IdenTrust® TrustID® Extended Validation (EV) Code Signing Certificate

IdenTrust TrustID EV Code Signing Certificate Benefits*:*

- Removes the "Unknown Publisher" warning
- Digitally signs unlimited number of software applications or executables
- Compatible with major platforms
- Immediate reputation with Microsoft® SmartScreen
- 24X7 Support

SECURE SOFTWARE CODE WITH IDENTRUST TRUSTID EXTENDED VALIDATION (EV) CODE SIGNING CERTIFICATE

- **Establish trust with your customer –** Allows your customers to verify the organization name, address and country of the user who has signed the code.
- **Reputation with Microsoft® SmartScreen –** Instantly establishes reputation with Microsoft SmartScreen Application filter.
- **Eliminate security warnings –** Avoids "Unknown Publisher" warning messages from browser and operating systems to establish trust in your organization as a software provider. The Extended Validation (EV) vetting process significantly reduces the likelihood that these certificates are issued to fraudsters.

Security Challenges

As we continue our journey into the digital transformation era, a wide range of software programs such as firmware, drivers, desktop applications, mobile applications and application container images must be distributed and updated in a secure way to prevent tampering and forgery. Hackers are discovering new ways to use sophisticated malware attacks against government and private organizations. Security researchers have found that digitally signing code is an effective and common method to protect software programs. It ensures both data integrity to prove that the code was not compromised by hackers and source authentication to identify who was in control of the code at the time it was signed.

IdenTrust TrustID EV Code Signing Certificate

An IdenTrust Extended Validation (EV) code signing certificate provides higher level of assurance for publisher's identity as the organization must go through strict vetting processes before receiving the certificate. By default, IdenTrust TrustID EV Code Signing certificates are issued into FIPS 140-2 Level 2 compliant USB tokens or Smart Cards and require two-factor authentication to access the certificate in order to sign code. It provides immediate reputation with Microsoft SmartScreen Filter and removes the warning message that the application might be malicious.

IdenTrust also provides a free RFC 3161 compliant Timestamp Authority service that can be used for applying timestamp to any digitally signed code. It helps organizations reduce potential liability and provides long-term validation and non-repudiation of the time and date when the code was signed. Recipients can verify when the code was digitally signed as well as confirm that the code was not altered after the timestamp.

The solution is designed to:

- Provide Extended Validation of software publisher based on CA/ Browser Forum requirements
- Instantly establish reputation with Microsoft® SmartScreen Application Reputation filter
- Store certificates on a FIPS 140-2 Level 2 compliant hardware USB token or Smart Card to prevent certificate theft
- Allow certificates to be used in multiple ways such as firmware signing, driver signing, trusted application stores, application software signing
- Support certificate status for a minimum of 10 years after certificate revocation or expiration

Benefits include:

- Support of all major file formats including Microsoft Authenticode, Adobe® Air, Apple®, Java®, Mozilla® object files and Microsoft® Silverlight applications
- Self-service Certificate procurement through the IdenTrust website
- An offering for medium-to-large enterprises that provides custom approval workflow and HSM-based key storage
- Availability of IdenTrust TrustID EV Code Signing certificates to applicants from most countries except those with US trade restrictions
- A timestamping service that allows an entity verifying code to accept the signature on the code as valid if the signing key was valid at the time the code was signed, even if the key has already expired at the time of verification or if the key was compromised sometime after the code was signed

SPECIFICATIONS

IdenTrust TrustID EV Code Signing Certificate	
Supported Use Cases	✦ Software application or executable signing ✦ Firmware signing ✦ Mobile Application Signing ✦ Browser add-on signing
Trust Models	✦ Public ✦ Private (e.g. firmware signing)
Validity Period	✦ 1 or 3 years
Information Displayed in Certificate	✦ Organization legal name ✦ Organization business category ✦ Organization jurisdiction of incorporation • Locality, state/province and country ✦ Organization registration number
Certificate Storage	✦ FIPS 140-2 level 2 compliant USB token or Smart Card
Certificate Hash	✦ SHA-256 hash
Timestamping CA Authority	✦ RFC 3161 compliant ✦ Extends the longevity of signed code

For IdenTrust Sales Inquiries: +1 866 763 3346 | sales@identrus.com