Certifikati - X.509

Peter Škoda
0035102084
Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu

31. svibnja 2004.

Sadržaj

1. Uvod

Kada se javite na telefon, kako znate da je osoba koja vas je nazvala zaista ona kojom se predstavlja? Naravno, morate unaprijed znati nešto o toj osobi, npr. boju njenog glasa, ali to nije uvijek dovoljno. Često su potrebne sigurnije metode. Morate biti sigurni u identitet sugovornika prije nego razgovor zaista započne.

Srž problema je *identitet* i *izvornost*. Oba sugovornika moraju na neki način moći jedan drugome ustanoviti identitet i taj identitet mora biti izvoran.

Digitalni certifikat je registrirani, a prema tome i izvorni, identitet. Certifikat X.509 uspostavlja identitet i izvornost.

2. Digitalni potpis i certifikat

Provjera je bilo koji postupak kojim se dolazi do spoznaje o izvornosti informacije i tu se primjenjuje digitalni potpis.

Digitalnim potpisom Ivan može potpisati elektronički dokument i poslati ga Ani. Ana će uz pomoć Ivanovog digitalnog potpisa moći odrediti je li dokument izvoran. Za stvaranje digitalnog potpisa koriste se dvije tehnike - *kriptografija javnog ključa* i *računanje* hash *sume*.

2.1. Kriptografija javnog ključa

Za kriptografiju javnog ključa potrebna su dva ključa: *javni ključ* i *privatni ključ*. Javni ključ je poznat svima i može se slobodno dijeliti, dok se privatni ključ mora čuvati tajnim. Taj par ključeva je u jedinstvenom odnosu koji omogućuje da se poruka koja je šifrirana jednim ključem dešifrira drugim ključem.

Ivan objavi svoj javni ključ tako da je dostupan svima. Ana sada može šifrirati dokument Ivanovim javnim ključem, ali samo Ivanov privatni ključ može dešifrirati taj dokument. Taj privatni ključ je tajni i ima ga samo Ivan.

2.2. Računanje *hash* sume

Računanje *hash* sume možemo opisati kao sažimanje. To je jednoznačna funkcija koja sažme poruku bilo koje duljine na poruku fiksne duljine. Postupak se može primijeniti na bilo koju vrstu podataka. Bez obzira na veličinu dokumenta, *hash* suma je uvijek iste duljine i dokument ne može biti rekonstruiran iz nje. Postoje razni *hash* algoritmi - npr. MD5 i SHA.

2.3. Digitalni potpis

Ivan šalje poruku Ani i želi da ona provjeri izvornost poruke. Ivan želi da Ana može odrediti je li poruku poslao on i da li je na putu bila promijenjena.

Ivan prvo izračuna *hash* sumu poruke. Zatim je *hash* suma šifrirana Ivanovim privatnim ključem i rezultat je digitalni potpis. Digitalni potpis se doda u poruku i pošalje zajedno s njom. Poruka može, ali ne mora, biti šifrirana. Sada Ana može provjeriti izvornost poruke. Prvo se potpis dešifrira Ivanovim javnim ključem, što daje *hash* sumu koji je pošiljatelj (Ivan) izračunao. Zatim Ana izračuna *hash* sumu poruke i usporedi sa *hash* sumom pošiljatelja. Ako su te dvije *hash* sume jednake, dokazano je sljedeće:

1. pošiljatelj je Ivan jer samo Ivan može šifrirati potpis i
2. poruka nije bila promijenjena na putu do Ane.

Potvrđeni su i identitet i izvornost.

2.4. Certifikati

Da je Ivan zaposlen u nekoj većoj organizaciji imao bi mnogo dodatnog posla s osvježavanjem svoje baze javnih ključeva svaki put kad bi se nešto promijenilo ili zaposlio novi radnik, a isto biti bilo i za sve Ivanove kolege.

