Teknologien: Fra digitale signaturer til offentlig-nøkkel infrastruktur

Jon Ølnes
Norsk Regnesentral (NR)
Jon.Olnes@nr.no

Seminar om elektronisk kommunikasjon med digitale signaturer
Statskonsult, 4/4 2000

Innhold

- Hva kan kryptografi brukes til, dig. sign. behov?
- Symmetrisk krypto, off. nøkkel krypto, dig. sign.
- Meldingssikkerhet
- Sertifikater og sertifikattjenester
- Tillitsmodeller - strukturering
- PGP
- Forvaltningsnettsamarbeidet (FNS)
- Bruksområder og beskrivelse av bruk
- Konklusjoner

Hva kan kryptografi brukes til?

Sikkerhet i åpne nettverk KREVER bruk av kryptografi

- Autentisering
  Bli kvitt passord over nettet (dig. sign.)
- Dataintegritet
  Beskytte mot uautoriserte endringer (dig. sign.)
- Konfidensialitet
  Beskytte mot innsyn (kryptering)
- Sporbarhet / ikke-benekting
  Bevis for hendelser i ettertid (dig. sign.)
- Aksesskontroll / autorisasjon
  Sentral adm. / bevis for rettigheter (dig. sign.)

Hvorfor er ikke kryptografi så mye brukt?

- Politiske restriksjoner
  Eksportrestriksjoner fra USA - er lettet på nå
- Dårlig integrasjon med systemer / produkter
- Liten etterspørsel inntil de siste årene
  Funksjonalitet først - sikkerhet prioriteres ned

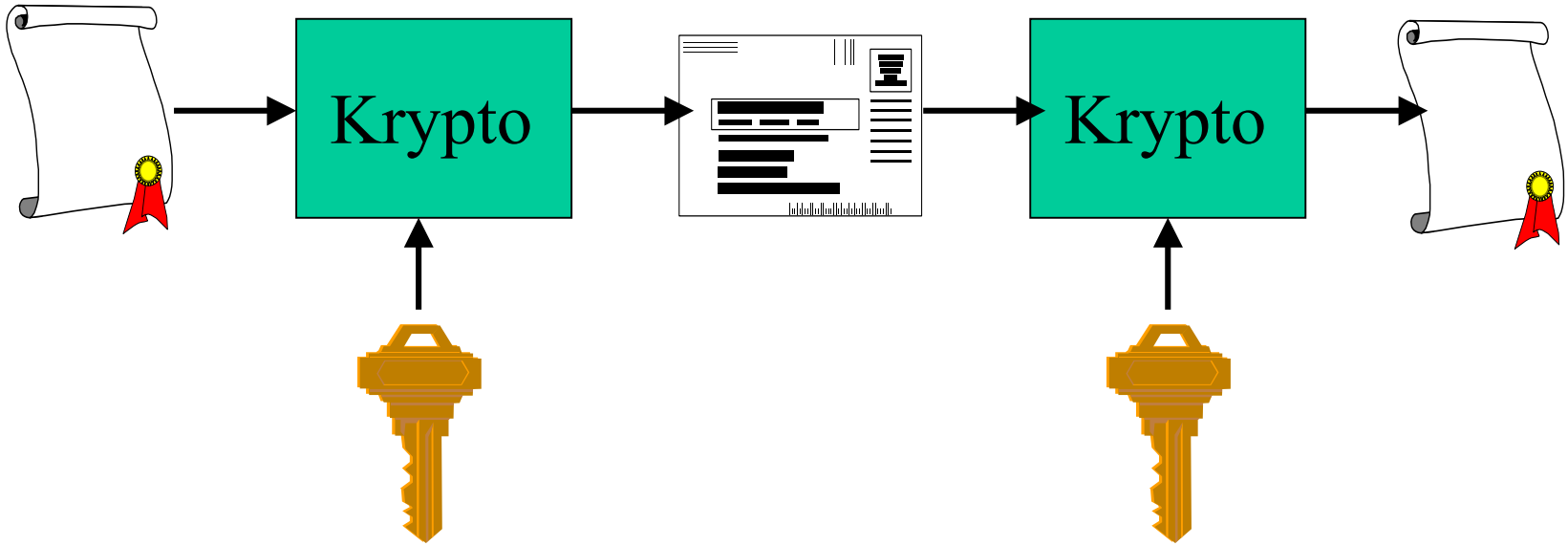
- Sikkerhet og krypto er vanskelig!
  Kjeden er så sterk som svakeste ledd.
  Krypto brukes i et system - sammen med andre tiltak

Digital signatur - hva er behovet?

