Sicherer Online-Datentransfer mit SSL

EIN ÜBERBLICK ÜBER SSL-ZERTIFIKATE, *ihre Funktionen und Anwendung…*

1. Überblick

thawte ist ein weltweit führender Anbieter von SSL-Zertifikaten. Anhand eines *thawte* SSL-Zertifikats auf dem bzw. den Web-Servern Ihres Unternehmens können Sie vertrauliche Informationen sicher online abrufen und den Umsatz steigern, indem Sie Ihren Kunden das nötige Vertrauen hinsichtlich der Sicherheit der getätigten Vorgänge entgegenbringen.

Diese Anleitung ist eine Einführung in das Konzept der SSL-Sicherheit und behandelt die grundlegenden Funktionen. Erläutert werden ebenfalls die verschiedenen Anwendungen von SSL-Zertifikaten und die entsprechenden Einsatzbereiche, zusammen mit einer Beschreibung, wie Sie SSL-Zertifikate auf Ihrem Web-Server testen können.

2. Was ist SSL?

Secure Socket Layer (SSL) ist ein von Netscape im Jahr 1996 entwickeltes Protokoll, das sich rasch zur gängigsten Methode entwickelte, Datenübertragungen über das Internet abzusichern. SSL ist ein wesentlicher Bestandteil der meisten Web-Browser und Web- Server und funktioniert mit dem von RSA entwickelten Verschlüsselungssystem basierend auf einem öffentlichen-privaten Schlüsselpaar.

Um eine SSL-Verbindung aufzubauen, muss einem Server für das SSL-Protokoll vorab ein digitales Zertifikat installiert worden sein. Ein digitales Zertifikat ist eine elektronische Datei, mit der die Identität von Einzelpersonen und Servern bestimmt wird. Digitale Zertifikate sind eine Art digitaler Pass oder Zeugnis, die den Server vor Aufbau der SSL-Verbindung beglaubigen. Digitale Zertifikate werden üblicherweise seitens einer unabhängigen und vertrauenswürdigen Drittinstanz signiert, um ihre Gültigkeit zu bescheinigen. Der "Signierer" eines Zertifikats wird als Zertifizierungsstelle (CA) bezeichnet, beispielsweise *thawte*.

SSL sorgt durch die Kombination der folgenden zwei Elemente für sichere Kommunikation:

1] Authentisierung – Ein digitales Zertifikat ist mit einer bestimmten Domain verbunden, und eine CA führt eine Reihe von Überprüfungen durch, um die Identität des beantragenden Unternehmens vor Ausstellung des Zertifikats zu bestätigen. Auf diese Weise kann das Zertifikat einzig und allein auf der Domain installiert werden, gegenüber der es beglaubigt wurde. Somit wird den Benutzern das notwendige Vertrauen gegenübergebracht.

2] Verschlüsselung – Unter Verschlüsselung versteht man das Verfahren, mittels dem Information so umgewandelt werden, dass sie für unbefugte Dritte unlesbar sind und lediglich vom rechtmäßigen Empfänger genutzt werden können. Das bildet die Grundlage der im E-Commerce notwendigen Unversehrtheit und des Schutzes von Daten.

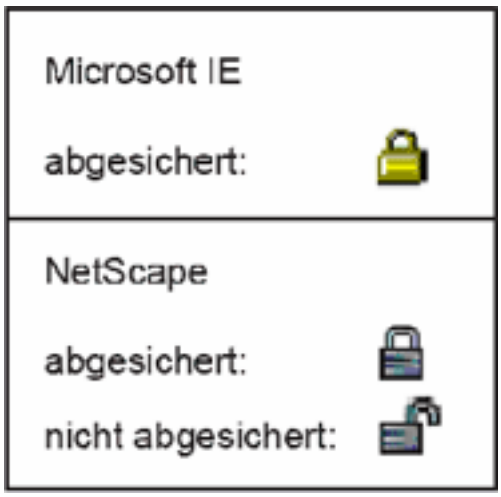
Hinweis

Am häufigsten werden SSL-Zertifikate zur Sicherung von Datentransfers zwischen Web-Browsern und Web-Servern angewendet. Obwohl SSL auch zur Sicherung von Server-zu-Server-Kommunkationen eingesetzt werden kann, werden die SSLFunktionen in dieser Anleitung anhand von Browser-Server Beispielen erklärt.

