifikate sich nahtlos in die vorhandene Infrastruktur ein.

Informieren Sie sich ausführlich über [ECC und Algorithmenfähigkeit](#).



## 6. Always-On SSL



Am besten verschlüsseln Sie Ihre gesamte Website mit SSL. Das geht am einfachsten mit Always-On SSL. Dieses kostengünstige Sicherheitsprinzip schützt Website-Besucher von der Suche über den Meinungsaustausch mit anderen Kunden bis hin zum Einkauf lückenlos und zuverlässig.

Unternehmen, die großen Wert auf den Schutz ihrer Kunden und auf ihren guten Ruf legen, sollten sich für Always-On SSL mit SSL-Zertifikaten einer renommierten Zertifizierungsstelle wie Symantec entscheiden. Always-On SSL ist eine grundlegende, einfach zu implementierende Sicherheitsmaßnahme, die alle übertragenen Daten vor unbefugtem Zugriff, Manipulation und Missbrauch schützt. Insbesondere werden alle Cookies verschlüsselt.

Deshalb empfiehlt die Online Trust Alliance (OTA), dass alle Unternehmen ihre Website mit Always-On SSL schützen: „Always-On SSL ist gut umsetzbar, hat sich bewährt und sollte auf allen Websites, auf denen die Besucher vertrauliche Daten eingeben oder angezeigt bekommen, implementiert werden.“

Viele der erfolgreichsten Websites weltweit werden bereits mit Always-On SSL vor Bedrohungen wie Side-jacking, Hackerangriffen mit Tools wie Firesheep und dem Einschleusen von Malware geschützt.

Mit Always-On SSL signalisieren Sie den Besuchern Ihrer Website, dass Sie Benutzersicherheit und Datenschutz ernst nehmen und deshalb angemessene Schutzmaßnahmen ergreifen.



## 7. Public Key Pinning: eine Sache des Vertrauens



Mit der HTTP-Erweiterung Public Key Pinning (HPKP) können Website-Betreiber festlegen, welche Zertifizierungsstellen Zertifikate für ihre Server ausstellen dürfen.

HPKP etabliert eine Verbindung zwischen einem Host und seinem rechtmäßigen Zertifikat bzw. öffentlichen Schlüssel. Sobald der öffentliche Schlüssel für einen Host bekannt ist, wird er an diesen Host „geheftet“.

Laut dem CA Security Council können Website-Betreiber mit HPKP festlegen, dass ihr SSL-Zertifikat mindestens eines der folgenden Merkmale aufweisen muss:

- einen bestimmten öffentlichen Schlüssel,
- die Signatur einer Zertifizierungsstelle (Certificate Authority, CA) mit diesem öffentlichen Schlüssel,
- eine hierarchische Vertrauenskette zu einer CA mit diesem öffentlichen Schlüssel.

Website-Betreiber können auch mehrere Schlüssel verschiedener Zertifizierungsstellen an ihre Domänen „heften“. Alle entsprechenden Schlüssel werden dann von Browsern, die HPKP unterstützen, als gültig betrachtet. Wird einem solchen Browser dagegen ein Zertifikat einer Zertifizierungsstelle präsentiert, die nicht an diese Website „geheftet“ ist, wird eine Warnmeldung angezeigt.

Der Website-Betreiber vertraut also darauf, dass die Zertifizierungsstelle seiner Wahl keine nicht autorisierten Zertifikate für seine Domäne ausstellt. Aus diesem Grund verlangen viele CA, dass alle Zertifikate für die Domänen eines Website-Betreibers von denselben, dazu befugten Personen beantragt werden.

Das von Google bereits 2011 implementierte Verfahren für das Public Key Pinning wurde vom CA Security Council jedoch als nicht skalierbar eingestuft, da es voraussetzt, dass Browser die öffentlichen Schlüssel aller Domänen speichern. Inzwischen wurde eine neue, skalierbare HPKP-Lösung in einem IETF RFC (Internet Engineering Task Force Request for Comments) dokumentiert.

Bei diesem Lösungsvorschlag werden die öffentlichen Schlüssel in http-Kopfzeilen vom Server an den Browser geschickt. Der Vorschlag sieht unter anderem Optionen für die Hash-Algorithmen SHA-1 und SHA-256, die maximale Gültigkeitsdauer der HPKP-Daten, die Strenge ihrer Anwendung und die Angabe vor, ob sie auch für Subdomänen gültig sind.



## 8. Abwehr von Lauschangriffen mit Folgenlosigkeit



Lauscher können Ihre verschlüsselt übertragenen Daten heute zwar aufzeichnen, aber nicht lesen. Das kann sich jedoch ändern, wenn es denselben Lauschern in Zukunft gelingt, an Ihre alten privaten Schlüssel zu gelangen.

