IdenTrust™
part of HID Global

DIGITAL CERTIFICATES

TrustID | IdenTrust TLS/SSL | Organization Identity | Extended Validated (EV) Certificate

Product Summary

TrustID | IdenTrust TLS/SSL | Organization Identity | Extended Validated (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 IdenTrust TLS/SSL | Organization Identity | Extended Validation 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 TrustID | IdenTrust TLS/SSL | Organization Identity | 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:	Proof of domain ownership and affiliation with sponsoring organization
CSR Submission:	You will need to provide a Certificate Signing Request (CSR), also known as PKCS#10. Visit our How to Generate a CSR page if you need assistance
Forms Packet Required:	Yes – You are required to submit a complete forms packet with your application
Trust Model:	This certificate is publicly and natively trusted in browsers
Assurance Level:	Organization Identity
Certificate Type:	This is a standard X.509 (V3) 2048+ bit key length SSL/TLS with SHA-256 hashing algorithm issued to you as the machine operator, and the server that you manage. This certificate secures one or multiple domains, as Extended Validated (EV)
Validity Periods:	Available in one (1) year validity period
Storage Type:	Server certificates store
Available to Non-U.S. Residents:	Yes – This certificate is offered on a limited basis in pre-approved non-U.S. countries, see our Supported Countries list

Specifications

- X.509 v3 digital certificates
- 2048+ bit key length
- SHA-256 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

TrustID | IdenTrust TLS/SSL | Organization Identity | Extended Validated (EV) certificates are publicly trusted and natively trusted in most popular browsers.

Certificate Usage

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

- Data and Communications Encryption
- Server Authentication
- Client Authentication

TrustID | IdenTrust TLS/SSL | Organization Identity | Extended Validated (EV) 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:

- Acceptable Forms of Identification
- TrustID Forms, Agreements and Policies
- TrustID FAQs

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