//CertyfikatySSL.pl

// CERTYFIKATY CODE SIGNING

Kto potrzebuje certyfikatu CODE SIGNING **?**

Oprogramowanie pobierane przez Internet jest narażone na wiele zagrożeń. Jeżeli korzystasz z tego kanału dystrybucji swoich produktów i chcesz zlikwidować ryzyko **nieuprawnionej modyfikacji, podszywania się lub niekontrolowanej dystrybucji**, skutecznie umożliwią Ci to certyfikaty CODE SIGNING.

Wraz ze wzrostem liczby aplikacji mobilnych i desktopowych, przeznaczonych dla konsumentów, rośnie lawinowo liczba zagrożeń dla nich.

Certyfikaty CODE SIGNING **:**

// potwierdzają autentyczność wydawcy

// gwarantują integralność zawartości

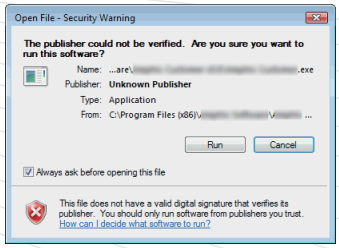
// zabezpieczają oprogramowanie przed manipulacją

// zabezpieczają kanał dystrybucji

// zapobiegają alarmom i ostrzeżeniom przy pobieraniu i instalacji oprogramowania

Jak działa certyfikat CODE SIGNING **?**

1. Developer dodaje cyfrowy podpis do kodu lub zawartości, używając klucza prywatnego z certyfikatu.
2. Gdy użytkownik pobierze lub natrafi na podpisany kod, system lub aplikacja użytkownika używa publicznego klucza od odszyfrowania podpisu.
3. System szuka zaufanego certyfikatu root w celu uwierzytelnienia podpisu.
4. System porównuje hash użyty do podpisu z hashem pobranej aplikacji.
5. Jeżeli hash'e są zgodne, kontynuuje pobieranie lub wykonywanie.
6. Jeżeli certyfikat root jest niezaufany lub hash'e do siebie nie pasują, system przerywa pobieranie i wyświetla komunikat błędu.



Certyfikaty dostępne na naszych stronach pomagają tworzyć **bezpieczne aplikacje** dla platform takich jak:

Java ADOBE AIR Silverlight Microsoft Office

Zapoznaj się z naszą ofertą certyfikatów Code Signing **czołowych wystawców**:

COMODO swiss sign thawte Symantec.

Właścicielem serwisu CertyfikatySSL.pl jest firma Domeny.pl
ul. Marcika 27/C-D — 30-443 Kraków — tel.: +48 12 296 36 63 — e-mail: info@certyfikatyssl.pl