RSA generiert öffentliche und private Schlüssel zum Ver- und Entschlüsseln von Nachrichten. Da dieselben wiederherstellbaren Schlüssel wiederholt genutzt werden, können Angreifer gespeicherte Daten entschlüsseln, wenn sie in den Besitz der Schlüssel gelangen. Wenn ein Angreifer beispielsweise den Aufbau einer Verbindung, den sogenannten SSL-Handshake, aufzeichnet und später in den Besitz der dabei verwendeten privaten Schlüssel gelangt, kann er den Verbindungsaufbau, einschließlich der Sitzungsschlüssel, entschlüsseln. Mit diesen Sitzungsschlüsseln kann er dann die gesamte Sitzung entschlüsseln. Für Sie als Website-Betreiber ist das natürlich beunruhigend. Deshalb sollten Sie den Einsatz der sogenannten Folgenlosigkeit erwägen.

Mit Folgenlosigkeit werden nicht wiederherstellbare, kurzfristig gültige Sitzungsschlüssel generiert und nach dem Ende des Datenaustauschs gelöscht. Bei richtiger Implementierung mit Elliptische-Kurven-Kryptografie (ECC, siehe Punkt 5) ist die Folgenlosigkeit zudem sicherer und schneller als der RSA-Algorithmus.

Mit Folgenlosigkeit gibt es keine Verbindung zwischen dem privaten Schlüssel eines Servers und den verschiedenen Sitzungsschlüsseln. Wenn sowohl der Client als auch der Server die Folgenlosigkeit unterstützen, wird eine Variante des Diffie-Hellman-Protokolls verwendet, bei dem Client und Server anhand gesichert ausgetauschter Zufallszahlen unabhängig voneinander dasselbe sogenannte „Diffie-Hellman-Secret“ errechnen. Ein Lauscher kann dieses „Diffie-Hellman-Secret“ selbst dann nicht erraten, wenn er den gesamten Sitzungsaufbau mithört.

Weitere Informationen über die Folgenlosigkeit finden Sie in dieser [Infografik von Symantec](#).



## 9. HTTP Strict Transport Security: Ihr Sicherheitsnetz



Ihre Website und deren Besucher können nicht „zu sicher“ sein. Manchmal reichen Standardmaßnahmen nicht aus, um das erforderliche Maß an Sicherheit zu erzielen.

Mit SSLStrip und anderen Man-in-the-Middle-Angriffen in drahtlosen Netzwerken können Hacker Browser-Aufrufe von HTTPS-Websites abfangen und die verlangten Webseiten via HTTP zurückschicken. Daraufhin wird die Verbindung nicht mehr verschlüsselt und der Hacker kann Daten abfangen, die das Opfer auf einer vermeintlich sicheren Website eingibt. Die meisten Website-Besucher achten nicht bei jedem Seitenwechsel innerhalb einer Website darauf, ob in der Adresszeile `https:` oder `http:` steht. Deshalb haben Hacker gute Chancen, bei einem solchen Angriff unbemerkt zu bleiben. Auch der Browser kann die Opfer nicht vor einem solchen Angriff schützen, da er nicht „wissen“ kann, dass der Aufruf von einem Hacker abgefangen und geändert wurde.

Mit HTTP Strict Transport Security (HSTS) können Server eine Nachricht an den Browser schicken, um zu verlangen, dass immer HTTPS verwendet wird. Der so informierte Browser sorgt dann dafür, dass alle Webseiten, die Ihre Kunden aufrufen, verschlüsselt übertragen werden. Damit sind Ihr Unternehmen und Ihre Kunden vor Man-in-the-Middle-Angriffen geschützt.

Sie können HSTS mit einer einzigen Kopfzeile auf der Website, dem sogenannten „HTTP Response Header“, aktivieren. Browser wie Chromium, Google Chrome, Firefox, Opera und Safari, die HSTS unterstützen, verhindern dann unsichere Verbindungen zu Ihrer Website, indem sie alle Links zu `http`-Adressen automatisch in Links zu den äquivalenten `https`-Adressen umwandeln.

Internet Explorer unterstützt HSTS bislang nicht, Microsoft hat diese Option jedoch für Internet Explorer 12 angekündigt.

© 2015 Symantec Corporation. Alle Rechte vorbehalten.  
Symantec, das Symantec-Logo, das Häkchen im Kreis  
und das Norton Secured-Logo sind Marken oder  
eingetragene Marken der Symantec Corporation oder  
ihrer Partnerunternehmen in den USA und anderen  
Ländern. Andere Namen sind möglicherweise Marken  
ihrer jeweiligen Eigentümer.