Besser geht immer.

BURN A BIT

- SSL Verschlüsselung -

Notwendigkeiten, Hintergründe, Vorteile, Kosten

Sicherheit zum Festpreis.

Eine SSL Verschlüsselung bringt klare Vorteile

Sicherheit zuerst

Durch SSL verschlüsseln Sie die Verbindung zwischen Ihnen und den Besuchern Ihrer Webseite.

Sichtbare Seriosität

Mehr Erfolg für Ihre Website durch Vertrauen und deutlich sichtbare Seriosität.

Besseres Suchmaschinenranking

Google belohnt Sicherheit mit einem besseren Ranking Ihrer Seite.

burnabit macht das für Sie

Wir übernehmen die „Buchung“ und die Integration der SSL Zertifikate in Ihre Website.
Zum Festpreis (zzgl. SSL-Kosten).

Wer braucht eine SSL Verschlüsselung?

Alle gewerblichen Webseiten-Betreiber, denn

- es gilt eine **Pflicht für sichere Verbindungen** (SSL) **bei Verwendung von Kontaktformularen**.

Seit dem 01.01.2016 gilt weiterhin die Pflicht für eine SSL Verbindung zu Webseiten mit Kontaktformularen. Diese Pflicht gilt allgemein für deutsche Webseitenbetreiber, welche personenbezogenen Daten mittels ihrer Webseite erheben.

Gesetzliche Grundlage / juristischer Hintergrund:
Die Pflicht eines Webseitenbetreibers, der Diensteanbieter im Sinne des § 2 Nr. 1 Telemediengesetz (TMG) ist, im Rahmen der Verwendung von Kontaktformularen zur Übertragung von personenbezogenen Daten ein anerkanntes Verschlüsselungsverfahren zu implementieren, ergibt sich direkt nunmehr aus § 13 Abs. 7 TMG, welcher im Zuge des Inkrafttretens des IT-Sicherheitsgesetzes seit Sommer 2015 gilt.

[...]
(7) **Diensteanbieter haben**, **soweit** dies **technisch möglich** und **wirtschaftlich zumutbar** ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen **sicherzustellen, dass**

1. **kein unerlaubter Zugriff** auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und

2. diese
a) gegen Verletzungen des **Schutzes personenbezogener Daten** und
b) gegen **Störungen, auch soweit sie durch äußere Angriffe** bedingt sind,

gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die **Anwendung eines** als sicher anerkannten **Verschlüsselungsverfahrens**.
[...]

SSL Verschlüsselungen sind die richtige Wahl

SSL-Zertifikate sind für Ihre Webseite die richtige Wahl, wenn Sie:

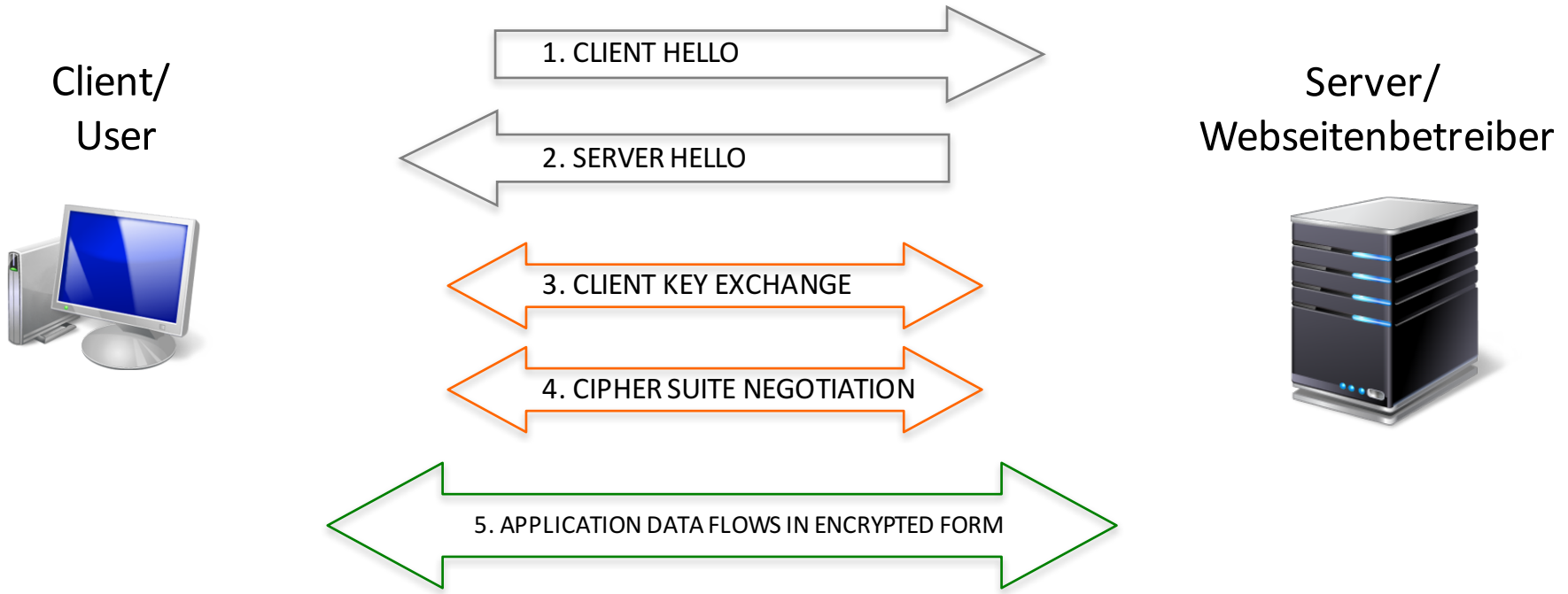
- ein **Kontaktformular** für Ihre Kunden zur Verfügung stellen
- einen Kunden- oder **Benutzer-Login-Bereich** auf Ihrer Webseite haben und persönliche Daten Ihrer Nutzer abfragen
- **Ihren eigenen Login-Bereich schützen** möchten, z.B. für den WordPress-Adminbereich
- einen Online-Shop haben oder Bezahlmöglichkeiten auf Ihrer Webseite anbieten

Das HTTPS-Protokoll ist ein seit langem verbreitetes Verschlüsselungsverfahren beim Transport von Daten im Internet. Insofern ist es auch **nicht** so **verwunderlich**, **dass dieses als „Stand der Technik" heute eingefordert wird**, wenn persönliche Daten übertragen werden.

Wir sind der Meinung: Daten, die über das Internet oder in einem Netzwerk versendet werden, sollen und müssen vertraulich bleiben.

Wie funktioniert eine SSL-Verschlüsselung?

Schematischer Ablauf des Verschlüsselungs-Prozesses

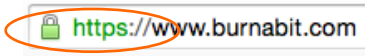


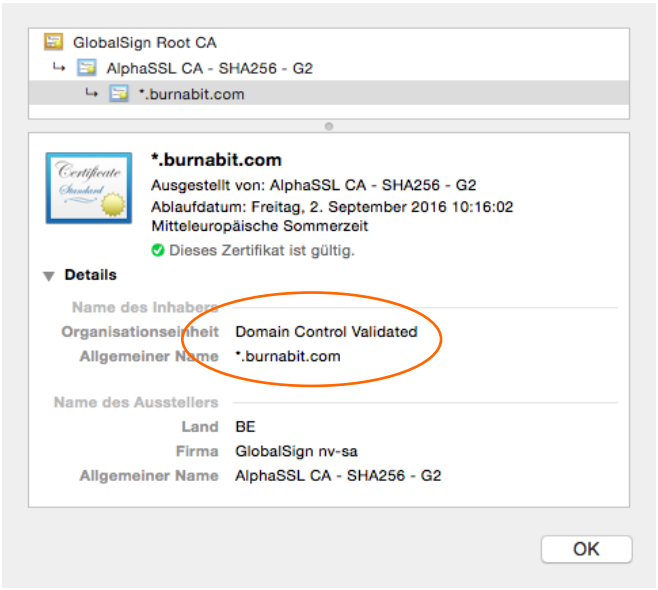
Mit SSL-Zertifikaten sichern Sie die Verbindung zwischen Ihnen und Ihren Besuchern. Sensible Informationen wie Login- oder Kontodaten werden verschlüsselt übertragen und so vor fremden Zugriffen geschützt, vergleichbar mit einem versiegelten Brief. Damit stärken Sie das Vertrauen in die Sicherheit Ihrer Webseite. Zudem wird der Webseitenbetreiber vor der Ausstellung eines SSL-Zertifikats durch die Zertifizierungsstelle überprüft. So können Nutzer sicher sein, dass sie auch tatsächlich auf Ihre Webseite zugreifen.

