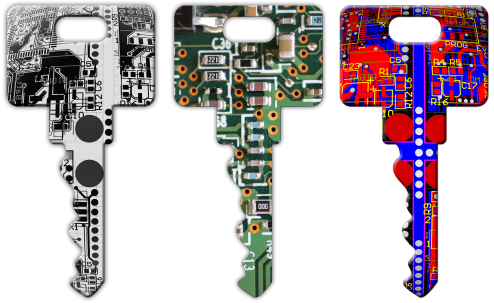
SSL Zertifikate



Grundsätzlich kann jede unverschlüsselte Datenübertragung im Internet abgefangen, mitgelesen oder gar manipuliert werden. Verfügt die Website über ein gültiges Sicherheitszertifikat, entsteht eine verschlüsselte Verbindung und die Datenübertragung wird „abhörsicher“. Insbesondere, wenn über eine Website sensible Daten abgefragt werden, zum Beispiel bei einem Webshop, sollte dies ausschließlich über verschlüsselte Seiten erfolgen. Spätestens seit Mai 2018 darf in der EU jede Art von personenbezogenen Daten nur noch verschlüsselt übertragen werden.

Für die Verschlüsselung der Datenübertragung beim Aufruf einer Website sorgt ein sogenanntes SSL-Zertifikat. SSL steht für „Secure Sockets Layer“ und ist eigentlich eine veraltete Bezeichnung. Denn die ursprüngliche SSL-Verschlüsselung wurde schon vor Jahren durch das TLS-Protokoll abgelöst. Im Sprachgebrauch ist aber die alte Bezeichnung der SSL-Zertifikate weiterhin offiziell bestehen geblieben. Selbst bei den Anbietern der Zertifikate findet man die Bezeichnung TLS erst auf den zweiten Blick. TLS steht für „Transport Layer Security“, wörtlich übersetzt „Transport-Ebenen-Sicherheit“. Tatsächlich kann man sich die Zertifikate wie „Transportebenen“ vorstellen, über die der Datenaustausch stattfindet.

Verfügt eine Website über ein gültiges SSL- bzw. TLS-Sicherheitszertifikat, wird dieses beim Aufruf der Seite an den Browser übermittelt. Dieser überprüft, ob das Zertifikat für diese Seite auch wirklich gültig ist. Ist dies der Fall, entsteht eine verschlüsselte Verbindung zwischen dem Server mit der Website und dem Rechner, der die Seite aufruft. Die Seite wird dem Besucher als sicher angezeigt.

SSL-Zertifikate unterscheiden sich voneinander in folgenden Punkten: Browser-Akzeptanz, Art der Validierung und der Anzahl der Domains, die sich mit einem Zertifikat schützen lassen. Generell gilt folgende Faustregel: Je weniger ein Zertifikat kostet, um so weniger Zeit steht für die Validierung zur Verfügung. Zertifikate mit einer zu einfachen Validierung werden schnell ausgestellt, bieten aber eine geringere Sicherheit. Daher werden diese Zertifikate nicht von jedem Browser akzeptiert. Besonders Browser von mobilen Geräten (wie iPad, iPhone, Android-Geräte usw.), zeigen eine Warnung beim Aufruf einer Website mit einem unsicherem Zertifikat an.

Unterschiedliche Arten

Mit SSL-Zertifikat enkann man nicht nur Webseiten, sondern auch die E-Mailkommunikation oder selbstentwickelte Softwares c

	hützen. Eine Übersicht erhalten Sie hier: https://www.telematica.at/hosting/ssl

Domain Validierung (DV) ist die einfachste Art ein SSL-Zertifikat auszustellen. Bei dieser Art der Validierung sendet die CA (Vergabestelle der Zertifikate) einen Aktivierungs-Link an eine EMail-Adresse, die nur dem Inhaber der Domain gehören kann (z.B. webmaster@domainname.tld). Der Inhaber der Domain kann dann der Ausstellung des Zertifikates über den Aktivierungslink zustimmen.

Deutlich sicherer ist die **Organisation Validierung (OV)**. Hier prüft die CA die Existenz des Zertifikat-Inhabers. Durch das Zertifikat wird die Identität Ihrer Firma bestätigt, nicht nur die Echtheit Ihrer Domain. Ihre Kunden sind durch einen Klick auf das Siegel oder Schloss in der Lage zu prüfen, dass Sie kein Opfer eines Phishingversuchs sind.

Die **erweiterte Validierung (EV)** bietet zur Zeit die sicherste Form der Validierung an. Diese Zertifikate werden nur nach einer strengen Prüfung durch die CA ausgestellt. Belohnt wird dieses mit einer grünen Adresszeile auf der Seite des Websitennutzers. Mit dieser deutlich sichtbaren Veränderung versichern Sie Ihren Kunden, dass Sie den Schutz ihrer Daten sehr Ernst nehmen. Zertifikate mit EV werden für den Austausch von streng vertraulichen Informationen genutzt, z.B. von Geldinstituten.

Wir von Telematica bieten unseren Kunden eine Vielzahl an Zertifikaten an. Weitere Informationen dazu finden Sie auf unserer Webseite https://www.telematica.at/hosting/ssl

Hier finden Sie Informationen dazu, wie Sie SSL-Zertifikate bei Ihrem System einrichten können:

- cPanel SSL Zertifikate
- HCP SSL Zertifikate