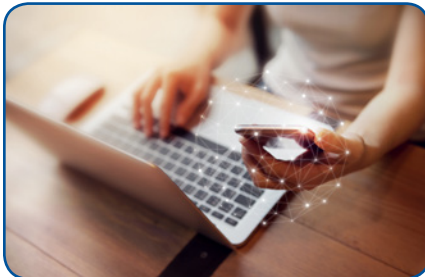


# TrustID® TLS/SSL Single Domain Certificate



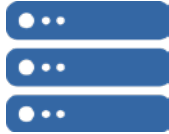
### Product Summary

TrustID TLS/SSL Single Domain Certificates establish an encrypted connection between a browser or user's computer and a server or website. This connection protects in transit, sensitive data from interception by non-authorized parties, allowing online transactions to be conducted with complete confidence.

TrustID TLS/SSL Single Domain Certificates are publicly trusted and are natively trusted in popular browsers. You will apply for a TLS/SSL certificate and act as the sponsor and manager of the certificate and server. This is a software certificate and is stored on the server to which it is issued.

<b>Identity Authentication Method:</b>	As the server sponsor, your affiliation with the sponsor is verified.
<b>Identity Proofing Requirements:</b>	Affiliation with the sponsoring organization and domain ownership
<b>Forms Packet Required:</b>	No - You are not required to submit a forms packet with your application
<b>CSR Submission:</b>	You will need to provide a Certificate Signing Request (CSR), also known as a PKCS#10. Visit our <a href="#">How to Generate a CSR</a> page if you need assistance.
<b>Trust Model:</b>	This certificate is publicly and natively trusted in browsers
<b>Type of Certificate:</b>	This is a standard X.509 (V3) 2048+ bit key length SSL/TLS with SHA-256 hashing algorithm certificate that it is issued to you and the server that you will manage. This certificate is for a single domain, (DV) and Organization validation (OV).
<b>Validity Periods:</b>	Available in one (1) year validity period
<b>Storage Type:</b>	Server certificate store
<b>Available to Non-U.S. Residents:</b>	Yes - This certificate is available to applicants in a limited number of foreign countries. View our <a href="#">Supported Countries</a> list.

### Specifications



- X.509 v3 digital certificates
- 2048+ bit key length
- SHA-245 hashing algorithm
- Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) validation
- Natively trusted in browsers
- Comply with the industry-standard requirements for the Certification Authority Browser Forum (CA/B Forum)
- Audited under the annual WebTrust for Certification Authority

### Browser Support



#### Interoperable with:

- Apple® Safari (for OSX and iOS)
- Blackberry®
- Google® Chrome (for Windows®, Apple® OSX and Android®)
- IBM®
- Microsoft® Internet Explorer and Edge
- Mozilla® Firefox (in Windows®, Apple® OSX and Linux® environments)
- Oracle® Java

### Certificate Usage



#### The main purpose of this certificate is for securing websites via:

- Data and Communications Encryption
- Server Authentication
- Client Authentication

### Other Resources



#### Related information:

- [TrustID FAQs](#)