DIGITAL CERTIFICATES

IdenTrust
part of HID Global

DoD ECA Medium Assurance TLS/SSL Certificate

Product Summary

DoD ECA Medium Assurance TLS/SSL certificates secure your domain name (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.

DoD ECA Medium Assurance TLS/SSL are approved by the Department of Defense for systems that need to communicate with U.S. Federal Government systems.

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.

Identity Authentication Method:	As the server sponsor, your identity must be verified by a Notary Public, Trusted Correspondent or a Registration Authority
Identity Proofing Requirements:	Affiliation with the sponsoring organization and domain ownership
Forms Packet Required:	Yes - You are required to submit a forms packet with your application
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.
Trust Model:	This certificate is government trusted
Assurance Level	Medium Assurance
Certificate Type:	This is a standard X.509 (V3) 2048+ bit key length SSL/TLS with SHA-256 hashing algorithm issued to you and the server that you will manage This is a single domain (DV), Organization validation (OV) certificate.
Validity Periods:	Available in one (1), two (2) and three (3) year validity periods
Storage Type:	Browser certificate store of a single server
Available to Non-U.S. Residents:	Yes – This certificate can be issued on a limited basis outside of the U.S. See our **Supported Countries** list.
Certificate Delivery Time:	3-5 business days after IdenTrust receives your forms packet

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
- 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 to secure websites interacting with the U.S. Federal government using via:

- Data and Communications Encryption
- Server Authentication
- Client Authentication

Other Resources

Related information:

- **ECA FAQs**

2020-08-18-identrust-dod-eca-med-assur-tls-ssl-cert-ds-en

For IdenTrust Sales Inquiries: +1 801 384-3481 | sales@identrust.com