Smart-NiC

Smart-NIC GmbH SSL Zertifikate

FÜR RESELLER

Ein optimaler Mix aus verschiedensten SSL Zertifikaten für jeden Einsatzzweck und mehrere Wege diese bequem zu verwalten...

thawte COMODO Creating Trust Online® GeoTrust® Symantec. Norton SECURED powered by VeriSign

SSL Zertifikate von Smart-NIC

SSL – was ist das?

SSL steht für „Secure Socket Layer". Das hilft aber auch nur bedingt weiter. Insofern möchte wir Sie in unserem SSL Produktblatt aufklären was genau ein SSL Zertifikat ist, was es macht, wie man es bekommt, welche Unterschiede es gibt und wo bzw. wie man es am besten einsetzen kann.

Grundsätzlich sei gesagt, dass SSL Zertifikate das Surfen im Internet sicherer machen. Jeder von uns besucht täglich verschiedenste Webseiten. Besucht man eine Webseite, findet zwischen dem eigenen Computer und der Webseite eine Kommunikation statt. Man spricht von einer „Client-Server" Kommunikation. Ist eine Webseite nicht durch SSL geschützt (Webseiten die durch SSL geschützt sind erkennt man am „s" beim https://) findet diese Kommunikation unverschlüsselt statt.

In den meisten Fällen ist das kein Problem da keine allzu sensiblen Daten ausgetauscht werden. Spätestens aber wenn man personenbezogene Daten angibt (z. B. Kreditkarten-Daten), sollte die Verbindung durch ein SSL Zertifikat gesichert sein.

Ein SSL Zertifikat verschlüsselt die Kommunikation zwischen unserem Computer und der Webseite.

SSL macht aber noch mehr. SSL identifiziert den Betreiber einer Webseite. Je nach Klasse (Validierung) des Zertifikats erhält man Informationen über den Betreiber und kann so sicher gehen, dass man auch auf der richtigen Webseite ist.

SSL Zertifikate schützen also auf zwei Arten:

- durch Verschlüsselung der Client ⇔ Server Kommunikation
- durch die Identifikation des Betreibers der Webseite

Wie komme ich an ein SSL Zertifikat?

Zunächst möchten wir die verschiedenen sich im Umlauf befindenden Begriffe erklären. Man spricht bei SSL Zertifikaten oft von „Klassen" oder der „Validierung".

Die Klassifizierung von SSL-Zertifikaten beschreibt das jeweilige Verfahren der Validierung und Authentifizierung. Die Klassen sind jedoch nicht standardisiert, sodass jede Zertifizierungsstelle selbst bestimmen kann, wie sie ihre Zertifikate klassifiziert.

Wir unterteilen die Zertifikate daher in die Bereiche „domainvalidiert (DV)", „organisationsvalidiert (OV)" und „erweitert validiert (EV)".

Made in Germany PREMIUM QUALITÄT

Unsere Technologiepartner:

Symantec - Deutschland
Wappenhalle
Konrad-Zuse-Platz 2-5
81829 München

www.symantec.de

Thawte - Südafrika
The Gateway
Century Lane
7441 Kapstadt

www.thawte.de

GeoTrust - USA
350 Ellis Street
Mountain View
CA 94043-2202

www.geotrust.com/de/

Comodo - England
Trafford Road , Salford
M5 3EQ Manchaster

www.comodo.com

RapidSSL - USA
350 Ellis Street
Mountain View
CA 94043-2202

www.rapidssl.com

Kontakt:

Smart-NIC GmbH
Agnes-Bernauer-Str. 151
80687 München · Germany

Tel. +49. 89. 41610756 - 2
smart@smart-nic.de
www.smart-ssl.eu

Die Informationen die in einem Zertifikat gespeichert sind, hängen also von der Art der Validierung ab.

Bei den „domainvalidierten (DV)" SSL Zertifikaten handelt es sich um die schwächste Form der Validierung. In der Regel reicht es aus, eine von der Zertifizierungsstelle verschickte E-Mail zu bestätigen. Ebenfalls möglich sind Validierungen via HTTP (Datei auf dem Server) und DNS (CNAME-Eintrag).

