Informaciona bezbednost

Public Key Infrastructure

dr Milan Stojkov

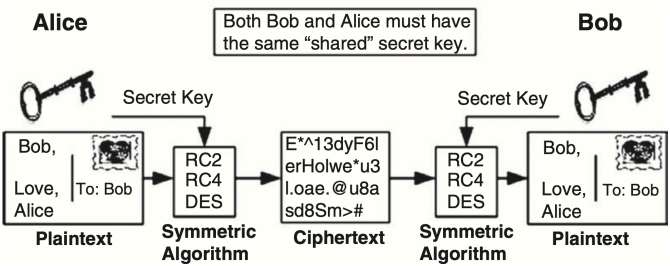
Katedra za informatiku

2022.

Fakultet tehničkih nauka
Univerzitet u Novom Sadu

Komunikacija pomoću simetričnih algoritama

1. Alice i Bob dogovore algoritam
2. Alice i Bob dogovore ključ
3. Alice svoju poruku šifruje dogovorenim algoritmom i ključem
4. Alice šalje šifrirani tekst Bobu
5. Bob dešifruje poruku istim algoritmom i ključem



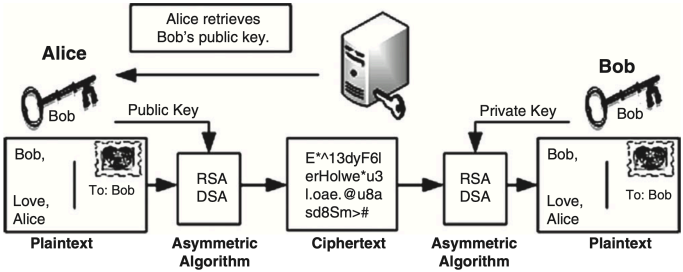
Slika preuzeta iz: *Computer Security Handbook*, Seymour Bosworth, M. E. Kabay, Eric Whyne, Wiley, 2014.

Komunikacija pomoću simetričnih algoritama - Mane

1. Mora se nekako obaviti razmena ključeva jer se koristi isti
2. Manjkavost pri obezbeđivanju poverljivosti, kontrole ili autentičnosti
   - Svako sa simetričnim ključem može da šifrira izvornu poruku i obrnuto

Komunikacija pomoću asimetričnih algoritama

1. Alice uzima Bobov javni ključ iz KDC
2. Alice šifruje svoju poruku Bobovim javnim ključem
3. Alice šalje šifrovanu poruku Bobu
4. Bob dešifruje poruku svojim tajnim ključem



Slika preuzeta iz: *Computer Security Handbook*, Seymour Bosworth, M. E. Kabay, Eric Whyne, Wiley, 2014.

Prednosti asimetričnih algoritama

1. Zahteva se upravljanje sa manje ključeva
   - Svaka strana (n) ima par ključeva, tako da je ukupan broj ključeva $2n$ umesto n^2
2. Privatni ključevi ne moraju da se distribuiraju drugoj strani
   - sistemi koji koriste asimetrične ključeve treba da demonstriraju integritet i autentičnost javnog ključa
   - to se postiže potpisivanjem treće strane kojoj se veruje
3. Pošto se tajni ključevi ne prenose preko mreže, ne mogu se tako lako kompromitovati čak i kada javni ključevi treba da se promene
4. Javni ključevi svih učesnika u komunikaciji se mogu koristiti da se šifrira privremeni ključ (session key) da se izbegne veće računarsko opterećenje sistema koji koristi asimetrične algoritme
5. Digitalni potpisi funkcionišu po ovom principu i predstavljaju osnovu za dokazivanje neporecivosti

Asimetrični VS Simetrični

Tip	Prostor ključeva	Brzina
Asimetrični	Redak	Spori
Simetrični	Gust	Brzi

Kombinacija oba pristupa

- Bezbedna razmena dokumenata
  - Za dokumente se bira simetrični algoritam i generiše nasumični ključ
  - Dokument se šifrira
  - Simetrični ključ se sifrira asimetričnim javnim ključem svakog od primaoca i dodaje se u zaglavlje dokumenta
- Digitalno potpisivanje dokumenata
  - Koristi se hash algoritam za kreiranje hash vrednosti dokumenta
  - Hash se šifrira (potpisuje) tajnim ključem potpisnika i dodaje uz dokument
  - Javni ključem potpisnika se dešifruje (verifikuje) hash koji služi za proveru integriteta dokumenta

