

# Eine Sichere Verbindung – SSL-Zertifikate

## Verbindung verschlüsseln

Die Verbindung beispielsweise zu einer Website sollte verschlüsselt werden, wenn sensible Daten wie Telefonnummern, Anfragen oder Kontodaten übertragen werden.

Dazu wechselt die Website ihr Übertragungsprotokoll, von http:// auf https://.

Die Übertragung kann dann anders als bei einer unverschlüsselten Verbindung nicht mehr von den Systemen mitgelesen werden, die sich um den Transport der Daten kümmern.

## Mails verschlüsseln

Ein SSL-Zertifikat kann die verschlüsselte Übertragung zwischen dem eigenen Mailprogramm und dem Mailserver überprüfbar absichern.

## Der Website vertrauen

Woher weiß ich nun aber, dass ich wirklich die Website des Unternehmens sehe, dem ich meine Daten anvertrauen möchte?

Dazu verwendet man Zertifikate, die von anerkannten Zertifizierungsstellen ausgegeben und überwacht werden.

Die Zertifikate dieser Stellen werden vom Browser geprüft. und auf Klick angezeigt.

## Domainvalidiertes Zertifikat

Ein domainvalidiertes Zertifikat prüft, ob die Domain und die Server-IP zusammenpassen. Im Zertifikat enthalten sind neben der Domain die Zertifizierungsstelle und das Ablaufdatum.

## Unternehmensvalidiertes Zertifikat

Für ein unternehmensvalidiertes Zertifikat prüft der Zertifizierer darüber hinaus, ob der Inhaber der Domain mit dem Unternehmen, seiner Anschrift, seiner Telefonnummer und gegebenenfalls seiner Handelsregisternummer übereinstimmt.

Die Angaben werden über eine E-Mail, über eine Personalausweiskopie oder einen Handelsregisterauszug beziehungsweise Gewerbenachweis sowie über einen Telefonanruf überprüft.

Dazu muss die Telefonnummer im Telefonbuch oder in den Gelben Seiten stehen.

## Siegel verwenden

Wer ein Zertifikat auf seiner Website einsetzt, darf dies durch ein SSL-Siegel demonstrieren.



## Zertifikate aus der Schweiz

Im Zuge der Debatte um Edward Snowden und die NSA ist ein Problem deutlich geworden, das auch Zertifikate betreffen kann: Die NSA hat legal erheblichen Einfluss auf US-Unternehmen. Das reicht von der zwangsweisen, massenhaften Lieferung von Daten über das Mitschneiden von Datenströmen bis hin zur Manipulation von Zugriffen auf amerikanische Server. Die meisten Zertifizierer kommen aber aus den USA.

Wir bieten als Alternative ein Zertifikat des schweizer Anbieters



swissign. Die Schweiz ist ein vergleichsweise sicheres und autarkes Land. Ein Zugriff und eine Manipulation durch NSA, GCHQ, BND & Co wird dadurch zumindest erheblich erschwert.

## Was wir für Sie tun

Wir betreuen die Beantragung des Siegels.

Wir binden das Siegel technisch auf dem bei uns betriebenen Server in Ihre Website ein.

Wir aktualisieren das Siegel automatisch bei Ablauf neu, falls wir nichts Gegenteiliges hören.

## Was wir von Ihnen benötigen

Welchen Zertifikattyp möchten Sie verwenden?

Für welche Laufzeit?

Für welche Domain soll das Zertifikat gelten?

Auf wen wird das Zertifikat ausgestellt?

### Nur unternehmensvalidiertes Zertifikat:

Bei Privatpersonen benötigen wir eine Kopie beider Seiten des Personalausweises oder eine Meldebescheinigung.

Bei Unternehmen benötigen wir den Gewerbenachweis oder den Handelsregisterauszug.

Unter welchem Namen findet sich ein Eintrag im Telefonbuch oder in den gelben Seiten?

## Kosten

Zertifikate sind für eine Laufzeit ab einem Jahr buchbar. Die Abrechnung erfolgt jährlich vorab.

### Einrichtung

einmalig 35,00 EUR

### SSL-Zertifikat, domainvalidiert

Laufzeit		normal	Schweiz
1 Jahr	monatlich	13,00 EUR	20,00 EUR
2 Jahre	monatlich	12,50 EUR	19,00 EUR
3 Jahre	monatlich	12,00 EUR	18,00 EUR
4 Jahre	monatlich	11,50 EUR	
5 Jahre	monatlich	11,00 EUR	

### SSL-Zertifikat, unternehmensvalidiert

Laufzeit		normal	Schweiz
1 Jahr	monatlich	16,00 EUR	31,00 EUR
2 Jahre	monatlich	15,00 EUR	28,00 EUR
3 Jahre	monatlich	14,50 EUR	27,00 EUR
4 Jahre	monatlich	14,00 EUR	
5 Jahre	monatlich	13,50 EUR	

Alle Preise zuzüglich Mehrwertsteuer.