Bei „organisationsvalidierten (OV)" Zertifikaten geht die Identitätsprüfung einen Schritt weiter. Hier findet in der Regel eine Validierung via E-Mail und zusätzlich über öffentliche Einträge (z. B. Telefonbuch, Handelsregister, etc.) und/oder ein Telefonat statt.
Je nach Zertifikat müssen ggf. auch verschiedene Dokumente geliefert werden.

Bei „erweitert validierten (EV)" Zertifikaten wird zusätzlich zu den OV-Maßnahmen eine persönliche Prüfung des Antragsstellers durchgeführt. Dies geschieht in der Regel durch einen Anruf der Zertifizierungsstelle über eine öffentlich einsehbare Rufnummer.
Die EV Zertifikate stellen die höchste Form der Validierung dar und sind an der grünen Adresszeile im Browser erkennbar.

Nachdem Sie das für Ihren Verwendungszweck optimale Zertifikat gefunden haben, können Sie über unser Web-Interface bequem den Auftrag einleiten. Alles was Sie hierfür noch brauchen ist ein CSR – File welches Sie vom Hoster Ihres Vertrauens erhalten (oder selbst auf Ihrem Server generieren können).

Auf den nachfolgenden Seiten geben wir eine kleine Hilfestellung bei der Auswahl des optimalen Zertifikats.

Wie unterscheiden sich die SSL Zertifikate in Ihrer Leistung?

Abgesehen von der Validierung gibt es noch verschiedene andere Punkte in denen sich die Zertifikate der verschiedenen Hersteller unterscheiden:

Unterschiede gibt es
- bei der Versicherungs- bzw. Garantiesumme
- bei der Verschlüsselung
- bei der Browser – Kompatibilität
- bei den Zusatzfeatures
- im Preis

Die jeweilige ***Absicherung*** wird dann wirksam, wenn eine Zertifizierungsstelle ein Zertifikat ausgestellt hat, sich jedoch später herausstellt, daß der Zertifizierte nicht ordnungsgemäß validiert wurde und dessen Kunden, die dem Zertifikat vertraut haben, dadurch dass sie dem Zertifikat vertraut haben, Schaden genommen haben. Der Kunde erhält in diesem Fall das ihm verloren gegangene Geld bis zur maximalen Höhe der Absicherung ausgezahlt. Je nach Höhe der Absicherung kann das auch nur ein Teil seines Verlustes sein.

SSL-Glossar

SSL
Secure Sockets Layer, die alte Bezeichnung für Transport Layer Security, ein Netzwerkprotokoll zur sicheren Übertragung von Daten

Validierung
Die Validierung bezeichnet die Überprüfung der bei der Bestellung angegebenen Daten auf Richtigkeit. Durch zunehmende Intensität der Validierung entsteht ein höheres Sicherheitslevel.

Man unterscheidet zwischen domainvalidiert (DV), organisationsvalidiert (OV) und erweitert validiert (EV).

CSR
CSR steht für „Certificate Signing Request" und ist ein standardisiertes Format zum Anfordern eines digitalen Zertifikats (SSL). Das CSR enthält den öffentlichen Schlüssel eines Schlüsselpaares und muss von der Registrierungsstelle auf Authentizität geprüft werden.

SGC
Als Server-Gated Cryptography bezeichnet man eine spezielle Technik mit der es möglich ist, die Verschlüsselung alter Browser auf ein Niveau von min. 128 Bit (statt 40 Bit) anzuheben.

Kontakt:

Smart-NIC GmbH
Agnes-Bernauer-Str. 151
80687 München · Germany

Tel. +49. 89. 41610756 - 2
smart@smart-nic.de
www.smart-ssl.eu

Alle heute gängigen SSL Zertifikate haben eine Schlüssellänge von 2048 Bit und beherrschen eine ***Verschlüsselung*** von 128 bis 256 Bit.
Manche Zertifikate beherrschen sogar eine Verschlüsselung von 40 bis 256 Bit. Das spielt besonders bei veralteten Browsern eine Rolle, da diese oft nur eine 40 Bit Verschlüsselung beherrschen.

Einige wenige Zertifikate verfügen über die sogenannte „SGC" – Technik, welche es ermöglicht, bei alten Browsern ebenso eine Verschlüsselung bis zu 256 Bit zu erreichen. Zertifikate mit SGC Technik erreichen zudem die höchste ***Browser-Kompatibilität*** bei mobilen Geräten.

