SSL4less

CODE SIGNING CERTIFICATES

//SECURE YOUR SOFTWARE!

Software downloaded via the Internet is exposed to many threats. If you distribute your products over networks, secure against unauthorized modification, uncontrolled distribution or impersonation under your code signing regulations.

CODE SIGNING CERTIFICATE

- *Confirms the authenticity of the publisher*
- *Guarantees the integrity of content*
- *Protects the software against manipulation*
- *Protects the distribution channel*
- *Prevents alarms and warnings when downloading and installing software*

HOW DOES THE CODE SIGNING CERTIFICATE WORK?

1. Developer adds a digital signature to the code or content using the private key from the certificate.
2. When a user downloads or encounters a signed code, the user's system or application uses a public key to decrypt the signature.
3. The system looks for a trusted root certificate to authenticate the signature.
4. The system compares the hash used for the signature with the hash of the downloaded application.
5. If the hashes match, system continues downloading or executing.
6. If the root certificate is untrusted or the hashes do not match, the system stops downloading and displays an error message.

Certificates available on our website help create secure applications for platforms such as:

Windows, Apple, Java, Firefox, ADOBE AIR, Microsoft Silverlight, Office

Choose the best Code-Signing certificate from among the leading vendors!

COMODO, Certum by asseco, digicert, DomenySSL, SUPERFAST, GeoTrust, Entrust Datacard

The owner of the SSL4lessl website is H88 S.A.
tel.: +48 12 296 36 63 — e-mail: info@ssl4less.eu