- Elektronisk korrespondanse skal være like pålitelig og juridisk bindende som korrespondanse ved bruk av papir

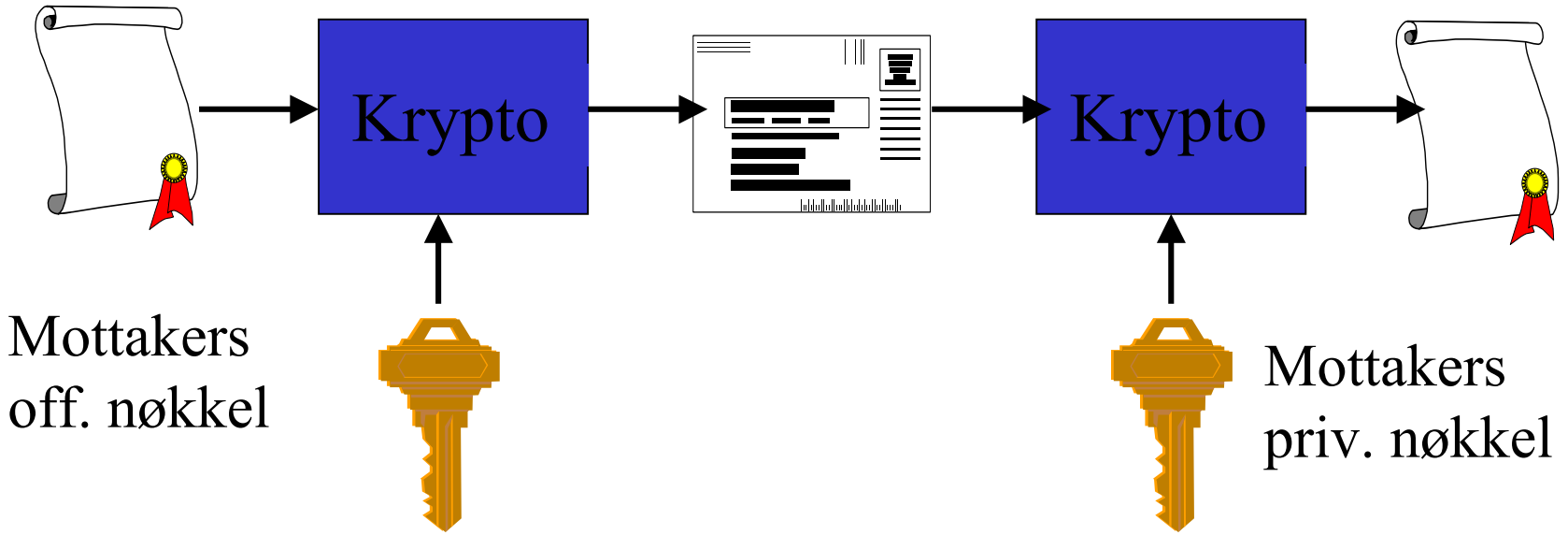
  ("Den norske IT-veien, bit for bit")
- Signaturkrav (eller ønske) i mange tilfeller
- Krav / ønske om kryptering av sensitiv info.
- Men pålitelig elektronisk kommunikasjon krever mye mer enn signaturer …..

