SSL certificates
Your trusted presence on the net

Advantages at a glance

1. Made in Germany – Certificate products from Bundesdruckerei’s trust service provider
2. Secure – Outstanding security thanks to the use of the latest signature algorithms
3. Transparent – A transparent license model for all SSL certificate types
4. Flexible – Compatible with all customary browsers and operating systems
5. Legally secure – Trust services according to eIDAS
6. Reliable – Support from Bundesdruckerei’s call and support centre

Bank accounts, passwords or other personal data are all sensitive information.
Your business partners expect this data to be transmitted in a reliable and secure manner. As an operator of web or communication applications, you should always be in a position to prove beyond doubt both your identity and the trustworthiness of your Internet domain.

Bundesdruckerei, an expert in Secure ID, can help you to provide unambiguous proof of your identity and to guarantee highly secure Internet applications using SSL certificates. Irrespective of the requirements or purpose of your website, we offer the entire range from the basic SSL version to the implementation of the highest certificate standards. Make use of the latest signature algorithms and highly complex encryption methods in order to warrant truly trustworthy proof of identity and to actively protect your customers against bogus identities or phishing attacks.
**Applications**

D-TRUST SSL certificates are suitable for:
- Registered organizations and public agencies
- eCommerce, eGovernment and eBusiness applications with registered domain names
- Securing server-to-server or client-to-server data transmissions on the Internet, intranet or extranet using HTTPS combined with SSL/TLS, for example, in the case of:
  - Websites with a registration or log-in function
  - Payment portals, shopping basket software
  - POP, SMTP, IMAP, etc.

**System requirements**

D-TRUST SSL certificates can be used with server and client software that:
- Supports the use of X.509v3 SSL/TLS certificates
- Supports the use of SSL/TLS certificates with hash algorithm SHA-256 according to the latest security standards

**Properties**

D-TRUST SSL certificates have:
- Key length of at least 2,048 bits
- Encryption depth of up to 256 bits
- Full OCSP and CRL support
- 1st and 2nd level e-mail- and telephone support (local rate)
- Certificate types (always with verification of the organization)
  - Organization/Extended Validation (EV)
  - Subject Alternative Names (OV SAN/UCC)
  - Wildcard option (OV)
  - Qualified Website Certificates (QWACs)
- Distribution of the SSL root CAs from:
  - 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

**HOW SSL CERTIFICATES WORK**

User

Display in the user’s web browser via a secure data connection

Hacker

Protection against data manipulation, eavesdropping, phishing

Server SSL secured

Unambiguous identification of providers on the Internet