BENEFITS

- Establishes a trusted identity
- Altered code is invalidated
- Removes 'Unknown Publisher' security warnings
- Instant reputation recognition
- Provides assurance to digitally downloaded software
- Prevents installation of unverified software
- Brand protection
- Certificate management system
- 24x5 unlimited tech support

ENTRUST CODE SIGNING CERTIFICATES™

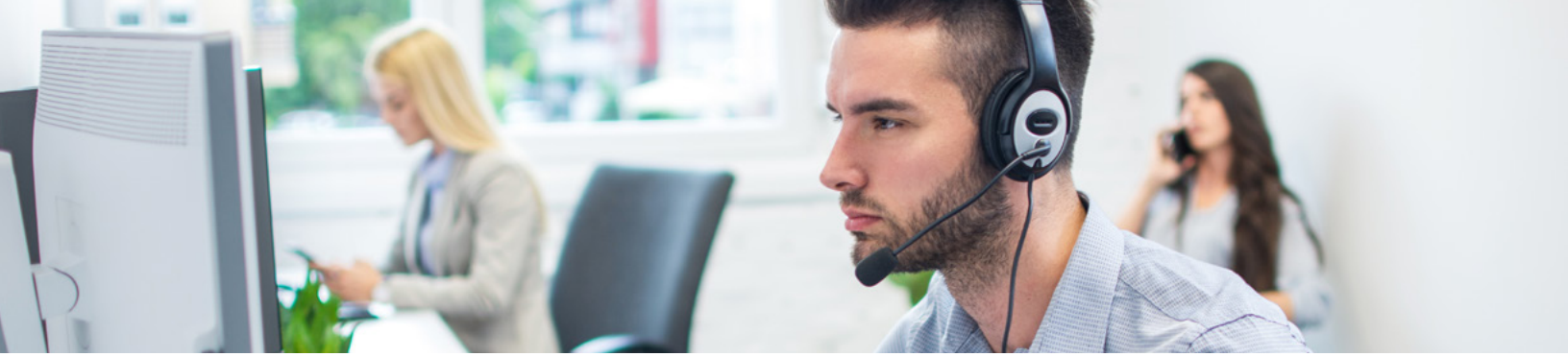
ACCELERATE TRUST WITH A TAMPER-PROOF SEAL FOR SOFTWARE DOWNLOADS

Entrust Code Signing Certificates authenticate the publisher's identity and verify that the digitally signed executables and scripts have not been tampered with since signing. This assures customers that the signed software will be downloaded from the Internet as the developer intended. Signed certificates help software publishers establish trust with their customers, preventing unverified software from being installed on organizational desktops. And, they build a positive Application Reputation at twice the rate of unsigned applications. Customers feel confident knowing that the publisher was verified by Entrust Datacard, a WebTrust-accredited certification authority (CA).

BUSINESS CHALLENGE

The continued proliferation of malware and nefarious websites make users cautious of downloading code and applications digitally. If they are unable to determine who the publisher is or whether or not the software has been tampered with since signing, chances are they will avoid downloading it.

So, how do publishers increase trust with customers and the major platforms?



KEY FEATURES

- Meets EV and OV requirements
- EV and OV verified by a WebTrust accredited CA
- Minimum key size: 2048-bit RSA
- Supports SHA-2 algorithms
- Includes FIPS-compliant token
- Integrates with most third-party development tools
- SmartScreen Application Reputation recognition
- Establishes trusted relationship
- Prevents trust dialogs
- Verifies software publisher
- Assures code authenticity
- Imports time stamp
- Unlimited signing
- 30-day reissue
- Expiration notification
- Easy purchasing options
- 1, 2, or 3-year licensing terms

SOLUTION

Entrust Code Signing Certificates give customers the needed assurance that your code or application has not been tampered with since getting a digital signature.

Establishes a Trusted Identity — Publisher's identity is verified by a WebTrust-accredited CA, Entrust Datacard, building a trusted relationship with your customers.

Authenticates Code — Dialog box indicates whether the code or application has been tampered with since signing, giving users the confidence they need to decide whether or not to download it.

Removes "Unknown Publisher" Dialogs — Significantly reduces trust dialog boxes from appearing during installation, giving users assurance that the software is safe to download.

Instant Application Reputation for Microsoft SmartScreen® Filter — Builds a positive SmartScreen Application Reputation at twice the rate of unsigned applications.

Available in EV or OV — Choose between EV- or OV-verified certificates depending upon the level of trust you want to provide your customers.

▶entrust.com/code-signing-certificates

SIGNING CAPABILITIES

Comprehensive signing capabilities for a wide-range of applications:

- Device drivers
- Operating systems
- Freeware
- Packaged software
- OEM software
- Utility software
- Shareware
- Enterprise applications
- Web applications
- Middleware

SUPPORTED SYSTEMS

By packaging applications and macros for online software distribution, it provides a digital signature and certification for most applications and is compatible with major platforms including:

- Authenticode
- Java
- Visual Basic Script
- Microsoft® Windows® platforms
- Adobe Air
- Microsoft Office® macros
- VBA-Web applications

SYSTEM REQUIREMENTS

The private key must be stored on a FIPS 140-2 Level 2-compliant device. Options include the FIPS-compliant token provided by Entrust Datacard or an HSM device purchased separately.

Certificate Download Requirements

- Token Software – provided by Entrust Datacard upon purchase
- Microsoft Internet Explorer 11
- Microsoft Windows Operating System – version 7,8 and 10
- Microsoft Windows Server Operating System – version 2008, 2012 and 2016

Entrust Code Signing Certificate are x.509-based certificates anchored to a trusted root, allowing users to sign the following code:

- Microsoft Authenticode
- Microsoft Windows Kernel Drivers
- Microsoft Marketplace Apps
- Microsoft Office and VBA
- Java Applets
- Adobe Air
- Apple[1]

NOTE: All code signing certificates require an integrated development environment/software solution that enables application signing. For example, in order to sign Microsoft code, a free tool is required by Microsoft to enable signing (e.g., SignTool, VisualBasics, etc.)

[1] Does not support all Apple applications. Please contact us for details.

A FULL LINE OF DIGITAL CERTIFICATES (AND A COMPREHENSIVE WAY TO MANAGE THEM ALL)

- SSL/TLS Certificates
- Secure Email Certificates
- Document Signing Certificates
- Mobile Device Certificates

EXPANDED OFFERINGS (additional fees apply)

- Platinum Support — 24x7 support and automated SSL server testing
- Discovery — Manage all certificates from one dashboard regardless of vendor

About Entrust Datacard Corporation

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

Corporate Headquarters

U.S. Toll-Free Phone: 888-690-2424
International Phone: +1-952-933-1223

info@entrustdatacard.com
entrustdatacard.com

Entrust Datacard®