Distribucija ključeva

Osnovne funkcije zaštite

- Tajnost
- Autentifikacija
- Integritet
- Neporecivost

- Tajnost se realizuje šifrovanjem, a preostale tri tehnologijom elektronskog potpisa

Distribucija ključeva

- Distribucija ključeva pomoću simetričnog šifrovanja
- Distribucija ključeva pomoću asimetričnog šifrovanja
  - Distribucija javnih ključeva
    - Certifikati X.509
  - Primena šifrovanja javnim ključem za distribuciju tajnih ključeva

Distribucija ključeva pomoću simetričnog šifrovanja

Simetrično šifrovanje

- Ručna isporuka ključa
- Dinamička dodela ključa
  - Šifrovanje pomoću starog ključa
  - Dostava ključa od treće strane preko šifrovanog linka (KDC key distribution center)
    - Ključ sesije
    - Trajni ključ

Opšte funkcionisanje KDC-a

- Kada A želi da uspostavi vezu sa B, on šalje zahtev KDC-u. Komunikacija između A i KDC se šifruje pomoću glavnog tajnog ključa koji je zajednički samo za A i KDC
- Ako KDC odobri zahtev za vezu, on pravi jedinstveni jednokratni ključ sesije. Šifruje taj ključ pomoću tajnog ključa koji deli sa A i isporučuje šifrovani ključ sesije korisniku A
- Slično šifruje ključ sesije pomoću tajnog ključa koji deli sa B i isporučuje šifrovani ključ sesije računaru B
- A i B mogu da uspostave logičku vezu i razmenjuju poruke

Kerberos

- Kerberos je servis za distribuciju ključeva i za autentifikaciju korisnika razvijen na MIT univerzitetu
- Oslanja se isključivo na simetrično šifrovanje i ne koristi šifrovanje javnim ključem
- Omogućava da se autentifikuju korisnici serverima i serveri korisnicima

Kerberos verzija 4

- Korisnik se prijavljuje i zahteva pristup serveru V
- Klijentski modul C u korisnikovoj radnoj stanici traži korisnikovu lozinku i šalje serveru za autentifikaciju – AS, poruku koja sadrži
  - ID korisnika
  - Lozinku korisnika
  - ID servera

- AS proverava u svojoj bazi podataka lozinku i pravo pristupa serveru
- Ako su provere uspešne AS označava korisnika autentičnim
- AS pravi tiket koji sadrži:
  - ID korisnika
  - Mrežnu adresu korisnika
  - ID servera
- Tiket se šifruje ključem,tajnim zajedničkim za AS i traženi server
- Tiket se vraća klijentu - C

- Klijent C serveru za dodelu tiketa šalje svoj ID i tiket
- Server – V dešifruje tiket i proverava da li je ID klijenta iz tiketa ista kao primljena ID
- Ako je korisnik autentifikovan odobrava mu se tražena usluga

Server za dodelu tiketa – TGS(Ticket Granting Server)

- Omogućava korisniku da jednom ukuca lozinku, a da više puta može da koristi isti servis
- Izbegava da se lozinka prenosi kao otvoren tekst
- Uvodi vremenski pečat (TimeStamp) – datum i vreme izdavanja tiketa
- Uvodi životni vek (lifetime) – koliko vremena tiket važi

- Jednom za svaku sesiju korisničkog prijavljivanja:
  1. C -> AS: IDc i IDtgs
  2. AS -> C: E(Kc, $Ticket_{tgs}$)
- Jednom za svaku vrstu servisa:
  3. C -> TGS: IDc i IDv i $Ticket_{tgs}$
  4. TGS -> C: $Ticket_v$
- Jednom za svaku sesiju servisa:
  5. C -> V: IDc i $Ticket_v$

$Ticket_{tgs}$ = E(K_{tgs}, [IDc i ADc i ID_{tgs} i TS_1 i $Lifetime_1$])

$Ticket_v$ = E(K_v, [IDc i ADc i ID_v i TS_2 i $Lifetime_2$])

Potencijalni problemi

- Problem uhvaćenog tiketa (koji je za višekratnu upotrebu) kome nije istekao životni vek i može biti zloupotrebljen:
  - Uvodi se autentifikator koji se koduje jednokratnim ključem sesije
  - Ključ isporučuje servis za autentifikaciju i to odredištu u tiketu koji samo on može da otvori i klijentu inicijatoru uz tiket i vremensku oznaku
  - Na taj način tiket važi samo uz jednokratni ključ
  - Autentifikator ima kratak životni vek i moristi se samo jednom
  - Na taj način utvrđuje se da je osoba koja koristi tiket, osoba koja ga je i legitimno dobila, kao i da server koji odgovara nije lažni server (pošto zna jendokratni ključ)

- Razmena servisa autentifikacije da bi se dobio tiket za dodelu tiketa:
  1. C -> AS: ID_c i ID_{tgs} i TS_1
  2. AS -> C: $E(K_c, [K_{c,tgs}$ i ID_{tgs} i TS_2 i $Lifetime_2$ i $Ticket_{tgs}])$
- Razmena servisa dodele tiketa da bi se dobio tiket za odobrenje servisa:
  3. C -> TGS: $Autheticator_c$ i ID_v i $Ticket_{tgs}$
  4. TGS -> C: $E(K_{c,tgs}, [K_{c,v}$ i ID_v i TS_4 i $Ticket_v])$