Neben der angesprochenen SGC (Server-Gated Cryptography) Technik bei einzelnen Zertifikaten verfügen vor allem Symantec (ehemals VeriSign) Zertifikate über verschiedene ***zusätzliche Features***. Dazu zählen:

- **tägliche Schwachstellenanalyse und Website-Malware-Scans**

  → Symantec führt einen täglichen Check der Webseite durch und benachrichtigt den Betreiber im Falle einer Infektion. Der Betreiber kann so frühzeitig vom Schadcode erfahren und diesen entfernen bevor die Webseite z. B. in Suchmaschinen gesperrt wird.
- **Seal-in-Search**

  → Man sieht direkt in den Google Suchergebnissen das die dahinterliegende Webseite durch ein Symantec Zertifikat geschützt ist. Dieses Feature erhöht die Klickraten.

Fast jedes Zertifikat berechtigt, ein sogenanntes „Site Seal" zu führen. Diese Siegel sollen dem Besucher auf dem ersten Blick zeigen, dass die Webseite mit SSL gesichert ist. Ebenso wie die grünen Adresszeilen, die bei EV – Zertifikaten enthalten sind.

Administration und Reselling leicht gemacht

Wir bieten Ihnen verschiedene Möglichkeiten der Administration und Integration in Ihre bestehenden Prozesse an.

Zunächst können Sie die Zertifikate bequem über unsere Weboberfläche verwalten. Diese geht Hand in Hand mit unserer Domain Verwaltung. Ein Interface für Domains & SSL Zertifikate.

Zudem ist es möglich, alle SSL Prozesse über unsere SOAP-API abzubilden. Eine vollständige Integration in Ihre bestehende Infrastruktur ist also mit überschaubarem Aufwand möglich.

WHMCS User können zudem unser SSL Modul nutzen um die Bestellung der Zertifikate im WHMCS über uns laufen zu lassen.

Beratung & Verkauf

Wir gehen mit Ihnen gerne Ihre Anforderungen durch und beraten Sie bei der Auswahl des richtigen Zertifikats.

Kontakt:

Smart-NIC GmbH
Agnes-Bernauer-Str. 151
80687 München · Germany

Tel. +49. 89. 41610756 - 2
smart@smart-nic.de
www.smart-ssl.eu

Smart-NiC

SSL – Konditionen

Domainvalidierte (DV) Einzelzertifikate	
COMODO Positive SSL	11,80 USD
Thawte SSL123	30,00 USD
RapidSSL	20,00 USD
GeoTrust QuickSSL Premium	34,00 USD

Domainvalidierte (DV) Wildcardzertifikate	
COMODO Login SSL Wildcard	139,00 USD
RapidSSL Wildcard	149,00 USD

Organisationsvalidierte (OV) Einzelzertifikate	
COMODO Instant SSL	43,00 USD
Thawte SSL Webserver	76,00 USD
Thawte SGC SuperCerts	123,00 USD
GeoTrust True BusinessID	80,00 USD
VeriSign SecureSite	299,00 USD

Organisationsvalidierte (OV) Wildcardzertifikate	
COMODO Wildcard SSL	185,00 USD
Thawte SSL Webserver Wildcard	306,00 USD
GeoTrust True BusinessID Wildcard	349,00 USD

Extended Validation (EV) Einzelzertifikate	
COMODO EV SSL	155,00 USD
GeoTrust True BusinessID EV	175,00 USD
VeriSign SecureSite EV	755,00 USD

1.) Alle Preise verstehen sich als Jahrespreise zzgl. der gesetzl. MwSt. Preise für längere Laufzeiten sind auf Anfrage erhältlich.

2.) Weitere Zertifikate (z. B. Mulit-Domain, Unified Communication, etc.) sind auf Anfrage erhältlich.

thawte COMODO Creating Trust Online GeoTrust Symantec Norton SECURED powered by VeriSign

Welches ist das richtige Zertifikat?

Es gibt verschiedenste Kriterien anhand dieser man das optimale Zertifikat auswählen kann. Unsere groben Empfehlungen sehen wie folgt aus:

Geht es um einen Login-Bereich (wie z. B. ein Kundencenter), empfehlen wir unser **Comodo Login SSL**. Es handelt sich um die einfachste Art der Validierung (DV) und ist dementsprechend günstig. Ein weiterer Vorteil des „Login SSL" ist, dass die Subdomain „www." automatisch mit abgesichert ist, wenn man für die reine Domain ein Zertifikat ausstellt. Also zwei zum Preis von einem .