Um mehr über die SSL-Sicherung von Server-zu-Server-Kommunkationen zu erfahren, wenden Sie sich bitte an einen *thawte* Handelsvertreter.

3. Wie kann man feststellen, dass eine Website sicher ist?

Der erste Hinweis darauf, ob eine Website anhand eines SSL-Zertifikats gesichert ist oder nicht, ist in der Statuszeile des Browsers ersichtlich - schauen Sie, ob dort ein Vorhängeschloss angezeigt wird. In IEBrowsern wird dieses Icon bei nicht sicheren Seiten nicht angezeigt. Wenn jedoch eine SSL-Verbindung aufgebaut wird, wird das orhängeschloss angezeigt. In Netscape gibt es "verschlossene" und "unverschlossene"Vorhängeschlösser, die sichere und nicht sichere Websites anzeigen.



Der nächste Hinweis findet sich in der Adresszeile. Beim Aufbau einer sicheren Verbindung zwischen dem Browser und dem Web-Server wird der Teil “http:” der Webadresse in “https” um benannt, z.B.: wird zu https://www.thawte.com”.

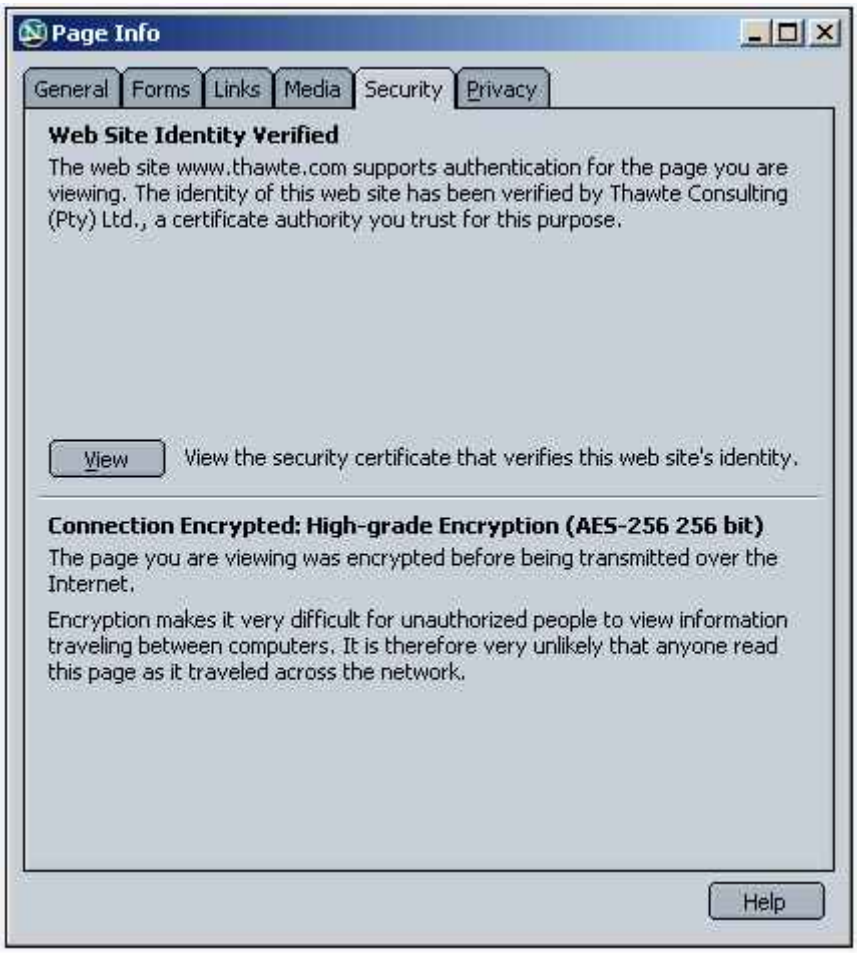
Ebenso kann die Verschlüsselungsstufe einer bestimmten SSL-Verbindung erkannt werden. In IE-Browsern bewegen Sie einfach die Maus über das Vorhängeschloss, um die Zuverlässigkeit der erschlüsselungs zu ersehen.

In Netscape klicken Sie zweimal auf das Vorhängeschloss, um das Zertifikat aufzurufen. Die Verschlüsselungsstufe ist unter der ersten Karteikarte des Zertifikats abgelegt.