Potreba za infrastrukturom javnih ključeva

- I za digitalno potpisivanje i za šifrovanje mora se koristiti odgovarajući javni ključ kako bi se osigurala bezbednost
- Mehanizam za distribuciju i korišćenje javnih ključeva zove se infrastruktura javnih ključeva - *Public Key Infrastructure* (PKI)
- Potpisanim javnim ključem se postiže poverenje inherentno ako je potpisnik neko kome se veruje
- Postojanjem jednog popisnika kome svi veruju (certificate authority) obezbeđuje se poverenje milionima sertifikata
- Pritom poverenje ne mora biti apsolutno već može biti kontekstualno (npr. sertifikatu potpisanom od strane poslodavca može se verovati samo u delu koji ima veze sa zaposlenjem, ne u delu koji ima veze sa kreditnom karticom)

Digitalni sertifikati

- Tehnika koja je skalabilna koristi sertifikate sa javnim ključevima koji su izdati od potpisnika kome svi veruju (CA)
- CA izdaju sertifikate sa javnim ključem raznim entitetima tako što pakuju zajedno informacije o time entitetima i potpisuju ih svojim tajnim ključem
- Generalno prihvaćeni standard za sertifikate sa javnim ključevima je X.509 verzija 3
- X.509 sertifikati su izraženi specijalnom binarnom notacijom - Abstract Syntax Notation 1 (ASN.1)
- Kako bi se poslali e-mailom, sertifikati su obično MIME (Base64) enkodovani kako bi se binarna reprezentacija predstavila ASCII znakovima

Digitalni sertifikati

- Svaki CA sertifikat može da sadrži:
  - Verzija sertifikacionog standarda
  - Serijski broj sertifikata (jedinstven za svaki sertifikat izdat od strane CA)
  - Algoritam i pridruženi parametri koje koristi CA za potpisivanje sertifikata
  - Ime CA
  - Period validnosti sertifikata
  - Ime subjekta kome se izdaje sertifikat
  - Javni ključ subjekta, algoritam i pridruženi parametri
  - Jedinstveni identifikator CA (opciono)
  - Jedinstveni identifikator subjekta (opciono)
  - Ekstenzije povezane sa sertifikatom (opciono)
  - Digitalni potpis CA

Digitalni sertifikati

- Subjekti kojima se izdaju sertifikati moraju imati javni ključ CA kako bi mogli da verifikuju digitalne potpise
- Subjekti moraju da veruju javnom ključu CA (koji su dobili tokom procesa registracije)
- Kada se potpisi verifikuju, svi mogu koristiti ime i javni ključ subjekta u sertifikatu i verovati informacijama koje se nalaze tu jer veruju CA

Certificate Revocation List

- U određenim situacijama CA mora da povuče vezu između subjekta i njegovog javnog ključa
  - Npr. tajni ključ subjekta je kompromitovan
- Pošto je sertifikat elektronski objekat koji može da postoji na više mesta u isto vreme, nije praktično niti moguće da se svi primerci povuku ili obrišu
- Da bi se invalidirao sertifikat, CA kreira listu nevalidnih sertifikata - *Certificate Revocation List* (CRL)
- Svi koji koriste subjektov sertifikat moraju da konsultuju CRL pre korišćenja javnog ključa
- Ako je sertifikat u CRL, javni ključ se ne sme koristiti
- CA potpisuje CRL da dozvoli svima da verifikuju njen integritet i autentičnost

Certificate Revocation List

- Ključne informacije koje X.509 verzija 2 CRL sadrži su:
  - Verzija CRL standarda
  - Algoritam i pridruženi parametri koje koristi CA za potpisivanje sertifikata
  - Ime CA
  - Vreme izdavanja CRL
  - Vreme izdavanja sledeće CRL (opciono)
  - Lista povučenih sertifikata (za svaki sertifikat):
    - Serijski broj sertifikata
    - Vreme kada je CA obavešten o povlačenju
    - Ekstencije povezane sa povučenim sertifikatom (opciono)
  - Ekstenzije povezane sa CRL (opciono)
  - Digitalni potpis CA