Das richtige Zertifikat für Sie (Auswahlschritt 1)

Domainvalidierte Zertifikate...

... garantieren, dass der Zertifikatsinhaber Zugriff auf die Domain hat.



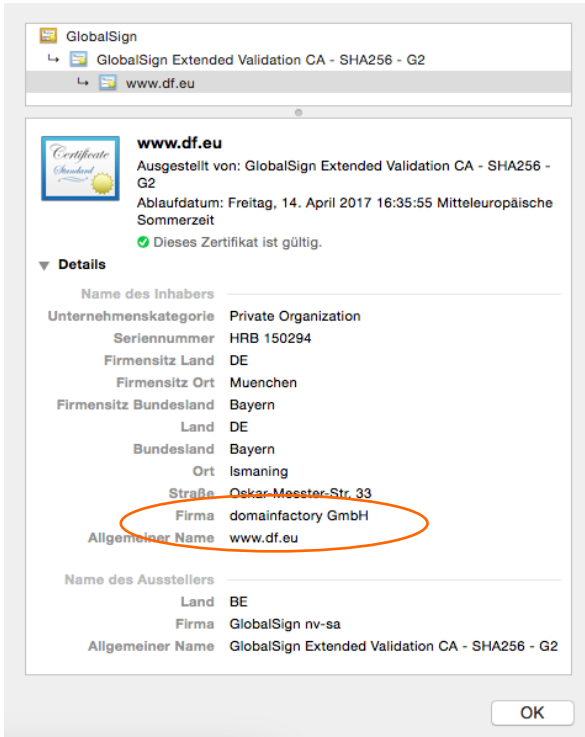


VS

Organisationsvalidierte Zertifikate...

... fordern einen Nachweis vom Domain-Inhaber, dass das Unternehmen existiert und die angegebene Adresse korrekt ist. Der Name des Inhabers wird in den Zertifikatsdetails aufgeführt und kann von Besuchern überprüft werden.

*Grüne Adressleiste im Browserfenster, nur in bestimmten Fällen des organisationsvalidiertem Zertifikat möglich (zB „Global Sign ExtendedSSL" bei df.eu) .



Das richtige Zertifikat für Sie (Auswahlschritt 2)

BURN A BIT

Wollen Sie ...

... eine einzelne Website schützen?

Einfache SSL-Zertifikate decken nur eine Domain ab.

VS

... eine Webseite mit allen Subdomains schützen?

Betreiben Sie weitere Subdomains unter dieser Domain, benötigen Sie ein **Wildcard SSL-Zertifikat** (*.meine-seite.de).

VS

... mehrere Webseiten schützen?

Für den Schutz unterschiedlicher Domains ist ein **Multidomain SSL-Zertifikat** vonnöten.

Oder Sie investieren in mehrere SSL-Zertifikate.

