ok-webhosting, Markus Clemenz
Krähwinkelweg 23
71229 Leonberg

Telefon +49 (0)7152 - 401 82 52
Telefax +49 (0)7152 – 401 82 53
E-Mail Kontakt@ok-webhosting.de
Web www.ok-webhosting.de

Ust-IdNr. DE 251821832

Secure Socket Layer (SSL) - Zertifikate

Einführung

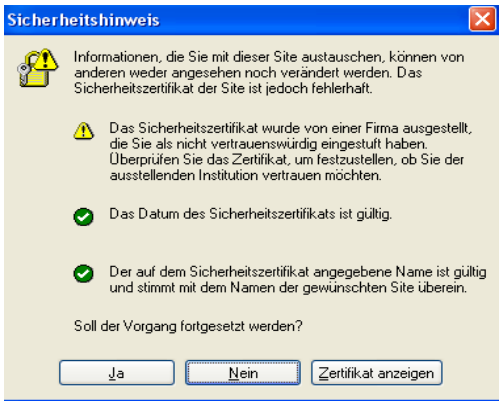
Zur Übertragung sensibler Daten über das Internet wurde das SSL-Protokoll entwickelt.
SSL steht für **S**ecure **S**ocket **L**ayer (dt. "sichere Sockelschicht") das von der Firma Netscape und RSA Data Security entwickelt wurde. Hierbei gewährleistet das SSL-Protokoll, dass **Daten während der Übertragung nicht gelesen oder manipuliert** werden können und stellt die Identität einer Internetseite sicher.

Neben dem Netscape Navigator unterstützten die meisten anderen verbreiteten Browser, wie der Internet Explorer von Microsoft, Firefox, Mozilla, Opera und weitere, Secure Socket Layer.

Das SSL-Protokoll wird dadurch initiiert, dass dem bekannten http ein s (=secure, dt. sicher) in der URL der Verbindung angehängt wird. Dann lautet die Internetadresse, wie Sie es zum Beispiel beim Login in unser Confixx-System beobachten können, https://secure.ok-webhost10.de

Bei jedem Aufruf einer https-Seite, prüft Ihr Browser hierbei, ob der Anbieter der Internetseite ein gültiges SSL-Zertifikat hat. Hat er das nicht, dann warnt Sie Ihr Browser mit einer Nachricht:

"*Diese Website kann leider nicht als sicher verifiziert werden. Wollen Sie wirklich weitermachen?*"



Beispiel Sicherheitshinweis

Bei einer solchen Warnung Ihres Browsers sollten Sie sich in jeden Fall überlegen, ob Sie auf den Seiten dieses Anbieters weiter surfen wollen, da dessen Zertifikat entweder unbekannt oder abgelaufen ist.

ok-webhosting, Markus Clemenz
Krähwinkelweg 23
71229 Leonberg

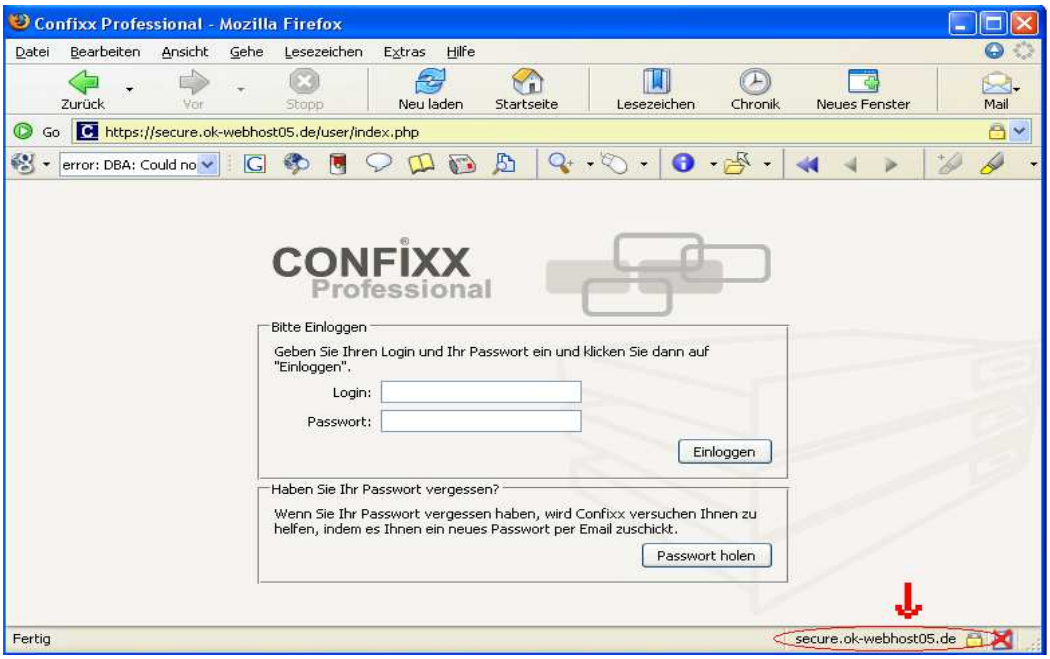
Telefon +49 (0)7152 - 401 82 52
Telefax +49 (0)7152 – 401 82 53
E-Mail Kontakt@ok-webhosting.de
Web www.ok-webhosting.de

