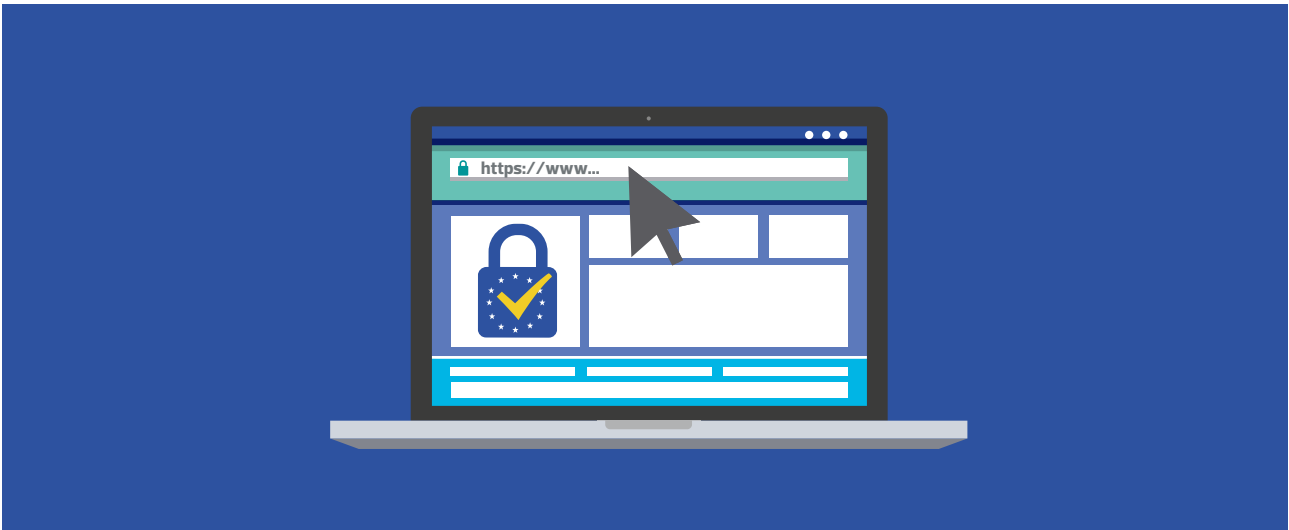




Qualifizierte Website-Zertifikate nach eIDAS

Höchstes Vertrauen für Ihren Webauftritt



Ihre Vorteile

- 1** Made in Germany – Zertifikatsprodukte vom Trustcenter der Bundesdruckerei
- 2** Höchste organisatorische Sicherheit – Zertifizierung durch BSI und TÜVIT
- 3** Flexibel – Kompatibilität mit allen gängigen Browsern bzw. Betriebssystemen
- 4** Rechtssicher – gemäß eIDAS-Verordnung und Vertrauensdienstegesetz
- 5** Höchste technische Sicherheit – Verwendung aktueller Signatur- und Verschlüsselungsalgorithmen

Konto-, Sozial-, und Gesundheitsdaten, Passwörter oder andere persönliche Informationen sind schützenswerte Daten.

Ihre Kunden vertrauen Ihnen, dass Sie sorgsam mit diesen umgehen und sie sicher übertragen werden. Mit Umsetzung der eIDAS-Verordnung wurde für SSL-/TLS-Zertifikate die Kategorie der qualifizierten Website-Zertifikate eingeführt. Die Zertifikate basieren technisch auf den Anforderungen für sogenannte „Extended-Validation-Zertifikate“, die durch die Vereinigung der Zertifizierungsstellen für SSL-/TLS-Zertifikate und der Browser-Hersteller (das sogenannte CA/B-Forum) festgelegt wurden. In Deutschland werden Anbieter durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach Vorgaben der „EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ (eIDAS) zertifiziert.

Die Bundesdruckerei stellt als erster Anbieter in der EU qualifizierte Website-Zertifikate gemäß eIDAS-Verordnung bereit. Die neuen Zertifikate ermöglichen die zuverlässige Authentifizierung einer Webseite. Sie geben dem User die Sicherheit, dass hinter einer Internetpräsenz eine echte und vertrauenswürdige Person oder Institution steht. Sowohl die Vorgaben des Vertrauensdienstegesetzes, des BSI, der eIDAS-Verordnung als auch des CA/Browserforums werden umgesetzt.

Anwendungsszenarien

Qualifizierte Website-Zertifikate der Bundesdruckerei eignen sich:

- Für Banken und FinTechs zur Erfüllung der EU-Zahlungsdienstrichtlinie PSD 2
- 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

Bundesdruckerei SSL-/TLS-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-/TLS-Zertifikaten mit Hash-Algorithmus SHA-256 unterstützt

Eigenschaften

Bundesdruckerei SSL-/TLS-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)
- Definierte Organisationsvalidierung:
 - Extended Validation (EV)
 - Subject Alternative Names (SAN/UCC)
- Verbreitung der SSL-/TLS-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



Server SSL-gesichert

Eindeutige Identifizierung
von Anbietern im Internet



Hacker

Schutz vor Datenmanipulation,
Ausspähen, Phishing