



ENTRUST



Entrust Code Signing Certificates

Accelerate trust with a tamper-proof seal for software downloads

Market 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?

Solution

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 corporate devices. And, they build a positive application reputation at twice the rate of unsigned applications. Users feel confident knowing that the publisher was verified by Entrust, a WebTrust-accredited certification authority (CA).

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

LEARN MORE AT [ENTRUST.COM](https://www.entrust.com)



Entrust Code Signing Certificates

Entrust Code Signing Certificates at a glance

Entrust Code Signing Certificates give users 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, building a trusted relationship with your users.

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.

Entrust EV or OV Code Signing Certificates.

Choose extended validation (EV) to provide your customers with the highest level of trust and to sign Microsoft Windows Kernel drivers. Alternatively, another option is organization verified (OV) certificates.



entrust.com/code-signing-certificates

Features

- Meets EV and OV requirements
- EV and OV verified by a WebTrust-accredited CA
- Minimum key size: 3072-bit RSA
- Supports SHA-2 algorithms
- Includes Common Criteria-certified 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 timestamp
- Unlimited signing
- 30-day reissue
- Expiration notification
- Easy purchasing options
- 1, 2, or 3-year licensing terms



Entrust 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, Entrust Code Signing Certificates provide a digital signature and certification for most applications and are compatible with major platforms including:



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



Entrust Code Signing Certificates

System requirements:

The private key must be stored on a FIPS 140-2 Level 2 or Common Criteria Level 4+ compliant device. Entrust provides tokens that are compliant with Common Criteria Level 5. Alternatively, an HSM device can be purchased separately.

Certificate download requirements

- Token Software – provided by Entrust 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 CertificateS 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
- Apple¹

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)

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

Expanded offerings*

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

* Additional fees apply



Learn more at
entrust.com



ENTRUST

Entrust and the Hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer. ©2020 Entrust Corporation. All rights reserved. SL21Q2-code-signing-certificates-ds

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