$Autheticator_c = E(K_{c,tgs} [ID_c$ i AD_c i $TS_3])$

- Razmena autentifikacije klijent/server za dobijanje servisa:
  5. C -> V: $Autheticator_c$ i $Ticket_v$
  6. V -> C: $E(K_{c,v} [TS_5 + 1])$

$Autheticator_c = E(K_{c,v} [ID_c$ i AD_c i $TS_5])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs}$ i ID_c i AD_c i ID_{tgs} i TS_2 i $Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v}$ i ID_c i AD_c i ID_v i TS_4 i $Lifetime_4])$

Kerberos područje (Kerberos realm)

- To je skup upravljanih čvorova sa zajedničkom Kerberos bazom
- Kerberos server mora u svojoj bazi podataka imati sve korisničke identifikatore (ID-ove) i hešove lozinki za sve korisnike koji učestvuju
- Svi korisnici se registruju na Kerberos serveru
- Kerberos server mora da deli ključ sa svakim povezanim serverom
- Svi serveri se registruju na Kerberos serveru

Kerberos verzija 5

- Ne mora da koristi DES kao verzija 4, već bilo koja tehnika šifrovanja
- Koristi razne vrste adesa, a ne samo IP adrese kao verzija 4
- Strukture podataka su definisane pravilima što nije bio slučaj kod verzije 4
- Tiketi sadrže početno i završno vreme – nije vremenski ograničen kao verzija 4(1280min)
- Omogućava klijentu da pristupi serveru i uputi taj server da pristupi drugom serveru u ime klijenta
- Jednostavnija autentifikacija između Kerberos područja
- Izbegava se duplo šifrovanje
- Moguće je generisati ključeve podsesije
- Obe verzije su osetljive na napad lozinkom

- Razmena servisa autentifikacije da bi se dobio tiket za dodelu tiketa:
  1. C -> AS: ID_c i ID_{tgs} i Times i $Nonce_1$ i $Realm_c$ i Options
  2. AS -> C: $E(K_c, [K_{c,tgs}$ i ID_{tgs} i Times i $Nonce_1$ i $Realm_{tgs}])$ i ID_c i $Realm_c$ i $Ticket_{tgs}$
- Razmena servisa dodele tiketa da bi se dobio tiket za odobrenje servisa:
  3. C -> TGS: $Authenticator_c$ i ID_v i $Ticket_{tgs}$ i Times i $Nonce_2$ i Options
  4. TGS -> C: $E(K_{c,tgs}, [K_{c,v}$ i ID_v i i Times i $Nonce_2$ i $Realm_v])$ i $Realm_c$ i ID_c i $Ticket_v$

$Authenticator_c = E(K_{c,tgs} [ID_c$ i $Realm_c$ i $TS_1])$

- Razmena autentifikacije klijent/server za dobijanje servisa:
  5. C -> V: Options i $Authenticator_c$ i $Ticket_v$
  6. V -> C: $E(K_{c,v} [TS_2$ i Subkey i Seq#$])$

$Authenticator_c = E(K_{c,v} [ID_c$ i TS_2 i Subkey i Seq# i $Realm_c])$

$Ticket_{tgs} = E(K_{tgs}, [Flags$ i $Realm_c, K_{c,tgs}$ i ID_c i AD_c i Times$])$

$Ticket_v = E(K_v, [K_{c,v}$ i ID_c i AD_c i Flags i $Realm_c$ i Times$])$

Distribucija ključeva pomoću asimetričnog šifrovanja

- Distribucija javnih ključeva
  - Problem: neko zlonameran bi mogao da distribuira falsifikovani javni ključ i predstavlja se kao korisnik
  - Rešenje: Certifikat javnog ključa
    - Javni ključ i ID vlasnika ključa
- Primena šifrovanja javnim ključem za distribuciju tajnih ključeva
  - Problem: Diffie-Hellmanova razmena ključeva nema nikakvu autentifikaciju korisnika u komunikaciji
  - Rešenje:
    - Poruka koju priprema korisnik A
    - Šifrovanje poruke jednokratnim ključem sesije
    - Šifrovanje ključa sesije javnim ključem korisnika B
    - Prilaganje šifrovanog ključa sesije poruci

Distribucija javnih ključeva

- Certifikat javnog ključa
  - Javni ključ i ID vlasnika ključa potpisuje treća strana od poverenja- CA(certificate authority)
- Od korisničkog ID-a, korisnikovog javnog ključa i certifikacionih informacija generiše se heš kod
- Heš kod se šifruje privatnim ključem sertifikacionog tela i dobija se potpis koji se dodaje svim podacima od kojih se dobija heš kod
- Primalac može da proveri potpis tako što poredi heš vrednost koju izračuna sa heš vrednosti koju dobije dešifrovanjem potpisa javnim ključem sertifikacionog tela

Certifikati X.509

- ITU-T preporuka X.509 je deo serije preporuka X.500 koje definišu servis direktorijuma
- Direktorijum održava bazu podataka informacija o korisnicima
  - Korisnička imena i mrežne adrese
  - Sertifikati javnih ključeva
  - Informacije o korisnicima
- Direktorijum pruža svojim korisnicima usluge autentifikacije