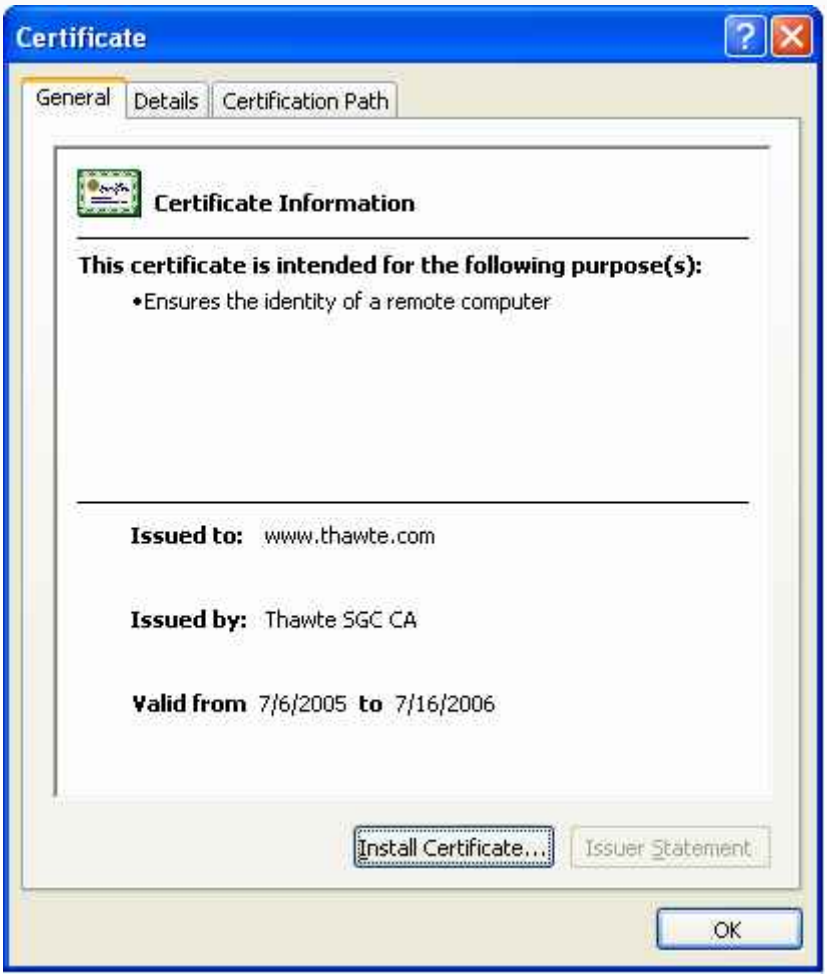
4. Wie sieht ein SSL-Zertifikat aus?

Um das Zertifikat einer Website aufzurufen, klicken Sie zweimal auf das verschlossene Vorhängeschloss in der unteren Statuszeile.

Ein digitales Zertifikat bei Benutzung eines Netscape 7.0 Browsers:



Ein digitales Zertifikat bei Benutzung eines IE 6.0 Browsers:



Mit einem SSL-Web-Server-Zertifikat oder einem SGC SuperCert von *thawte* können Ihre Kunden die folgenden Informationen ersehen:

- Die Domain, für die das Zertifikat ausgestellt wurde. Somit können sie überprüfen, dass das SSL-Web-Server-Zertifikat für genau Ihren Host und Ihre Domain ausgestellt wurde ().
- Wer der Eigentümer des Zertifikats ist. Das ist eine zusätzliche Rückversicherung, da die Kunden somit sehen können, mit wem Sie es geschäftlich zu tun haben.
- Wo sich der Eigentümer befindet. Auch das ist eine weitere Bestätigung für die Kunden, dass sie es mit einem rechtmäßigen Unternehmen zu tun haben.
- Die Gültigkeitsdaten des Zertifikats. Das ist ein extrem wichtiger Aspekt, denn daran können die Benutzer rkennen, dass Ihr digitales Zertifikat aktuell gültig ist.