Ust-IdNr. DE 251821832

Wie funktioniert SSL?

Am "https" erkennt Ihr Browser, dass er vom angesprochenen Server ein Zertifikat anfordern soll. Damit der Server dem Browser ein Zertifikat überhaupt zurückschicken kann, muss er sein Zertifikat von der Zertifizierungsstelle erhalten. Anschließend meldet der Server dieses Zertifikat direkt an den Browser zurück. Der Browser erhält dann vom Verzeichnisdienst der Zertifizierungsstelle die Information, ob das Zertifikat noch gültig ist. Anhand dieser übermittelten Daten kann der Browser nun überprüfen, ob er wirklich mit dem Server verbunden ist, der in der URL angegeben ist. Ist das der Fall, gibt Ihnen Ihr Browser eine entsprechende Information.

Beim Internet Explorer und anderen erkennen Sie das am geschlossenen Bügelschloss, das meist unten rechts in Ihrer Browserleiste zu sehen ist. Beim Netscape Navigator/Communicator wird eine sichere Seite durch den intakten Schlüssel signalisiert!



Beispiel verschlüsselte Übertragung

ok-webhosting, Markus Clemenz
Krähwinkelweg 23
71229 Leonberg

Telefon +49 (0)7152 - 401 82 52
Telefax +49 (0)7152 – 401 82 53
E-Mail Kontakt@ok-webhosting.de
Web www.ok-webhosting.de

Ust-IdNr. DE 251821832

Anschließend verständigen sich die beiden Rechner auf einen symmetrischen Schlüssel. Diese Verständigung passiert in der sicheren asymmetrischen Verschlüsselung. Um wirklich auf Nummer sicher zu gehen, schickt Ihr Browser dem Server vor dem Beginn des eigentlichen Datenaustausches einige Testnachrichten. Diese kann der Server nur beantworten, wenn es wirklich der Server ist, der er zu sein vorgibt.

Betrachtet man noch einmal die drei Ziele der Verschlüsselung: bewirkt das SSL-Protokoll damit eine sichere Verbindung:

1. Ihre Daten sind **vertraulich**, weil der Inhalt Ihrer Nachrichten nur verschlüsselt über das Netz geht.
2. Die **Authentizität** des Servers steht fest.
3. Ihre Daten sind vor **Manipulation geschützt**, da wirkungsvolle Algorithmen prüfen, ob die Daten vollständig und unverändert ihren jeweiligen Empfänger erreichen.

Inzwischen hat sich SSL als Standard für die Browser-Verschlüsselung etabliert.

Wer benötigt SSL?

SSL wurde zur Übertragung sensibler Daten wie Sie zum Beispiel bei Bestellungen anfallen (Personalien, Anschrift, Bankverbindung, Kreditkartendaten usw.) entwickelt.

Ihre Kunden erwarten einen entsprechend gebührenden Umgang mit diesen sensiblen Daten. den Sie unter Anderem durch den Einsatz des SSL-Protokolls dokumentieren.