X.509

Zasniva se na korišćenju kriptografije javnih ključeva i digitalnih potpisa

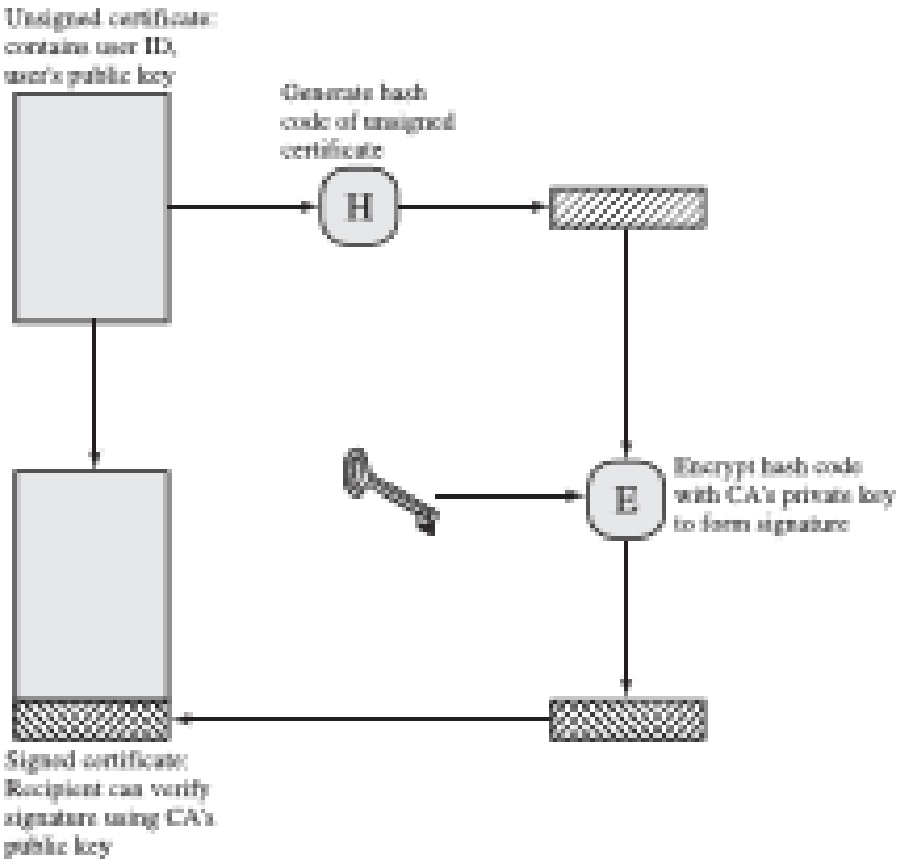
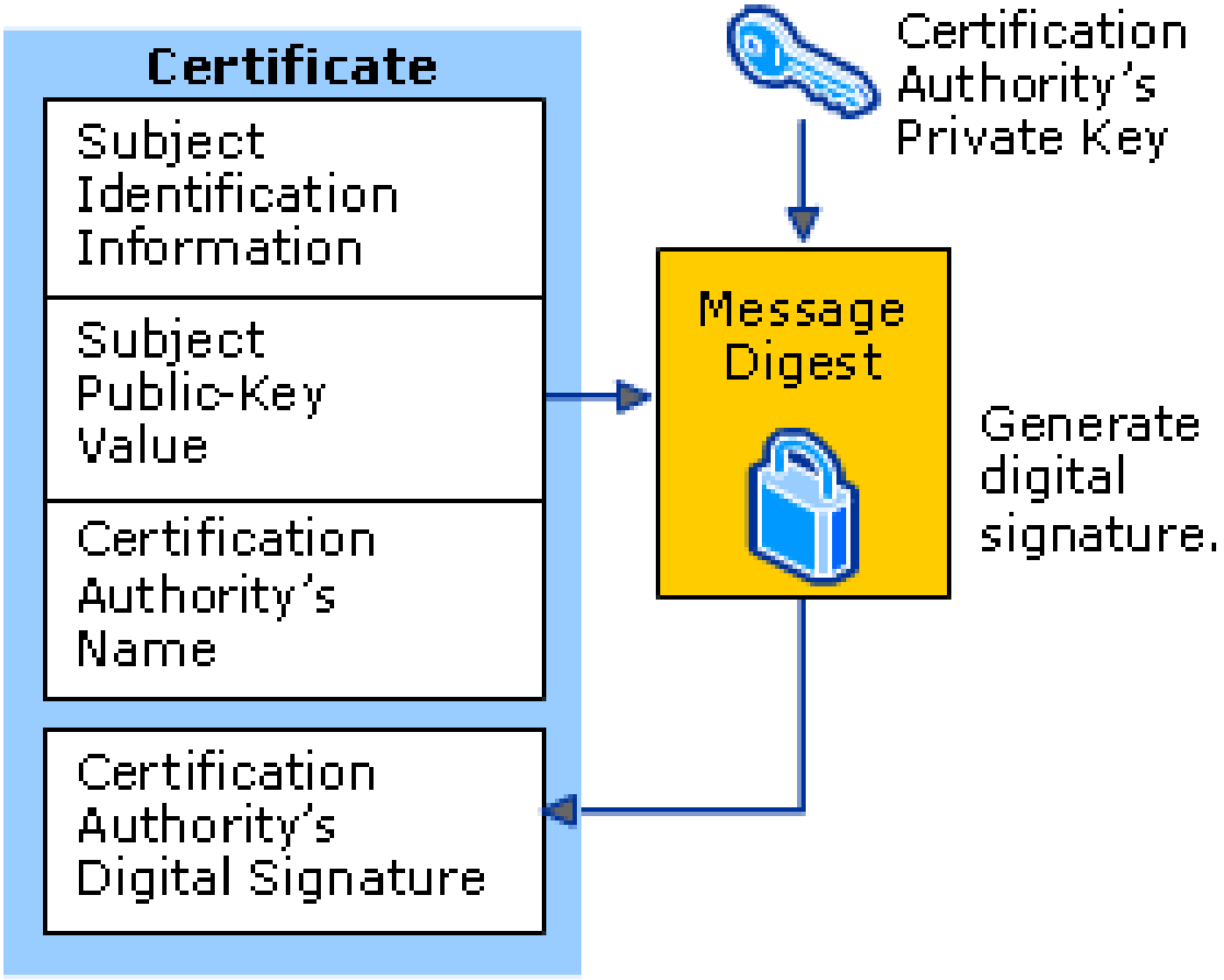


