Leistungsbeschreibung
htp Business SSL-Cert

1 Allgemeines

Der Leistungsumfang für das Produkt htp Net Business SSL-Cert bestimmt sich nach dieser Leistungsbeschreibung, sowie nach dem Auftragsformular und den Allgemeinen Geschäftsbedingungen der htp GmbH für die Erbringung von Telefon- und Internetdienstleistungen.

2 Leistungsmerkmale

htp stellt dem Kunden mit dieser Leistung ein SSL-Zertifikat bereit. Das Zertifikat wird von einer globalen, vertrauenswürdigen Zertifizierungsstelle (root-CA) im Format X.509 ausgestellt und ist an den Hostnamen bzw. die Domain des Kunden gebunden. Das Zertifikat dient dem Kunden der Nachweisbarkeit seiner Authentizität gegenüber Dritten. Das Zertifikat kann für die Kommunikation bei Webservern, Mailservern, VPN-Servern, etc. eingesetzt werden.

2.1 Zertifikatstypen

htp bietet die folgenden Zertifikatstypen mit den genannten Eigenschaften an. Der Typ wird vom Kunden mit Beauftragung festgelegt.

	SSL-Webserver	**SSL-Webserver mit EV**	**SSL Webserver Wildcard**
Authentifizierungsgrad der Zertifizierungsstelle	Volle Unternehmensvalidierung: • Domaininhaber wird bestätigt • Unternehmen wird validiert • Auftrag wird verifiziert	Höchste Unternehmensvalidierung: • Domaininhaber und ausschließliches Nutzungsrecht werden bestätigt • Unternehmen wird validiert • Auftrag und Kontaktperson werden verifiziert	Volle Unternehmensvalidierung: • Domaininhaber wird bestätigt • Unternehmen wird validiert • Auftrag wird verifiziert
Anwenderinformation für Webserver	• https-Prefix der URL • Browserspezifische Hinweise (z.B. Schloss-Symbol) • Zertifikatsansicht im Browser	• https-Prefix der URL • Browserspezifische Hinweise (z.B. Schloss-Symbol) • Zertifikatsansicht im Browser • Einfärbung der Browserleiste (browserabhängig) • CA und Inhaber werden in der Browserleiste angezeigt (browserabhängig)	• https-Prefix der URL • Browserspezifische Hinweise (z.B. Schloss-Symbol) • Zertifikatsansicht im Browser
Anzahl abzusichernder Subdomains / Hosts	1	1	beliebig unterhalb einer Domain
Minimale Verschlüsselung	40 Bit	128 Bit	40 Bit
Maximale Verschlüsselung	256 Bit	256 Bit	256 Bit
Validierung	per Telefon	per Telefon	per Telefon
IDN-Unterstützung	ja	ja	ja

2.2 Beauftragung

Die Beauftragung erfolgt schriftlich durch eine natürliche, zeichnungsberechtigte Person des Kunden. Der Kunde benennt mit Beauftragung einen administrativen Kontakt (Admin-C) mit folgenden Parametern:

- Titel, Name, Vorname
- Organisation (Firma)
- Adresse geschäftlich (Straße, Hausnummer, Postleitzahl, Stadt, Bundesland, Staat)
- Telefon, Telefax, E-Mail-Adresse

Der administrative Kontakt wird von htp an die Zertifizierungsstelle gemeldet und seitens der Zertifizierungsstelle im Rahmen der Validierung kontaktiert.

htp benennt gegenüber der Zertifizierungsstelle einen technischen Kontakt (Tech-C), der bei technischen Fragen von der Zertifizierungsstelle kontaktiert werden kann.

Des Weiteren stellt der Kunde htp mit Beauftragung eine Kopie seines aktuellen Handelsregisterauszuges zur Verfügung.

Für die Beantragung gegenüber der Zertifizierungsstelle ist zwingend ein elektronischer CSR-Antrag („certificate signing request“) im Format PKCS#10 erforderlich. Dieses CSR kann auf Wunsch des Kunden von htp erstellt werden. Der Kunde benennt hierzu mit Beauftragung folgende Parameter:

- Staat (2-Buchstaben ISO-Code)
- Bundesland
- Stadt
- Firmenname (Dieser Name sollte exakt mit dem Domaininhaber identisch sein)
- Organisationseinheit/Abteilung (optional)
- Name des zu zertifizierenden Hosts (FQDN)
- Kontakt E-Mail Adresse

Zusammen mit dem CSR wird auch der private Schlüssel („private key“) generiert, der für die Installation auf den Server erforderlich ist. Der private Schlüssel ist sicher und vor Dritten unzugänglich aufzubewahren.

Alternativ kann der Kunde das CSR eigenständig erstellen und an htp senden. Der private Schlüssel kann dann beim Kunden verbleiben.

Sollte der Firmenname des Zertifikatsinhabers den Inhaberdaten der Domain nicht entsprechen, sorgt der Kunde dafür, dass seitens des Domaininhabers der Beantragung des SSL-Zertifikates mit einem „domain authorisation letter“ zugestimmt wird.

Der Kunde stellt auf Anforderung der Zertifizierungsstelle weitere erforderliche Dokumente bzw. Nachweise zur Verfügung.

2.3 Aushändigung

Das ausgestellte Zertifikat wird von der Zertifizierungsstelle an die hinterlegten Adressen des administrativen Kontaktes und des technischen Kontaktes per E-Mail übermittelt.

htp übermittelt dem Kunden auf Anfrage den privaten Schlüssel, sofern dieser mit dem CSR von htp erstellt wurde. Die Übermittlung des Schlüssels erfolgt per E-Mail an den administrativen Kontakt innerhalb eines mit einem Kennwort verschlüsselten ZIP-Archives. Das zugehörige Kennwort wird dem Kunden per E-Mail oder telefonisch gesondert übermittelt.

2.4 Laufzeit und Erneuerung

Die Mindestvertragslaufzeit für die Leistung htp Business SSL-Cert beträgt, sofern nicht anders vereinbart, 12 Monate. Der Vertrag verlängert sich automatisch um jeweils 12 Monate, soweit er nicht mit einer Frist von 3 Monaten zum jeweiligen Vertragsende gekündigt wird.

2.5 Zusätzliche Lizenzen

Das Zertifikat gilt für einen Server. Für die Installation des Zertifikates auf mehreren Servern mit gleichen FQDN (Beispiel: Serverfarm hinter einem Loadbalancer) werden zusätzliche kostenpflichtige Lizenzen benötigt. Der Kunde benennt bei Beauftragung die Anzahl von zusätzlich erforderlichen Lizenzen.