

# TrustID TLS/SSL Software Storage

Organization Identity (OV or EV)



## PROGRAM

The IdenTrust TrustID program delivers a comprehensive framework for digital identity assurance, enabling secure authentication, encryption and digital signing across a broad spectrum of applications. TrustID certificates are issued by a globally recognized certificate authority and are designed to support critical use cases including code signing, secure email (S/MIME) for signing and encryption, TLS/SSL for secure communications and document signing. With a strong emphasis on compliance, interoperability and scalability, the TrustID program ensures high assurance and trust for both public and private sector environments.

IdenTrust's TLS/SSL Certificates are recognized by major browser providers and operating systems globally including Edge, Chrome, Firefox and Safari.

## ASSURANCE LEVEL

The TrustID Organization Identity Validation provides an assurance that the Organization is in existence at the Organization Validation (OV) affiliate level. There is assurance of the identity and the relationship with the organization is validated.

Choosing an Extended Validation (EV) provides an elevated level of trust for the relationship between the individual and the organization shown on the digital certificate, because it also confirms the existence and operation of the organization.

## AFFILIATION

A verification of affiliation between the organization and the employee is the Organization Validation that IdenTrust performs to provide a level of assurance on the Organization associated with the digital certificate. Processes to ensure the organization is in operational existence support a basis of trust for objects secured with TLS/SSL certificates.

An Extended Validation (EV) is an elevated level of assurance that the organization is trustworthy.

The application requirements to satisfy the validation levels may be provided entirely online and does not require any physical paperwork.

## USE CASES

**Public Website Hosting** — Domain owners who host websites publicly on the internet use TLS/SSL certificates to indicate their legitimacy to site visitors. These digital certificates indicate a valid chain of trust to IdenTrust's issuing CA, which is globally trusted by the browser community. This chain of trust shows the user that the website owner may be trusted for legitimacy, assuring the end user they are on a reputable genuine website.

**Data Encryption** — Sensitive data may be protected while in-transit from non-authorized parties by establishing an encrypted connection using a TLS/SSL certificate. This trusted connection between an end user's browser or computer and a server or website, allows the sender and receiver to communicate trustworthy data that has not been altered while in transit.

## STORAGE

The IdenTrust TLS/SSL | Organization Identity | Organization Validated & Extended Validated (OV and EV) certificates are available to download in .pem, .pfx and .p12 formats.

## KEY FEATURES

**Native Browser Trust** — Major browser providers like Microsoft, Google, Mozilla and Apple provide native trust of IdenTrust TLS/SSL certificates in their browsers, which provides a seamless experience to trust domain ownership of websites for the end user

**X.509 v3 certificates** — Available in RSA 2048+ bit key length with SHA-256 hashing algorithm

**CSR retrieval** — Customers may request and retrieve certificates using their own Certificate Signing Request (CSR)

**Multi-Domain Validation** — TrustID TLS SSL certificates from IdenTrust are able to include multiple domains to simplify certificate management in your environment. This supports easier scaling, as well as simplifies security management practices while offering flexibility for complex environments.

**Continuous Customer Support** — Resources to support IdenTrust customers are continuously available at [identrust.com](https://identrust.com), with specialized teams regularly available during MST business hours

**Revocation checking** — IdenTrust supports Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) checking for real-time validation of TLS/SSL digital certificates issued by IdenTrust CA.

## ABOUT IDENTRUST

IdenTrust, part of HID, is a leading provider of trusted identity solutions, delivering digital certificates that secure online transactions, encrypt communications and authenticate identities. Recognized by financial institutions, healthcare providers, government agencies and enterprises worldwide, IdenTrust ensures compliance, security and operational efficiency across industries.

As the only bank-developed identity authentication system, IdenTrust provides a legally and technologically interoperable environment for identity authentication in more than 175 countries. With millions of active certificates and supporting billions of validations per year, IdenTrust sets the gold standard in digital trust.

## CORE PRINCIPLES

- **Trust & Compliance** — IdenTrust certificates comply with global security standards, including WebTrust, SOC2, DirectTrust, Federal PKI, GDPR and DEA EPCS mandates, ensuring businesses meet regulatory requirements
- **Scalability & Integration** — Offering SSL/TLS, client authentication, document signing, code signing, S/MIME for email signing and encryption, and IoT certificates, that are publicly trusted or trusted by the U.S. Government. IdenTrust provides seamless integration with enterprise and cloud-based systems.
- **Reliability & Automation** — With 99.9%+ system uptime, IdenTrust ensures uninterrupted validation and issuance while enabling certificate lifecycle management through web portal and APIs

Headquartered in Salt Lake City, UT, IdenTrust operates from its primary datacenter with additional support from its London, UK office, serving banking and financial customers in EMEA. By combining trusted identity authentication, global compliance and industry-leading reliability, IdenTrust empowers businesses, governments and individuals to transact securely with confidence in an increasingly digital world.

## RELATED INFORMATION:

- [TrustID | IdenTrust TLS/SSL | Organization Identity | Extended Validated Certificate Forms Packet](#)
- Offered for US and other countries. Please visit the State Department for embargoed countries in their Sanction Programs and Country Information page [Sanctions Programs and Country Information | Office of Foreign Assets Control](#).

## FOR IDENTRUST INQUIRIES:

**Sales** — +1 888-824-1098 or [Sales@IdenTrust.com](mailto:Sales@IdenTrust.com)

**Support** — +1 888-339-8904. Submit a question via our [portal](#)



### HID Regional Offices

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769

Europe, Middle East, Africa: +44 1440 714 850

Asia Pacific: +852 3160 9800 | Latin America: +52 (55) 9171-1108

**For more global phone numbers click here**

© 2025 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

2025-12-10-iams-identrust-trustid-tls/ssl-organization-identity-software-storage-ds-en

Part of ASSA ABLOY