Certificate Revocation List

- Kao i X.509 sertifikati, CRL su predstavljene u ASN.1 formatu
- Postoji nekoliko vrsta CRL:
  - *Full and complete CRL*
  - *Authority revocation list (ARL)*
  - *Distribution-point CRL*
  - *Delta CRL*

Full and complete CRL

- Sadrži sve informacije o povlačenju svih sertifikata izdatih od CA
- Retko se viđa
- Umesto toga CRL uključuje samo informacije o povučenim sertifikatima koji trenutno nisu validni, ne uključuje istekle sertifikate

Authority revocation list (ARL)

- ARL je CRL koja sadrži informacije o povlačenju za sve CA sertifikate izdate od CA
- ARL je podskup CRL za sertifikate koji su izdati drugim CA
- Obično je kratka jer CA sertifikuje manje CA nego drugih neCA subjekata
- Za sve sertifikate sem jednog samo ARL treba da se proveri jer su svi sem poslednjeg sertifikata u lancu izdati od strane CA

Distribution-point CRL

- Predstavlja mehanizam sa nekoliko funkcija:
  - Može da replicira CRL
  - Može da sumira informacije od više CA u jednu CRL
  - Može da particioniše informacije o povlačenju u manje delove

Delta CRL

- Redukuje veličinu CRL objavljujući samo razlike u povučenim sertifikatima u odnosu na prethodnu CRL (baznu CRL)
- Mehanizam je primenjiv na sve prethodne vrste CRL
- Da bi se proverile informacije o povlačenju moraju se proveriti sve delte i bazni CRL

Alternativni pristupi za povlačenje ključeva

- Drugi mehanizam podrazumeva odlaganje procesiranja informacija o povlačenju na server kroz *Online Certificate Status Protocol* (OCSP) ili *Simple Certificate Validation Protocol* (SCVP)
- Treći mehanizam omogućava korisnicima da provere status pojedinačnog sertifikata iz direktorijuma i dozvoljava CA da ažurira status tog sertifikata u direktorijumu
- Četvrti mehanizam omogućava CA ili drugom pouzdanom serveru da organizuje informacije o povlačenju u strukturu B-stabla

Online Certificate Status Protocol

- Kada zainteresovana strana zatraži validnost sertifikata, OCSP zahtev se šalje OCSP Responderu
- OCSP Responder proverava određeni sertifikat kod pouzdanog autoriteta za sertifikaciju i OCSP odgovor se šalje nazad sa odgovorom **good**, **revoked** ili **unknown**

Online Certificate Status Protocol

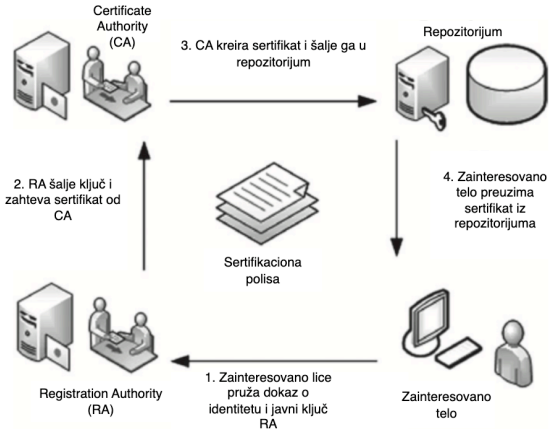
- OCSP nudi veću efikasnost u odnosu na CRL za veće deloymente
- OCSP serveri konzumiraju CRL-ove kako bi pružili indikaciju da li je sertifikat povučen
- OCSP mora da osveži CRL po nekom rasporedu kako bi osigurao da pruža ažurne informacije o povlačenju
- Napredni OCSP proizvodi pružaju mogućnost OCSP-u da direktno upita bazu podataka CA
- Ovo omogućava povlačenje u realnom vremenu i stavljanje sertifikata na belu listu (*certificate whitelisting*)
- Stavljanje sertifikata na belu listu pruža dodatnu bezbednost krajnjim entitetima i potvrđuje da je CA zaista izdao sertifikat
- U poređenju sa CRL, OCSP zahtevi sadrže daleko manje podataka, pa su lakši za rukovanje jer sistemi ne moraju da preuzimaju najnoviju listu svakog povučenog potpisa kad god se proverava sertifikat