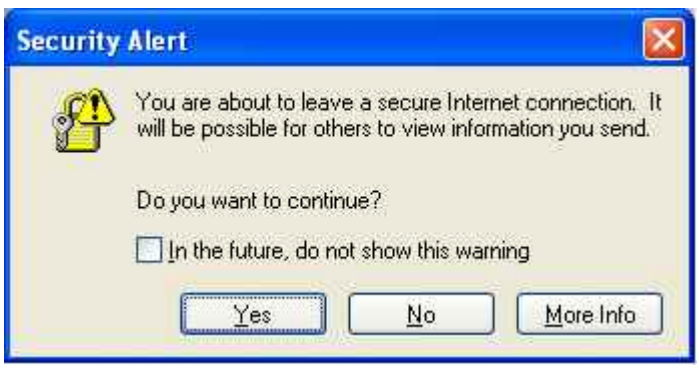
5. Sicherheitsalarme des Browsers

Ihr Browser hat eine integrierte Sicherheitsfunktion, die Warnmeldungen anzeigt, wenn Sie versuchen, Informationen an eine Website zu senden, die Probleme mit dem Zertifikat aufweist.

Dies ist ein Beispiel einer Warnmeldung in Microsoft IE:

Im obigen Beispiel wird der Sicherheitsalarm ausgelöst, da derDomainname nicht mit dem der aufgerufenen Website übereinstimmt. Es wird davor gewarnt, dass die Website, auf der das Zertifikat installiert wurde, nicht zur Nutzung des Zertifikats berechtigt ist. Weitere Sicherheitsalarme werden ausgelöst, wenn die Gültigkeitsdauer eines Zertifikats abgelaufen ist. Ähnlich wird eine Warnung angezeigt, falls das Zertifikat mit einer nicht erkannten Root, also einer Wurzel signiert ist (d.h. eine Root, die nicht standardmäßig im Browser integriert ist).

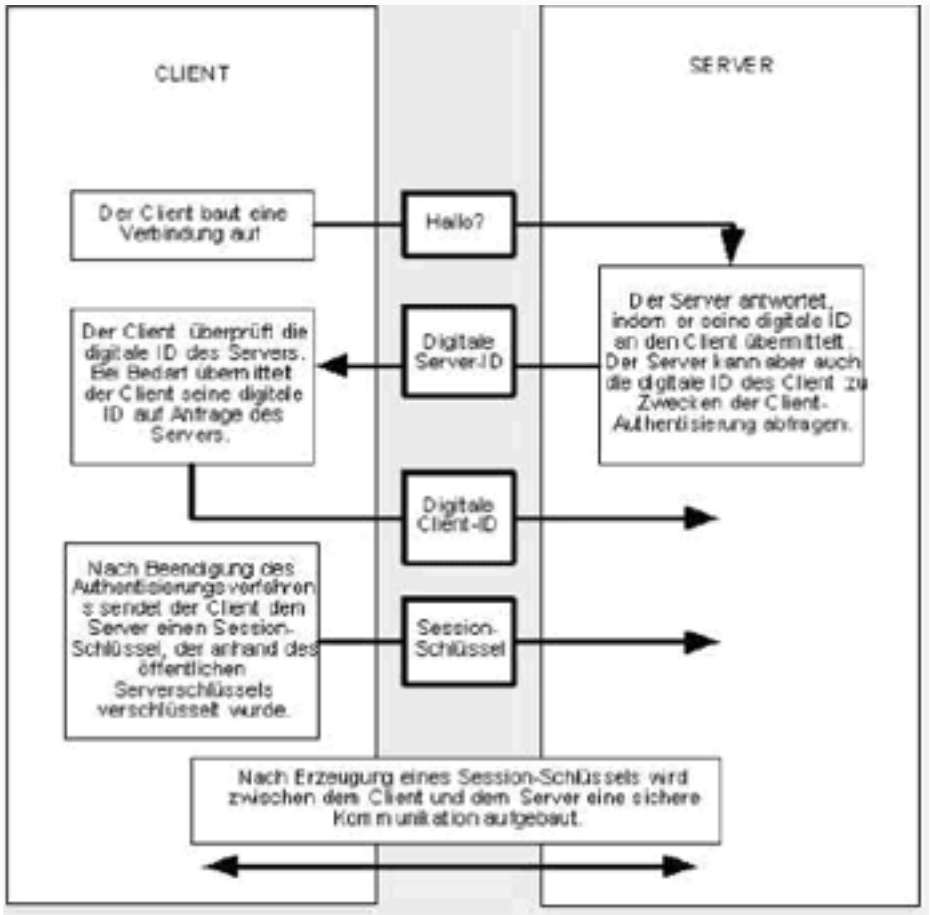
Demgegenüber wird ein Benutzer, der eine Website mit einem gültigen Zertifikat aufruft, darüber informiert, dass die von ihm besuchte Website ein von einer anerkannten Zertifizierungsstelle (CA), z.B. *thawte*, ausgestelltes Zertifikat hat, und dass die von ihm gesendeten Daten verschlüsselt werden. Durch Überprüfung des Zertifikats kann der Kunde bestätigen, dass die Website und der entsprechende Domainname tatsächlich zu einer richtigen Firma gehören.