U većim organizacijama potrebna je osoba zadužena za izdavanje certifikata - *certifikator*. Neka je Igor certifikator u organizaciji. Tada je Igor taj koji izdaje certifikate za svakoga u organizaciji.

Ivan od Igora zatraži certifikat. Igor unese podatke o Ivanu i njegovom javnom ključu i izda certifikat. Ana je također od Igora primila certifikat. Sada ona može provjeriti Ivanov certifikat, a time i njegov identitet, tako da dešifrira certifikat certifikatorovim javnim ključem koji otvara potpisane informacije o Ivanu i njegovom javnom ključu.

Osim problema raspodijele, certifikatom se rješava i problem izvornosti javnih ključeva. Zamislimo da Ana i Ivan nikad prije nisu komunicirali. Kako Ivan zna da je javni ključ koji je primio zaista Anin? Što ako taj javni ključ zapravo pripada nekoj zlonamjernoj trećoj osobi koje želi presretati i manipulirati komunikaciju između Ane i Ivana? Ovdje ulazi Igor (certifikator), osoba od povjerenja, koji izdaje certifikate i jamči izvornost javnih ključeva.

Certifikati pod nekim uvjetima mogu postati nevažeći. Postoji mnogo razloga za opoziv certifikata, npr. istekao rok valjanosti, promjena para ključeva za digitalni potpis, itd.

Ivan je odlučio promijeniti svoj par ključeva koji koristi za digitalni potpis. Za taj novi par ključeva zatražio je novi certifikat, a za stare ključeve i njihov certifikat je zatražio da se proglase nevažećim. Igor će stari certifikat staviti na popis opozvanih certifikata i izdati Ivanu novi certifikat za novi ključ.

3. ITU X.509

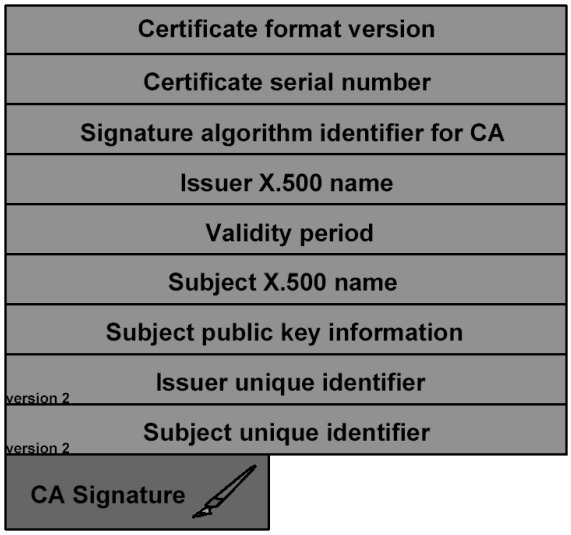
Na koji način će Igor - certifikator - formirati certifikate? Postoji mnogo mogućih načina, a jedan od načina je propisan preporukom ITU X.509.

ITU X.509 je preporuka da digitalne certifikate. Prvi puta je objavljena 1988. kao dio ITU X.500 preporuke za imeničke servise. Kasnije su objavljene još dvije verzije preporuke. Verzija 2 objavljena je 1993., a sada aktualna verzija 3 je objavljena 1996.

ITU X.500 je preporuka za baze podataka o entitetima (osobe, računala, programi...) namijenjena za globalnu uporabu. Zamislite globalni telefonski imenik. Svaka organizacija bi upravljala dijelom baze podataka koja je povezana s entitetima tih organizacija. X.500 nije šire prihvaćen u praksi, ali X.509 se ukorijenio i sada je vodeća osnova za usluge certifikata.

3.1. X.509 certifikat verzije 1 i 2

U ovom dijelu će biti opisana polja certifikata objavljena u verzijama 1 i 2 preporuke za certifikate. Struktura certifikata je prikaza na slici 1.



Slika 1.: Struktura certifikata X.509.

Version

Version polje sadrži informaciju o verziji formata X.509 certifikata - verzija 1, 2 ili 3.

