DIGITAL CERTIFICATES

TrustID | Code Signing | Organization Identity | Hardware Storage Certificate

TrustID | Code Signing | Organization Identity | Hardware Storage Certificate Benefits:

- Digitally signs unlimited number of software applications or executables.
- Compatible with major platforms
- 24x7 Support
- Free Timestamping CA Authority service to extend the life of the longevity of the signed code.

SECURE SOFTWARE CODE WITH TRUSTID | CODE SIGNING | ORGANIZATION IDENTITY | HARDWARE STORAGE CERTIFICATE

- **Enhanced user trust:** The thorough verification process help establish stronger reputation for software publishers, potentially increasing user confidence and download rates.
- **Improved Protection against insider attacks and external threats** – The private key must be store on a hardware security module, making it more secure and harder to compromise.
- **Time-sensitive signatures:** IdenTrust Code Signing certificate signatures remain valid even after the certificate expires, providing long-term integrity for signed code.

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.

TrustID | Code Signing | Organization Identity | Hardware Storage Certificates

An IdenTrust TrustID | Code Signing certificate provides a higher level of assurance for publisher's identity as the organization must go through strict verification processes before receiving the certificate.

By default, TrustID | Code Signing | Organization Identity | Hardware Storage certificates are issued into FIPS 140-2 Level 2 compliant USB tokens requiring two-factor authentication to access the certificate in order to sign code.

CSR Enabled

Use of CSR (Certificate Signing Request) is supported during the Code Signing certificate application; once approved, the certificate can be installed in an applicant's hardware security module (HSM) meeting standard security equivalent to FIPS 140-2 level 2 or Common Criteria EAL 4+. Enforcement of this requirement is handled via the Subscriber Agreement.

RFC 3161 Compliance

IdenTrust 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 timestamp.

The solution is designed to:

- Provide validation of software publisher based on CA/Browser Forum Requirements
- Store certificates on a FIPS 140-2 Level 2 compliant hardware USB token or HSM device 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 certificates 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-services 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 TrustID | Code Signing | Organization Identity | Hardware Storage certificates to applicants from most countries except those with U.S. trade restrictions
- A timestamping CA Authority 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

TrustID | Code Signing | Organization Identity | Hardware Storage Certificate

Supported Use Cases	• Software application or executable signing • Firmware signing • Mobile application signing • Browser add-on signing
Trust Model:	• Public • Private (e.g., firmware signing)
Validity Periods:	Available up to a three (3) year validity period
Information Displayed in Certificate	• Organization legal name • Organization business category • Organization jurisdiction or incorporation • Locality/State/Province and country • Organization registration number
Storage Type:	• IdenTrust FIPS 140-2 level 2 USB token, or • Customer HSM FIPS 140-2 level 2 or Common Criteria EAL 4+
Certificate Hash	• X509 v3 digital certificate with SHA-256 hash minimum 3072 or maximum 4096 RSA Keys
Timestamping CA Authority	• RFC 3161 compliant • Extends the longevity of signed code
Available to Non-U.S. Residents:	Yes – This certificate is available to applicants in a limited number of foreign countries, view our Supported Countries list

For IdenTrust Sales inquiries: +1 (866) 763-3346 | sales@identrust.com

An ASSA ABLOY Group brand

ASSA ABLOY