6. Wie richtet man eine SSL-Verbindung ein?

Beim Verbindungsaufbau zu einem sicheren Web-Server, wie https://www.thawte.com, muss der Server sich zunächst gegenüber dem Web-Browser anhand eines digitalen Zertifikats bestätigen, bevor eine sichere Verbindung hergestellt werden kann.

Das nachstehende Schaubild zeigt die einzelnen Schritte, die zum Einrichten einer SSL-Verbindung notwendig sind:



Während diesem Vorgang überprüft der Web-Browser, dass:

• der im Zertifikat enthaltene Domainname mit der Senderdomain Übereinstimmt

• das Zertifikat nicht abgelaufen ist

• die CA, die das Zertifikat signiert hat, vom Web-Browser als vertrauenswürdig eingestuft wird.

Das ist ein nahtlos ablaufender Vorgang, da der Benutzer die einzelnen Schritte nicht erkennen kann. Das Zertifikat ist Beweis dafür, dass ein unabhängiger, vertrauenswürdiger Dritter, beispielsweise *thawte*, überprüft hat, dass die Domain zu einem echten Unternehmen gehört und daher als vertrauenswürdig eingestuft werden kann. Ein gültiges Zertifikat vermittelt den Kunden das nötige Vertrauen, dass sie persönliche Information sicher an den beglaubigten Empfänger leiten.

7. Öffentliche und Private Schlüssel

Bei Antrag eines Zertifikats erzeugen Sie ein Schlüsselpaar auf Ihrem Server -einen öffentlichen und einen privaten Schlüssel. Bei der Generierung eines Schlüsselpaars für Ihr Unternehmen wird der private Schlüssel auf Ihrem Server installiert. Dabei ist wichtig, dass niemand außer Ihnen Zugang zu diesem Schlüssel hat. Ihr privater Schlüssel erzeugt digitale Signaturen, die Sie höchst wirkungsvoll als Online-Stempel Ihres Unternehmens einsetzen können. Es ist überaus wichtig, dass dieser Schlüssel so sicher wie nur möglich aufbewahrt wird. Sollten Sie Ihren privaten Schlüssel verlieren, können Sie Ihr Zertifikat nicht länger nutzen. Aus diesem Grund ist es unabdingbar, dass Sie sich für ein optimales Schlüsselmanagement eine Sicherungskopie des privaten Schlüssels erstellen.

Der dazu passende öffentliche Schlüssel wird auf Ihrem Web-Server als Teil des digitalen Zertifikats abgelegt. Der öffentliche und der private Schlüssel stehen zwar in mathematischer Beziehung zueinander, sind jedoch nicht identisch. Kunden, die mit Ihnen privat (über SSL) kommunizieren möchten, benutzen den öffentlichen Schlüssel Ihres Zertifikats, um die Information, die sie senden wollen, vorab zu verschlüsseln. Dieser für den Benutzer nahtlose Vorgang wird im Nu ausgeführt. Lediglich der private Schlüssel des Web-Servers ist in der Lage, diese Information zu entschlüsseln. Ihre Kunden fühlen sich sicher, dass niemand die von ihnen an Ihren Server gesendeten Daten einsehen kann.

8. SSL-Anwendungen

Es gibt zwei Hauptanwendungsbereiche von SSL-Zertifikaten:

1] Die Sicherung von Kommunikation vom Browser an den Web-Server -
Die Sicherung von Kommunikation von einem Browser an einen Web-Server ist derzeit der Hauptanwendungsbereich und wird am häufigsten auf E-Commerce Websites angewendet, um die Übermittlung von Zahlungsinformation abzusichern. Die Art der Daten, die als vertraulich angesehen werden, reicht derzeit von finanziellen Informationen bis hin zu persönlichen Identifikationsdaten, darunter Ausweis- und Sozialversicherungsnummern, sowie zunehmend auch E-Mail-Adressen.