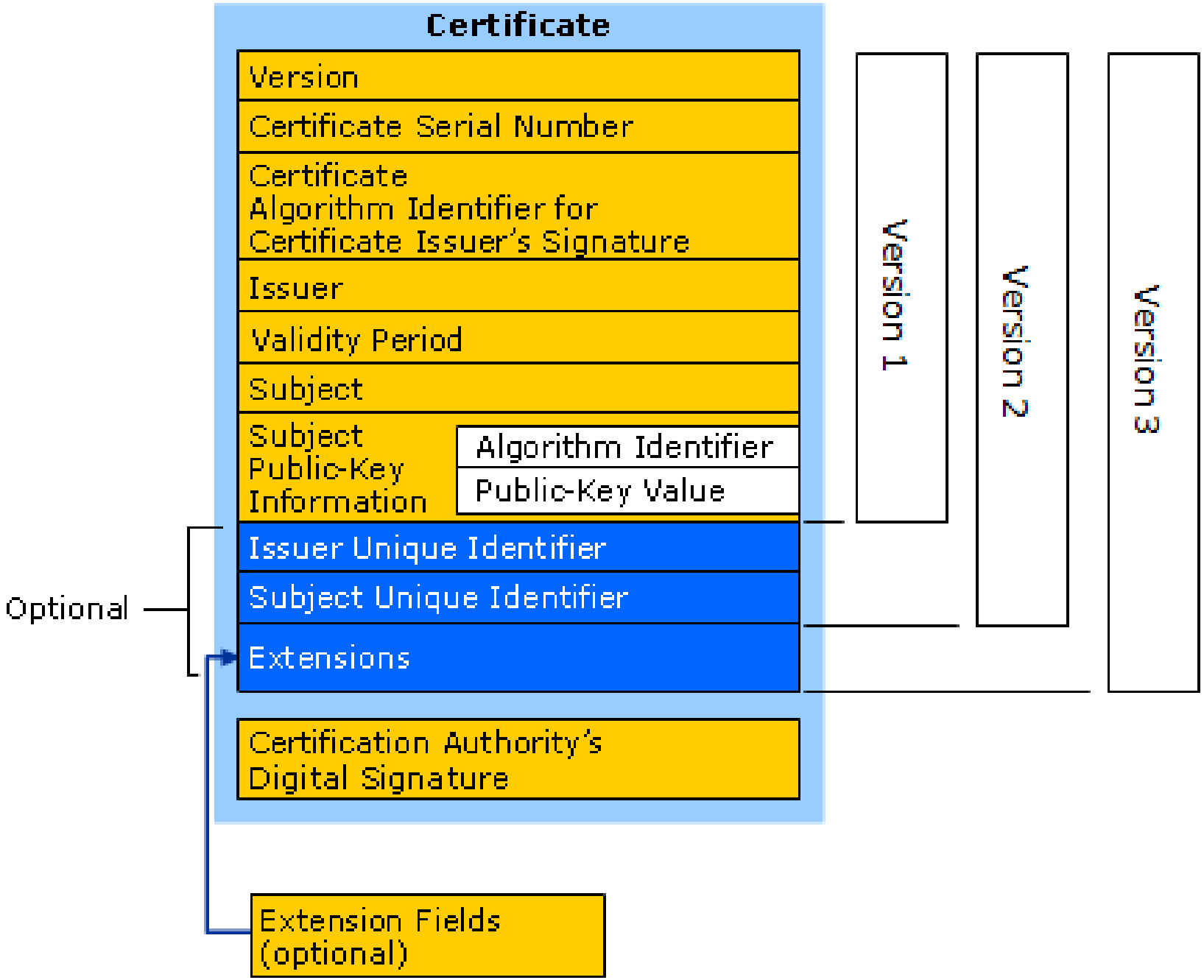
Figure 4.3 Public-Key Certificate Use

Opšti format elektronskog sertifikata X.509 sadrži sledeće elemente:

- Verzija,
- Serijski broj,
- Identifikator algoritma potpisa – ove informacije su ponovljene u polju potpis
- Ime izdavalaca
- Period važenja – dva datuma (prvi i poslednji važenja)
- Ime subjekta – ovaj sertifikat potvrđuje javni ključ subjekta koji drži odgovarajući privatni ključ
- Informacije o subjektovom javnom ključu – javni ključ subjekta plus identifikator algoritma za koji ovaj ključ treba da se koristi plus povezani parametri
- Jedinstveni identifikator izdavalaca – neobavezno polje u slučaju da je njegovo ime ponovo upotrebljeno za druge entitete
- Jedinstveni identifikator subjekta – neobavezno polje u slučaju da je njegovo ime ponovo upotrebljeno za druge entitete
- Proširenja
- Potpis – sadrži heš kod ostalih polja šifrovan privatnim ključem sertifikacionog tela, plus identifikator algoritma potpisa, plus potrebne parametre

X.509 formati sertifikata




Certificate
Version
Certificate Serial Number
Certificate Algorithm Identifier for Certificate Issuer's Signature
Issuer
Validity Period
Subject
Subject Public-Key Information
Algorithm Identifier
Public-Key Value
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Certification Authority's Digital Signature
Optional
Extension Fields (optional)
Version 1
Version 2
Version 3

X.509 verzija 3

- Sadrži niz opcionih proširenja koja mogu da se dodaju verziji 2
- Proširenja se mogu svrstati 3 glavne kategorije:
  - Informacije ključa i polise
  - Atributi subjekta i izdavalaca sertifikata
  - Ograničenja putanje sertifikata

Funkcije CA sertifikacionog tela

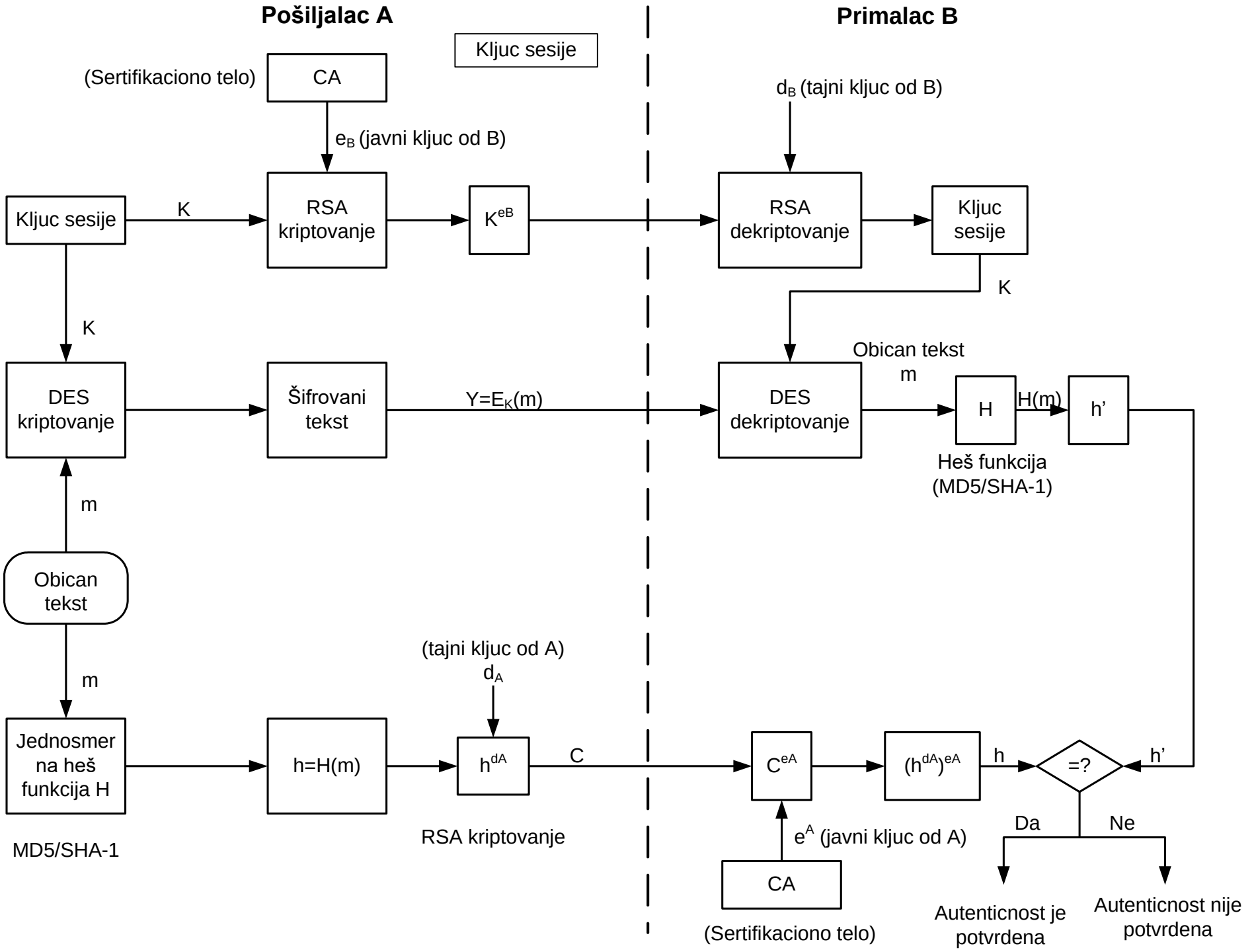
- certifikuje javne ključeve,
- kreira certifikate,
- distribuira certifikate,
- generiše i distribuira liste ukinutih certifikata (Certificate Revocation Lists)-CRL

