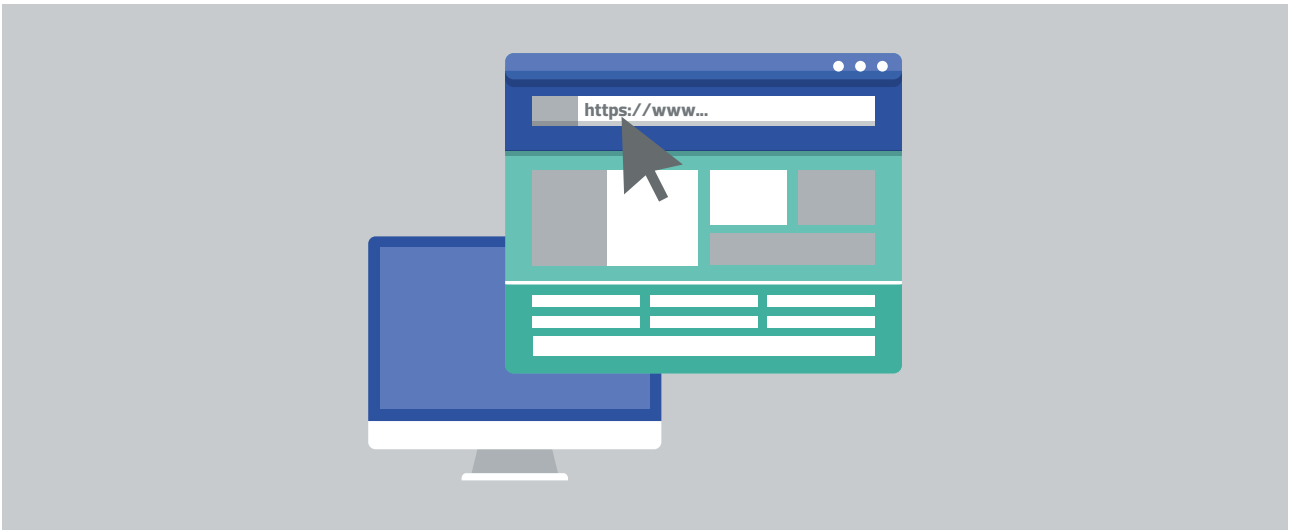




SSL-Zertifikate

Ihr vertrauenswürdiger Webauftritt



Ihre Vorteile

- 1** Made in Germany – Zertifikatsprodukte vom Trustcenter der Bundesdruckerei
- 2** Sicher – höchste Sicherheit durch Verwendung aktueller Signaturalgorithmen
- 3** Transparent – transparentes Lizenzmodell für alle SSL-Zertifikatstypen
- 4** Flexibel – kompatibel mit allen gängigen Browsern bzw. Betriebssystemen
- 5** Rechtssicher – Vertrauensdienstleistungen nach eIDAS
- 6** Verlässlich – Support durch das Call- und Supportcenter der Bundesdruckerei

Bankverbindungen, Passwörter oder andere persönliche Daten sind sensible Informationen.

Ihre Geschäftspartner erwarten, dass diese verlässlich und sicher übertragen werden. Als Betreiber von Web- oder Kommunikationsanwendungen sollten Sie deshalb jederzeit in der Lage sein, Ihre Identität und die Vertrauenswürdigkeit Ihrer Internetdomain eindeutig nachzuweisen.

Als Spezialist für sichere Identitäten unterstützt die Bundesdruckerei Unternehmen beim Nachweis eindeutiger Identitäten und bei der Gewährleistung hochsicherer Internetanwendungen durch SSL-Zertifikate. Ganz gleich, welche Anforderungen oder Verwendungszwecke Ihren Webauftritt auszeichnen: Von der SSL-Einstiegsversion bis zur Realisierung höchster Zertifikatsstandards bieten wir das gesamte Spektrum an. Nutzen Sie neueste Signaturalgorithmen und hochkomplexe Verschlüsselungsverfahren, um einen rundum vertrauenswürdigen „Proof of Identity“ zu gewährleisten und Ihre Kunden aktiv vor Scheinidentitäten oder Phishing-Attacken zu schützen.

Anwendungsszenarien

D-TRUST SSL-Zertifikate eignen sich:

- Für registrierte Organisationen und Behörden
- Für eCommerce-, eGovernment- und eBusiness-Anwendungen mit registrierten Domainnamen
- Zur Absicherung von Server-to-Server- oder Client-to-Server-Datenübertragungen im Inter-, Intra- oder Extranet auf Basis von HTTPS in Kombination mit SSL / TLS, zum Beispiel bei:
 - Websites mit Registrierungs- oder Log-in-Funktionalität
 - Zahlungsportalen, Warenkorbsoftware
 - POP, SMTP, IMAP etc.

Systemvoraussetzungen

D-TRUST SSL-Zertifikate können mit Server- und Client-Software verwendet werden, die:

- Den Einsatz von X.509v3-SSL / TLS-Zertifikaten vorsieht
- Gemäß aktueller Sicherheitsstandards die Verwendung von SSL-Zertifikaten mit Hash-Algorithmus SHA-256 unterstützt

Eigenschaften

D-TRUST SSL-Zertifikate umfassen:

- Mindestens 2.048 Bit Schlüssellänge
- Bis zu 256 Bit Verschlüsselungstiefe
- Vollen OCSP- und CRL-Support
- First- und Second-Level E-Mail- und Telefonsupport (Ortstarif)
- Zertifikatstypen (immer mit Prüfung der Organisation)
 - Organisation / Extended Validation (OV / EV)
 - Subject Alternative Names (OV SAN / UCC)
 - Wildcard-Option (OV)
 - Qualified Website Certificates (QWACS)
- Verbreitung der SSL-Root CAs ab:
 - Microsoft Internet Explorer 7
 - Google Chrome 27
 - Apple Safari 7
 - Mozilla Firefox 23
 - Opera 9.5
 - Apple OS X 10.8
 - Microsoft Windows XP SP3
 - Google Android 4.3
 - Apple iOS 7
 - Microsoft Windows Phone 7.5

FUNKTIONSWEISE VON SSL-ZERTIFIKATEN



Anwender

Anzeige im Webbrowser
des Nutzers über sichere
Datenverbindung



Hacker

Schutz vor Datenmanipulation,
Ausspähen, Phishing



Server SSL-gesichert

Eindeutige Identifizierung
von Anbietern im Internet