Symmetrisk kryptering



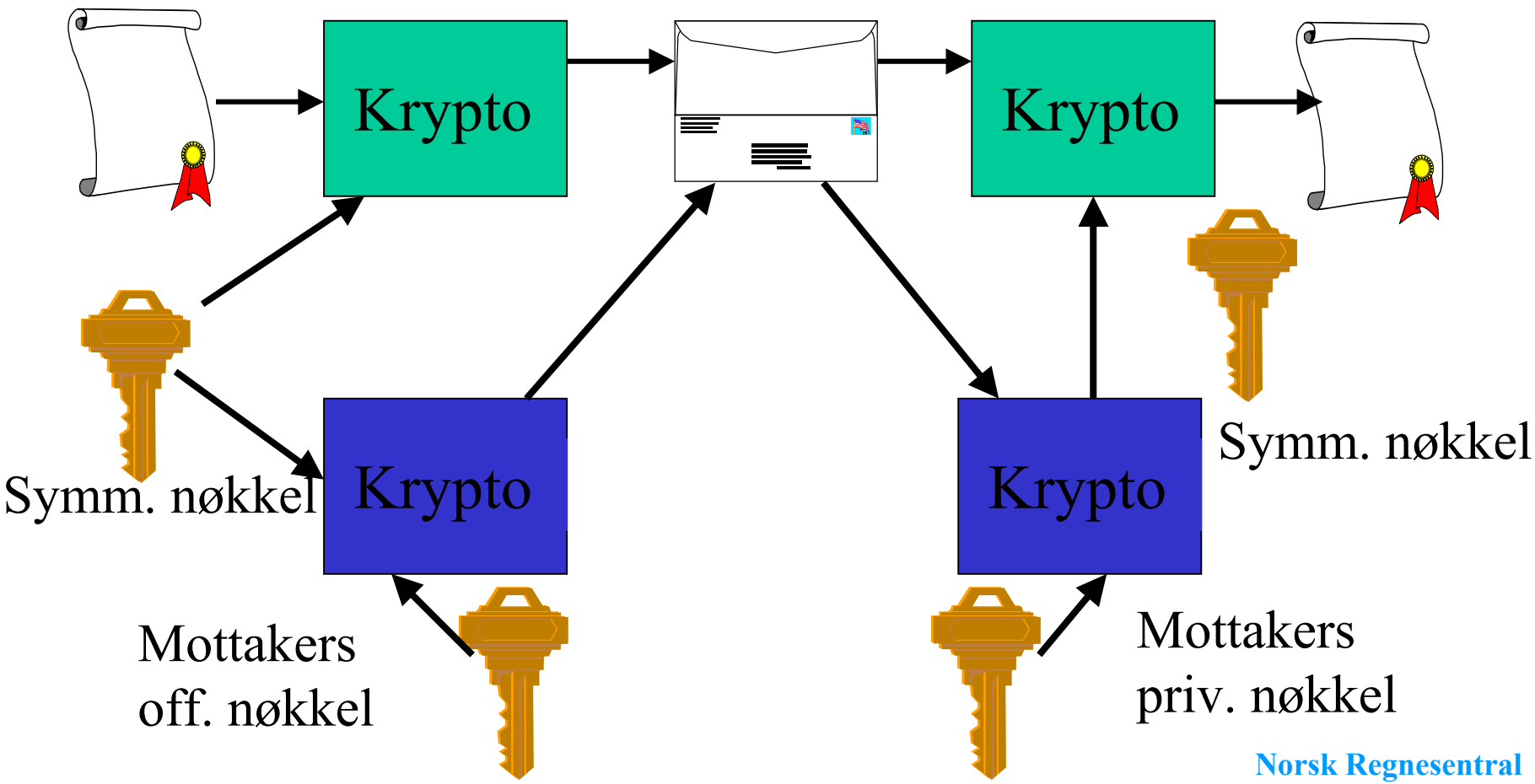
- Samme nøkkel for kryptering og dekryptering
- N(N-1) nøkler for N parter
- DES, Triple-DES, IDEA, RC2, RC4 etc.