Serial number

Polje *serial number* sadrži jedinstvenu numeričku oznaku za svaki certifikat koji je izdan od certifikatora. Ukratko - serijski broj. Serijski broj je kritičan pri opozivu certifikata. Tada se šalje popis serijskih brojeva certifikata i taj je popis certifikator potpisao. Stoga serijski broj *mora biti jedinstven* u domeni koju pokriva certifikator.

Signature algorithm

U polju *signature algorithm* se određuje algoritam koji certifikator koristi za potpisivanje certifikata. Algoritam je određen identifikacijskim brojem koji je registriran pri međunarodno priznatoj standardizacijskoj organizaciji, npr. ISO. Taj broj određuje algoritam javnog ključa kao i *hash* algoritam, npr. RSA i MD5.

Issuer X.500 name

Poljem *issuer X.500 name* određuje se X.500 razlikovno ime (*distingushed name* - DN) certifikatora koji je izdao certifikat. Npr. *c=HR*, *o=FER* bi se koristio kao DN certifikatora koji izdaje certifikate za zaposlenike Fakulteta elektrotehnike i računarstva u Republici Hrvatskoj.

Validity period

Poljem *validity period* određuju se datumi i vremena početka i kraja roka valjanosti certifikata. Svaki put kada se certifikat upotrijebi provjerava se je li certifikat unutar roka valjanosti.

Subject X.500 name

Poljem *subject X.500 name* određuje se X.500 DN entiteta koji je vlasnik privatnog ključa za koji se izdaje certifikat. Npr. *c=HR*, *o=FER*, *cn=Peter Škoda* bi bio X.500 DN Petera Škoda, studenta Fakulteta elektrotehnike i računarstva u Republici Hrvatskoj.

Subject public key information

U polju *subject public key information* daju se dva važna podatka:

1. javni ključ za koji se izdaje certifikat i
2. identifikacijski broj algoritma koji se koristi uz javni ključ.

Identifikacijski broj algoritma određuje i algoritam javnog ključa i *hash* algoritam.

Issuer unique identifier (verzija 2)

Polje *issuer unique identifier* je propisano u verziji 2 preporuke. To polje ne mora biti korišteno. U polju se određuje niz bitova koji jedinstveno identificiraju *issuer X.500 name*, u slučaju da je jedan X.500 DN kroz vrijeme bio dodijeljen više nego jednom certifikatoru.

Subject unique identifier (verzija 2)

Polje *subject unique identifier* je propisano u verziji 2 preporuke. To polje ne mora biti korišteno. U polju se određuje niz bitova koji jedinstveno identificiraju *subject X.500 name*, u slučaju da je jedan X.500 DN kroz vrijeme bio dodijeljen više nego jednom entitetu. Npr. Ivan Novak napusti FER, a nekoliko mjeseci kasnije na FERu se zaposli neki drugi Ivan Novak.

3.2. X.509 certifikat verzija 3

U verziji 3 preporuke X.509 uvodi se mehanizam "proširivanja" certifikata radi uključivanja dodatnih informacija. "Proširenje" se odnosi na dodatna polja u certifikatu. U preporuci se definiraju *standardna proširenja* za neke šire primjenjiva proširenja verzije 2 preporuke. Ali certifikati nisu ograničena samo na standardna proširenja već svatko može registrirati proširenje kod odgovarajućih ustanova (npr. ISO). Očekuje se da će se kroz vrijeme nova šire upotrebljavana proširenja dodati skupu standardnih proširenja.

3.2.1. Struktura proširenja

Svako proširenje se sastoji od tri polja:

1. *type* – tip,
2. *critcality* – kritičnost i
3. *value* – vrijednost.

Struktura proširenja je prikazana na slici 2.

Slika 2.: Struktura proširenja certifikata.

