

# DoD ECA Medium Assurance TLS/SSL Certificate



### Product Summary

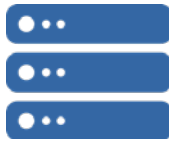
DoD ECA Medium Assurance TLS/SSL certificates secure your domain name (DV and organization's (OV) identity by establishing an encrypted connection between a browser or user's computer and a server or website. This connection protects in transit, sensitive data from interception by non-authorized parties, 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.

<b>Identity Authentication Method:</b>	As the server sponsor, your identity must be verified by a Notary Public, Trusted Correspondent or a Registration Authority
<b>Identity Proofing Requirements:</b>	Affiliation with the sponsoring organization and domain ownership
<b>Forms Packet Required:</b>	Yes - You are 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 PKCS#10. Visit our <a href="#">How To Generate a CSR</a> page if you need assistance.
<b>Trust Model:</b>	This certificate is government trusted
<b>Assurance Level</b>	Medium Assurance
<b>Certificate Type:</b>	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.
<b>Validity Periods:</b>	Available in one (1), two (2) and three (3) year validity periods
<b>Storage Type:</b>	Browser certificate store of a single server
<b>Available to Non-U.S. Residents:</b>	Yes - This certificate can be issued on a limited basis outside of the U.S. See our <a href="#">Supported Countries</a> list.
<b>Certificate Delivery Time:</b>	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](#)