Offentlig-nøkkel kryptering

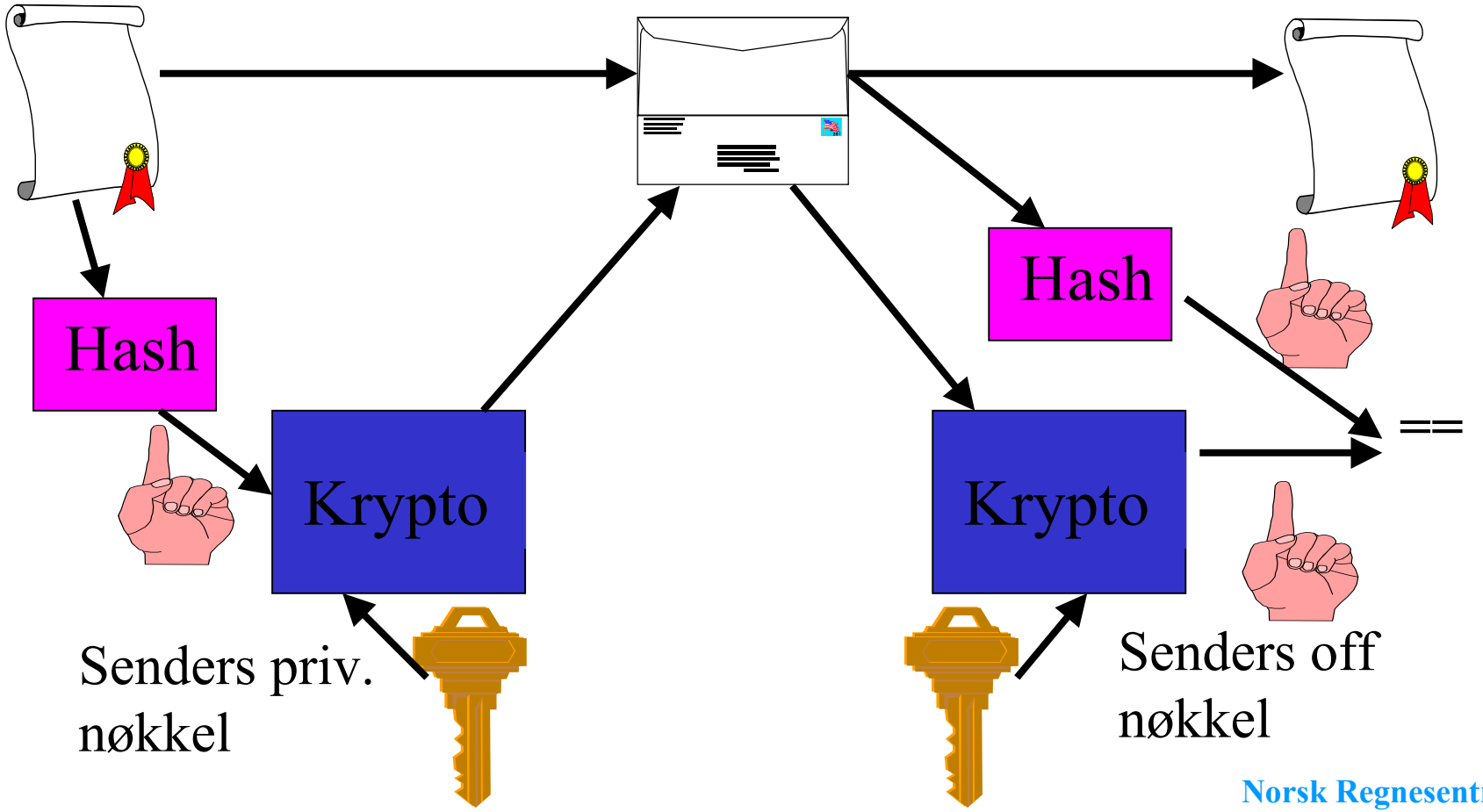


- Kryptere med offentlig nøkkel, dekryptere med privat
- N offentlige nøkler for N parter
- RSA, ElGamal, elliptisk kurve etc.