2] Die Sicherung von Server-zu-Server-Kommunikation -
Mehr und mehr Firmen nutzen SSL-Zertifikate zur Sicherung von Server-zu-Server-Kommunikationen. Hierbei handelt es sich um einen Anwendungsbereich, der Unternehmen verschiedene Möglichkeiten bietet, die Daten- und Netzwerksicherheit zu verbessern. Derzeit ist die Kommunikationssicherung zwischen E-Mail-Servern der am häufigsten genutzte Anwendungsbereich. Doch es ist unter anderem auch möglich FTP-Sites, Datenbanken und Anwendungsserver zu sichern.

9. Wann ist der Einsatz von SSL-Zertifikaten angebracht?

Die Entscheidung, ein SSL-Zertifikat einzusetzen hängt davon ab, wie wichtig die Sicherheit von Online-Datentransfers jeweils eingestuft wird. Wenn Sie beispielsweise finanzielle Transaktionen auf Ihrer Website handhaben, benötigen Sie zweifelsohne ein SSL-Zertifikat. Wenn Sie mit vertrauenswürdigen Kundendaten, wie Sozialversicherungsnummern oder Ausweisnummern, umgehen, sollten Sie den Einsatz eines SSL-Zertifikats durchaus in Betracht ziehen - vor allem wenn Sie der Sicherheit und dem Datenschutz Ihrer Kunden/Mitglieder Vorrang gewähren möchten.

Von einem rein geschäftlichen Blickwinkel aus betrachtet schafft der Einsatz von SSL-Zertifikaten bei den Kunden/Benutzern eine Vertrauensbasis, da sie wissen, dass sie somit keinerlei Risiken bei der Übermittlung von Daten über ein offenes Netzwerk ausgesetzt sind. Und daraus ergeben sich für Ihr Unternehmen zahlreiche Vorteile, die meist das Resultat einer besseren Vertrauensbasis bei der Handhabung von Online-Vorgängen mit Ihrer Firma sind. Falls Ihr Unternehmen also auf das Schaffen von Vertrauensverhältnissen mit Kunden setzt, um Online-Transaktionen.

10. thawte SSL-Zertifikate Lösungen

SSL123 Zertifikat
Das SSL123 Zertifikat gewaehrleistet die Sicherheit bzw. Guelitgkeit der Domain. Abhaengig von ihrem "Browser" ist eine 128-bit Verschluesselung moeglich. Dieses Produkt steht ihnen innerhalb weniger Minuten zur Verfuegung und eignet sich besonders um Sicherheit zwischen ihrem Kunden und Ihrer Website bzw. fuer generelle Anwendungen und Intranets herzustellen.

SSL-Web-Server-Zertifikate
Abhaengig von ihrem Browser ist mit dem “*thawte* SSL Web Server Zertifikat " eine 128-bit Verschluesselung moeglich. Dieses Zertifikat eignet sich besonders fuer Kunden die ihre verifizierten Unternehmensdaten fuer ihre Geschaefte im Internet benoetigen.

SGC SuperCerts
Ein "*thawte* SGC SuperCert" ermoeglicht auch ihrem Kunden mit folgenden Browsern eine 128-bit Verschluesselung: IE 5.01 und Netscape 4.7x und höher - die nur 40-Bit- oder 56-Bit-Verschlüsselungen zulassen. Wenn Sie hoch vertrauliche Information und eine Verschlüsselung bei 128-Bit wollen, sind das die idealen Zertifikate für Sie.

Starter-PKI Programm (SPKI)
Das SPKI Programm von *thawte* ist ideal für alle die Unternehmen, die drei oder mehr Zertifikate pro Jahr für den eigenen Nutzen fortlaufend benötigen. Mit unserem SPKI Programm haben Sie absolute Kontrolle über den Bedarf an Zertifikaten und ernten darüber hinaus die Gewinne aus erheblichen Einsparungen.