Dadurch bauen Sie gegenüber Ihren KundenVertrauen auf und signalisieren Seriosität!

ok-webhosting, Markus Clemenz
Krähwinkelweg 23
71229 Leonberg

Telefon +49 (0)7152 - 401 82 52
Telefax +49 (0)7152 – 401 82 53
E-Mail Kontakt@ok-webhosting.de
Web www.ok-webhosting.de

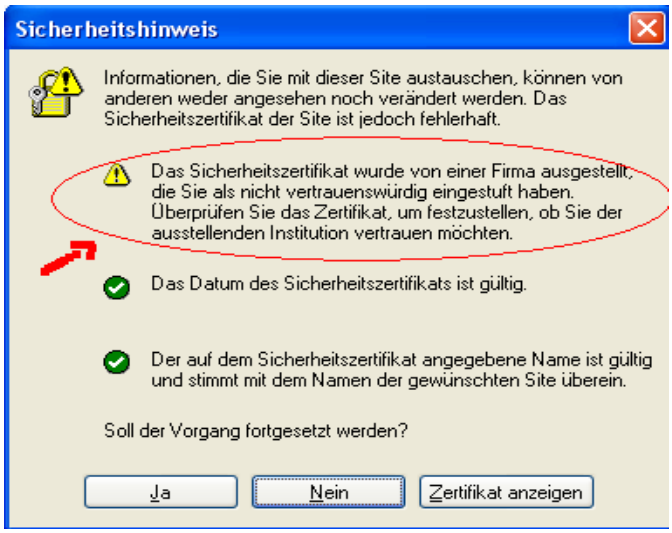
Ust-IdNr. DE 251821832

Unsere Lösungen/Unterscheidungen:

Wir bieten Ihnen im Bereich SSL ab sofort 3 Produktlinien an.

Sehr wichtig hierbei:

Viele Zertifikate werden vom Browser von Haus aus nicht unterstützt, da Sie schlichtweg keine weite Verbreitung finden bzw. nicht unbedingt als vertrauenswürdig anerkannt sind. Hier erhält Ihr Kunde beim Aufruf der SSL-Verschlüsselten Seite zunächst einen entsprechenden Hinweis.



Beispiel für ein nicht unterstütztes Zertifikat

Der Hinweis deutet daraufhin, dass der Browser ein verwendetes Zertifikat nicht von Haus aus als vertrauenswürdig einstuft, sondern diesbezüglich zumindest eine Bestätigung durch den Kunden voraussetzt, ob dieser diesem Zertifikat auch tatsächlich vertrauen möchte. Dies führt beim Kunden leider all zu oft zu Unsicherheiten.

Die durch ok-webhosting zum Einsatz kommenden Zertifikate finden in den gängigsten Browser vollständige Unterstützung wodurch Ihr Kunde in der Regel nicht mit der o.g. Frage kompromittiert wird.

ok-webhosting, Markus Clemenz
Krähwinkelweg 23
71229 Leonberg

Telefon +49 (0)7152 - 401 82 52
Telefax +49 (0)7152 – 401 82 53
E-Mail Kontakt@ok-webhosting.de
Web www.ok-webhosting.de

Ust-IdNr. DE 251821832

Bitte entnehmen Sie der beiliegenden Übersicht ab welcher Browserversion unsere eingesetzten Zertifikate entsprechend von vornherein als Vertrauenswürdig erkannt werden. Ihr Kunde wird bei Nutzung eines entsprechenden Browsers übergangslos auf die verschlüsselten Seiten gelangen.

Die Unterschiede der Produktlinien:

SSL-Self

Sie nutzen hierbei die **kostenlosen X.509-Zertifikate Let's Encrypt der Internet Security Research Group**.

Wir stellen Ihnen innerhalb der Administrationsoberfläche LiveConfig lediglich ein entsprechendes Modul zur Verfügung mit welchem Sie die Zertifikate des o.g. Anbieters weitestgehend automatisiert verwalten können (Erstellung, Validierung, Einrichtung und Erneuerung der Zertifikate). Die Zertifikate nutzen hierbei Server Name Indication (SNI), die es ermöglicht, dass sich mehrere verschlüsselt abrufbare Websites unterschiedlicher Domains eine IP-Adresse teilen.

Die durch die Internet Research Group augestellten Let's Encrypt Zertifikate sind „**Domain Control Validated**“ und geben daher die entsprechende Domain wieder, nicht die Organisation (Firma).

