

SSL-ZERTIFIKATE

Leistungsbeschreibung, Stand 01.01.2021

Produktbeschreibung

SSL-Zertifikate von netclusive bieten höchste Sicherheit für die Internet- und Netzwerkkommunikation der Kunden. In Zusammenarbeit mit dem namhaften Internet-Security-Dienstleister Comodo stellt netclusive drei unterschiedliche Typen von SSL-Zertifikaten zur Auswahl. Je nach Sicherheitsbedarf und Anzahl der zu schützenden Domains gibt es drei unterschiedliche Verschlüsselungsangebote: Domain Validation (SSL Entry), Organization Validation (SSL Profi) und Extended Validation (SSL Extended). Alle Zertifikate können auf beliebigen Systemen eingebunden werden und sind nicht IP-gebunden. Mindestens 99,9% der weltweit verwendeten Browser akzeptieren die SSL-Zertifikate von netclusive, sodass höchste Kompatibilität und Sicherheit in der Übertragung sensibler Daten erreicht wird. SSL-Zertifikate gewährleisten:

- Integrität von Inhalten und den Schutz vor Manipulation
- Geheimhaltung übertragener Informationen und somit Unterbindung von Ausspähungen
- Geprüfte Identität des Anbieters und dadurch Schutz vor betrügerischen Identitäten

Funktionsweise

Sobald über einen Browser eine Website aufgerufen wird, die durch ein SSL-Zertifikat geschützt ist, wird zwischen Webserver und Browser ein verschlüsselter Kanal im Internet aufgebaut. Dazu prüft der Browser die Glaubwürdigkeit des Zertifikats einer Domain, bevor der Kanal aufgebaut wird und Daten ausgetauscht werden. Der öffentliche Schlüssel (Public Key) des Zertifikats ist für die Verschlüsselung der Daten zuständig, der private Schlüssel (Private Key) entschlüsselt Daten. Die Verschlüsselungsstärke ist von diversen Parametern abhängig, z. B. dem Zertifikat, dem Browser sowie dem Betriebs- und Hostsystem.

Das SSL-Zertifikat fungiert als gesicherter Nachweis der wahren Identität einer Domain, da die Herkunft von einer unabhängigen Zertifizierungsstelle überprüft ist. Details zum Zertifikat können mit einem Klick auf das Vorhängeschloss in der Adressleiste des Browsers abgerufen werden und sind damit für jeden Nutzer einsehbar.

Zielgruppen

SSL-Zertifikate sind nicht mehr nur im E-Commerce wichtig. Jede Website, auf der persönliche Daten ausgetauscht werden, sollte durch ein Zertifikat geschützt sein. Das betrifft Bank- und Kreditkartendaten genauso wie Logins und Kontaktformulare. Ferner unterstützen sie eine sichere Kommunikation in E-Mail-/Webmailanwendungen und in Intranets/Extranets sowie bei Plattformen, die auf der Cloud oder einer Virtualisierung aufbauen. Nicht zuletzt bedeutet eine SSL-verschlüsselte Seite auch ein besseres Abschneiden in Suchergebnissen, da diese Seiten eine Bonus der Suchmaschinen erhalten.

Zertifikatstypen

Zwar nutzen alle Zertifikatstypen (SSL Entry, SSL Profi und SSL Extended) die gleiche Methode, um übertragene Daten zu sichern und zu verifizieren, dennoch unterscheiden sich die Typen in ihrem Sicherheitslevel. Aufgrund der unterschiedlichen Authentifizierungsmethoden unterscheiden sich die Typen auch in der Dauer, die ihre Ausstellung benötigt.

SSL Entry (Domain Validation)

Das Einsteiger-Zertifikat von netclusive ist die einfachste Art der Validierung. Mit diesem Zertifikat wird lediglich bestätigt, dass die Domain registriert ist und von derjenigen Organisation verwaltet und kontrolliert wird, die die Zertifizierungsanfrage gestellt hat. Die Ausstellung des Zertifikats SSL Entry beansprucht vergleichsweise wenig Zeit. Seiten, die mit dem Zertifikat SSL Entry versehen sind, zeigen ein Vorhängeschloss in der Adresszeile des Browsers an.