OCSP i SCVP

- Ovi pristupi imaju nekoliko mana:
  - Pošto se informacije o povlačenju proizvode na serveru, komunikacioni kanal između zainteresovane strane i servera mora biti obezbeđen, uglavnom korišćenjem digitalnih potpisa
  - Pošto se informacije o povlačenju proizvode na serveru, šema zahteva pouzdan i bezbedan server
  - Povlačenje javnog ključa servera zahteva metod za proveru statusa javnog ključa servera
  - Mora postojati bezbedan mehanizam da CA pruži informacije serveru kojem se veruje, tj. CA treba da zna da li je informacija stigla do servera ili ne
  - Ne postoje standardi za CA koji bi definisali mehanizme za prenos informacija o povlačenju do servera od poverenja

Enterprise PKI

- Korišćenje sertifikata je jednostavno, ali uspostavljanje poverenja da bi se utvrdilo da je sertifikat validan je kompleksno



Enterprise PKI

- Svaka grupa korisnika koju pokriva jedan CA naziva se domen
- Svi korisnici unutar domena dobijaju sertifikate sa javnim ključevima od strane odgovarajućeg CA
- CA je odgovoran za generisanje sertifikata korisnika i za CRL
- CA postavlja potpisane objekte u repozitoriju odakle zainteresovana tela (vlasnici) mogu da ih preuzmu
- CA takođe arhivira sertifikate i CRL za slučaj da su potrebni u budućnosti za rešavanje sporova između vlasnika sertifikata i korisnika

Registracioni autoritet (RA)

- Registracioni autoritet (RA) je predstavnik CA kome se veruje i koji je odgovoran za autentifikovanje klijenata
- Odgovornosti RA:
  - Autentifikuje identitet korisnika (npr. RA može da zahteva validnu ličnu kartu ili pasoš)
  - Preuzima javni ključ od korisnika
  - Predaje javni ključ CA korisniku
  - Šalje zahtev za kreiranje sertifikata CA (obično kreira e-mail koji sadrži ime i javni ključ korisnika, digitalno potpisuje poruku i šalje CA)

Sertifikaciona polisa (CP)

- Da bi se obezbedila PKI potrebno je da:
  - Tajni ključevi budu poverljivi
  - Tajne ključeve koriste samo vlasnici
  - Se obezbedi poverenje u integritet javnog ključa CA
  - Inicijalna autentifikacija korisnika bude jaka da se ne desi krađa identiteta u procesu kreiranja sertifikata
  - Sistemi i aplikacije koje koriste CA i RA budu zaštićeni (tampering)
  - Zahtevi za nivo poverenja moraju biti jasno definisani

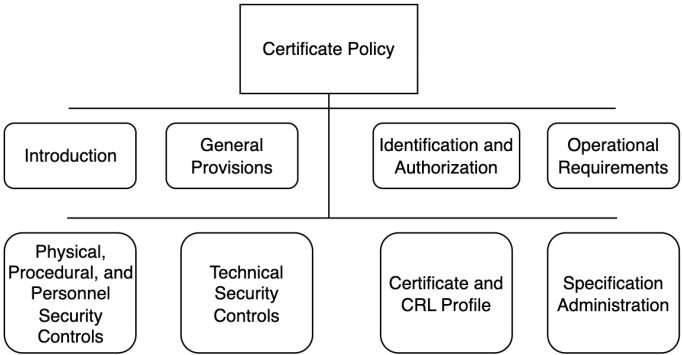
Sertifikaciona polisa (CP)

- X.509 standard definiše sertifikacionu polisu kao *imenovani skup pravila koji ukazuje na primenjivost sertifikata na određenu zajednicu i/ili klasu aplikacija sa zajedničkim bezbednosnim zahtevima*
- Sertifikaciona polisa mora da specificira šta će biti sadržaj sertifikata (i osnovnih polja i ekstenzija)
- Bilo šta što nije specificirano polisom ne sme se naći u sertifikatu
- Korisnik sertifikata može da koristi CP da odluči da li su sertifikat i veza između sertifikata i vlasnika dovoljno pouzdani za određenu aplikaciju

Certification Practice Statement (CPS)

- *Izjava o praksama koje sertifikaciono telo primenjuje u izdavanju sertifikata*
- CP definiše bezbednosne zahteve i obaveze za PKI, a CPS opisuje kako se ti zahtevi zadovoljavaju
- RFC 3647 sadrži uputstva za kreiranje CP i CPS

Certification Practice Statement (CPS)



Slika preuzeta iz: *Computer Security Handbook*, Seymour Bosworth, M. E. Kabay, Eric Whyne, Wiley, 2014.