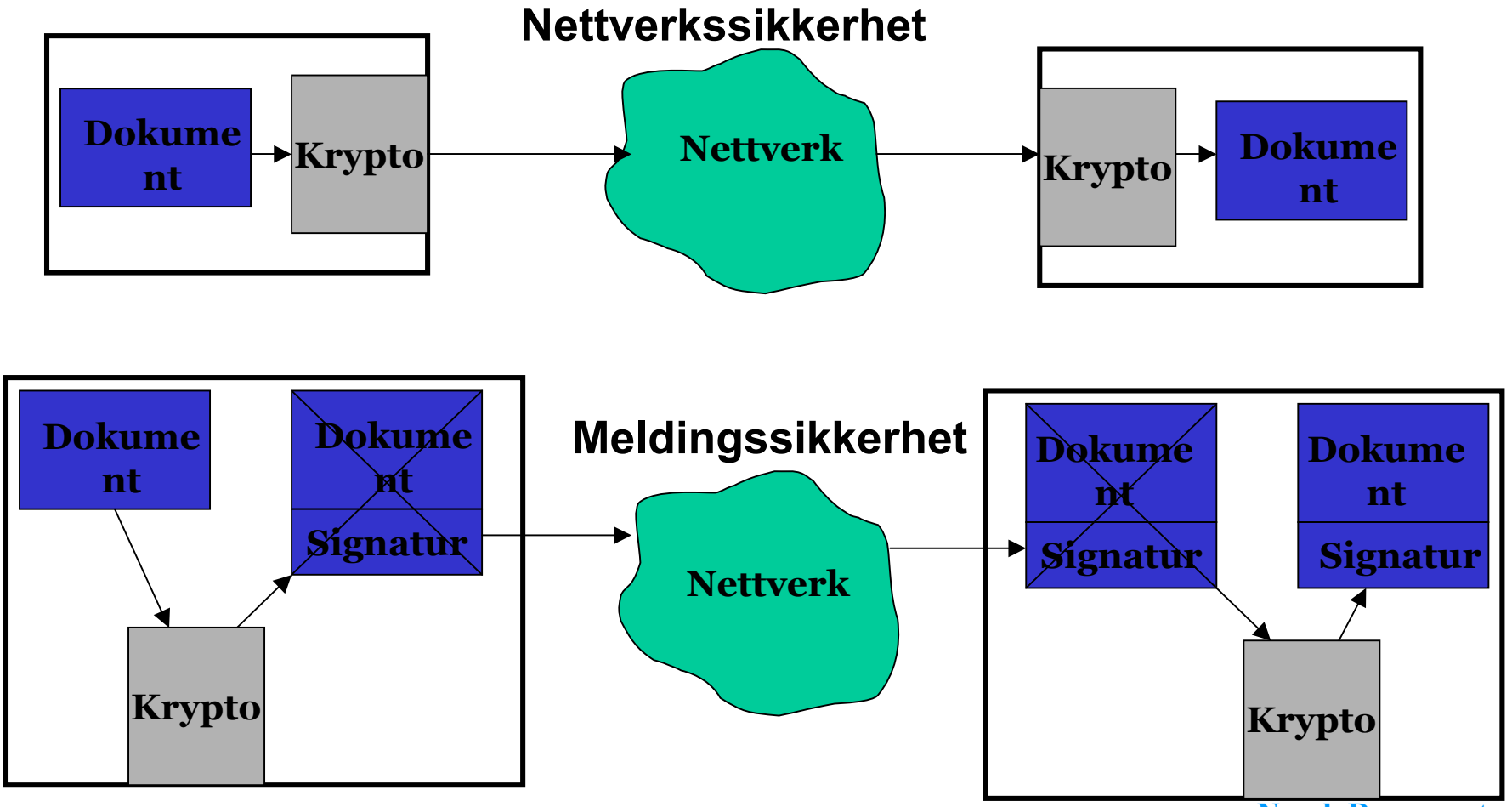
Hybrid metode



Digital signatur



Meldingssikkerhet / Nettverkssikkerhet



Egenskaper ved meldingssikkerhet

- Digital signatur:
  - Krever meldingssikkerhet
  - Autentiserer avsender
  - Beskytter melding mot endringer (oppdages)
  - Også beskyttelse mot innsideangrep
- Meldingskryptering:
  - Beskytter mot innsyn (spesifiserer mottakere)
- Kan bruke usikre nettverk, med mellomlagring
- PC og lokalt nettverk må være sikret
  - Trojanske hester kan medføre feil ved signering eller ”uautorisert signering”