SSL Profi (Organization Validation)

Das Verfahren bei einem Zertifikat, das auf der Organization Validation beruht, ist etwas aufwendiger, bietet dafür aber auch mehr Vertrauenswürdigkeit. Vor der Ausstellung werden sowohl die Inhaberschaft der Domain als auch grundlegende Unternehmensdaten abgefragt und überprüft. Im Zertifikat selbst wird der Unternehmensname eingetragen, sodass Nutzer sich darauf verlassen können, dass die Website und das dahinterstehende Unternehmen vertrauenswürdig sind. Die Zertifizierung beansprucht mehr Zeit als bei SSL Entry.

SSL Extended (Extended Validation)

Zertifikate, die das höchste Maß an Sicherheit liefern, daher aber auch den größten Aufwand im Zertifizierungsverfahren verursachen. Um das Zertifikat SSL Extended ausstellen zu können, werden umfangreiche Angaben zum anfragenden Unternehmen (z. B. Rechtsform und Berechtigung des Antragstellers zur Anfrage) verlangt. Mit diesem Zertifikat ausgezeichnete Seiten aktivieren bei Aufruf das Vorhängeschloss, die grüne Adressleiste des Browsers und zeigen darin den Namen des Unternehmens, zu dem die Domain gehört. SSL Extended ist in allen Bereichen, in denen sensible Kundendaten abgefragt werden, unverzichtbar.

Preise und Varianten

	SSL Entry	SSL Profi	SSL Extended
Zertifikatsart			
Zertifizierungsstelle	Comodo	Comodo	Comodo
Zertifikat	PositiveSSL	InstantSSL PremiumSSL UnifiedCommunication	EV SSL
Validierung	Domain Validation (DV)	Organization Validation (OV)	Extended Validation (EV)
Einzel-Zertifikate (Single)	●	●	●
Wildcard	●	●	—
Multidomain	●	●	●
Multidomain-Wildcard	●	●	—
Eigenschaften			
Versicherungssumme	bis zu \$ 10.000	bis zu \$ 250.000	bis zu \$ 1.750.000
Logo	Comodo SiteSeal	Comodo Trust	Comodo Trust
Einzel-Zertifikate¹			
1 Jahr (netto/brutto)	19,00 / 22,61 €	65,00 / 77,35 €	225,00 / 267,75 €
Wildcard-Zertifikate¹			
1 Jahr (netto/brutto)	110,00 / 130,90 €	225,00 / 267,75 €	—
Multidomain-Zertifikate (für die ersten drei Domains)¹			
1 Jahr (netto/brutto)	60,00 / 71,40 €	145,00 / 172,55 €	260,00 / 309,40 €
Multidomain-Zertifikate (ab der vierten Domain)¹			
1 Jahr (netto/brutto)	25,00 / 29,75 €	60,00 / 71,40 €	100,00 / 119,00 €
Multidomain-Wildcard-Zertifikate (für die ersten drei Domains)¹			
1 Jahr (netto/brutto)	330,00 / 392,70 €	615,00 / 731,85 €	—
Multidomain-Wildcard-Zertifikate (ab der vierten Domain)¹			
1 Jahr (netto/brutto)	105,00 / 124,95 €	210,00 / 249,90 €	—

Einzel-Zertifikat: Eine beliebig gewählte Domain oder Subdomain wird verschlüsselt (domain.de beinhaltet immer auch www.domain.de). Die Domain kann während der Laufzeit nicht kostenfrei abgeändert werden.

Wildcard-Zertifikat: Alle Subdomains einer Hauptdomain werden verschlüsselt. Die Hauptdomain kann während der Laufzeit nicht kostenfrei abgeändert werden.

Multidomain-Zertifikat (auch SAN-Zertifikat genannt): Bis zu 100 verschiedene Domains oder Subdomains werden mit nur einem Zertifikat abgesichert (www.domain.de wird, entgegen der Regelung eines Einzel-Zertifikats, separat gezählt). Im Zertifikat sind standardmäßig bis zu drei Domains im Preis inklusive, weitere Domains können anschließend problemlos hinzugefügt werden.

¹ Bruttopreise verstehen sich inkl. Mehrwertsteuer.