

CERTYFIKATY CODE SIGNING

//ZABEZPIECZ SWOJE OPROGRAMOWANIE!

Oprogramowanie pobierane przez Internet jest narażone na wiele zagrożeń. Jeżeli dystrybuujesz swoje produkty przez sieci zabezpiecz się przed nieuprawnioną modyfikacją, niekontrolowaną dystrybucją lub podszywaniem się pod Ciebie stosując certyfikaty CODE SIGNING.

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.

Wybierz najlepszy dla siebie certyfikat Code-Signing spośród czołowych wystawców!

SECTIGO

 **Certum**
by CURESCO

 **digicert**

Domery SSL

SUPERFAST»

 **GeoTrust**

 **Entrust
Datacard**