ELEKTRONIČKI POSLUŽITELJSKI CERTIFIKATI

Branko Mažar

CARNet

Branko.Mazar@CARNet.hr

01/6661-721

Sažetak

Elektronički poslužiteljski certifikati služe za kriptiranje komunikacije između klijenata i poslužitelja kao i za provjeru vjerodostojnosti odnosno utvrđivanje identiteta poslužitelja. Na ovaj način komunikaciju nije moguće neovlašteno presresti, a u isto vrijeme može se jednoznačno utvrditi da li je komunikacija uspostavljena s pravim poslužiteljem. Kako bi se nedvojbeno mogao utvrditi identitet poslužitelja, certifikati moraju biti izdani od strane tijela kojem korisnici i proizvođači programske podrške vjeruju.

OSNOVNO O KRIPTOGRAFIJI

Prijenos i pohranjivanje informacija podrazumijeva i mogućnost neovlaštenog pristupa informacijama kao i njihovog neovlaštenog korištenja i mijenjanja. Pored kontrole pristupa, najčešće korištena metoda za zaštitu informacija je kriptiranje. Kriptiranje podrazumijeva skup tehnika kojima se sadržaj koji je čitljiv prema određenom ključu pretvara u sadržaj koji postaje nečitljiv. Taj se postupak naziva enkripcija, a vraćanje sadržaja u prvobitni čitljivi oblik naziva se dekripcija.

Postoje dvije osnovne vrste kriptografije: simetrična i asimetrična kriptografija. Glavno obilježje simetrične kriptografije je korištenje istog ključa za enkripciju i za dekripciju. U slučaju asimetrične kriptografije koristi se par ključeva – javni i privatni ključ. Javni ključ je, kako mu i ime kaže, javno dostupan podatak dok je privatni ključ tajan i dostupan je samo vlasniku para ključeva. Enkripcija se vrši korištenjem javnog ključa dok se dekripcija izvodi uz pomoć privatnog ključa. Na taj je način osigurano da kriptiranu poruku može dekriptirati samo primatelj poruke, odnosno vlasnik javnog ključa.

Provjera cjelovitosti sadržaja odnosno provjera da li je sadržaj izmijenjen vrši se korištenjem digitalnog potpisa. Za digitalno potpisivanje se koristi privatni ključ i taj postupak ne rezultira kriptiranjem sadržaja već on ostaje i dalje čitljiv. Provjera ispravnosti digitalnog potpisa obavlja se uz pomoć pripadajućeg javnog ključa.

ELEKTRONIČKI CERTIFIKATI

Prilikom korištenja asimetrične kriptografije nužno je moći jednoznačno utvrditi kome pripada javni ključ kako bi se osiguralo da kriptirani sadržaj bude dostupan isključivo onome kome je i namijenjen. Kako bi to bilo moguće, nužno je uspostaviti određeni lanac povjerenja putem kojeg će uvijek biti moguće nedvojbeno utvrditi kome pripada pojedini javni ključ. Nakon što se utvrdi vlasništvo nad javnim ključem, povjerenje se potvrđuje digitalnim potpisivanjem istog.

Elektronički certifikati predstavljaju skup podataka koji, između ostalih informacija, sadrže javni ključ te informacije o njegovom vlasniku, a sve to zajedno je digitalno potpisano od strane izdavača elektroničkog certifikata. Na taj način izdavač elektroničkog certifikata jamči za točnost informacija koje certifikat sadrži te je stoga neophodno da certifikat bude izdan od strane izdavača kojem korisnici i proizvođači programske podrške vjeruju. Organizacije zadužene za izdavanje elektroničkih certifikata nazivaju se Certificate Authorities ili skraćeno CA. Postoji više globalnih CA-ova čiji su javni ključevi priznati od većine proizvođača programske podrške.

Ovisno njihovoj namjeni, postoji nekoliko vrsta elektroničkih certifikata. Osobni certifikati namijenjeni korisnicima sadrže privatne podatke poput imena i prezimena, a poslužiteljski certifikati koji su namijenjeni za ostvarivanje kriptirane komunikacije s pojedinim servisima na poslužitelju sadrže podatke poput FQDN-a poslužitelja. U posljednje vrijeme sve se češće koriste certifikati za potpisivanje softvera čime proizvođači programske podrške potvrđuju autentičnost pojedinih proizvoda.

Podaci u certifikatu su zapisani u formaliziranom formatu, a danas je to općeprihvaćeni format X.509. Kroz vrijeme ovaj je format doživio nekoliko izmjena, a aktualna je njegova treća inačica.

INSTALACIJA I KORIŠTENJE POSLUŽITELJSKIH ELEKTRONIČKIH CERTIFIKATA

Poslužiteljski elektronički certifikati služe za osiguranje kriptirane komunikacije s pojedinim servisima na poslužitelju. Najčešće se koriste za kriptiranu komunikaciju s pojedinim web sjedištima čime informacije koje se razmjenjuju putem inače tekstualnog protokola HTTP postaju nečitljive trećim stranama. Pored navedenog, često se koriste za ostvarivanje sigurnog pristupa poslužiteljima elektroničke pošte kao što je komunikacija putem protokola IMAPS, sigurnog slanja elektroničkih poruka putem protokola SMTPS te brojne druge servise.

Certifikati se generiraju na temelju zahtjeva za certifikatom. Generiranje zahtjeva za certifikatom se izvodi korištenjem kriptografskih programskih rješenja, kao što je npr. OpenSSL, a uključuje generiranje para ključeva te specificiranje podataka o poslužitelju. Kao rezultat nastaje tzv. certificate request (CSR) datoteka koja sadrži javni ključ i podatke o poslužitelju, a sve navedeno je potpisano pripadajućim privatnim ključem.

Na temelju ovako definiranog zahtjeva CA generira elektronički certifikat koji je potom potrebno specificirati u konfiguraciji pojedinog servisa. Nakon njegove uspješne instalacije klijentima će prilikom pristupa certifikat biti isporučen i time omogućena identifikacija poslužitelja te ostvarivanje kriptirane komunikacije.

U ovoj će se radionici, između ostalog, analizirati struktura X.509 i njeni osnovni elementi, obraditi detalji generiranja zahtjeva za certifikatom, načini naručivanja i dobivanja certifikata te upoznati s radom kriptografskih alata koji se koriste u tu svrhu. Pored toga, proučit će se načini instalacije certifikata na pojedine servise, tehnike za provjeru ispravnosti certifikata te analizirati načine korištenja i upotrebe poslužiteljskih elektroničkih certifikata.