SSL4less

// CODE SIGNING CERTIFICATES

Who needs a CODE SIGNING?

Software distributed over the Internet is endangered by plenty of threats. If you use online distribution channel, you should take extra care to minimize the risk of unauthorized modification, impersonation and unauthorized re-distribution by malicious third parties. Our CODE SIGNING certificates will protect your software against those threats.

With an increasing number of mobile and desktop applications for consumers exponentially increasing amount of threats to them.

CODE SIGNING **certificates:**

// verifies publisher's identity

// maintains integrity of content

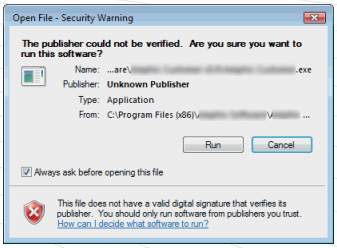
// safeguards software from tampering

// creates a trusted distribution model

// prevents alarms and warnings when downloading and installing software

How CODE SIGNING **works**?

1. A developer adds a digital signature to code or content using a unique private key from a code signing certificate.
2. When a user downloads or encounters signed code, the user's system software or application uses a public key to decrypt the signature.
3. The system looks for a root certificate with an identity that it trusts or recognizes to authenticate the signature.
4. The system then compares the hash used to sign the application against the hash on the downloaded application.
5. If the system trusts the root and the hashes match, then the download or execution continues.
6. If the system does not trust the root or the hashes do not match, the system interrupts the download with a warning or the download fails.



Our certificates helps you to create **safe apps** for these platforms:

Java ADOBE AIR Silverlight Microsoft Office

Compare our offer of CODE SIGNING certificates **provided by leading vendors**:

COMODO swiss sign thawte Symantec.

Domeny.pl sp. z o.o. [LLC], Marcika Street. 27/C-D, 30-443 Kraków
ssl4less.eu | e-mail: info@ssl4less.eu