11. So testen Sie SSL-Zertifikate auf Ihrem Web-Server

Um Ihnen das praktische Verständnis von SSL-Zertifikaten nahe zu bringen können Sie sich ein SSL-Testzertifikat von *thawte* zu Bewertungszwecken herunterladen. Diese Zertifikate haben eine Gültigkeitsdauer von 21 Tagen. Sie haben damit die Möglichkeit, sich mit dem Installationsvorgang vertraut zu machen und die Kompatibilität mit Ihrer Web-Serverkonfiguration zu überprüfen. Das kostenlose Testzertifikat finden Sie hier: www.thawte.com/ucgi/gothawte.cgi?a=w14100158267049000

Ebenso können Sie eine der *thawte* Anleitungen herunterladen, in den Ihnen von Expertenhand Schritt für Schritt erklärt wird, wie Sie SSL-Zertifikate für die beiden gängigsten Web-Serverplattformen beantragen, konfigurieren und installieren:

Anleitung für Apache
Anleitung für Microsoft IIS

Installationsanleitungen für andere Web-Serverplattformen finden Sie auf unserer Supportseite - klicken Sie bitte hier, http://www.thawte.com/support.

12. Das thawte Site Seal

Alle Kunden, die das SSL-Web-Server-Zertifikat oder das SGC SuperCert von *thawte* benutzen, können das *thawte* Site Seal auf Ihren Websites anbringen und auslegen. Das Site Seal istein sicheres Icon, das den sichtbaren Beweis Ihres Vertrauensstatus erbringt, dass Sie vollstens beglaubigt wurden und dass Benutzer mit Ihnen sicher und ohne Bedenken Vorgänge tätigen können.
Das Site Seal ist in mehreren Sprachen und Größen erhältlich, um es bequem an das Design Ihrer bestehenden Website anzupassen. Ausführlichere Information ersehen Sie unter: http://www.thawte.com/ssl123/index.html

13. Nützliche URLs

Ausführlichere Informationen zu den SSL-Web-Server-Zertifikaten von thawte ersehen Sie unter: http://www.thawte.com/ssl/index.html

Die häufigsten Probleme mit SSL-Web-Server-Zertifikaten werden in der Wissensdatenbank von *thawte* behandelt: http://kb.thawte.com

Nützliche Information finden Sie ebenfalls in unseren FAQs: http://www.thawte.com/support/

Kaufen Sie SSL-Web-Server-Zertifikate: http://www.thawte.com/buy

14. Welche Rolle übernimmt thawte?

thawte Technologies ist eine CA (Certification Authority / Zertifizierungsstelle), die SSL-Web-Server-Zertifikate an Unternehmen und Einzelpersonen weltweit erteilt. thawte stellt Überprüfungen darüber an, ob es sich bei dem, das Zertifikat beantragende, Unternehmen um eine eingetragene Firma handelt und ob die Person, die das Zertifikat für das Unternehmen beantragt hat, tatsächlich dazu berechtigt ist.

thawte überprüft ebenfalls, ob das Unternehmen gleichzeitig Eigentümer der entsprechenden Domain ist. Die digitalen Zertifikate von thawte sind vollkommen kompatibel mit der jeweils aktuellsten Software von Microsoft und Netscape. Auf diese Weise können Sie beim Kauf eines Web-Server-Zertifikats von *thawte* sicher sein, das Vertrauen Ihrer Kunden in die Unversehrtheit Ihres Systems zu gewinnen. Ihre Kunden können sich darauf verlassen, sichere Online-Geschäfte zu führen.

15. Der Authentifizierungswert

Informationen stellen einen entscheidenden Wert für Ihr Unternehmen dar. Um die Unversehrtheit und Sicherheit Ihrer Informationen zu garantieren, ist es zunächst wichtig festzustellen, mit wem Sie in Kontakt treten, und ob die Daten, die Sie erhalten, auch vertrauenswürdig sind. Authentifizierung kann dazu beitragen, eine Vertrauensbasis zwischen den, in einer Unmenge von geschäftlichen Transaktionen voneinander abhängigen, Kommunikationspartnern zu bilden, und zwar durch die Einbindung von eindeutigen Sicherheitsaspekten:

Website-Manipulation: Die geringen Kosten von Website Design und die Einfachheit, Webseiten kinderleicht zu kopieren, schafft eine nahrhafte Grundlage für illegale Websites, die, so soll glaubhaft gemacht werden, von seriösen Firmen veröffentlicht werden. Tatsache ist jedoch, dass Trickbetrüger auf illegale Art Kreditkartennummern erlangen, indem Sie professionell erscheinende Storefronts errichten, die rechtmäßig begründete Geschäfte nachahmen.

