Avaliku võtme infrastruktuurid

- Avalikud ja salajased võtmed
- Sertifikaat
- Sertifitseerimiskeskused
- X.509
- HTTPS
- PGP
- SPKI, SDSI
- Autentimine vs allkiri
- Notariseerimine ja ajatembeldamine
- Blockchain

Avalikud ja salajased võtmed

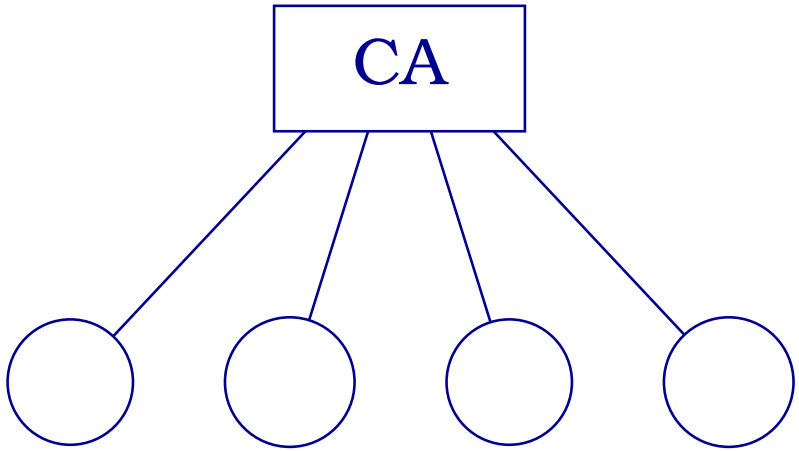
- Igal kasutajal on oma võtmepaar: salajane ja avalik võti
- Salajane võti hoitakse enda teada
- Avalik võti on kõigile teada
- Oma salajase võtmega krüpteerimine on signeerimine, signatuuri saab kontrollida signeerija avaliku võtme abil
- Kellegi avaliku võtmega krüpteeritu saab lahti ainult vastava salajase võtme omanik
- Näiteks RSA, DSA, Diffie-Hellman, ElGamal, ECDSA

Sertifikaat

- Oleks vaja siduda inimesed vastavate avalike võtmetega
- Avalikest võtmetest saab teha avaliku kataloogi
- Kust tuleb usaldus selle seostamise vastu?
- Usaldatud isik võib teiste avalikke võtmeid signeerida
- Isikusertifikaat — signeeritud kinnitus avaliku võtme ja nime sidumiseks
- Atribuutsertifikaat — signeeritud kinnitus nime ja õiguste sidumiseks
- Kes on usaldatud isik (isikud)?
- Kui kaua sertifikaat kehtib?