Polje *extension type* definira tip podatka u polju *extension value*. Tip može biti tekst, numerička vrijednost, datum, grafika ili neka složena struktura podataka. Poželjno je da su svi tipovi registrirani kod neke međunarodno priznate standardizacijske organizacije.

Polje *extension criticality* je jednobitna oznaka. Kada je polje označeno kao kritično znači da polje *extension value* sadrži podatak toliko važan da se ne smije zanemariti. Ako se kritično proširenje ne može obraditi, certifikat se mora odbaciti.

Potrebno je istaknuti razliku između kritičnog proširenja i nužnog podatka u certifikatu. Određeno proširenje može biti nužno nekoj aplikaciji, ali to ne znači da takvo polje mora biti označeno kao kritično. Kritična polja su namijenjena samo za podatke tolike važnosti da ga moraju razumjeti sve aplikacije, npr. informacije važne za sprečavanje pogrešne uporabe certifikata. Stoga je velika većina proširenja nekritična. Kritična proširenja se trebaju dodavati s oprezom i tek nakon pažljivog razmatranja jer mogu prouzročiti probleme pri korištenju certifikata.

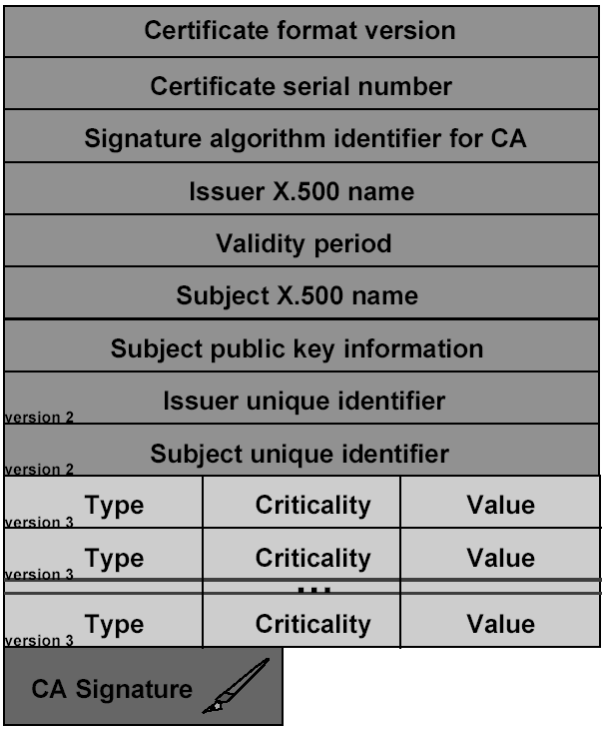
Polje *extension value* sadrži podatke. Tip podataka je definiran u polju *extension type*.

Polja X.509 verzije 3 certifikata su prikazana na slici 3.

3.2.2. Standardna proširenja

Standardna proširenja certifikata podijeljena su u sljedeće četiri grupe:

1. Informacije o ključu
   Polja u ovoj skupini sadrže informacije o namjeni certifikata i para ključeva.
2. Informacije o politici (*policy*)
   Polja u ovoj skupini daju mehanizam koji omogućuje certifikatoru da definira način na koji se određeni certifikat mora koristiti i interpretirati.



Slika 3.: Struktura certifikata X.509 verzije 3.

3. Atributi korisnika i certifikatora
   Polja u ovoj skupini daju dodatne mehanizme kojima se određuju informacije za identifikaciju korisnika i certifikatora.

4. Ograničenja na stazu certifikacije
   Polja u ovoj skupini daju mehanizme kojima certifikator upravlja i ograničava povjerenje "prošireno" na treće osobe. Primjenjuje se pri *cross-certification*.

Pojedinačna standardna proširenja ovdje neće biti razmatrana. Detaljan opis standardnih proširenja možete naći u [1].

4. Popis pojmova

Asimetrični kriptografski algoritam
: Kriptografski algoritam koji koristi dva različita ključa. Ključevi su u takvom odnosu da se podaci šifrirani jednim ključem mogu dešifrirati samo drugim ključem.

