# TrustID Code Signing

## Hardware Storage (Token or HSM)
## Organization Identity (OV or EV)


### USE CASES

Professional Use — Affiliated Individuals of organizations use IdentTrust code signing certificates to display trusted authorship of the code and executable packages they develop. This supports practices for trusted sharing of scripts, libraries, firmware, drivers, etc. internally within an organization, and externally offering executable packages for public consumption.

### 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 TrustID digital certificates are issued under the TrustID Certification Policy program and are publicly trusted by the major browsers and operating systems. TrustID certificates are designed to provide different levels of trust for identities. The identities TrustID certificates validate are individuals, organizations, email addresses and servers.

End users can trust the authenticity of an executable file's author when it signed with a TrustID Code Signing Certificate. These certificates are compatible with platforms such as Microsoft Authenticode (kernel and user mode files, like .exe, .cab, .dll, .ocx, .msi, .xpi and .xap), Java, Apple applications, Microsoft Office Macro and VBA.

### 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 authorship on code signing certificates.

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



IdenTrust part of HID

## STORAGE

The Code Signing | Organization Identity | Hardware Storage (OV or EV) certificate is available with two storage options:

Hardware Token — Downloaded to a FIPS 140-2 compliant USB token, available to purchase from IdenTrust during application

Hardware HSM — Installed on the FIPS 140-2 compliant Hardware Security Module (HSM)

## KEY FEATURES

**Unlimited Number of Signatures —** While the certificate has an expiration date, there is no limit to how many times the certificate may be used to sign artifacts during its validity period. Sign as many items as you like, enjoying an unlimited lifetime maximum of digital signatures from an IdenTrust code signing certificate.

**Continuous Customer Support —** Resources to support IdenTrust customers are continuously available at identrust.com, with specialized teams regularly available during MST business hours

**Trusted Authorship —** Long-term validation and non-repudiation of the contents of the signed files indicates the contents of the files are the same as when they were signed. This ensures the consumer is accessing content the author produced, as of when the file was signed with the code signing certificate.

**Compliance —** Generating, storing and using the subscriber's private key on FIPS-compliant hardware conforms to CA/B forum Baseline Requirements and supports a globally publicly trusted code signing certificate. This allows authors of files to make and share content where the recipients can be confident they are exchanging information in a safe-guarded way that does not put their business at risk of inadvertently exposing sensitive information.

**MS-Defender Trust —** IdenTrust issuing Certificate Authority (CA) that issues code signing certificates is trusted by MS-Defender. Signing a package with a code signing certificate issued by a CA trusted by MS Defender is one criteria to pass the Windows Defender SmartScreen.

**Non-exportable —** The private key is marked as non-exportable once it resides on hardware; meaning it cannot be copied, backed up, or transferred from its secure hardware location. This ensures that cryptographic operations (e.g., signing, decryption) can only be performed on the device where the certificate resides.

**Timestamp —** RFC 3161 compliant timestamping authority service is applied to digital signatures using code signing certificates. This free service is offered on all IdenTrust code signing certificates and remains on digitally signed artifacts even after the digital certificate used to sign the artifact expires. This provides organizations with long-term validation and non-repudiation of when the code was signed, even after the digital certificate is no longer valid for use.

## 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 | Code Signing | Organization Identity Certificate Forms Packet
- TrustID | EV Code Signing | Organization Identity 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
**Support —** +1 888-339-8904. Submit a question via our portal

IdenTrust part of HID

**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**


2025-12-10-iams-identrust-trustid-code-signing-org-identity-hardware-storage-ds-en
Part of ASSA ABLOY