BSEP – Sertifikati

Sertifikat možemo posmatrati kao neki dokument, kao strukturu podataka, kako god hoćemo, u suštini to je neki dokument koji će reći ovaj javni ključ pripada toj i toj osobi ili tom i tom računaru. Poenta je da poveže javni ključ sa nekim imenom i prezimenom. Za to neko treba da garantuje. Kao što MUP garanutuje za ličnu kartu. U ovom slučaju to je Certificate Authority (CA) ili sertifikaciono telo.

CA može biti pravno lice ali nama niko ne brani da podignemo neki sistem i da se proglasimo za CA. On ima javni ključ koji je poznat svima. Obično tih CA-ova ima jako mnogo i kada instaliramo neki operativni sistem dobijamo CA-ove. CA će napraviti neki dokument u kome će staviti naš javni ključ, naše ime i prezime ili naš email, šta god, sve to će potpisati i tim potpisom će praktično garantovati da taj javni ključ pripada toj osobi. U tom dokumnetu imamo minimalno 3 stvari – javni ključ, kome pripada i digitalni potpis koji je CA napravio. Javni ključ CA-ja je opšte poznat, stoji svuda na netu, u okviru računara i nije nešto što može lako da se fejkuje.

CA hijerarhija ili lanac sertifikata

Na vrhu hijerarhije nalazi se CA koji se obično zove root CA. On je glavni. Obično postoji 2 do 3 nivoa ali može ih biti i više. Root CA je na primer na nivou univerziteta, subordinate CA je za svaki fakultet, ispod njega sertifikati za nastavnike i studente, ispod njih sertifikati koji se izdaju krajnjim korisnicima. Zašto se upošte pravi hijerarhija? Zbog podela odgovornosti. Na primer ako se kompromituje privatni ključ CA 4 (3. nivo hijerarhije), onda svi sertifikati koje je on izdao padaju u vodu, svi su kompromitovani. Ako se kompromituje CA od root CA svi sertifikati ispod njega padaju u vodu. Zato se pravi podela odgovornosti, u slučaju kompromitovanja javnog ključa nekog u hijerarhiji propada samo njegovo podstablo.

Da bi ovo funkcionisalo kako treba root CA treba da bude posebno zaštićen, tj njegov privatni ključ treba da bude posebno zaštićen. Koje mere zaštite mogu da se sprovedu? Jedna od njih je HSM (Higher Security Module). To je poseban hardverski uređaj na kome se čuva privatni ključ. Uređaj je takav da ključ ne može da se pročita sa njega. Ukoliko je potrebno da se nešto potpiše privatnim ključem mi te podatke koje treba potpisati šaljemo uređaju, on ih potpisuje i vraća nam odgovor.

Root CA je uglavnom uređaj koji je offline. Ako pričamo o fizičkom računaru to je računar koji nikada nije uštekan u mrežu. Taj računar se uključuje samo kada treba izgenerisati novi sertifikat.

Lanac sertifikata – od našeg krajnjeg, koji je izdat kao krajnjem korisniku sve do root CA-ja.

Ko potpisuje root CA? Svi root CA su self-signed tj. root CA ima privilegiju da sam sebe potpiše. Bez obzira da li je to neki internacionalni pa ga svi koristimo ili lokalni za našu firmu.

Browseri sadrže „root CA“ sertifikate.

Svaki sertifikat sadrži „CA flag“ koji govori da li vlasnik ima pravo da izdaje nove sertifikate tj. da li je vlasnik sertifikata takođe CA.

X.509 standard

Definiše šta tačno sertifikat treba da ima. Postoje 3 verzije ovog standarda. (v1, v2, v3). Jedno od polja je **version**.

Serial number – ovaj serijski broj mora biti jedinstven u okviru jednog CA.

Signature algorithm ID – koji algoritam je korišćen za potpisivanje

Issuer name – podaci o CA-ju (pronaći sertifikate u browseru)

Validity period – od/ do datumi kada važi sertifikat

Subject name – podaci o nama, ime i prezime, email, matični broj ...

Subject public key info – naš javni ključ

Verzija v2 uvodi 2 nova polja:

Issuer unique ID

Subject unique ID

Verzija v3 je dodala gomilu nekih ekstenzija.

Extensions - Ključne ekstenzije jesu namene ključa. Recimo da se jedan ključ koristi isključivo za digitalno potpisivanje dokumenta. Drugi setifikat može da sadrži ključ koji će se koristiti za šifrovanje, treći će se koristiti za autentifikaciju. Ono što se obično koristi jesu dve grupe ključeva. Jedni se koriste za digitalno potpisivanje a drugi se koriste za autentifikaciju. Polje za ekstenziju može da sadrži i url do sledećeg u lancu sertifikata.

Signature

Periodi validnosti se razlikuju po nivoima hijerarhije. Naš krajnji važi od godinu do 2 godine. Subordinate do root – vreme važenja raste. Npr onaj iznad našeg važi 5 godina, iznad njega 10 godina, a za root CA period važenja je uglavnom 20 godina.

Ideja **X.500 standarda** je bila da postoji hijerarhija država, lokalitet(grad), organizacije, organizacione jedinice, krajnjeg korisnika... Svaki od ovih čvorova idejno bi imao svoj CA. Ovo u praksi nije zaživelo, bilo bi previše složeno. Odavde potiče hijerarhijska organizacija imena.

Problem distribucije ključeva pretvoren je u problem distribucije imena. Problem ljudi sa istim imenom i prezimenom u istoj organizaciji. Kako ih razlikovati?

Povlačenje sertifikata – svaki CA ima listu povučenih sertifikata koje je on izdao. Problem je što se lista obično ažurira jednom u pola godine, ili na nekoliko meseci. Postoje i alternative – kasnije. CRL lista

Kada dobijemo neki dokument koji je digitalno potpisan nama treba sertifikat u kome se nalazi javni ključ kojim ćemo proveriti taj potpis. Prvo iz sertifikata izvadimo javni ključ, javnim ključem proverimo da li je dokument(npr. neki pdf) dobar. Ako je to dobro, onda proveravamo sertifikat, tj. da li je taj sertifikat važeći i koja je njegova namena, da li može da potpisuje pdf-ove. Kada smo proverili taj sertifikat treba da proverimo hijerarhiju CA-ova. Sertifikat na nižem nivou hijerarhije proveravamo javnim ključem onog na višem nivou hijerarhije, zato što je CA na višem nivou svojim privatnim ključem potpisao sertifikat na nižem nivou.

Sertifikat može da bude povučen ako nam je kompromitovan privatni ključ, pa svako može da potpisuje umesto nas. Kod povlačenja sertifikata je bitno vreme povlačenja. Sve što je potpisano pre kompromitovanja je ok, a nakon toga nije.

. – pdf sa vezbi - *Postoje dve tehnike provere da li je sertifikat povučen, i to su upotreba listi za povučene sertifikate (engl. Certificate revocation list; CRL), i upotreba protokola za onlajn proveru statusa sertifikata (engl. Online Certificate Status Protocol; OCSP). CRL pati od niza problema i Firefox je potpuno napustio dati pristup, te se uzda na OCSP [3].*

U svojoj osnovi, OCSP predstavlja zahtev za proveru statusa sertifikata čiji serijski broj je prosleđen, i odgovor koji govori da li je dati sertifikat povučen. – pdf sa vezbi -