Opozivanje sertifikata

- U određenim situacijama potrebno je opozvati određeni sertifikat
- Razlozi za opoziv mogu biti:
  - Ugrožen korisnikov privatni ključ
  - Ugrožen CA-ov sertifikat
  - Korisnika više ne sertifikuje taj CA
- Lista opozvanih sertifikata sadrži:
  - Ime izdavača
  - Datum kada je lista napravljena i datum sledećeg ažururanja
  - Po jedna stavka za svaki opozvan sertifikat(serijski broj i datum opoziva)
  - Potpis

Primena šifrovanja javnim ključem za distribuciju tajnih ključeva

- K je tajni ključ sesije koja se generiše i važi samo za tu sesiju i DES algoritme
- Tajni ključ K se šifruje RSA algoritmom i javnim ključem klijenta B , a zatim se šalje klijentu B
- Poruka se šifruje DES algoritmom pri čemu se koristi tajni ključ sesije K.
- Za dobijanje sažetka poruke koristi se SHA-1 heš funkcija i sažetak se šifruje RSA algoritmom i privatnim ključem pošiljaoca A.


Pošiljalac A
Primalac B
Kljuc sesije
(Sertifikaciono telo)
CA
e_B (javni kljuc od B)
d_B (tajni kljuc od B)
Kljuc sesije
K
RSA kriptovanje
K^{eB}
RSA dekriptovanje
Kljuc sesije
K
K
Obican tekst
m
DES kriptovanje
Šifrovani tekst
$Y=E_K(m)$
DES dekriptovanje
H
H(m)
h'
Heš funkcija (MD5/SHA-1)
m
Obican tekst
m
(tajni kljuc od A)
d_A
Jednosmerna heš funkcija H
h=H(m)
h^{dA}
C
C^{eA}
$(h^{dA})^{eA}$
h
=?
h'
Da
Ne
MD5/SHA-1
RSA kriptovanje
e^A (javni kljuc od A)
CA
(Sertifikaciono telo)
Autenticnost je potvrdena
Autenticnost nije potvrdena

Tehnike elektronskog potpisivanje

Tehnike elektronskog potpisivanja obezbeđuju:

Autentičnost pošiljaoca

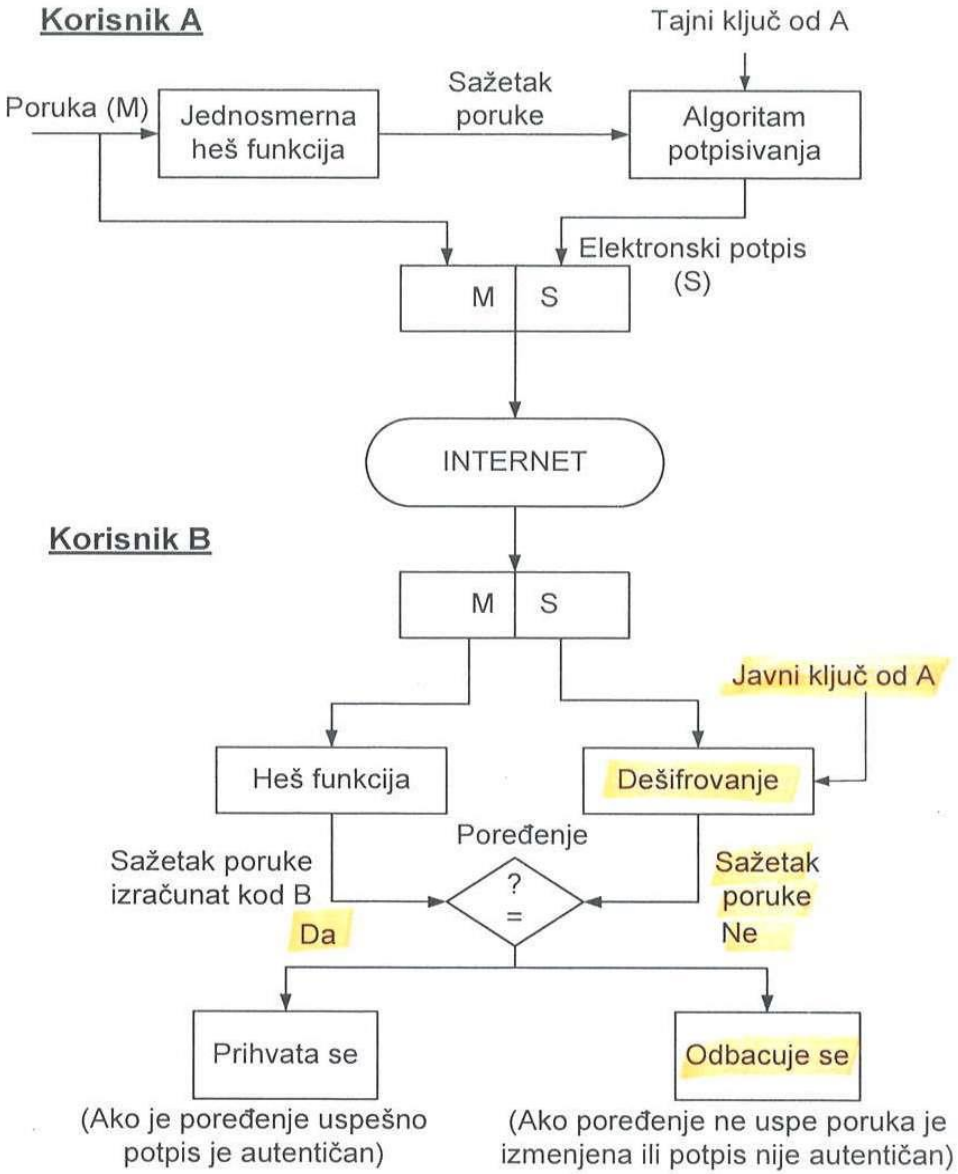
Integritet poruke

Sprečavanje nepriznavanje pošiljaoca

Obezbeđivanje tajnosto tajnog ključa

Čuvanje integriteta javnih ključeva

Elektronsko potpisivanje



Slika 5.1 – Opšta šema elektronskog potpisivanja

Primena tehnike elektronskog(digitalnog) potpisivanja

- Sigurnost elektronske pošte
- Finansijske transakcije
- Elektronsko popunjavanje
- Zaštita softvera
- Potpisivanje i autentifikacija

Uloga Sertifikacionog tela u PKI sistemu

- Osnovna uloga sertifikacionog tela (CA) je da generiše, objavljuje, opoziva i arhivira sertifikate javnih ključeva koji povezuju korisnikov identitet sa korisnikovim javnim ključem. Komercijalna CA tela naplaćuju izdavanje elektronskih sertifikata, dok ima i onih besplatnih.

Infrastruktura sistema javnih kritpografskih ključeva (PKI)

PKI je skup hardvera, softvera, ljudi, polisa i procedura potrebnih da bi se digitalnim certifikatima zasnovanim na asimetričnoj kriptografiji upravljalo, da bi se oni pravili, čuvali, distribuirali i da bi se opozvali.

Elementi:

1. krajnji entitet – korisnik ili subjekt
2. certifikaciono telo(CA) - izdavalac sertifikata
3. registraciono telo(RA) – neobavezni element, može da preuzme neke administrativne funkcije CA (registrovanje subjekta)
4. izdavalac CRL liste - neobavezni element, može da objavljuje CRL liste
5. Skladište – sve metode za čuvanje certifikata i CRL listi

Funkcije PKI sistema

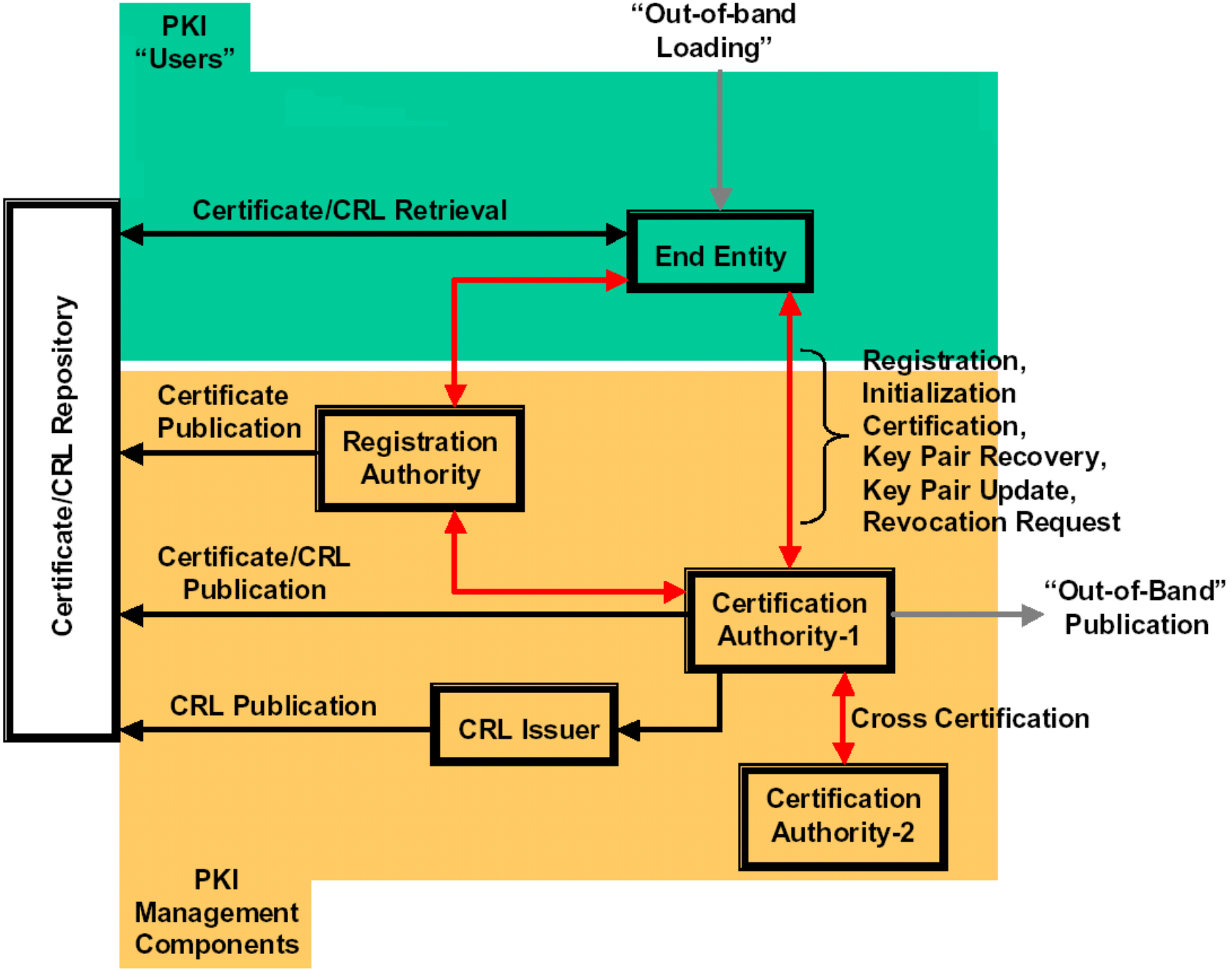
- Upravljanje javnim ključevima
- Sigurno povezivanje javnog ključa sa korisnikom
- Lanci poverenja