Geht es darum personenbezogene Daten oder gar Zahlungen abzusichern, sollte mindestens ein OV Zertifikat verwendet werden. Wir empfehlen unser **Comodo Corporate SSL**. Bei OV Zertifikaten von Comodo kann die telefonische Validierung in deutsch durchgeführt werden, was die Ausstellung oft enorm erleichtert.

Je nach Besucherzahl & Umsatz sollten Sie sogar ein EV Zertifikat verwenden. Wir empfehlen hier das **GeoTrust True BusinessID EV**. Ein EV Zertifikat zeigt auf den ersten Blick (durch die bekannte grüne Adresszeile) das die Seite gesichert ist und der Shop-Betreiber Wert auf Datensicherheit legt.

Geht es darum mehrere Subdomains abzusichern, können Sie mehrere Einzelzertifikate oder ein Wildcard Zertifikat verwenden. Wir empfehlen unser **Comodo Wildcard SSL** Zertifikat. Es handelt sich dabei um ein OV Zertifikat mit SGC Technik.

Für Anwendungen die speziell auf mobilen Endgeräten (Smartphone oder Tablet) laufen, empfehlen wir das **Thawte SGC SuperCert**. Durch die angewandte SGC Technik kann nicht nur die höchste Browserunterstützung auf mobilen Geräten erzielt werden, auch veraltete Browser erreichen dadurch eine maximale Absicherung (128- bis 256-Bit statt 40-Bit Verschlüsselung).

Den höchsten Bekanntheitsgrad haben die Zertifikate von Symantec (ehemals VeriSign). Das **Symantec SecureSite (Pro)** ist als OV oder EV erhältlich, bringt sowohl die SGC – Technik mit als auch weitere Features wie einen täglichen Malware-Scan der Webseite oder Seal-In-Search Technologie. Durch den hohen Bekanntheitsgrad haben die Internetnutzer vlt. auch das höchste Vertrauen in die Zertifikate von Symantec. Aber: Symantec SSL Zertifikate haben einen stolzen Preis.

Wenn es um das Thema SSL bzw. im speziellen IT-Security geht, halten wir uns immer an dieses Zitat:

Es ist unklug, zu viel zu bezahlen, aber es ist noch schlechter, zu wenig zu bezahlen. Wenn Sie zu viel bezahlen, verlieren Sie etwas Geld, das ist alles. Wenn Sie dagegen zu wenig bezahlen, verlieren Sie manchmal alles, da der gekaufte Gegenstand die ihm zugedachte Aufgabe nicht erfüllen kann.

John Ruskin (1819-1900)

Validierung der Zertifikate – auf was muss ich achten?

Vor der Bestellung

Es muss klar sein welches Zertifikat Sie benötigen. Dabei kann unsere Empfehlung auf der vorherigen Seite helfen oder aber Sie können sich persönlich an uns wenden. Wir sprechen dann eine Empfehlung aus und helfen so bei der Auswahl.

Zudem müssen Sie wissen, welche Software (z. B. Apache) auf dem Server läuft, auf dem das SSL Zertifikat eingebunden werden soll. Ihr Server-Administrator kann Ihnen hier weiterhelfen.

Das „CSR" muss vollständig vorhanden sein. Ebenso die vollständigen Kontaktdaten des Zertifikatinhabers. Diese Daten werden bei uns in Form eines „Handles" gespeichert, welches dann bei der Bestellung verwendet wird.

Zum Schluss spielt noch die Laufzeit eine Rolle für die das Zertifikat ausgestellt werden soll. Das spielt bei größeren/teureren Zertifikaten unter Umständen eine Rolle. Klären Sie also die anfallenden Kosten vorher intern ab.

Nach der Bestellung und vor der Ausstellung – die Validierung

Man muss unterscheiden zwischen „Domainvalidierung", „Organisationsvalidierung" und „Erweiterter Validierung". Wir haben unsere SSL Zertifikate für Sie in diese Gruppen aufgeteilt.

Bei *domainvalidierten Zertifikaten* geht eine E-Mail an den Zertifikatsinhaber. Diese E-Mail enthält in der Regel einen Code der an anderer Stelle eingegeben werden muss. Nachdem das geschehen ist wird das Zertifikat ausgestellt. Der Ganze Vorgang von Bestellung über Validierung bis Ausstellung kann innerhalb von Minuten abgeschlossen werden.