Globalni PKI

- Principi koji se primenjuju za implementaciju jednog PKI mogu se proširiti da podrže globalni PKI koji se sastoji od više CA koji mogu da sertifikuju druge CA
- Način na koji CA sertifikuju jedni druge zove se model poverenja (*trust model*) ili graf poverenja (*trust graph*)

Model Poverenja - Trust Model

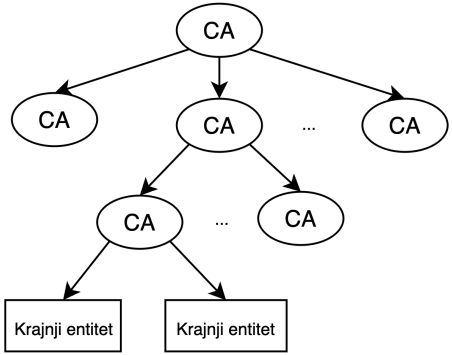
- *Trust model* se može posmatrati kao lanac gde je rep CA koji izdaje sertifikat a glava subjekat kojem se izdaje sertifikat
- Subjekat može biti drugi CA ili drugi krajnji entitet
- Da bi se proverio lanac sertifikata, potrebno je početi od glave i pratiti lanac do CA

Model Poverenja - Trust Model

- Primeri *trust modela*
  - Striktna hijerarhija (*strict hierarchy*)
  - Hijerarhija (*hierarchy*)
  - Most (*bridge*)
  - Višestruke tačke (sidra) poverenja (*multiple trust anchors*)
  - Mreža (*mesh*)
  - Kombinacija prethodnih

Striktna hijerarhija

- Predstavlja strukturu tipa stabla sa jednom korenom
- U ovom modelu da bi dve strane komunicirale bezbedno, potreban im je javni ključ zajedničkog pretka kao tačka poverenja
- Lanac sertifikata zahteva da strane imaju zajedničkog pretka

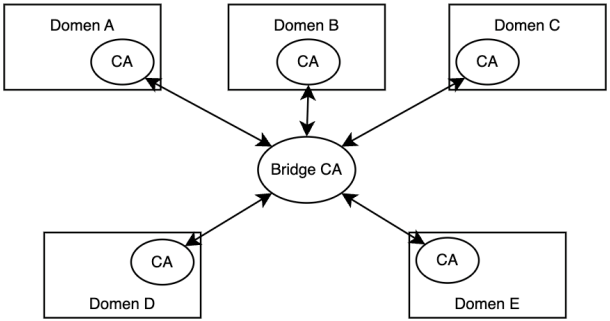


Hijerarhija

- U (nestriktnoj) hijerarhiji podređeni CA sertifikuju svoje nadređene
- Bilo koji CA može biti tačka poverenja (pošto je sada hijerarhija tipa grafa koji je usmeren)
- Obično je lokalni CA ta tačka (onaj CA koji je izdao sertifikat subjektu)

Most (Bridge)

- U ovom modelu jedan CA se kros-sertifikuje sa svakim CA iz drugih domena
- CA iz domena je tačka poverenja odakle se kreće, ne most

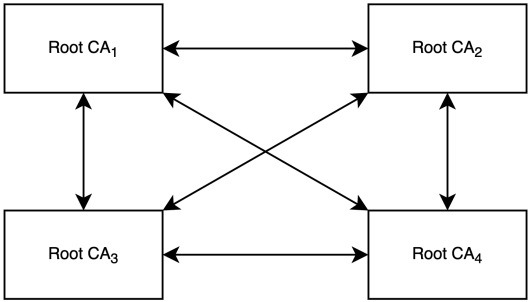


Višestruke tačke poverenja

- Zainteresovana strana dolazi do javnih ključeva CA na bezbedan način i koristi ih kao početnu tačku poverenja
- Ovaj pristup se koristi kada CA ne može ili ne želi da kros-sertifikuje sertifikate iz drugih domena a zainteresovana strana hoće da komunicira sa subjektom kojem je taj CA izdao sertifikat

Mreža (Mesh)

- Svaki root CA potpisuje svaki drugi root CA
- Ne postoje posebna pravila ili šabloni za proveru poverenja CA
- Zove se često i *web of trust*
- Kod ovog pristupa svaki učesnik mora da veruje drugom učesniku
- Nije skalabilan za veliki broj korisnika



Koju arhitekturu PKI odabrati?