Sertifikater - elektronisk legitimasjon

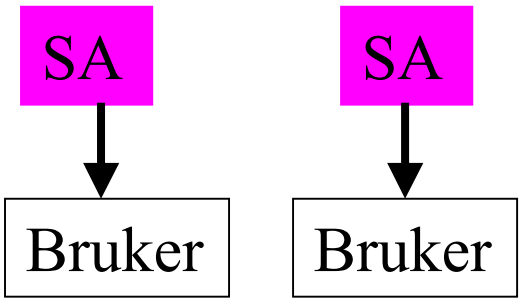
Navn	Off. nøkkel	Tid fra - til	Serienr	Alg. id.	SA navn	++
				Sign. Sertifikatautoritet		

- Knytter offentlig nøkkel til navn
- Utstedt av en tiltrodd sertifikatautoritet (SA)
- SAs offentlige nøkkel må spres på en sikker måte
- Sertifikater kan trekkes tilbake før tida - CRL

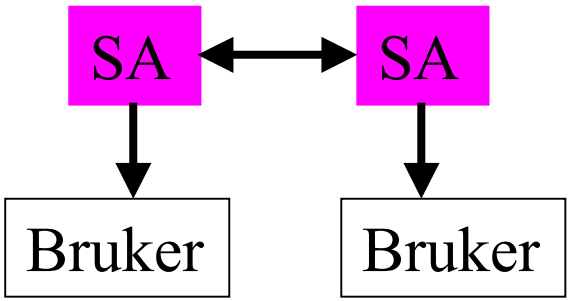
Sertifikattjeneste

- Sertifikatpolicy - sikkerhetspolicy for nivå / kvalitet
  Kan bestemmes av SA selv eller f. eks. myndigheter
- Sertifikatpraksis - hvordan er policy implementert
- Sertifikatformat - inkludert navngivning
- Opplysningstjenester / katalog
  For sertifikater, tilbakekallingslister (CRL) mm.
- Tillitsmodell - forhold til andre SA-tjenester
  Samvirke mellom SAer for å skape infrastruktur

Tillitsmodeller - samtrafikk (1)

