![IdenTrust — part of HID Global]

# ECA | Medium Assurance | TLS/SSL | Organization Validated (OV) Certificate

Product Summary

ECA | Medium Assurance | TLS/SSL | Organization Validated (OV) 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.

ECA | Medium Assurance | TLS/SSL | Organization Validated (OV) are approved by the Department of Defense for systems that need to communicate with U.S. Federal Government systems.

Identity Authentication Method:	Your identity must be verified by a Notary Public, Trusted Agent or an authorized Registration Authority
Identity Proofing Requirements:	Proof of identity and affiliation with the Sponsoring Organization, and domain ownership
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 completed forms packet with your application
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 as the machine operator, and the server that you 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 is offered on a limited basis in pre-approved non-U.S. countries, see our Supported Countries list

identrust.com

Specifications
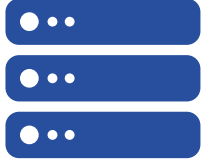
- X.509 v3 digital certificates
- 2048+ bit key length
- SHA-256 hashing algorithm
- Certificate revocation List (CRL) and Online Certificate Status Protocol (OCSP) validation
- Natively trusted in browsers
- Comply with the industry-standard requirements for the Certification Authority
- Audited under 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® 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:
- Acceptable Forms of Identification
- ECA Forms, Agreements and Policies
- ECA FAQs

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

An ASSA ABLOY Group brand

ASSA ABLOY

identrust.com