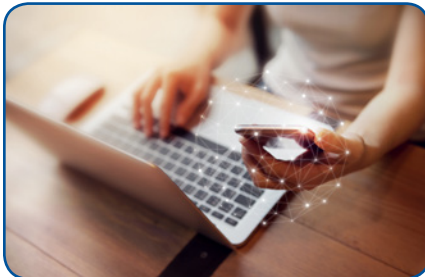


TrustID[®] TLS/SSL Multi-Domain Certificate



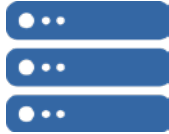
Product Summary

TrustID TLS/SSL Multi-Domain certificates secure your domain names (DV) and organization's (OV) identity by establishing 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. You can use this certificate to secure up to four (4) domains; however, up to 46 additional domains can be added to a multi-domain SSL/TLS certificate at an adjusted price.

TrustID TLS/SSL Multi-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(s). This is a software certificate and is stored on the server to which it is issued.

Identity Authentication Method:	As the server sponsor, your affiliation with the sponsor is verified.
Identity Proofing Requirements:	Affiliation with the sponsoring organization and domain ownership
Forms Packet Required:	No - You are not required to submit a forms packet with your application
CSR Submission:	You will need to provide a Certificate Signing Request (CSR), also known as a PKCS#10. Visit our How To Generate a CSR page if you need assistance.
Trust Model:	This certificate is publicly and natively trusted in browsers
Assurance Level	Affiliation with the sponsoring organization
Type of Certificate:	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 multiple domains, (DV) and Organization validation (OV).
Validity Periods:	Available in one (1) and two (2) year validity periods
Storage Type:	Server certificate store
Available to Non-U.S. Residents:	Yes- Yes, except in countries with US trade restrictions. View our TrustID approved foreign countries list .
Application Approval:	3-5 business days after Forms Packet submission

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 available at the following links:

- TrustID Forms, Agreements and Policies
- TrustID FAQs