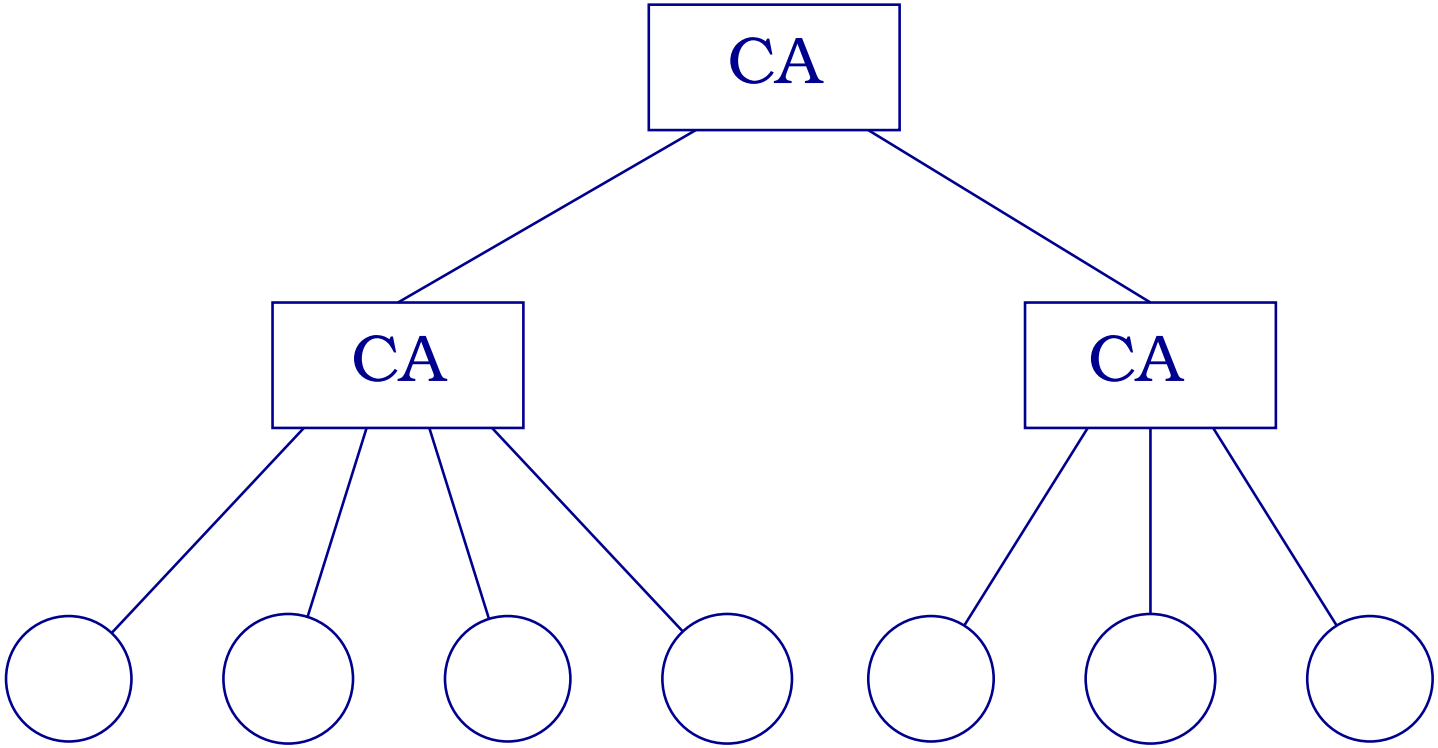
Sertifitseerimiskeskus

- Võtame usaldatud kolmanda osapoole tsentraalselt sertifikaate jagama
- CA (*Ceritification Authority*) — sertifitseerimiskeskus
- CA tuvastab isiku ja annab välja sertifikaadi isiku poolt näidatud avaliku võtmega



Sertifitseerimishierarhia

- Kes kinnitab CA võtme kehtivust? Teine CA



- Teoreetiliselt tekib üks suur hierarhia
- Praktikas tekib palju kohalikke hierarhiaid (puu asemel mets)

X.509

- X.509 on ISO/OSI standardformaat sertifikaatide jaoks
- X.500 — hierarhiline eraldusnimede süsteem (DN — *Distinguished Name*)
- Sertifikaadi omaniku nimi esitatakse X.500 eraldusnimena, näiteks

  `/C=EE/L=Tartu/O=Cybernetica`

  `/OU=Tartu labor/CN=Meelis Roos`
- Algselt *offline*-rakenduste jaoks, alates versioonist 3 toetab ka *online* tegevusi, praegu on viimane versioon 5
- Sertifikaadid publitseeritakse kataloogiteenuse kaudu (DAP, LDAP)
- OCSP – *Online Certificate Status Protocol*

X.509 sertifikaat

version	versioon
serialNumber	järjekorranumber
issuer	väljaandja DN
subject	omaniku DN
validity	kehtivusaeg
signature	signatuurialgoritm
key	omaniku avalik võti
extensions	laiendused
sig_alg	signatuuri algoritm
signature	signatuuri väärtus

X.509 praktikas (näide: HTTPS)

- Tahame autentida veebiservereid ja veebiteenuste kasutajaid
- Kõigil serveritel ja kasutajatel on oma salajane võti ja X.509 sertifikaat
- Serverite sertifikaadid annab välja firma oma CA
- Firma CA serdi annab välja rahvusvaheline CA
- Rahvusvaheliste CA-de serdid tulevad brauseritega kaasa
- Oma kohalike tipmiste CA-de serdid laaditakse kah brauserisse
- Klientidel on samasugused serdid (ahelaga mingi CA-ni, mida server usaldab)
- Kliendi ja serveri vaheliseks autentimiseks kasutatakse TLS protokolli, mis laseb kummalgi osapoolel teist autentida

PGP

- PGP (*Pretty Good Privacy*) — teistsuguse lähenemisega süsteem
- Usaldusvõrk — iga kasutaja sertifitseerib oma tuttavaid
- Tekib hajus võrk ilma tsentraalse keskuseta
- Sertifikaadid on avalikud ja kõigile kättesaadavad
- Isikutuvastus on reeglina nõrgem kui CA-del
- Kompensatsiooniks on kahe inimese vahelise usalduse kontrolliks võimalik paljusid teid kasutada (läviskeem)
- Kontrollija määrab ise, kuipalju ta mingit inimest usaldab
- Sarnasem reaalsele elule kui hierarhia
- Ei skaleeru eriti hästi
- Töötab hästi tihedalt seotud kasutajagruppide sees