Bei *organisationsvalidierten Zertifikaten* muss man bei der Bestellung ein Dokument beilegen das einen Nachweis über die Geschäftstätigkeit des Unternehmens erbringt. Das kann die Gewerbeanmeldung, ein Handelsregisterauszug oder auch die Markenanmeldung sein. Wichtig ist, dass das Dokument möglichst aktuell ist. Zudem erfolgt ein Anruf durch die Zertifizierungsstelle bei der Person die als Ansprechpartner aufgeführt ist. Bei diesem Anruf werden ein paar Fragen gestellt. Danach ist die Validierung abgeschlossen und das Zertifikat wird ausgestellt. Diese Art der Validierung dauert in der Regel ein bis zwei Werktage.

Bei der *„erweiterten Validierung"* gehen die Prüfungen noch etwas weiter. So müssen neben der Domain- und Organisations-Validierung zusätzliche Dokumente unterzeichnet werden (z. B. das man als einziger berechtigt ist die Domain zu nutzen). Auch fällt die telefonische Validierung umfangreicher aus (z. B. Anruf in der Personalabteilung ob die zuständige Person auch im Unternehmen beschäftigt ist). Die erweiterte Validierung dauert in der Regel fünf bis sieben Werktage.

Jede Zertifizierungsstelle handhabt den Validierungsprozess etwas anders. So kann es z. B. sein das bei der Organisationsvalidierung auch eine E-Mail ähnlich der Domainvalidierung bestätigt werden muss.

SSL – FAQ (häufig gestellte Fragen)

Wie funktioniert die Verlängerung eines SSL Zertifikats?

SSL Zertifikate können verschiedene Laufzeiten haben. Je nach Anbieter gibt es Laufzeiten von 1 bis 5 Jahre. Nähert sich ein Zertifikat dem Ende der Laufzeit, erhalten Sie mit ausreichend Vorlauf entsprechende Benachrichtigungen (via E-Mail) von uns. Der Vorgang der Verlängerung ist identisch zu dem einer Neubestellung. Sofern sich zur vorhergehenden Ausstellung keine Daten geändert haben, ist ein erneuter Identitätsnachweis (bei OV und EV Zertifikaten) nicht erforderlich.

* Restlaufzeiten werden bei Zertifikaten des gleichen Typs automatisch übernommen

Kann man ein Zertifikat von Provider A zu Provider B „transferieren"?

Ein Transfer, wie man ihn z. B. von Domains kennt, ist bei Zertifikaten nicht möglich. Wenn Sie den Provider wechseln wollen, müssen Sie beim künftigen Provider das SSL Zertifikat neu beantragen und ausstellen lassen. Um Kosten zu sparen empfehlen wir, das neue Zertifikat zum Ende der Laufzeit (mit ausreichend Vorlauf) beim neuen Provider zu beantragen und somit das bisherige Zertifikat beim alten Provider nicht zu „verlängern".

Was ist ein CSR und wie kann ich es erstellen?

Ein CSR (Certificate Signing Request) beinhaltet die Daten des Zertifikatsinhabers und die Webadresse in verschlüsselter Form sowie den öffentlichen Schlüssel. Das CSR sollte aus Sicherheitsgründen auf dem Server, auf dem das SSL später eingebunden wird, erstellt werden. Bei der Erstellung des CSR wird ein öffentlicher und ein privater Schlüssel erstellt. Der private Schlüssel befindet sich auf dem Server und sollte nicht veröffentlich werden, da dass Zertifikat im Prinzip diese Schlüssel verbindet und so sicher stellt, dass die Kommunikation mit der richtigen Stelle (Client – Server) stattfindet. Durch die im CSR enthaltenen Daten ist auch (bei OV und EV Zertifikaten) der Betreiber der Webseite ersichtlich (mit Klick auf das Zertifikat, Stichwort „Identifikation des Betreibers").

Bei der Erstellung des CSR ist in der Regel der Server-Betreiber behilflich.

Wie binde ich ein Zertifikat auf meiner Webseite ein?

Das SSL Zertifikat wird auf dem Server eingebunden, auf dem das Hosting der Webseite stattfindet. Kontaktieren Sie bitte Ihren Hosting-Support, dieser kann Ihnen am besten weiterhelfen.