Unbefugte Handlung: Ein Konkurrenzunternehmen oder ein verstimmter Kunde kann Veränderungen an Ihrer Website vornehmen, so dass diese nicht richtig funktioniert oder potentielle Neukunden abblockt.

Unbefugte Weitergabe von Informationen: Wenn Geschäftsinformationen “ahnungslos” weitergegeben werden, können Hacker die Datenübertragungen abfangen, um so an wichtige Informationen von Ihren Kunden zu gelangen.

Datenänderung: Der Inhalt eines Geschäfts kann abgefangen und während der Datenübertragung entweder böswillig oder unabsichtlich verändert werden. “Ahnungslos” gesendete Benutzernamen, Kreditkartennummern und Währungsbeträge können problemlos abgeändert werden.

16. Contacter thawte - Wenden Sie auch an thawte

Wenn Sie noch Fragen in Bezug auf den Inhalt dieser Gebrauchsanleitung oder auf Produkte und Service von *thawte* haben, wenden Sie sich bitte an einen unserer Verkaufsberater:

E-Mail: sales@thawte.com
Telefon: +27 21 937 8902
Fax: +27 21 937 8967

17. Glossar

Asymmetrische Kryptographie
Ein kryptographisches Verfahren mit Hilfe eines kombinierten öffentlichen und privaten Schlüsselbunds, um Nachrichten zu ver- und entschlüsseln. Um eine verschlüsselte Nachricht zu senden, verschlüsselt der Benutzer sie mit dem öffentlichen Schlüssel des Empfängers. Bei Empfang wird die Nachricht anhand des privaten Schlüssels des Empfängers wieder entschlüsselt. Die Benutzung verschiedener Schlüssel zur Ausführung von Ver- und Entschlüsselungsfunktionen wird als Falltür- oder Einweg-Funktion bezeichnet. Dies bedeutet, dass der öffentliche Schlüssel zwar zur Verschlüsselung der Nachricht verwendet wird, dass er aber später nicht zur Entschlüsselung derselben Nachricht benutzt werden kann. Ohne den privaten Schlüssel ist es praktisch unmöglich, diese Funktion umzukehren, wenn hierzu moderne und hochsichere kryptographische Algorithmen benutzt wurden.

Certification Authority / Zertifizierungsstelle
Eine CA (Certificate Authority) ist ein Unternehmen (wie z.B. thawte), das Sicherheitszeugnisse und öffentliche Schlüssel zum Zweck der Nachrichtenverschlüsselung ausstellt und verwaltet.

Certificate Signing Request (CSR)
Ein CSR ist ein öffentlicher Schlüssel, der auf Ihrem Server generiert wird und der die computerspezifischen Informationen Ihres Web-Servers sowie Ihres Unternehmens bei Beantragung eines Zertifikats von *thawte* bestätigt.

Privater Schlüssel
Ein privater Schlüssel ist ein Nummerncode, mit dem verschlüsselte Nachrichten wieder entschlüsselt werden, die vorab mit einem eindeutigen, ihm entsprechenden öffentlichen Schlüssel verschlüsselt wurden. Die Unversehrtheit der Verschlüsselung hängt stets vom privaten Schlüssel ab, der geheim gehalten werden soll.

Öffentlicher Schlüssel
Ein öffentlicher Schlüssel ist ein Nummerncode, der die Verschlüsselung von an den Inhaber des entsprechenden eindeutigen privaten Schlüssels gesendeten Nachrichten ermöglicht. Der öffentliche Schlüssel kann frei in Umlauf gesetzt werden, ohne dabei die Verschlüsselung zu gefährden. Mit diesem Schlüssel werden die Effizienz und der praktische Umgang verschlüsselter Kommunikationen erhöht.

Symmetrische Kryptographie
Ein kryptographisches Verfahren, wobei ein und derselbe Schlüssel für sowohl die Verals auch die Entschlüsselung verwendet wird. Der große Nachteil dieses Verfahrens liegt jedoch im Sicherheitsrisiko, das bei der Verteilung des Schlüssels besteht, da die Schlüsseleigenschaften zwar sowohl dem Sender als auch dem Empfänger mitgeteilt werden müssen, jedoch nicht in die Hände Dritter fallen sollen.