Sadržaj

Digitalni potpis

Osoba koja želi digitalno potpisati neki dokument čini to tako da svojim tajnim ključem (koji zna samo ta osoba) šifrira dokument koji želi digitalno potpisati. Takav digitalno potpisani dokument nije zaštićen od čitanja, pošto se dešifrovanje obavlja javnim ključem koji nije tajna, ali to i nije namera digitalnog potpisa.

Osoba koja primi taj dokument, dešifrira ga javnim ključem osobe koja je potpisala dokument i ukoliko je stvarno ta osoba, čiji se javni ključ koristi za dešifrovanje poruke, šifrirala (potpisala) dokument, dobijamo izvorni dokument.

Osnovna svojstva digitalnog potpisa su:

potpis je autentičan (proverava se javnim ključem potpisane osobe)

potpis je nekrivotvorljiv (potpisivanje se vrši tajnim ključem kojeg zna samo osoba koja je potpisala dokument)

potpis nije moguće koristiti više puta (potpis je nedeljivi deo dokumenta i nije ga moguće premestiti na drugi dokument)

potpisani dokument je nepromenljiv (ukoliko se promeni ma i jedan bit u dokumentu, više se ne može dešifrirati korišćenjem javnog ključa potpisane osobe)

potpis ne može biti negiran (tajni ključ koji je upotrebljen za potpisivanje zna samo osoba koja je vlasnik tog ključa)

Jedini način falsifikovanja potpisa je višestruko korišćenje istog potpisanog dokumenta (eng. resend-attack). Sam dokument je pravnosnazan i ne može se poništiti. Zbog toga se u potpisivanju dokumenata navode datum i vreme samog čina potpisa (eng. timestamping).

Tehnologija digitalnog potpisa takođe koristi tehniku simetričnog kriptovanja. Dakle, pošiljalac i primalac imaju par ključeva od kojih je jedan tajni, a drugi svima dostupan javni ključ. Ključevi predstavljaju matematičke algoritme koje je izdalo sertifikaciono telo.

Slika 1. Digitalni potpis

Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke ili integritet podataka (dokaz da poruka nije promenjena na putu od pošiljaoca do primaoca), kao i da osigura garantiranje identiteta pošiljaoca poruke. Osnovu digitalnog potpisa čini sadržaj same poruke. Pošiljaoc primenom određenih kriptografskih algoritama prvo od svoje poruke koja je proizvoljne dužine stvara zapis fiksne dužine (pr. 512 ili 1024 bita) koji u potpunosti oslikava sadržaj poruke. To prakticno znači da svaka promena u sadržaju poruke dovodi do promene potpisa. Ovako dobijen zapis on dalje šifrira svojim tajnim ključem i tako formira digitalni potpis koje se šalje zajedno porukom.

Da vidimo kako to funkcionise na našem primeru. Pera kreira digitalni potpis na osnovu poruke koju želi da pošalje Ani. Šifrira ga svojim tajnim ključem i šalje zajedno sa porukom. Ana po prijemu poruke dešifruje Perin potpis njegovim javnim ključem. Zatim primenom istog postupka kao i Pera i ona kreira potpis na osnovu poruke koju je primila i upoređuje ga sa primljenim potpisom. Ako su potpisi identični, može biti sigurna da je poruku zaista poslao Pera (jer je njegovim javnim ključem uspešno dešifrovala potpis) i da je ona stigla do nje nepromenjena (jer je utvrdila da su potpisi identični).