- Da li koristiti jedan CA ili više zavisi od više faktora:
  - Organizacione politike
  - Veličine sertifikacionog lanca
  - Broja subjekata kojima se izdaju sertifikati
  - Rasporstranjenost subjekata kojima se izdaju sertifikati
  - Količina povučenih sertifikata

Problem međusobne sertifikacije

- Do međusobne sertifikacije (kros-sertifikacije) dolazi kada se dva CA međusobno sertifikuju izdavajući sertifikate jedno drugom
- Ovde postoje dva problema:
  - Ako dva domena koriste drugačije proizvode, njihovi CA možda ne mogu da razmene informacije koje su potrebne za međusubnu sertifikaciju
  - CA koji izdaje sertifikat drugom CA mora da proveri da li je sve u skladu sa sertifikacionom polisom (CP)

Interoperabilnost PKI

- Nekoliko faktora utiče na interoperabilnost PKI:
  - Putanju poverenja (*trust path*) je moguće konstruisati
  - Korišćeni algoritmi moraju biti poznati i kompatibilni
  - Formati sertifikata i CRL moraju biti usaglašeni
  - Sertifikacione polise moraju biti usaglašene
  - Nazivi subjekata moraju biti različiti

Reizdavanje ključeva

- Sertifikati javnog ključa imaju definisan period važenja
- Kada istekne period važenja, potrebni su novi sertifikati (sertifikatu se treba dodeliti novi javni ključ)
- Dva osnovna razloga zašto sertifikati javnog ključa imaju ograničen vek trajanja:
  - Životni vek privatnog ključa treba biti dovoljno kratak da bi se mitigovale potencijalne pretnje kriptoanalizom
  - Može biti pomoć u kontroli veličine CRL-a jer nijedan sertifikat ne izlazi iz CRL-a dok ne istekne
- Subjekat može da zatraži od CA zanavljanje ključa
- CA može zanavljanje da odradi automatski

Oporavak ključeva

- Ponekad tajni ključ (npr. na hard disku, pametnoj kartici, itd.) može biti oštećen ili subjekat može zaboraviti lozinku povezanu sa ključem
- Tehnike oporavka ključeva su dizajnirane da zadovolje ove hitne potrebe za pristupom šifrovanim informacijama
- Same po sebi, one uvode *backdoor* pristup za ključeve i nameću dodatne troškove
- Potreba za obezbeđivanjem oporavka ključa treba pažljivo da se izbalansira u odnosu na potencijalne troškove i složenost
- Dva najpopularnija mehanizama za oporavak ključeva su:
  - Deponovanje ključeva (*key escrow*) - subjektov privatni ključ za dešifrovanje se pruža trećoj strani od poverenja koja se zove agent za oporavak ključeva (*key recovery agent* - KRA)
  - Enkapsulacija ključa - subjekat šifrira ključ za šifrovanje (simetrični za bezbednu komunikaciju) koristeći javni ključ KRA tako da KRA može dešifrovati podatke

Cena PKI

- Čini se da je uspostavljanje PKI skupo, ali te troškove treba uporediti sa alternativama
- Ne postoji drugi pristup osim kriptografije da se zaštite podaci koji se prenose preko mreže koja nepouzdana
- Izbor se svodi na simetrične i asimetrične algoritme
- Pored poteškoća za distribuciju simetričnih tajnih ključeva, ovakvi sistemi zahtevaju n^2 ključeva za n korisnika koji treba međusobno da komuniciraju
- PKI zahteva upravljanje samo sa $2n$ ključeva (jeftinije)
- Cena PKI se možda čini velikom kada se treba obezbediti globalno poverenje i interoperabilnost (što možda nije uvek ni zahtev)
- Alternativa je da se preuzmu rizici bez korišćenja PKI ☺