DIGITAL CERTIFICATES

IdenTrust
part of HID Global

IdenTrust TLS/SSL Extended Validated (EV) Certificates

Product Summary

IdenTrust TLS/SSL EV certificates offer the highest level of assurance for server certificates. Besides domain validation (DV) and standard organization validation (OV) requirements, EV certificates verify additional details of the applying organization such as place of business, jurisdiction of incorporation, registration number and any other supplied information. The issued EV TLS/SSL certificate contains the organization name, the fully qualified domain name (FQDN) of each supplied domain - up to 50, the jurisdiction of incorporation - state when applicable and country, organization type, registration number, organization identifier - when supplied, and locality.

You will apply for an IdenTrust TLS/SSL Extended Validated (EV) 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 secures one or multiple domains, as Extended Validated (EV).
Validity Periods:	Available in one (1) year validity period.
Storage Type:	Server certificate store.
Available to Non-U.S. Residents:	Yes, except in countries with US trade restrictions. View our *Supported Countries* list.
Application Approval:	3-5 business days after 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

IdenTrust TLS/SSL certificates are publicly trusted and are natively trusted in most popular browsers. See *IdenTrust CA Compatibility* webpage for details.

Certificate Usage

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

- Data and Communications Encryption,
- Server Authentication.
- Client Authentication.

IdenTrust TLS/SSL certificates secure your domain names and organization's 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.

Other Resources

Related information available at the following links:

- *TrustID Forms, Agreements and Policies*
- *TrustID FAQs*

For IdenTrust Sales Inquiries: +1 (866) 763-3346 | sales@identrust.com