PKIX

- Funkcije
  - Registracija
  - Inicijalizacija
  - Certifikovanje
  - Obnavljanje para ključeva
  - Ažuriranje para ključeva
  - Zahtev za opoziv
  - Međusobno sertifikovanje

Komponente PKI sistema

- Sertifikaciono telo
- Registraciono telo
- Javni imenik (direktorijum)
- Klijentske (korisničke) aplikacije


PKI
"Users"
"Out-of-band
Loading"
Certificate/CRL Retrieval
End Entity
Certificate/CRL Repository
Certificate
Publication
Registration
Authority
Registration,
Initialization
Certification,
Key Pair Recovery,
Key Pair Update,
Revocation Request
Certificate/CRL
Publication
Certification
Authority-1
"Out-of-Band"
Publication
CRL Publication
CRL Issuer
Cross Certification
Certification
Authority-2
PKI
Management
Components

Upravljanje identitetom

- To je centralizovan i automatizovan način koji svim ovlašćenim korisnicima obezbeđuje pristup svim traženim resursima
- Za svakog korisnika se definiše identitet kome se pridruže atributi i način na koji korisnik dokazuje svoj identitet
- Centralni koncept je korišćenje samo jednog prijavljivanja (SSO-single sign-on) - nakon jedne autentifikacije korisniku se omogućava pristup svim dozvoljenim mrežnim resursima

Glavni elementi sistema za upravljanje identitetom

- Autentifikacija
- Autorizacija
- Evidencija
- Rezervisanje
- Automatizovanje radnog procesa
- Delegirano administriranje
- Sinhronizacija lozinki
- Samostalno resetovanje lozinke
- Federalizacija

Federalizovanje identiteta

- Ovo je proširenje upravljanja identitetom na više bezbednosnih domena
- Cilj je da se obezbedi deljenje digitalnih identiteta tako da se korisnik jednom autentifikuje, a da može da pristupa resursima na više domena
- Domeni nemaju centralizovanu kontrolu pa je neophodno omogućiti bezbedno deljenje digitalnih identiteta

Upravljanje federalizovanim identitetima

- Sporazumi
- Standardi
- Tehnologije

Standardi

- Ideja je da provajderi korisnicima izdaju neku vrstu tiketa koji bi njihovi partneri mogli da obrade
- Standardi se bave definisanjem formata i sadržaja tih tiketa, kao i protokolima za razmenu i upravljačkim zadacima
- Upravljački zadaci su konfigurisanje sistema za transfer atributa i preslikavanje identiteta, kao i funkcije evidentiranja i praćenja

Glavni standardi su:

- XML (Extensible Markup Language) – jezik za označavanje koji koristi skupove oznaka kojima se opisuju izgled, funkcija, značenje ili kontekst tekstualnih elemenata unutar dokumenta
- SOAP (Simple Object Access Protocol) – dok XML definiše objekte i strukture podataka, SOAP obezbeđuje metod za razmenjivanje takvih objekata podataka i za izvršavanje poziva udaljenih procedura vezanih za te objekte

- WS-Security (Web Service-Security) – skup SOAP proširenja za implementiranje integriteta i poverljivosti poruka u veb servisima (svakoj poruci se dodeljuje bezbednosni token za autentifikaciju)
- SAML (Security Assertion Markup Language) – jezik zasnovan na XML-u za razmenu bezbednosnih informacija među onlajn poslovnim subjektima