digicert®

DigiCert Code Signing: Instilling Trust in Your Users

The Problem: "Can I Trust This Code?"

If you're distributing your software to users across the internet, how can you be sure it reaches them without being tampered with or altered? How can they be sure it's safe to download? Unfortunately, a malicious attacker could have easily intercepted a copy of your software, re-distributing it with some bundled malware.

One of the most common types of malware is called a Trojan Horse. This aptly-named villain hides malware in what appears to be a normal file, just as the Greeks snuck a force of men into Troy using a giant wooden horse—hence, Trojan Horse.

Common types of malware:

- **Spyware**: Collects personal information
- **Adware**: Downloads unwanted advertising material
- **Virus**: Infects program files
- **Worm**: Replicates itself across a network
- **Trojan Horse**: Poses as legitimate software

The Solution: Code Signing Certificates

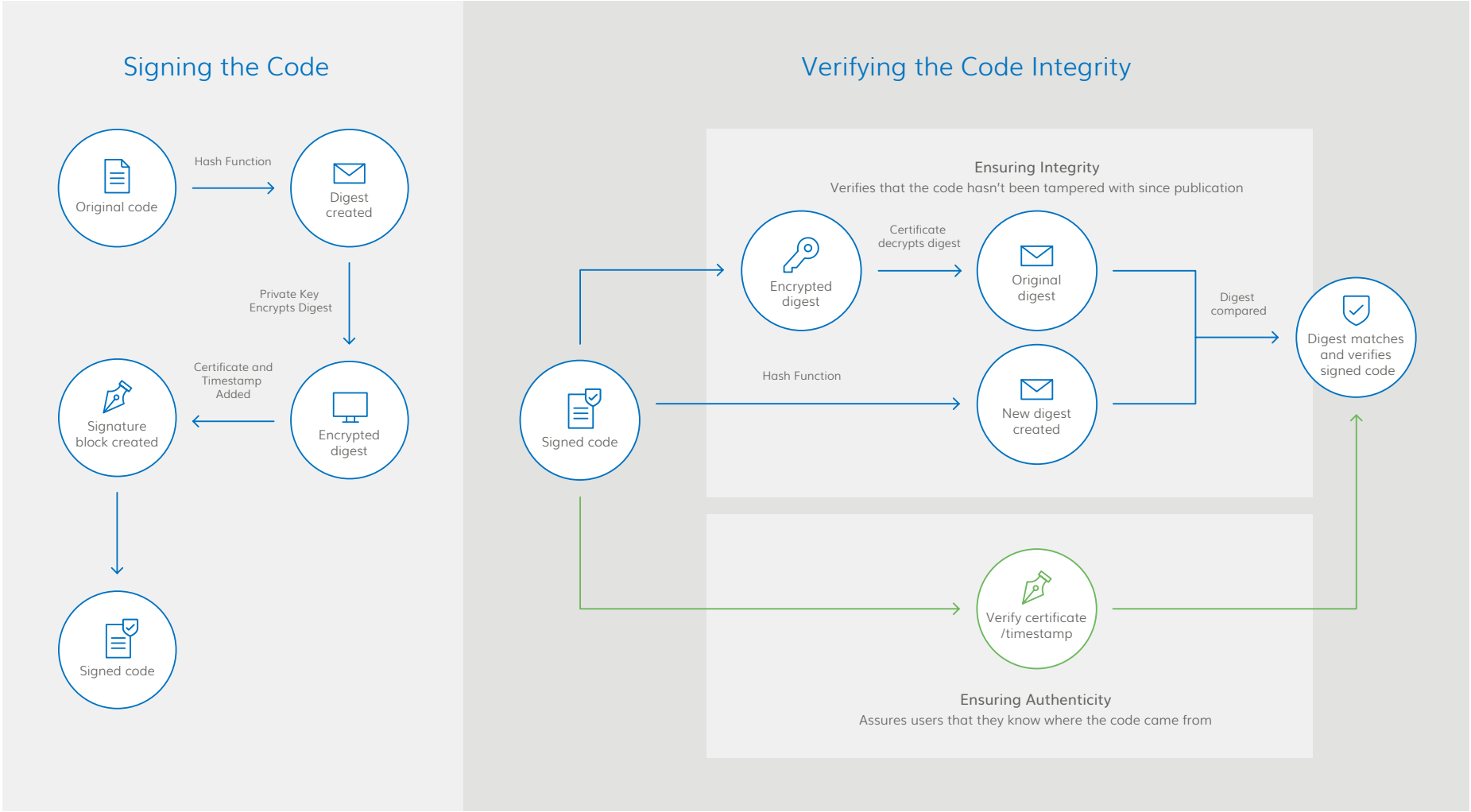
To avoid malware, software developers use code signing certificates to digitally sign apps, drivers, and software programs. This makes it so end users can verify that the code has not been compromised by a third party.

Code signing certificates use the same technology that an SSL/TLS certificate uses to authenticate the identity of a website. (Note: code signing certificates do not encrypt files or data). A code signing certificate uses a private/public key pair to digitally sign software, proving to the end user that the code is legitimate and can be trusted.

A code signing certificate contains:

- Your signature
- Your company's name
- A timestamp (if desired)

How Code Signing Works



Features & Pricing

	Code Signing	EV Code Signing
1-year price	$223 USD	$449 USD
2-year Price (per year)	$198 USD	$399 USD
3-year Price (per year)	$178 USD	$331 USD
Encrypted digital signature	✓	✓
Requires rigorous extended validation of organization		✓
Instant reputation with Microsoft Smartscreen Filter		✓
Requires two-factor authentication using hardware token		✓

DigiCert Code Signing Certificates are available as standard code signing or Extended Validation (EV). A DigiCert EV Code Signing Certificate adds a rigorous vetting process and hardware security requirement to the standard benefits of code signing. This gives you two-factor authentication using an encrypted token and Microsoft's SmartScreen® Application Reputation filter, which reduces end-user warning messages.

Benefits of DigiCert Code Signing

Protect your users

Signing code allows your users to verify that the code is authentic and has not been tampered with. It also protects your software against theft and malware.

Meet partner requirements

Your partners—and the channels that distribute your software—expect you to safeguard their customers' data. Signing software shows commitment to their safety.

Increase user adoption

Signing code helps avoid warning messages from browsers and builds trust in you as a publisher—resulting in more users.

digicert

Why Choose DigiCert?

Market-Leading Platform & Tools

Maintaining a secure network goes beyond purchasing and installing SSL certificates—it includes proper configuration, vulnerability scanning, ongoing monitoring, and timely renewal. The DigiCert platform and tools allow you to automate certificate tasks, making management easy.

24/7 Customer Support

DigiCert's award-winning technical support team is available any time you need help, and certificates are validated around the clock. Organizations are given a dedicated account representative who is a committed partner in your security.

Securing Top Brands

As the world's leading high-assurance digital certificate provider, we're lucky enough to work with some of the most innovative companies in the world, including those shaping the Internet of Things (IoT). Along the way, we secure more than 26 billion web connections every day.

facebook Nintendo IBM CISCO NASA hp invent Microsoft SONY Medtronic

To learn more, call 1.855.800.3444 or email sales@digicert.com.