**Infrastruktura me qelës publik**

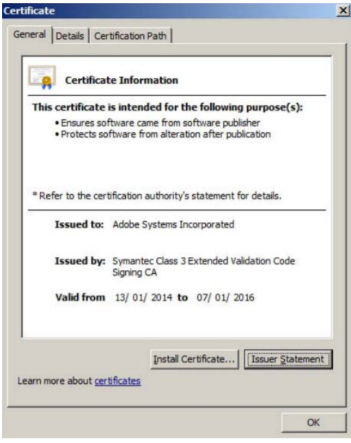
*Nënshrimi digjital* është teknik matematikore për të siguruar autheticitet, integritet dhe mosënjohje në formën e *nënshkrimit të kodit* dhe *certifikatave digjitale*.

*Nënshkrimi i kodit* : Përdoren për ta verifikuar integritetin e skedarëve të ekzekutueshëm të shkarkuar nga website. Duke e verifikuar identitetin e personit i cili e ka krijuar softuerin.

*Certifikata digjitale* : Përdoret për ta vërtetuar identitetin e një sistemi dhe për të shkëmbyer të dhëna konfidenciale.

Kemi tre alogritme për të gjeneruar dhe verifikuar *nënshkrimin digjital* : *RSA*, *DSA, ECDSA ( Algortimi për nënshkrim të algjeve eliptike )*.

Dosjet e ekzekutueshme mbështjellen me një *zarf* të nënshkruar në mënyr digjitale e cila i lejon end përdoruesit ta verifikoj nënshkrimin para se ta bëj instalimin.

Nënshrikimi digjital i kodeve na siguron se : *Kodi është autentik dhe vjen nga botuesi, Kodi nuk është modifikuar pasi që është larguar nga butuesi, Botuesi e publikon në mënyr të pa mohueshme kodin*.

*Certifikata digjitale* përdoret për të : *shkëmbyer mesazhe të sigurta nëpërmjet rrjetit*, *për të verifikuar dhe vërtetuar se përdoruesit që po dërgojn mesazhin janë ata që pretendojn se janë, për të siguruar konfidencialitetin e përdoruesit me mjete për kodimin e përgjigjies*.