Da für burnabit-SV-Kunden ein besonders sicherer Deploy-Prozess im „technischen Hintergrund“ liegt (staging.meine-seite.de (=Entwicklungsumgebung) zu production.meine-seite.de (=Liveumgebung)**, empfehlen wir in der Regel den Schutz Ihrer Website mit allen Subdomains.**

Das richtige Zertifikat für Sie (Auswahl-Matrix)

Umfang des Schutzes / Prüfungsprozess	Schutz einer Website	Schutz einer Webseite mit allen Subdomains (wildcard SSL)	Schutz mehrerer Webseiten
Domainvalidiert	Günstigste, aber nicht die beste Version	burnabit Empfehlung	Macht Sinn, wenn mehr als fünf Domains „gesichert“ werden sollen.
Organisations-validiert	Modell „Kanonen-auf-Spatzen“, oder wer eben unbedingt seinen Namen in den Details des Zertifikats lesen möchte.	Modell „Kanonen-auf-Spatzen“, oder wer eben unbedingt seinen Namen in den Details des Zertifikats lesen möchte.	Macht Sinn, wenn mehr als fünf Domains „gesichert“ werden sollen.
Extended Organisations-validiert	Modell „Kanonen-auf-Spatzen“, aber die **einzige Möglichkeit an die „grüne Adresszeile im Browser“** zu kommen.	Nicht buchbar	Nicht buchbar

Kosten/ Unser Festpreis Angebot

BURN A BIT

Die Kosten setzen sich zusammen aus:

Laufenden Kosten (SSL Anbieter)

Zwar sind die Anbieter von SSL-Zertifikaten providerunabhängig. D.h. Sie können jeden Anbieter wählen, auch wenn dort nicht Ihre Website gehostet ist. Das klingt gut – es sollte aber die „Komplexitäts-Schraube“ im technischen Nachgang beachtet werden. Wir empfehlen daher das SSL-Zertifikat auch bei Ihrem Hosting Anbieter zu buchen.
Mit welchen Kosten an diesem Punkt zu rechnen ist, müssen wir bei Interesse direkt bei Ihrem Hosting-Anbieter für Sie anfragen/ recherchieren.

Kosten: Anbieterabhänig

Einmaligen Kosten für die Einrichtung (burnabit GmbH)

Wir besprechen mit Ihnen den „richtigen SSL-Weg“ als Entscheidungshilfe. Danach „buchen“ wir für Sie bei Ihrem Anbieter das entsprechende SSL-Zertifikat. Im Anschluss hieran hinterlegen wir das Zertifikat, und passen die url-Struktur in Ihrer Webapplikation an. Ebenfalls schauen wir ganz genau in Ihre Datenbank um alle „http“-Ausreisser zu finden. Wir prüfen für Sie alle Seiten, und geben am Ende für Sie „grünes Licht“ für den „grünen Browserbalken“ und einer deutlich verbesserte Website.

Kosten: Festpreis Euro 349,00*

*Die Anpassung der Verlinkungen, einschl. Upload Ihrer Sitemap(s) auf Google Webmaster Tools (Umstellung auf HTTPS) sind nicht inkludiert. Dies können Sie dem Paket für Euro 159,00 hinzu buchen.

Überzeugt? Und wie weiter?

1. Check Anforderung an Ihr Zertifikat
   Lassen Sie uns gemeinsam besprechen, welches Zertifikat für Ihre Anwendung das Geeignete ist.

2. Check Angebot „SSL Anbieter“
   Wir recherchieren für Sie welche Kosten, für das Zertifikat bei Ihrem Hosting Anbieter entstehen (bspw. Anbieter DomainFactory ab 9,99 Euro/ Monat, Stand 07/2016).

3. Auftrags-Freigabe
   Nach Ihrer Freigabe unseres Angebotes und der Kosten für das Zertifikat legen wir los.

4. Umstellung auf SSL
   Innerhalb der nächsten Arbeitswoche (nach Freigabe) wird Ihre Website im neuen „verschlüsseltem Glanz“ erscheinen. Google wird es Ihnen mit verbesserten Ergebnissen ebenfalls belohnen.