Die Zertifikate weißen eine **Gültigkeit von jeweils 90 Tagen** auf und sollten daher entsprechend rechtzeitig automatisiert oder manuell verlängert werden.

Weitere Informationen finden sich auch unter https://de.wikipedia.org/wiki/Let%E2%80%99s_Encrypt

SSL-Self ist **im Profi-Paket bereits inkludiert** und erlaubt Ihnen die **Nutzung von SSL-Zertifikaten für alle über ok-webhosting verwaltete Domains** innerhalb Ihres Accounts.

SSL-Starter

Es kommt hierbei ein Domain-Validiertes Zertifikat der **Ausstellenden CA COMODO** zum Einsatz. erlaubt. Dieses Zertifikat weißt eine **Gültigkeit von mindestens 12 Monaten** auf und wird **eigens für eine Domain ausgestellt** und ist ebenfalls „**Domain Control Validated**“.

ok-webhosting, Markus Clemenz
Krähwinkelweg 23
71229 Leonberg

Telefon +49 (0)7152 – 401 82 52
Telefax +49 (0)7152 – 401 82 53
E-Mail Kontakt@ok-webhosting.de
Web www.ok-webhosting.de

Ust-IdNr. DE 251821832

SSL-Profi

Hier kommt ebenfalls ein Zertifikat der Ausstellenden CA Comodo zum Einsatz. Das Zertifikat wird wie das SSL-Starter Zertifikat für **eine Ihrer Domains** ausgestellt und ist **für mindestens 12 Monate gültig**. Die Überprüfung zur Erlangung des Zertifikates ist nochmals deutlich gründlicher und erfordert den Nachweis Ihrer Identität durch entsprechende Dokumente. Hier wird das jeweilige Zertifikat nicht auf Ihre Domain, sondern auf Ihre Identität (Organisation) zertifiziert (**Identity Assured**).

Eine Übersicht/Zusammenfassung der entsprechenden Zertifikate sowie Angaben zu Preisen und Zahlungsmodalitäten finde Sie auf der Folgeseite.

Bei weiteren Fragen stehen wir Ihnen selbstverständlich jederzeit gerne zur Verfügung

Mit freundlichen Grüßen

ok-webhosting
Markus Clemenz

Anlagen: -1- Übersicht/Preise SSL-Zertifikate & Trustlogo

ok-webhosting, Markus Clemenz
Krähwinkelweg 23
71229 Leonberg

Telefon +49 (0)7152 – 401 82 52
Telefax +49 (0)7152 – 401 82 53
E-Mail Kontakt@ok-webhosting.de
Web www.ok-webhosting.de

Ust-IdNr. DE 251821832

Übersicht/Preisliste
SSL-Zertifikat & Trustlogo

Produkte	SSL-Self	SSL-Starter	SSL-Profi
Logo (Muster)	SiteSeal	SiteSeal	TrustLogo
Brückenzertifikat erfoderlich	Ja	Ja	Ja
Untersützte Browser ohne Fehlermeldung (Zertifikat wird vorgehalten)	ab 8.00 ab 1.0 ab 5.0 ab 8.0 ab 1.0 ab 1.0 ab 2.0	ab 5.01 ab 1.0 ab 5.0 ab 8.0 ab 1.0 ab 1.0 ab 1.0	ab 5.01 ab 1.0 ab 5.0 ab 8.0 ab 1.0 ab 1.0 ab 1.0
Ausstellende CA	Let's Encrypt	Comodo	Comodo
Produkt	Let's Encrypt	PositiveSSL	InstantSSL
Validierung	LiveConfig Modul	E-Mail-Robot	Dokumente
Zertifiziert	**Domain Control Validated** Domaininhaber	**Domain Control Validated** Domaininhaber	**Identity Assured** Identität
1 Jahr	24,-- EUR*	60,-- EUR*	99,-- EUR*
Wildcard	--	Auf Anfrage	Auf Anfrage

* zahlbar 1 Jahr im Voraus / Einrichtung nach Zahlungseingang
bei SSL-Self Einrichtung sofort/schnellstmöglich

Es gelten die allgemeinen Geschäftsbedingungen (AGB) der ok-webhosting

*** Preise enthalten die gesetzliche MwSt.**