Autentifikacija – Authentication
: Proces utvrđivanja identiteta osobe ili integriteta određene informacije. Osoba se identificira digitalnim certifikatom. Kod poruke, autentifikacija uključuje utvrđivanje njena izvora, te da nije mijenjana ili zamijenjena u prijenosu.

Certifikat – Certificate
: Elektronički dokument koji identificira računalo, osobu, poduzeće ili certi-

fikatora. Sadrži ime ili identifikaciju vlasnika certifikata, njegov javni ključ, period valjanosti certifikata, te digitalni potpis izdavača certifikata.

Certifikator – Certification Authority
Osoba koja izdaje certifikat.

Cross-certification
Postupak u kojem jedan certifikator uspostavi povjerenje prema drugom certifikatoru koji nije odmah do njega u hijerarhiji. Certifikati iz domene drugog certifikatora tada postaju valjani u domeni prvog certifikatora.

Digitalni potpis – Digital signature
Elektronička zamjena rukom pisanom potpisu, nije digitalizirana slika ručnog potpisa. Omogućava identifikaciju sudionika komunikacije i integritet podataka. Za provjeru identiteta i integriteta se koristi javni ključ sadržan u certifikatu.

***Hash* algoritam – Hash algorithm**
Postupak kojim se iz originalne poruke dobije podatak fiksne dužine (bez obzira na dužinu poruke) koja se pridodaje poruci. Taj niz bitova jednoznačno definira poruku pa svaka promjena sadržaja originalne poruke uzrokuje promjenu sadržaja *hasha*. Poruka se ne može rekonstruirati iz *hasha*.

ITU X.500
Norma za elektronički imenik.

ITU X.509
Norma, opisuje strukturu elektroničkog certifikata.

Integritet podataka
Sigurnost da podaci u prijenosu ili obradi nisu uništeni ili promijenjeni.

Javni ključ – Public Key
Ključ za šifriranje i dešifriranje podataka asimetričnim kriptografskim algoritmima. Poznat je svakome tko želi komunicirati s vlasnikom ključa. Koristi se za provjeru digitalnog potpisa.

Kriptografija javnog ključa – Public Key Criptography
Asimetrična kriptografija. Koristi par ključeva - tajni za izradu digitalnog potpisa, te javni za njegovu provjeru.

Par ključeva – Public key pair
Privatni i javni ključ koji se koriste u kriptografiji javnog ključa.

Privatni ključ – Private key
Ključ za šifriranje i dešifriranje podataka asimetričnim kriptografskim algoritmima. Drži se tajnim i poznat je samo vlasniku.

Provjera – Verification
Proces ispitivanja poruke ili integriteta digitalnog potpisa računanjem *hash* sume na strani pošiljatelja i primatelja poruke, te uspoređivanjem rezultata.

Proširenje – Extension
Dodatno polje X.509 certifikata. Postupak proširenja certifikata je propisan u preporuci ITU X.509 verzije 3.

Standardna proširenja – Standard extensions
Proširenja certifikata definirana u preporuci ITU X.509 verzije 3.

Literatura

[1] Ian Curry: Version 3 X.509 Certificates, Entrust Techonologies, 1996, http://www.entrust.com, 10.05.2004

[2] Peter Bærentzen: X.509 digital certificates – the digital signature, Intermate A/S, 2003, http://www.intermate.com, 17.05.2004

[3] Todd Sunstead: Construct secure networked applications with certificates, http://www.javaworld.com, 17.05.2004

[4] X.509 certificates (Linktionary term), http://www.linktionary.com, 10.05.2004

[5] X.509 Certificates and Certificate Revocation Lists (CRLs), http://java.sun.com, 15.05.2004

[6] OpenPGP and X.509, http://www.itsecurity.com, 17.05.2004

[7] Elektroničko poslovanje – popis pojmova, http://www.hgk.hr, 25.05.2004