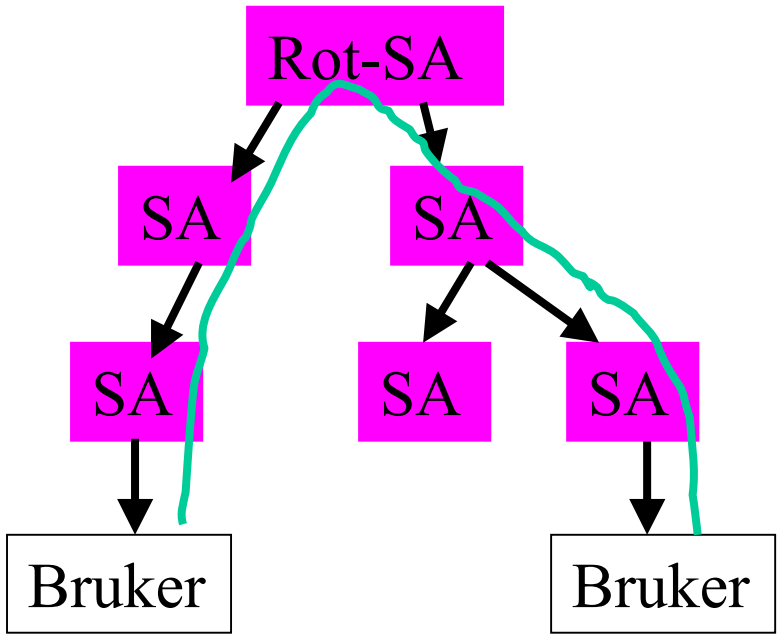


Monolittisk
- Bruker må stole på alle SAer
- Dagens situasjon på Internett

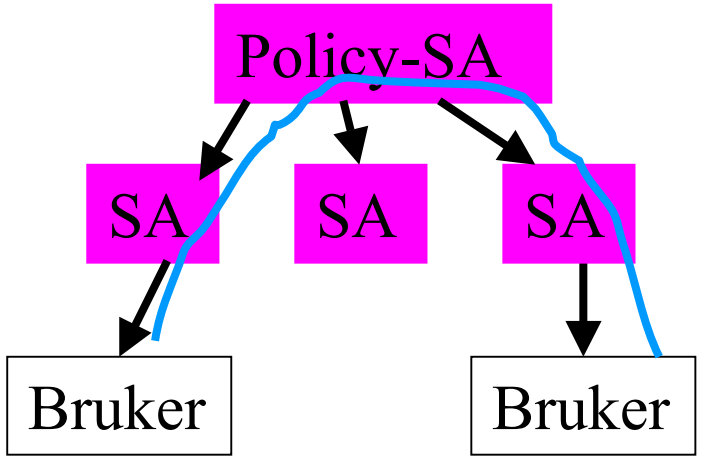


Kryssertifisering
- Utsteder sert. for hverandre
- Betyr: Andre SA følger sin policy og praksis
- Policy mapping: Andre SAs tjeneste er på samme nivå

Tillitsmodeller - samtrafikk (2)



Hierarki
- SA er f.eks. Arbeidsgiver
- Tillitskjede - mange sert. Gir tunge beregninger, lav tillit



Grunne hierarkier
- To nivåer (kanskje tre)
- Policy settes av roten
- Tysk dig. sign. system
- Internasjonale Postunion

Pretty Good Privacy (PGP)

- Gratis program for kryptering og signatur
  Sterke algoritmer, men ikke “juridisk” signatur
  Kryptert lagring tilbys
- Ingen SA - brukere signerer sertifikater for hverandre
  Tillitsmodell: “Chain of trust”
  Glimrende for mindre grupper
  Trenger ingen infrastruktur
- Mangler integrasjon med andre programmer
  Men ellers lett å bruke

http://www.pgpi.org

Forvaltningsnettsamarbeidet (FNS)

- Innkjøpsavtaler for hele norsk offentlig sektor
- Gode tilbud på utstyr, programvare og noen tjenester
- Egne rammeavtaler for dig.sign., kryptering, sert.tj.
  Smartkort, kortlesere, prog.vare for dig. sign og meldingskrypt., tjeneste for sertifikater
- (Oppfyller ikke Sikkerhets- / Beskyttelsesinstruksene)

- http://forvaltningsnett.dep.no

Kravområder

- Standardisering for utveksling av informasjon
  - Algoritmer, meldingsformater
- Utstedelse av sertifikater - SA-tjenester
  - Sikre tilstrekkelig tiltro til signaturer
- Katalogtjeneste for sertifikater og tilbakekallinglister
- Smartkort og kortlesere - spesifikasjoner
- Programstruktur
  - Integrasjon med brukerprog., API'er, etc.
  - Mulig med forskjellige deler fra forskjellige leverandører
- Støttefunksjoner, opplæring, dokumentasjon etc.

FNS' leverandører innen DS og TTP

- Totalleverandører:
  - Posten SDS
  - Strålfors (med Merkantildata)
  - Telenor Bedrift
- Programvare + kort og lesere
  - Giesecke & Devrient
- Smartkort og lesere
  - Bull (kun kortlesere)
  - NORSIK
  - Unikey

