Entrust Code Signing as a Service

Highly secure cloud-based key storage for EV/OV code signing certificates

Market Challenge

EV and OV code signing certificates have undergone changes to strengthen private key protection, aligning with the CA/Browser Forum baseline requirements, based on Ballot CSC-17: Subscriber Private Key Extension. With the latest Code Signing ballot, code signing keys for all public trust code signing certificates must be created in secure FIPS or Common Criteria certified hardware. The move to require the use of secure hardware is intended to prevent possible theft of signing keys by ensuring proper key protection. It is universally followed by all participants in public trust code signing by only allowing the use of secure compliant hardware.

Solution

- **Entrust Code Signing as a Service** ensures the integrity of code, containers, and firmware. The solution secures private keys, automates signing software, and interacts seamlessly with your existing tools and development workflow. It is fully integrated with the Entrust PKI cloud suite.
- **Entrust Signing Automation Service** is a cloud-based service designed to help developers and organizations securely store and digitally sign their code and applications with a trusted certificate authority (CA).

BENEFITS

- Cloud-based solution that meets the demands of a remote workforce
- Automated key generation, key protection, and signing
- Ease of setup and management
- Signs code from anywhere at any time
- Low cost of ownership
- 24x5 unlimited customer support
- Brand protection
- Entrust certificate management system

KEY FEATURES

- FIPS 140-2 Level 3 certified key storage
- Seamless integration with automated CI/CD pipelines
- PKCS #11 and KSP/CNG Signing Client

Learn more about the Entrust Code Signing Solution at entrust.com

Entrust Code Signing as a Service

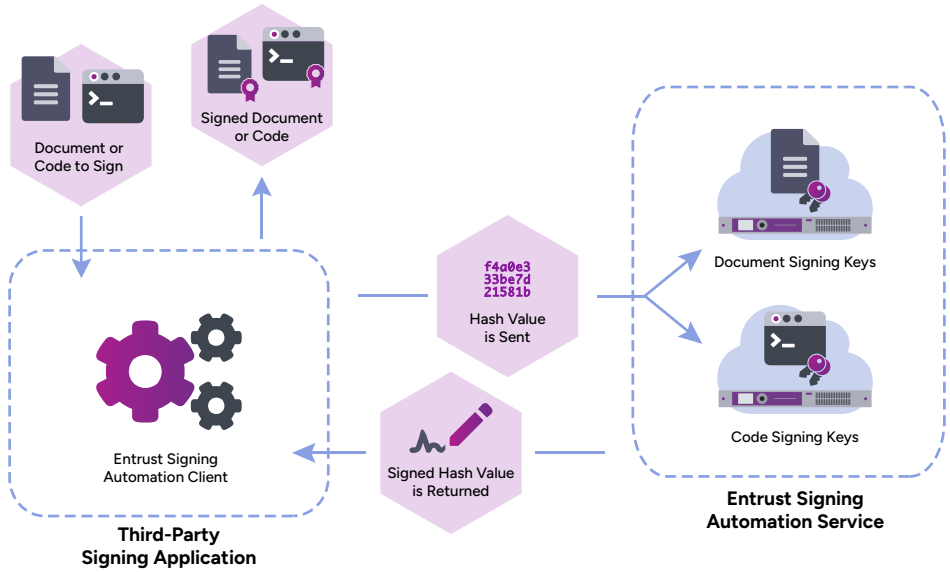
Entrust Code Signing as a Service at a Glance

Entrust helps you build an automated and secure signing process for your code and software to publish externally, without the need to manage secure hardware for the signing keys.

- Public Trust Code Signing EV/OV Certificates - Choose extended validation (EV) to provide your customers with the highest level of trust and to sign Microsoft Windows Kernel drivers or organization validated (OV) certificates
- No hardware requirement, eliminating the reverification process every 13 months
- Available REST API and PKCS #11 library interfaces for automation and CI/CD integration
- For PKCS #11 environments, a Windows/Linux Signing Automation client is provided
- Public timestamping service that supports the IETF RFC 3161 Timestamp Protocol
- FIPS 140-2 Level 3 Entrust-hosted HSM compliant with Common Criteria EAL4
- Removes “unknown publisher” dialogs during the software installation process, giving users the assurance that the software is safe to download
- Authenticates signed code indicating whether the code or application has been tampered with since signing, giving users the confidence they need to decide whether or not to install the software
- Builds a positive Microsoft SmartScreen® application reputation at twice the rate of unsigned applications

Architecture

The Entrust Signing Automation Service can be connected to code signing applications and workflows in order to automatically generate digital signatures for software and code.



Learn more about the Entrust Code Signing Solution at entrust.com

Entrust Code Signing as a Service

Native Integration: Agents for Windows and Linux support PKCS #11. It's a Windows KSP/CNG provider and compatible with platform-native tools to enable remote signing.

Automation: Accelerate trust with a tamper-proof seal for software downloads using RESTful APIs integration with automated CI/CD pipelines.

Usability and Accessibility: Segregate and manage certificates/keys with different virtual tokens for different signing use cases.

Multi-Tenant Signing Key Management: Enables requests to generate signing keys by the signing key management service and automatically selects the nShield HSM that will generate and wrap the signing keys.

Signing operation requests made to the signing key management service unwrap the signing key within the signing key database and sign the document hash.

Technical Specification

Features	Details
Signing Windows files with the Entrust KSP library	Windows, Microsoft Installers (MSI), Cabinet files (CAB), Catalog files (CAT), Windows packages (APPX/MSIX), Microsoft Dynamics 365 extension packages, NuGet packages and scripts (PowerShell, VBScript, JScript, WSF)
RESTful API	Supports generic hashes and automation of signing for artifacts, binaries, and builds in CI/CD environments
Operating System (Signing Client)	Windows 10, version 1909 (64-bit) Linix: Ubuntu 20.04.x (64-bit), RHEL 8.x
Signing PDF documents with iText	PDF other document types

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223