SDSI, SPKI

- SDSI (*Simple Distributed Security Infrastructure*) — sertifikaadi ID seob võtme ja nime ainult sertifikaadi väljaandja jaoks
  - Usaldusseosed esitatakse võtmetel
  - Sulandunud SPKI uude versiooni
- SPKI — Simple Public Key Infrastructure
  - Originaalses SPKI-s oligi avalik võti kasutaja identifikaatoriks
  - Volitatakse võtmeid, mitte inimesi
  - SPKI-st on olemas läviskeem — autentimine õnnestub, kui n isikust vähemalt k-l leiduvad autentimisteed autenditava objektini

Autentimine vs allkirjad

- Oma salajaste võtmetega tehtavaid operatsioone võime laias laastus kaheks jagada:
  - Autentimine
  - Signeerimine (digitaalallkiri)
- Mõlemal juhul on meil vaja teada sertifikaadi täpset kehtivusinfot
- Autentimise puhul on seda kontrollida vaja vaid autentimise hetkel
- Signatuuri puhul on oluline, et seda saaks kontrollida suvalisel hilisemal ajahetkel — ka siis, kui sertifikaat ise enam ei kehti

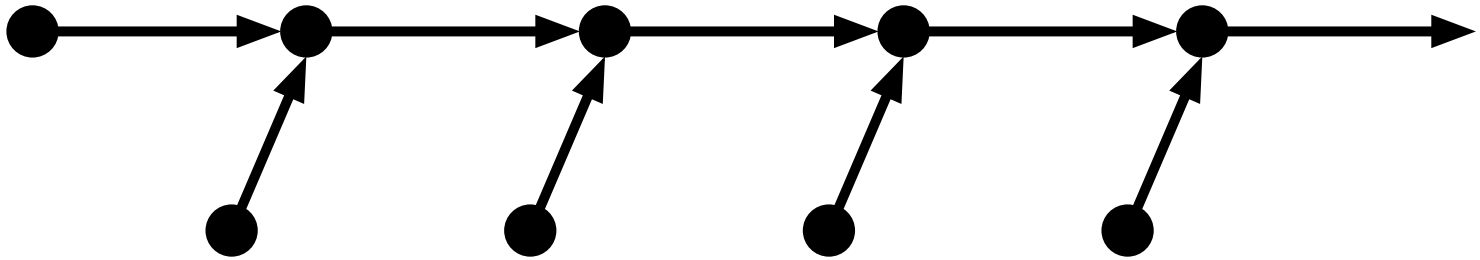
Notariseerimine

- Notar reaalelus — keegi autoriteet, kes kontrollib osapoolte isikut, volitusi ja vaba tahet
- Notariseerimine digitaalallkirjade puhul — kontrollib osapoolte sertifikaatide kehtivust mingil ajahetkel
- Signatuurile lisatakse tõend sertifikaadi kehtivuse kohta
- Selle tõendi abil saab hiljem kontrollida, et tõendi väljastamise ajal kasutaja tuvastus kehtis
- Näide: usaldatav kolmas osapool, kes vaatab hetke kehtivusinfot ning signeerib vastuse
- Usaldatav — see, kes saab käkki keerata nii, et teised hiljem tõestada ei saa, et see tema oli
- Me ei taha lisada usaldatavat osapoolt, kui see pole möödapääsmatu

Ajatemplid

- Mis toimus enne, kas võlakirja allkirjastamine või selle allkirja tegemiseks kasutatud võtme avalikustumine?
- Missugune digitaalse testamendi versioon on hilisem?
- Dokumendi sisse kirjutatud aeg on meelevaldselt valitav
- Ajatembelduse idee: loome krüptograafilised meetodid dokumentide ajalise järjestuse kontrolliks
- Notariseerimist saab teha ajatembelduse abil: ajatembeldame kõik dokumendid ning kõik sertifikaatide kehtivuse muutused
- Ajatembelduse näide: räsifunktsiooni abil võltsimatu ahela ehitamine

Ajatempliahel



Blockchain

- Ajatembeldusahela seisu tuleb aegajalt kuhugi tagasivõetamatult publitseerida
- Blockchain — tagasivõetamatu publitseerimine käib avalikult replitseeritava ajaloo abil
- Osalejate enamus otsustab, missugune ajalugu on õige
- Ükski osaleja ei tohi saada liiga suurt osakaalu (muidu muutub tõenäosus, et tema saab ajalugu võltsida, järjest suuremaks)
- Osalejaid peab kuidagi motiveerima
- Bitcoin, Ethereum, . . .