PKI-tjenester for offentlig sektor

VALG 1: Kjøpe tjenester - ikke etablere offentlig TTP

Stimulere et gryende marked - ikke konkurrere med dette

VALG 2: Ønsker avtale med mer enn en TTP

Av konkurransehensyn, og for å oppnå standardiseringseffekt

VALG 3: Kryssertifisering kreves mellom alle TTPer

Samtrafikk, ikke isolerte tjenester

VALG 4: Smartkort for lagring av private nøkler

For å sikre et forsvarlig sikkerhetsnivå

VALG 5: Dekker kun arbeidsgiver / ansatte

Ikke privat sektor

VALG 6: Nordisk / internasjonal samordning og standardisering

Sertifikattyper

- Ansattsertifikater
  - Personnavn, virksomhetsnavn, organisasjonsnummer etc.
- Profesjonssertifikater
  - Personnavn, akkrediterende myndighet med org.nummer, helsepersonellnummer el.
- Organisasjonssertifikater
  - Virksomhetsnavn, organisasjonsnummer etc.
- Sertifikater for organisasjonsenhet
  - Org. enhet navn, virksomhetsnavn, organisasjonsnummer
- Sertifikater for organisatorisk rolle
  - F. eks. postmottak

Navngivning etc.

- Valgt å skille ”jobbsertifikater” fra ”privatsertifikater”
  - Ikke generelt elektronisk id. kort (som i Sverige og Finland)
  - Sertifikat kopler identitet og arbeidssted til offentlig nøkkel
  - Bruker ikke unik id. (fødselsnummer) i sertifikater
- Epostadresse er med i sertifikater
  - Søker ofte på dette
  - Avverger noen trusler

Katalogtjenester

- Alle sertifikater lagres i katalog
  - Kan be om unntak
- Kun gyldige sertifikater lagres
  - Arkiv for tilbakekalte / utløpte sertifikater
- SAenes kataloger skal videreformidle søk
  - Brukere forholder seg bare til ”sin” leverandør
  - Har vist seg å være et meget ambisiøst krav!
- Tilbakekallingslister i kataloger
  - CRL distribution point extension i sertifikater
  - Skal være gratis og åpen adgang til CRLer

Hvordan bruker jeg dette?

- Sett inn smartkort
- Menyer i Word, Notes, epost-program etc.
- Velg ”signer” eller ”signer og krypter”
- Du blir spurt om PIN-kode
- Send signert / kryptert epost (eller vedlegg)

- Eventuelt eget program med fil inn og fil ut

Mottakersiden

- Mottar melding
- Får beskjed om å sette inn smartkort og slå PIN
- Melding dekrypteres, signatur sjekkes
- Melding på skjermen om ”signatur OK” mm.

Serverløsninger

- Mottaker kan være en virksomhet / rolle
  - Adressér til virksomhet, automatisk mottak, kopling mot bakenforliggende systemer (f. eks. EDI)
- Kan også ”samle opp” på server for sending
  - Får ikke ”ekte” signatur

Postmottak etc.

- Kan legge funksjoner i epost-tjener:
  - Kryptere utgående post
  - Legge på signatur for virksomheten
  - Dekryptere innkommende post (adressert til virk.)
  - Arkivere, journalføre (utgående og innkommende)

Hva trenger jeg?

- Smartkort og kortleser
- Lokal programvare for DS og kryptering
  - … integrert med de systemene du skal bruke
- Avtale med TTP-leverandør:
  - Utsteder sertifikater (elektronisk legitimasjon)
  - Ansvar for å legge informasjon på smartkortene
  - Katalogtjeneste

- Pris per bruker typisk ca. 2000 -2500 kr.

Inngå avtale med TTP

- Velg leverandør - tegn kontrakt
- Utnevn en RA (RegistreringsAutoritet)
  - Innen egen virksomhet normalt
- RA trenger utstyr, opplæring og sertifikat mm.

Sertifikater for brukere

- RA er TTPens ”forlengede arm”
- Personlig frammøte hos RA
  - Legitimering
  - Frammøte hos TTPen er upraktisk
- Forespørsel til TTP (fra RA / bruker)
- TTP utsteder sertifikat
- Smartkort:
  - Sendes fra TTP (evt. underleverandør) - tar et par dager
  - Gis ut av RA (hvis RA kan legge inn informasjon)

Konklusjoner

- Digital signatur, kryptering for sikker kommunikasjon
- Signatur krever off.nøkkel og meldingssikkerhet
- Sertifikater er elektronisk legitimasjon
- Tiltrodde sertifikattjenester
- Samtrafikk mellom sertifikattjenester
- FNS har avtaler innen området
- Bruksmessig integrasjon med programmer